STAGE OLYMPIQUE DE VALBONNE 2015

du 17 au 27 août 2015

Avant-propos

Le stage olympique de Valbonne 2015 a été organisé par l'association Animath.

Son objet a été de rassembler 63 collégien-ne-s et lycéen-ne-s de quatrième à première,
de 11 à 17 ans, passioné-e-s de mathématiques
sélectionnés parmi les quelque 450 candidats à la COUPE ANIMATH,
dont certains représenteront la France aux compétitions internationales :
Olympiades Internationales de Mathématiques (IMO),
Olympiades Balkaniques Junior de Mathématiques (JBMO),
Olympiades Européennes de Filles de Mathématiques (EGMO),
Romanian Masters of Mathematics (RMM),
Olympiades Mathématiques du Bénélux (BxMO),
Mediterranean Youth Mathematical Championship (MYMC).
Quatre membres de l'équipe de France 2015 des Olympiades Internationales de Mathématiques
sont présents à ce stage,
et un certain nombre d'autres animateurs et stagiaires
ont déjà participé à l'une des compétitions ci-dessus.

Nous tenons à remercier le Centre International de Valbonne pour son excellent accueil.

Table des matières

I. Déroulement du stage

C'est la troisième fois, après 1999 et 2006, qu'Animath organise son stage au Centre International de Valbonne, mais le stage est beaucoup plus important qu'en 2006 : il dure dix jours (du 17 août après midi au 27 août au matin) et accueille 63 stagiaires (un peu moins qu'en 2014). Pour des raisons financières, nous avons dû réduire les dépenses et, notamment, n'imprimer qu'une version réduite du polycopié. La version complète sera néanmoins accessible, au format pdf, sur notre site.

La plupart des quelque 450 candidats à la coupe Animath ont passé une épreuve éliminatoire, et 361 d'entre eux ont atteint l'épreuve finale, le 2 juin 2015 au matin. Avec des critères de sélection un peu modifiés par rapport à l'an dernier, nous avons retenu 63 stagiaires de 11 à 17 ans (âge moyen 15,7 ans), dont 9 filles (en prévision des Olympiades Européennes de Filles : même proportion que l'an passé), 9 jeunes nés en 2001 ou après (en prévision des Olympiades Balkaniques Junior : moins que l'an passé). Nous avons fixé des quotas par classe, de sorte que nous avions comme l'an passé 49% d'élèves de première et moins d'élèves des Académies de Paris et Versailles (37%). 21 animateurs, pour la plupart d'anciens stagiaires (dont certains très jeunes : âge moyen 25 ans), ont assuré les 168 heures de cours, les soirées, les tests, la muraille, le polycopié...

Le stage était structuré comme celui de l'an dernier : deux périodes de quatre jours (18 - 21 août et 22 - 25 aout), trois de cours / exercices, un test le matin du quatrième jour (8h30 à 12h30 pour le groupe D, 9h à 12h pour les autres), une excursion à Biot (musée Fernand Léger et village) le vendredi 21 après-midi et une après-midi libre le mardi 25. Enfin, le mercredi 26 aout, dernier jour du stage, était consacré à des cours non sanctionnés par un test, sur des sujets plus larges que la stricte préparation olympique. C'est la journée d' "ouverture". Les tests étaient corrigés le soir même, les soirées étaient libres les veilles de tests ainsi que le dernier jour (soirée spéciale sans contrôle d'heure de coucher). Même les autres soirs, l'heure de coucher n'était guère contrôlée.

Le deuxième soir, mardi 18 août, Jean-Louis Tu, responsable des activités olympiques d'Animath et président du jury, a remis la coupe Animath aux 5 lauréats, avant une conférence de géométrie de Xavier Caruso. Joseph Najnudel, double médaillé d'or des Olympiades Internationales (1997 et 1998), a présenté une conférence sur les permutations le samedi 22 août. Les 19 et 23 août ont eu lieu la présentation par Thomas Budzinski des différentes Olympiades Internationales et la soirée ITYM - TFJM, coordonnée par Mathieu Barré. Nous n'étions pas seuls sur le campus, il y avait différents groupes pour un total de 250 personnes environ. Nous avions trois étages d'un bâtiment pour nous (contre quatre prévus initialement), presque tous les stagiaires et animateurs étaient en chambre individuelle avec sanitaire dans la chambre. Chaque participant avait sa carte magnétique de chambre et sa carte de restauration, plusieurs cartes de chambre ont dû être remagnétisées en cours de stage, et quelques cartes de restau-

ration ont été perdues. L'horaire des repas était un peu plus large que d'habitude : 7 h à 9 h pour le petit déjeuner, 12 h à 13 h 30 pour le déjeuner, 19 h à 20 h pour le dîner.

Le lundi 17 août, en raison d'un problème de photocopieuse, les livrets d'accueil (programme, plan du campus, liste des stagiaires et animateurs...) n'étaient pas prêts à l'arrivée des élèves, ils ont été distribués pendant la présentation du stage (17 h). Puis, les élèves ont répondu à un questionnaire d'évaluation en une heure et demie, afin d'être répartis dans quatre groupes de niveaux autant que possible homogènes (les groupes valaient pour l'ensemble du stage). Ce n'est que le mercredi 19 août que nous avons distribué les tee-shirts ainsi que les bics Animath.

Quelques liens utiles pour poursuivre le travail réalisé pendant ce stage :

— Le site d'Animath : http://www.animath.fr
— Le site MathLinks : http://www.mathlinks.ro
— Les polycopiés de stages olympiques précédents : http://www.animath.fr/spip.php?article260
— Les cours de l'Olympiade Française de Mathématiques : http://www.animath.fr/spip.php?article255

		Groupe A	Groupe B	Groupe C	Groupe D
Lundi 17/08		Arrivée, accueil des élèves, présentation du stage (17 h 00) et première évaluation			
Mardi 18/08	9h - 12h	stratégies de base (Arsène)	logique (Nicolas)	géométrie (Victor)	arithmétique (Igor)
	14h - 17h+ε	stratégies de base (Eva)	stratégies de base (Cécile)	géométrie (Thomas)	arithmétique (Xavier)
	20h30 -21h30	Conférence : Dessine-moi une planète (Xavier)			
Mercredi 19/08	9h - 12h	stratégies de base (Clara)	stratégies de base (Victor)	géométrie (Nicolas)	arithmétique (Jean-Louis)
	14h - 17h+ε	algèbre (Mathieu Barré)	stratégies de base (Gabriel)	géométrie (Jean-Louis)	géométrie (Thomas)
	20h30 -21h30	Conférence : les Olympiades de Mathématiques (Thomas)			
Jeudi 20/08	9h - 12h	algèbre (Vincent)	algèbre (Xavier)	polynômes (Igor)	géométrie (Joseph)
	14h - 17h+ε	logique (Nicolas)	algèbre (Arsène)	polynômes (Thomas)	géométrie (Jean-Louis)
	20h30 - 21h 30	Soirée libre			
Vendredi 21/08	9h - 12h	Test de mi-parcours			
	Après-midi	Excursion à Biot : musée Fernand Léger et village			
	20h30 - 21h 30	Correction du Test			
Samedi 22/08	9h - 12h	géométrie (François)	géométrie (Julien)	arithmétique (Gabriel)	combinatoire (Guillaume)
	14h - 17h+ε	géométrie (Mathieu Barré)	géométrie (Cécile)	arithmétique (Guillaume)	combinatoire (Joon)
	20h15 - 21h	Conférence : Echanger des choses au hasard, qu'est-ce que ça donne ? (Joseph)			
Dimanche 23/08	9h - 12h	géométrie (Clara)	géométrie (Vincent)	arithmétique (François)	combinatoire (Thomas)
	14h - 17h+ε	arithmétique (Eva)	arithmétique (Julien)	inégalités (Joon)	polynômes (Guillaume)
	20h - 21h	Conférence : ITYM et le TFJM (Mathieu Barré etc...)			
Lundi 24/08	9h - 12h	arithmétique (Julien)	arithmétique (Louise)	éq. fonctionnelles (Gabriel)	inégalités (Joon)
	14h - 17h+ε	arithmétique (Vincent)	arithmétique (Félix)	éq. fonctionnelles (Guillaume)	inégalités (Matthieu Piquerez)
Mardi 25/08	9h - 12h	Test de fin de parcours			
	Après-midi	Après-midi libre			
	20h30 - 21h 30	Correction du Test			
Mercredi 26/08	9h - 12h	graphes planaires (Félix)	groupes (Eva)	axiome du choix (Matthieu Piquerez)	diamant aztèque (Guillaume et Thomas)
	14h - 17h+ε	théorie des graphes (Cécile)	théorie des graphes (Joon)	théorie des graphes (Gabriel)	nombres p-adiques (Louise)
	20h - 23h30 +ε	Soirée/nuit libre			
Jeudi 27/08	Matinée	Petit déjeuner et départ. Rendez-vous au bus à 10 h 30			

II. Coupe Animath et évaluation initiale

1 Présentation

La "coupe Animath" qui, pour la deuxième année, se substitue au test de sélection du stage olympique, a été organisée le 2 juin 2014. Pour la première fois, elle était réservée aux élèves qui soit étaient lauréats d'une compétition, soit avaient franchi avec succès l'épreuve éliminatoire en ligne. Une centaine de candidats ont échoué (ou abandonné) à l'épreuve éliminatoire. La coupe Animath elle-même est une compétition de 3 heures pour les collégiens, 4 heures pour les lycéens, qui sert notamment à sélectionner les stagiaires, mais pas uniquement. Les résultats de la coupe Animath sont publiés sur notre site. Pour la sélection au stage, on applique des bonifications qui modifient quelque peu le classement : les filles, les nouveaux entrants, les lauréats de Kangourou ou de l'Olympiade Académique de Première, ainsi que ceux dont le taux de réussite de l'établissement scolaire au bac ou au brevet n'est pas 100% bénéficient d'une bonification selon une formule plus sophistiquée que l'an dernier. Ceci afin de favoriser l'égalité des chances. Cela a un peu amélioré la proportion de filles ainsi que de stagiaires provinciaux.

Pendant la deuxième soirée du stage, le président du jury, Jean-Louis Tu, a remis une coupe aux meilleurs élèves de chaque catégorie :
Première : Félix Breton et Baptiste Collet,
Seconde : Savinien Kreczman,
Troisième : Pierre-Alexandre Bazin,
Quatrième : Théodore Fougereux.

2 Eliminatoires collégiens : énoncés

Les exercices ne sont pas classés par ordre de difficulté.

Exercice 1 Soient x et y deux nombres réels vérifiant $y - x = 1$ et $y^2 = x^2 + 6$. Déterminer la valeur de $x + y$.

Exercice 2 Calculer $\dfrac{\sqrt{2^{999} + 2^{998} + 2^{998}}}{2^{498}}$.

Exercice 3 Calculer $\dfrac{8^{1345}}{4^{2015}}$.

Exercice 4 Un joueur dispose de quatre cartes distinctes. De combien de manières peut-il les ordonner ?

Exercice 5 Une grille est formée de 5 droites horizontales et 6 droites verticales. Déterminer le nombre de rectangles dont chacun des côtés est inclus dans l'une de ces droites.

Exercice 6 Les mots de la langue aayyaa sont les successions de 1 à 10 caractères qui sont soit des "a", soit des "y". Déterminer le nombre de mots de cette langue.

Exercice 7 Le nombre 6 a 4 diviseurs : 1, 2, 3 et 6. Le plus grand diviseur de 6 qui est différent de 6 est 3. Déterminer le plus grand diviseur de 2015 qui est différent de 2015.

Exercice 8 Déterminer la somme de nombres compris entre 1200 et 1300 qui sont divisibles par 5 et par 9.

Exercice 9 Soit n le nombre entier tel que $2^5 \times 3^8 \times 4^9 \times 5^{10} \times 6^{11}$ soit divisible par 2^n mais pas par 2^{n+1}. Déterminer n.

Exercice 10 Soit $ABCDE$ un pentagone régulier. On suppose que tous ses sommets sont situés sur un cercle de centre O. Déterminer la valeur en degrés de l'angle $\widehat{OAB}$.

Exercice 11 Soit $A_1A_2A_3 \cdots A_{120}$ un polygone régulier. Déterminer la valeur en degrés de l'angle $\widehat{A_1A_3A_5}$.

Exercice 12 Soit $ABCD$ un losange tel que $BD = 50$ et $AC = 100$. Soit M le milieu de $[BC]$ et N le milieu de $[AD]$. Déterminer l'aire du quadrilatère $ABMN$.

3 Eliminatoires lycéens : énoncés

Les exercices ne sont pas classés par ordre de difficulté.

Exercice 1

Soient a, b, c trois nombres réels tels que $a^2 + b^2 + c^2 = 8$, $a + b + c = 4$ et $abc = 1$. Calculer $\frac{1}{a} + \frac{1}{b} + \frac{1}{c}$.

Exercice 2 Soient x et y des nombres réels tels que $x^2 - 200x + y^2 + 10000 = 0$. Calculer $x + y$.

Exercice 3 a et b sont des entiers tels que $(a + b\sqrt{2})^2 = 41 + 24\sqrt{2}$. Déterminer la valeur de $a^2 + b^2$.

Exercice 4 Une grille est formée de 5 droites horizontales et 6 droites verticales. Déterminer le nombre de rectangles dont chacun des côtés est inclus dans l'une de ces droites.

Exercice 5 On donne 20 points dans le plan, trois à trois non alignés. Combien de triangles dont les sommets figurent parmi ces 20 points peut-on former ?

Exercice 6 Dans un tiroir se trouvent 5 paires de chaussettes distinctes. On tire quatre chaussettes au hasard. La probabilité de tirer deux paires est égale à une chance sur n. Déterminer la valeur de n.

Exercice 7 Déterminer le plus petit entier n dont le chiffre des unités est 5, tel que $\sqrt{n}$ est un entier dont la somme des chiffres vaut 9.

Exercice 8 Combien y a-t-il de multiples de 3 compris entre 1 et 2015 dont le chiffre des unités dans l'écriture décimale est un 2 ?

Exercice 9 Le nombre 6 a 4 diviseurs : 1, 2, 3 et 6. Déterminer la somme de tous les nombres entre 1 et 1000 qui admettent exactement 7 diviseurs.

Exercice 10 Un carré $ABCD$ a une aire égale à $4\sqrt{3}$. Ses quatre sommets sont situés sur un cercle Γ. On suppose que le cercle Γ est tangent aux trois côtés $[MN]$, $[NP]$ et $[PM]$ d'un triangle équilatéral MNP. Déterminer l'aire du triangle MNP.

Exercice 11 Soit ABC un triangle rectangle dont l'hypoténuse BC mesure 4cm. La tangente en A au cercle circonscrit à ABC rencontre la droite (BC) au point D. On suppose que $BA = BD$. Soit S l'aire de ACD, exprimée en centimètres carrés. Calculer S^2.

Exercice 12 Soit ABC un triangle rectangle en A tel que $AB = 156$ et $AC = 65$. On note H le pied de la hauteur issue de A. Déterminer la valeur de AH.

4 Eliminatoires collégiens : solutions

Solution de l'exercice 1 Réponse : 6, car $6 = y^2 - x^2 = (y-x)(y+x)$.

Solution de l'exercice 2 Réponse : 4, car $2^{998} + 2^{998} = 2^{999}$ et $\sqrt{2^{1000}} = 2^{500}$

Solution de l'exercice 3 Réponse : 32, car $8^{1345} = 2^{3\times 1345}$ et $\frac{2^{4035}}{2^{4030}} = 2^{4035-4030}$.

Solution de l'exercice 4 Réponse : $24 = 4 \times 3 \times 2 \times 1$

Solution de l'exercice 5 Réponse : $150 = 15 \times 10$. 15 choix possible du côté horizontal et 10 du côté vertical.

Solution de l'exercice 6 Réponse : 2046 = $2 + 2^2 + ... + 2^{10}$ car il y a 2^n mots de n lettres.

Solution de l'exercice 7 Réponse : $403 = \frac{2015}{5}$ car le plus petit diviseur de 2015 différent de 1 est 5.

Solution de l'exercice 8 Réponse : 2475. Ce sont les multiples de $9 \times 5 = 45$, soit 1215 et 1260.

Solution de l'exercice 9 Réponse : $34 = 5 + (2 \times 9) + 11$.

Solution de l'exercice 10 Réponse : 54 car $\widehat{AOB} = \frac{360}{5} = 72°$.

Solution de l'exercice 11 Réponse : 174. C'est la moitié de l'arc intercepté, qui vaut $\frac{116}{120} \times 360° = 348°$.

Solution de l'exercice 12 Réponse : 1250. C'est la moitié de l'aire du losange, qui elle même vaut $\frac{1}{2} \times AC \times BD$.

5 Eliminatoires lycéens : solutions

Solution de l'exercice 1 Réponse : 4 car $\frac{1}{a} + \frac{1}{b} + \frac{1}{c} = \frac{(a+b+c)^2-(a^2+b^2+c^2)}{2abc}$.

Solution de l'exercice 2 Réponse : 100 car $x^2 - 200x + y^2 + 10000 = (x-100)^2 + y^2$ s'annule si et seulement si $x - 100 = y = 0$

Solution de l'exercice 3 Réponse : 25 car $a^2+2b^2 = 41$ et $\left(a^2 - 2b^2\right)^2 = \left(41 + 24\sqrt{2}\right)\left(41 - 24\sqrt{2}\right) = 23^2$, donc $a = 3$ et $b = 4$.

Solution de l'exercice 4 Réponse : $150 = 15 \times 10$. 15 choix possibles du côté horizontal et 10 du côté vertical.

Solution de l'exercice 5 Réponse : $1140 = \frac{20\times 19\times 18}{6}$

Solution de l'exercice 6 Réponse : 21. Nombre de tirages avec deux paires : $\frac{5\times4}{2} = 10$. Nombre de tirages total : $\frac{10\times9\times8\times7}{24} = 210$.

Solution de l'exercice 7 Réponse : 2025. n est un carré parfait multiple impair de 5 et multiple de 3, mais c'est la somme des chiffres de $\sqrt{n}$ qui vaut 9, donc $\sqrt{n} = 45$.

Solution de l'exercice 8 Réponse : 67. Ce sont $12, 42, 72, \ldots, 1992$.

Solution de l'exercice 9 Réponse : 793. Seules les puissances sixièmes d'un nombre premier ont exactement 7 diviseurs, en l'occurrence $2^6 = 64$ et $3^6 = 729$.

Solution de l'exercice 10 Réponse : 18. Le rayon de Γ vaut $r = \sqrt{2\sqrt{3}}$ car le côté du carré vaut $r\sqrt{2}$, et l'aire du triangle MNP : $\frac{(3r)(2r\sqrt{3})}{2}$.

Solution de l'exercice 11 Réponse : 27. $\alpha = \widehat{ADB} = \widehat{BAD} = \widehat{ACB} = 30°$ car $\widehat{ABC} = 2\alpha$. Donc $AB = BD =$ rayon du cercle $= 2$, $CD = 6$ et la hauteur vaut $\sqrt{3}$.

Solution de l'exercice 12 Réponse : 60. Par Pythagore, $BC = 13 \times 13 = 169$, et l'aire du triangle rectangle vaut $\frac{1}{2} \times AB \times AC = \frac{1}{2} \times AH \times BC$.

6 Enoncés de la coupe Animath - 2 juin 2015

Instructions

— **Rédigez les différents problèmes sur des copies distinctes. Sur chaque copie, écrivez en lettres capitales vos nom et prénom en haut à gauche ainsi que votre classe, et le numéro du problème en haut à droite.**

— On demande des solutions **complètement rédigées** (sauf pour l'exercice 1), où toute affirmation est soigneusement **justifiée**. La notation tiendra compte de la **clarté** et de la **précision** de la copie.
Travaillez d'abord au brouillon, et rédigez ensuite au propre votre solution, ou une tentative, rédigée, de solution contenant des résultats significatifs pour le problème.
Ne rendez pas vos brouillons : ils ne seraient pas pris en compte.

— Une solution complète rapportera plus de points que plusieurs tentatives inachevées. Il vaut mieux terminer un petit nombre de problèmes que de tous les aborder.

— Règles, équerres et compas sont autorisés. Les rapporteurs sont interdits.
Les calculatrices sont interdites, ainsi que tous les instruments électroniques.

Les collégiens traitent les exercices 1 à 5. Les lycéens traitent les exercices 4 à 8.
Chaque exercice est noté sur 7 points.

Merci de bien vouloir respecter la numérotation des exercices. Rédigez les différents problèmes sur des copies distinctes. Sur chaque copie, écrivez en lettres capitales vos nom et prénom en haut à gauche ainsi que votre classe, et le numéro du problème en haut à droite.

Énoncés collège

Exercice 1 On dispose de trois opérations sur les entiers :

— L'opération A qui consiste à multiplier par 2 et à ajouter 4 au résultat.
— L'opération B qui consiste à multiplier par 4 et à ajouter 16 au résultat.

— L'opération C qui consiste à multiplier par 5 et à ajouter 25 au résultat.

a) Déterminer un entier x tel qu'en partant de x et après avoir utilisé successivement les opérations A, B et C dans cet ordre, on obtienne 1945.

b) Déterminer tous les entiers x tels qu'en partant de x et en utilisant successivement deux opérations différentes, on obtienne 2015.

Exercice 2 Soit ABC un triangle rectangle en A. Déterminer le ou les points P du périmètre de ABC tel(s) que $PA + PB + PC$ soit maximal.

Exercice 3 Pour tout entier n, on note $f(n)$ l'entier écrit en inversant l'ordre des chiffres. Par exemple, $f(2538) = 8352$.

Déterminer tous les entiers n possédant 4 chiffres tels que $f(n) = 4n + 3$.

Énoncés communs

Exercice 4 Soit ABC un triangle. On choisit M sur le côté $[BC]$, N sur le côté $[CA]$ et P sur le côté $[AB]$ de sorte que $BM = BP$ et $CM = CN$. On note D_B la droite passant par B et perpendiculaire à $[MP]$ et D_C la droite passant par C et perpendiculaire à $[MN]$. On suppose que les droites D_B et D_C se rencontrent en I. Prouver que les angles $\widehat{IPA}$ et $\widehat{INC}$ sont égaux.

Exercice 5 2015 entiers strictement positifs sont placés autour d'un cercle. Montrer qu'il est possible de trouver deux entiers voisins tels que, après les avoir supprimés, les nombres restants ne puissent pas être séparés en deux groupes de même somme.

Énoncés lycée

Exercice 6 On note $[x]$ la partie entière de x. Par exemple, $[15/4] = 3$. On note $f(n) = \left[\dfrac{n}{[\sqrt{n}]}\right]$. Trouver tous les entiers n tels que $f(n+1) > f(n)$.

Exercice 7 n points sont placés sur un cercle de diamètre n/π. On suppose que la longueur de n'importe quel arc entre deux de ces n points est strictement plus grande que le nombre de points sur cet arc (sans compter les points sur les extrémités). Montrer que le cercle peut être subdivisé en n arcs de même longueur contenant exactement un point chacun.

Exercice 8 Soit p, q, r des nombres premiers tels que chacun des trois nombres $pq + 1, pr + 1$ et $qr - p$ est le carré d'un entier. Prouver que $p + 2qr + 2$ est également le carré d'un entier.

7 Solutions

Énoncés collège

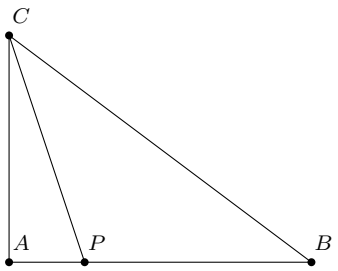
<u>Solution de l'exercice 1</u> a) Partant de x, on obtient successivement $2x+4$, $4(2x+4)+16 = 8x+32$ et $5(8x + 32) + 25 = 40x + 185$. On a donc $40x + 185 = 1945$. En soustrayant 185 membre à membre, on en déduit $40x = 1760$, donc $x = \dfrac{1740}{40} = 44$.

b) Si la dernière opération est A ou B, alors le nombre obtenu est pair donc ne peut être 2015. Donc la dernière opération est C.

Soit y l'entier obtenu après avoir appliqué la première opération. On a $5y + 25 = 2015$ donc $y = 398$. Or, un nombre obtenu après application de l'opération B est divisible par 4, et 398

n'est pas divisible par 4, donc la première opération est nécessairement A. On en déduit que $2x + 4 = 398$. Finalement, $x = 197$.

Solution de l'exercice 2 Supposons par exemple que $AB > AC$.



Lorsque $P \in [AB]$, on a $PA + PB + PC = (PA + PB) + PC = AB + PC$, qui est maximal lorsque $P = B$. Ce maximum vaut $AB + BC$.

Lorsque $P \in [BC]$, on a $PA + PB + PC = BC + PA$, qui est maximal lorsque $P = B$.

Enfin, lorsque $P \in [CA]$, on a $PA + PB + PC = AC + PB$, qui est maximal lorsque $P = C$. Ce maximum vaut $AC + BC$, qui est strictement plus petit que $AB + BC$.

Conclusion : si $AB > AC$ alors le maximum est atteint uniquement au point $P = B$. De même, si $AC < AB$ alors le maximum est atteint uniquement au point $P = C$, et enfin si $AB = AC$ alors le maximum est atteint aux points $P = B$ et $P = C$.

Solution de l'exercice 3 On note $\overline{abcd}$ l'entier dont l'écriture décimale s'écrit avec les chiffres a, b, c, d. On cherche $n = \overline{abcd}$ tel que $\overline{dcba} = 4\overline{abcd} + 3$. Déjà, $4n + 3 < 10000$ donc $n < 3000$. On en déduit que $a = 1$ ou $a = 2$.

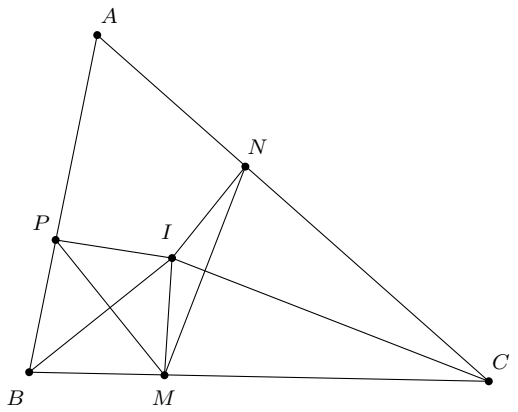
Comme $\overline{dcba} = 4n + 3$ est impair, a est impair donc $a = 1$. On a alors $4000 < 4n + 3 < 8000$, donc d est l'un des nombres $4, 5, 6, 7$. Comme le dernier chiffre de $4\overline{abcd} + 3$ est 1, on a a nécessairement $d = 7$.

L'équation $\overline{7cb1} = 4\overline{1bc7} + 3$ se traduit par $7001 + 100c + 10b = 4031 + 400b + 40c$, ou encore $2970 + 60c = 390b$.

En divisant membre à membre par 30, on obtient $99 + 2c = 13b$, donc $b > 7$ et $13b$ est impair. nécessairement, $b = 9$, donc $99 + 2c = 117$, ce qui donne $c = 9$. Finalement, $n = 1997$.

Énoncés communs

Solution de l'exercice 4



Comme BMP est isocèle en B, la hauteur D_B en B de ce triangle est un axe de symétrie, donc $\widehat{BPI} = \widehat{BMI}$, et de même $\widehat{CNI} = \widehat{CMI}$. En additionnant ces deux égalités, on obtient $\widehat{BPI} + \widehat{CNI} = 180°$, donc $\widehat{CNI} = 180° - \widehat{BPI} = \widehat{API}$.

Solution de l'exercice 5 Si tous les entiers sont pairs, on peut tous les diviser par 2 sans changer la propriété à démontrer. En répétant cette opération, on se ramène au cas où au moins l'un de ces entiers est impair.

Si la somme des 2015 entiers est paire, ces entiers ne sont pas tous impairs donc il y a deux voisins de parités différentes. On les élimine, et les termes restants ont une somme impaire donc ne peuvent pas être séparés en deux groupes de même somme.

Si la somme des 2015 entiers est impaire, on observe que les parités des nombres ne peuvent pas alterner car 2015 est impair, donc il y a deux voisins de même parité, et on les élimine.

Énoncés lycée

Solution de l'exercice 6 Soit $m = [\sqrt{n}]$. C'est l'unique entier tel que $m^2 \leqslant n < (m+1)^2$.

Si $n = (m+1)^2 - 1$, alors $[\sqrt{n+1}] = m+1$ donc $f(n) = \left[\dfrac{n}{m}\right]$ et $f(n+1) = \left[\dfrac{n+1}{m+1}\right]$.

Comme $f(n+1) > f(n)$, on a $\dfrac{n+1}{m+1} > \dfrac{n}{m}$, donc $(n+1)m > n(m+1)$. Après simplification, il vient $m > n$. Or, $m \leqslant \sqrt{n} \leqslant n$, donc $n < n$. Impossible.

Si $n < (m+1)^2 - 1$, alors $f(n+1) = \left[\dfrac{n+1}{m}\right]$. Alors $f(n+1) > f(n)$ si et seulement si $\dfrac{n+1}{m}$ est un entier. Comme $m^2 < n+1 < m^2 + 2m + 1$, ceci se produit si et seulement si $n+1 = m^2 + m$ ou $n+1 = m^2 = 2m$.

Conclusion : les solutions sont les entiers n de la forme $n = m^2 + m - 1$ ou $n = m^2 + 2m - 1$.

Solution de l'exercice 7 Le cercle est de périmètre n. On prend l'un de ces points comme origine, et on note a_k la longueur d'arc (parcourue dans le sens trigonométrique) comprise entre l'origine et le k-ième point. Notons $b_k = a_k - k$.

Si $k \leqslant \ell$, alors il y a $\ell - k - 1$ points sur l'arc entre a_k et a_ℓ, donc $\ell - k - 1 < b_\ell - b_k + \ell - k$, et donc $b_\ell - b_k < 1$. De même, en considérant l'autre arc on obtient $b_k - b_\ell < 1$.

Soient s et t tels que b_s est minimal et b_t est maximal. Soit x un réel strictement compris entre $b_t - 1$ et b_s. Alors pour tout k, on a $b_k \in]x, x+1[$, donc la subdivision du cercle en les n arcs d'extrémités $x, x+1, x+2, \ldots$ convient.

Solution de l'exercice 8 Il existe des entiers naturels a et b tels que $a^2 = pq+1$ et $b^2 = pr+1$. Sans perte de généralité, on peut supposer que $q \leqslant r$. On a $a^2 > pq \geqslant 4$, donc $a \geqslant 3$ et de même $b \geqslant 3$.

Comme $pq = a^2 - 1 = (a-1)(a+1)$, et comme p et q sont premiers, on a ($p = a-1$ et $q = a+1$) ou ($p = a+1$ et $q = a-1$). On en déduit que $q = p \pm 2$ et de même $r = p \pm 2$. Déjà, p, q, r sont impairs. De plus, comme $q \leqslant r$, les seules possibilités sont :

1) $q = r = p+2$. On a alors $qr - p = q^2 - q + 2$ est strictement compris entre $q^2 - 2q + 1$ et q^2, donc n'est pas le carré d'un entier.

2) $q = r = p-2$. On a alors $qr - p = q^2 - q - 2$, donc $qr - p < q^2$. Comme $qr - p$ est le carré d'un entier, on en déduit que $qr - p \leqslant (q-1)^2$, ce qui équivaut à $q^2 - q - 2 \leqslant q^2 - 2q + 1$, ou encore $q \leqslant 3$. Comme q est un nombre premier impair, il vient $q = r = 3$ et $p = 5$. On vérifie alors que $p + 2qr + 2 = 25 = 5^2$.

3) $q = p-2$ et $r = p+2$. On a alors $qr - p = p^2 - p - 4 < p^2$. Comme $qr - p$ est le carré d'un entier, on en déduit que $p^2 - p - 4 \leqslant (p-1)^2 = p^2 - 2p + 1$, donc $p \leqslant 5$. De plus, $p = q+2 \geqslant 5$, donc $p = 5$, $q = 3$ et $r = 7$. On vérifie alors que $p + 2qr + 2 = 49 = 7^2$.

8 Evaluation initiale

Le but de ce petit questionnaire est de nous aider à choisir le groupe le plus adapté à tes connaissances et dans lequel tu pourras évoluer à ton rythme.

Les quatre groupes du stage sont les suivants :

Groupe A : Groupe prioritairement destiné aux élèves sortant de 4ème et de 3ème qui ne sont pas encore familiers avec les exercices de type "olympiades".

Groupe B : Groupe prioritairement destiné aux élèves sortant de 2nde et de 1ère qui ne sont pas encore familiers avec les exercices de type "olympiades". Le groupe B abordera grosso modo les mêmes choses que le groupe A, mais avancera plus vite.

Groupe C : Groupe destiné aux élèves familiers avec les connaissances et outils de base du programme des Olympiades Internationales de Mathématiques.

Groupe D : Groupe destiné aux élèves les plus avancés.

Important : ce n'est pas du tout un souci si tu n'es pas familier avec les éléments ci-dessous qui ne sont pas abordés dans le cadre scolaire.

— As-tu déjà participé à des stages Animath ? OUI NON
Si oui, quand et lesquels ? Dans quel groupe étais-tu ?

— As-tu déjà participé à des clubs de mathématiques ? OUI NON
Si oui, quand et lesquels ?

— As-tu déjà été élève à l'Olympiade Française de Mathémiques (OFM) ? OUI NON

As-tu un avis sur le groupe dans lequel tu devrais être ?

Géométrie

— Connais-tu le théorème de l'angle inscrit ? OUI NON
Si oui, résous l'exercice suivant :
Soient $\mathscr{C}_1$ et $\mathscr{C}_2$ deux cercles qui se coupent en deux points A et B. Soient C et D deux points de $\mathscr{C}_1$. Les droites (AC) et (BD) recoupent $\mathscr{C}_2$ en E et F. Montrer que (CD) et (EF) sont parallèles.

— Connais-tu la puissance d'un point par rapport à un cercle ? OUI NON
Si oui, quel est la nature de l'ensemble des points ayant même puissance par rapport à deux cercles différents ?

— Sais-tu ce qu'est une homothétie ? OUI NON
— Sais-tu ce qu'est une similitude ? OUI NON

Combinatoire

— Connais-tu le principe des tiroirs ? OUI NON
— Sais-tu ce qu'est une démonstration par récurrence ? OUI NON
Si oui, résous l'exercice suivant :
Soit $n \geq 1$ un entier. Montrer que $1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$.

— Sais-tu ce qu'est un coefficient binomial ?
Si oui, que vaut $\binom{n}{k} + \binom{n}{k+1}$?

Algèbre

— Sais-tu ce que signifient les symboles $\sum_{i=1}^{n}$ et $\prod_{i=1}^{n}$? OUI NON
— Connais-tu la formule du binôme de Newton ? OUI NON
Si oui, écris-la :

— Sais-tu effectuer une division euclidienne polynomiale ? OUI NON
— Connais-tu l'inégalité arithmético-géométrique ? OUI NON
Si oui, essaie de résoudre l'exercice suivant :
Soient $a, b > 0$ deux nombres réels tels que $a^3b^2 = 1$. Montrer que $(1 + a)(2 + b) \geq 6$.

Arithmétique

— Sais-tu ce qu'est le PGCD de deux entiers ? OUI NON
Si oui, calcule le PGCD de 132 et de 63.

— As-tu déjà manipulé des congruences ? OUI NON
Si oui, est-il vrai que si $a \equiv b \mod n$ et $c \equiv d \mod n$, alors $a^c \equiv b^d \mod n$ (justifie ta réponse) ?

— Connais-tu le petit théorème de Fermat ? OUI NON
Si oui, écris-le :

— Essaie de résoudre l'exercice suivant :

(i) Trouver tous les entiers n tels que $2^n + 1$ soit un carré.

(ii) Trouver tous les entiers n tels que $2^n + 1$ soit un cube.

Si (et SEULEMENT si) tu as déjà fait tout ce que tu pouvais pour les questions précédentes, traite ces exercices (sur une feuille séparée) :

1) On écrit un entier strictement positif sur chaque face d'un dé. On attribue à chaque sommet le produit des trois faces qui l'entourent. La somme des valeurs des sommets vaut 105, quelle est la somme des nombres écrits sur les faces ?

2) Trouver les entiers naturels n tels que le produit de leurs chiffres soit égal à $n^2 - 15n - 27$.

III. Première période

Contenu de cette partie

1 Groupe A : stratégies de base

1 mardi 18 matin : Arsène Pierrot

Principe de l'invariant

Un invariant est une quantité qui ne change pas. Mais cette notion est évidemment peu intéressante dans un problème ou rien ne peut varier. En appelant au contraire " problème dynamique ", un problème dans lequel une ou plusieurs transformations sont possibles - avec répétition -, on arrive à la définition suivante :

Définition 1. Un **invariant** est une quantité qui, dans un problème dynamique, ne varie jamais.

On reconnait alors un " problème à invariant " grâce aux conditions suivantes : c'est un problème dynamique, dans lequel on demande s'il est possible de passer d'un état initial A à un état final B. Si la réponse est " oui ", il faut alors tenter de construire une suite de transformations permettant de passer de A à B. Mais, le plus souvent, cela est en fait impossible. La preuve de ceci consiste alors à trouver un invariant I tel que $I(A) \neq I(B)$.

Exemple 2. On a des piles de jetons. On peut prendre une pile et la diviser en deux autres (pas forcément de même taille), ou fusionner deux piles différentes. Peut-on passer d'une pile de 2014 jetons à 2015 piles de 1 jeton ?

On identifie ici un problème à invariant : on dispose de 2 transformations, que l'on peut répéter autant de fois que l'on veut, et on se demande s'il est possible de passer d'un état initial A (une pile de 2014 jetons) à un état final B (2015 piles de 1 jeton). Il reste à trouver un invariant I tel que $I(A) \neq I(B)$.

Dans cet exemple, c'est facile, I est tout simplement le nombre total de jetons. En effet, I ne change pas lorsque l'on fusionne deux piles ou que l'on en divise une, et $I(A) = 2014 \neq 2015 = I(B)$.

Exemple 3. Un dragon a 100 têtes. Un chevalier tente de le tuer en lui coupant 13, 17 ou 6 têtes - mais il ne peut pas couper plus de têtes qu'il n'en reste au dragon : si le dragon n'a plus que 5 têtes, il est invincible. Malheureusement, dans chacun de ces cas, des têtes repoussent. Plus précisément, il en repousse 7, 11, ou 9 respectivement. Le chevalier peut-il effectivement tuer le dragon ?

Vérifions tout d'abord qu'on a bien un problème à invariant. Le système dynamique est n, le nombre de têtes du dragon. On peut lui appliquer autant de fois que l'on veut - sous des hypothèses de positivité - les transformations suivantes : $(n \leftarrow n - 13 + 7)$, $(n \leftarrow n - 17 + 11)$, $(n \leftarrow n - 6 + 9)$. L'état initial est $A : n = 100$ et l'état final $B : n = 0$. On peut donc chercher un invariant intéressant. Il s'agit ici de $I = n \mod 3$. En effet, I reste inchangé après chacune des transformations (par exemple, $n - 13 + 7 \equiv n - 6 \equiv n \mod 3$), et $I(A) = 1 \neq 0 = I(B)$.

Une question naturelle survient alors : comment trouver l'invariant qui permet de résoudre le problème ? Il n'y a bien sûr pas de méthode générale, mais quelques invariants reviennent assez souvent :
- La somme ou la moyenne de certaines (souvent toutes) les quantités mises en jeu
- La différence - ou sa valeur absolue - de deux quantités
- La congruence modulo n d'une certaine quantité notamment avec $n = 2$ - c'est-à-dire avec la parité de cette quantité -, ou avec $n = 10$ ou $n = 9$ lorsque l'on travaille sur l'écriture décimale d'un entier. Cette dernière congruence est d'ailleurs la clé de la fameuse " preuve par 9 ", affirmant qu'un entier est toujours égal modulo 9 à la somme de ses chiffres en base 10.
- La somme des carrés de certaines quantités. Cela peut bien sûr faire penser au carré de la norme d'un certain vecteur, et implique en général une interprétation géométrique du problème.
- Un mélange des quantités ci-dessus.

Enfin, il arrive parfois que la quantité intéressante ne soit pas un invariant mais un "monovariant", c'est-à-dire une quantité ne faisant que croître - ou décroître.

Exercice 1
Soient (u_n) et (v_n) deux suites définies par $u_0 = 6$ et $v_0 = 4$ et
$\forall n \in \mathbb{N}, u_{n+1} = \frac{3}{5}u_n - \frac{4}{5}v_n$ et $v_{n+1} = \frac{4}{5}u_n + \frac{3}{5}v_n$. Existe-t-il k dans $\mathbb{N}$ tel que $u_k = 7$ et $v_k = 2$?

Exercice 2
Sur une île se trouvent des moutons magiques. Il y en a 22 bleus, 18 rouges, et 15 verts. Lorsque deux moutons de couleurs différentes se rencontrent, ils se prennent tous les deux la dernière couleur. Après un certains nombre de rencontres, tous les moutons ont la même couleur. Quelle est-elle ?

Exercice 3
On écrit n fois le nombre 1. A chaque étape, on remplace 2 des nombres écrits a et b par $\frac{a+b}{4}$ (a et b sont donc ensuite effacés). Au bout de $n-1$ étapes, il ne reste plus qu'un nombre, noté x. Montrer que $x \geq \frac{1}{n}$.

Exercice 4
On prend 2015 piles de jetons, la i-ème contenant p_i jetons, où p_i est le i-ème nombre premier (par exemple, la troisième pile contient 5 jetons). On s'autorise :
- à couper une piles en deux autres (pas forcément de tailles égales), et à rajouter un jeton à l'une des deux piles ainsi formées. - à fusionner deux piles, et à rajouter un jeton à la pile ainsi formée. Peut-on arriver à 2015 piles de 2015 jetons ?

Solution de l'exercice 1
Soit $I_n = u_n^2 + v_n^2$. On vérifie par simple calcul que la suite (I_n) est constante. On a donc trouvé un invariant I dont la valeur en l'état initial vaut $6^2 + 4^2 = 52$ et en l'état final devrait valoir $7^2 + 2^2 = 53$. C'est absurde. Il n'existe donc pas de tel k.

Solution de l'exercice 2
Notons respectivement R, V, B, le nombre de moutons rouges, verts, bleus. On remarque que $R - V \mod 3$ est invariant. En effet, si un mouton rouge rencontre un mouton vert, alors R et V diminuent tout deux de 1 ; et si un mouton rouge rencontre un mouton bleu, R diminue de 1 tandis que V augmente de 2 ; on raisonne de même si un mouton vert rencontre un mouton bleu. On a bien sur de la même façon que $V - B \mod 3$ et $B - R \mod 3$ sont des invariants du problème. Supposons par l'absurde que la couleur finale soit le rouge. On a alors $R = 55$ et $V = 0$. Mais alors $R - V \equiv 1[3]$, ce qui n'est pas sa valeur initiale. Absurde. De même si la couleur finale est le vert. Finalement la couleur cherchée est le bleu.

Solution de l'exercice 3
On rappelle que $\forall (a,b) \in {\mathbb{R}_+^*}^2, \frac{1}{a} + \frac{1}{b} \geq \frac{4}{a+b}$ (cette inégalité se démontre à l'aide de simples équivalences et d'une inégalité arithmético-géométrique). On en déduit alors que la somme des inverses des nombres écrits à l'étape k, notés S_k, ne peut que diminuer : c'est un monovariant décroissant. Ainsi $\frac{1}{x} = S_{n-1} \leq S_0 = n$. D'où le résultat voulu.

Solution de l'exercice 4
Non. Un invariant possible est la parité du nombre de piles de hauteur paires. Par exemple, si on effectue la première action sur une pile de hauteur paire, on peut la couper en "paire+paire" ou "impaire+impaire" ce qui donne "paire+impaire" après ajout d'un jeton. Le nombre de piles de hauteur paire n'a donc pas changé, et donc sa parité non plus. Les autres cas se

traitent de façon similaire.
On pouvait aussi étudier la parité du nombre de coup que l'on doit effectuer pour arriver à une contradiction : elle doit être paire car on doit couper autant de fois que l'on fusionne, mais elle doit aussi être impaire car on veut ajouter un nombre impair de jetons.

Principes de l'extremum

On dispose des deux théorèmes suivants, très intuitifs :

Théoréme 4. Dans une collection finie de nombres, il y en a un plus petit et un plus grand.

Théoréme 5. Dans une collection de nombres entiers naturels, il y en a un plus petit.

Remarque 6. Ici, " nombre " est à comprendre comme " nombre réel " et l'ordre étudié est l'ordre usuel dans $\mathbb{R}$.

Remarque 7. On peut avoir une collection de nombres, pas forcément entiers naturels, infinie, qui admette un plus petit ou un plus grand élément (ou les deux !). Par exemple, le segment $[0; 1]$. Mais cela n'est pas vrai dans le cas général (par exemple avec $\mathbb{R}_+$ ou $\mathbb{N}$).

Remarque 8. Le deuxième principe peut sembler très pratique car il se passe de l'hypothése de finitude mais en fait, on se servira le plus souvent du premier. De toutes façons, il est facile de savoir lequel utiliser d'après les hypothèses du problème (mots-clés : " entiers naturels " ou " fini ", qui peut éventuellement être caché sous la forme " il y a n personnes ... ").

Ces principes vont nous permettre, sous certaines hypothèses et à l'aide d'un raisonnement par l'absurde, d'exhiber un objet vérifiant une certaine propriété pour en déduire l'absurdité.

Exercice 5 Dans un tournoi, chaque participant rencontre tous les autres et il n'y a pas d'égalité. A la fin, chaque participant note sur une feuille le prénom de tous les joueurs qu'il a battus, ainsi que les prénoms de tous les joueurs qu'ils ont eux-mêmes battus. Montrer qu'il existe une feuille contenant tous les noms (à part celui du participant qui l'a rédigée).

Exercice 6 Soit E un ensemble de points du plan tel que $\forall x \in E$, x est le milieu de deux autres points de E. Montrer que E est infini.

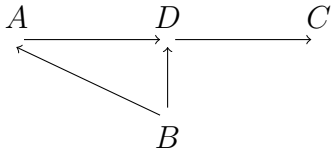
Exercice 7 Soient $A_1, ..., A_n$ et $B_1, ..., B_n$ des points du plan tels que trois quelconques d'entre eux ne sont jamais alignés. Montrer que l'on peut renuméroter les (B_i) de sorte que que les segments $[A_iB_i]$ ne se croisent jamais.

Exercice 8 Soit E un ensemble fini de points du plan tel que pour tout couple (A, B) de points de E, il y en a un troisième ($C \in E$) qui est sur la droite (AB). Montrer que tous les points de E sont alignés.

Solution de l'exercice 5 Les participants sont en nombre fini, donc on peut utiliser le premier principe pour considérer A, un des participants qui a la liste la plus longue (ce n'est pas nécessairement le seul !). Montrons que sa feuille contient tous les noms (à part le sien). Si, par l'absurde, B n'apparait pas sur cette feuille (avec $B \neq A$), alors cela veut dire que B a battu A. Ainsi, on trouve sur la liste de B le nom de A ainsi que des personnes que A a battu. Montrons que l'on trouve également le noms des joueurs qui ont été battus par au moins un joueur battu par A. Soit C un tel joueur, et D tel que A a battu D, qui a battu C. Si D avait battu B, alors B serait sur la liste de A, absurde. Donc B a battu D et ainsi C est sur la liste de B. Ainsi la

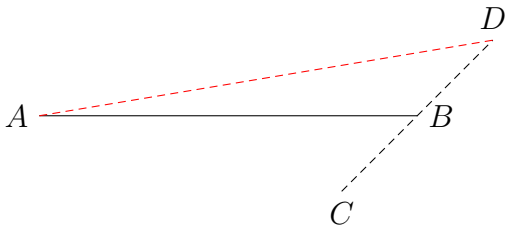
liste de B contient au moins le nom de A ainsi que tous les noms apparaissant sur la liste de A. Elle est donc strictement plus longue que celle de A, absurde. Finalement il existe bien une liste contenant tous les noms.

Figure 9. Représentation schématique de la fin du raisonnement :



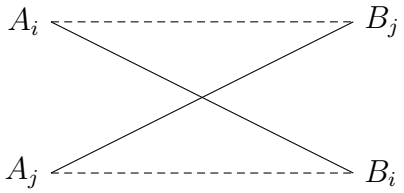
Solution de l'exercice 6 Si par l'absurde E était fini, alors le premier principe de l'extremum nous permettrait de A et B dans E tels que la distance AB soit la plus grande possible. Mais B est le milieu de deux autres points de E, disons C et D. La figure ci-dessous nous convainc alors que AC ou AD (éventuellement les deux) est en fait plus grande que AB, absurde.

Figure 10. AD va poser problème...



Solution de l'exercice 7 Puisque l'on a un nombre fini de B_i, on comprend aisément qu'il n'existe qu'un nombre fini de renumérotations possibles (exercice : montrer qu'il y en a exactement $n! = n \times (n-1) \times ... \times 2 \times 1$). Soit alors une renumérotation qui minimise la somme des longueurs des $[A_iB_i]$ (elle existe d'après le premier principe de l'extremum). Montrons qu'elle ne contient pas de " croisement ". Si par l'absurde il y en avait un, disons entre $[A_iB_i]$ et $[A_jB_j]$ (comme sur la figure), on pourrait renuméroter B_j en B_i et B_i en B_j. Cette nouvelle renumérotation donnerait une somme des longueurs des segments strictement plus petite qu'avant (cf figure et points non alignés), absurde. D'où le résultat voulu.

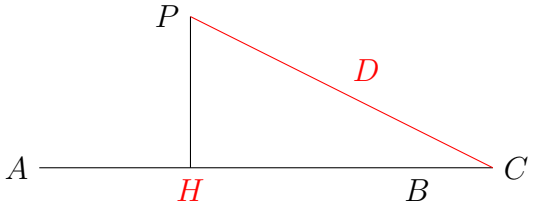
Figure 11. Figure exercice 7 :



Solution de l'exercice 8 Si par l'absurde les points de E n'étaient pas tous alignés, alors on aurait au moins un couple (P, Δ) avec Δ une droite passant par au moins 2 points de E et P un point de E qui n'appartient pas à Δ. E étant fini, ces couples sont également en nombre fini (exercice : combien il y a-t-il au plus de droite passant par deux points de E ?). On peut donc, d'après le premier principe de l'extremum, prendre celui qui minimise la distance de P à Δ. On note encore ce couple (P, Δ) par commodité et on remarque que la distance de P à Δ est strictement positive. D'après la définition de E, il y a au moins 3 points de E sur Δ, disons A, B et C comme sur le dessin. Mais alors, toujours avec les notations du dessin, (H, D)

est également un couple contre-exemple, qui de plus contredit la minimalité de (P, Δ) (l'hypoténuse d'un triangle rectangle est toujours sont plus grand côté). Absurde, d'où le résultat voulu.

Figure 12. H est plus proche de D que ne l'est P de (AC)...



2 mardi 18 après-midi : Eva Philippe

- Dénombrement -

Exercice 1 Un cadenas à code comporte 7 molettes de 10 chiffres. Combien de codes différents peut-on obtenir ?

Solution de l'exercice 1 10^7 Nombre de listes ordonnées avec répétition possible de k éléments pris dans un ensemble à n éléments : n^k car pour chacun des k éléments de notre liste on a n choix possibles.

Exercice 2 Lors d'une course entre quatre athlètes, combien de classements par ordre d'arrivée sont possibles ?

Solution de l'exercice 2 $4 * 3 * 2 * 1 = 4!$ Permutations de n éléments (réarrangements de nos n éléments dans dans un ordre différent) : $n! = n * (n-1) * (n-2) * ... * 3 * 2 * 1$ (on dit *factorielle* n)

Exercice 3 Une urne contient 25 boules de loto, toutes différentes, on en tire trois successivement. Combien de tirages sont possibles (en comptant l'ordre) ?

Solution de l'exercice 3 $25 * 24 * 23 = \frac{25!}{(25-3)!}$ Liste ordonnée de k éléments parmi n possibles : $\frac{n!}{(n-k)} = n * (n-1) * (n-2) * ... * (n-k+1)$ car pour le premier élément on a n choix possibles, pour le deuxième on n'en a plus que $(n-1)$ car on n'autorise pas les répétitions, et ainsi de suite jusqu'au *k*-ième élément pour lequel on n'a plus que $(n-k+1)$ choix possibles (si $k \leq n$ sinon c'est 0).

Exercice 4 Une libraire a reçu 13 nouveaux livres mais elle ne peut en placer que 4 dans sa vitrine, combien a-t-elle de possibilités ?

Solution de l'exercice 4 $\frac{13*12*11*10}{4*3*2*1} = \frac{13!}{(13-4)!*4!}$ Ensemble (non ordonné) de k éléments parmi n possibles : $\frac{n!}{k!(n-k)!} = n(n-1)(n-2)...(n-k+1)$ que l'on note $\binom{n}{k}$, c'est le *coefficient binomial* "k parmi n". Lorsque $k \leq 0$ ou $k \geq n+1$, on a $\binom{n}{k} = 0$.

À partir de maintenant, on ne va plus s'inquiéter de billes, de coureurs ni de livres mais d'ensembles abstraits d'éléments. Le nombre d'éléments d'un ensemble est appelé son *cardinal*.

Proposition 13. $\binom{n}{k} = \binom{n}{n-k}$

Démonstration 14. Choisir k éléments dans notre ensemble à n éléments, c'est exactement équivalent à choisir $n-k$ éléments dans ce même ensemble.

Question : Combien peut-on former de sous-ensembles (ou de parties) d'un ensemble à n éléments ?

Notation 15. Lorsqu'on veut faire une grosse somme de termes qui peuvent s'exprimer selon un entier, souvent noté k (ou i mais cela n'a pas d'importance), qui varie entre deux valeurs, on utilise le symbole $\sum$. Par exemple :

$$\sum_{k=0}^{n} 1 = 1 + 1 + ... + 1 = n + 1$$

$$\sum_{k=0}^{n} k = 0 + 1 + 2 + ... + n = \frac{n(n+1)}{2}$$

$$\sum_{k=0}^{n} \binom{n}{k} = \binom{n}{0} + \binom{n}{1} + ... + \binom{n}{n-1} + \binom{n}{n}$$

Pour un produit on utilise de la même manière le symbole $\prod$. Par exemple :

$$\prod_{k=1}^{n} k = n!$$

Proposition 16. Le nombre de sous-ensembles d'un ensemble à n éléments est :

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n$$

Démonstration 17.
— Si l'on classe nos sous-ensembles selon leur cardinal k qui peut varier entre 0 et n on obtient la somme $\sum_{k=0}^{n} \binom{n}{k}$
— On peut aussi dire que lorsqu'on choisit un sous-ensemble on a deux choix pour chacun des n éléments : soit on le prend soit on ne le prend pas. Il y a donc une correspondance (on dit une *bijection*) entre un sous-ensemble et une suite ordonnée de n chiffres 0 (on ne prend pas l'élément correspondant) ou 1 (on prend l'élément correspondant). D'après l'exercice 1, il y a donc 2^n sous-ensembles possibles.

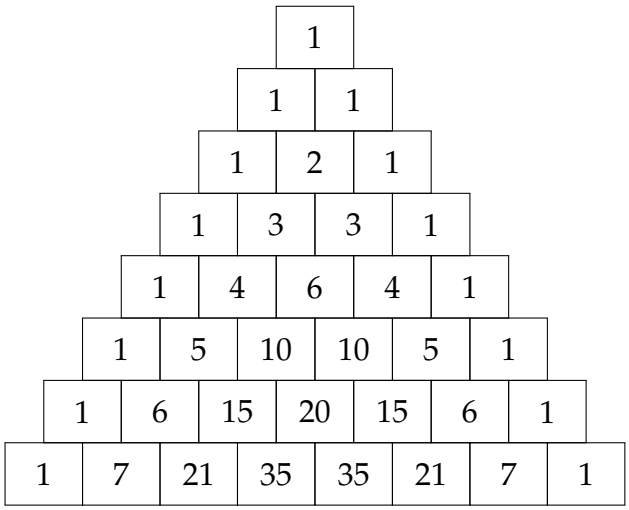
Cette démonstration illustre un principe très important en combinatoire : le *double-comptage*. Il permet d'établir une égalité entre deux quantités en comptant de plusieurs manières différentes le nombre d'éléments d'un même ensemble.

Proposition 18 (Formule de Pascal)**.**

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$$

Démonstration 19. Considérons notre ensemble E à n éléments et isolons un élément, noté x_0. $\binom{n}{k}$ correspond au nombre de parties de E à k éléments. On peut distinguer ces parties selon que x_0 soit dans cette partie ou non : il y a $\binom{n-1}{k}$ parties qui ne contiennent pas x_0 (on choisit notre partie parmi les $n-1$ éléments restants une fois que x_0 a été enlevé) et $\binom{n-1}{k-1}$ parties qui contiennent x_0 (il ne reste plus que $k-1$ éléments à choisir parmi les $n-1$ restants). On a le résultat. (Comme la plupart des résultats sur les coefficients binomiaux on peut également établir ce résultat par le calcul grâce à la formule avec les factorielles).

La formule de Pascal nous permet ensuite de construire le triangle de Pascal, que vous connaissez peut-être déjà. La case située dans la k-ième colonne de la n-ième ligne contient le coefficient binomial $\binom{n-1}{k-1}$. D'après la formule de Pascal, on obtient donc chaque case comme la somme des deux cases qui sont au-dessus.



On constate qu'il y a un lien entre la n-ième ligne du triangle de Pascal et le développement de $(a+b)^n$! ! !

Proposition 20 (Formule du binôme de Newton)**.**

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$

Démonstration 21. Après la première étape de notre développement, on obtient une somme de termes de la forme $a^k b^{n-k}$. Chacun de ces termes correspond au choix de k facteurs de la forme $(a+b)$ dans lesquels on prend a (et on prend b dans tous les autres). Il y a donc au total autant de termes de la forme $a^k b^{n-k}$ que de manières de choisir k parenthèses $(a+b)$ parmi les n dont le produit vaut $(a+b)^n$, c'est-à-dire $\binom{n}{k}$. Ce résultat peut aussi se démontrer par récurrence sur n.

Remarque 22. Avec $a=1$ et $b=1$ on retrouve le résultat $\sum_{k=0}^{n} \binom{n}{k} = 2^n$.

Exercice 5 Montrer que

$$k\binom{n}{k} = n\binom{n-1}{k-1}$$

Solution de l'exercice 5 Utilisons le principe de double-comptage en calculant le nombre de manières de choisir k sous-chefs et leur chef dans un comité de n personnes.

— On peut d'abord choisir les k sous-chefs ($\binom{n}{k}$ choix) puis parmi eux leur chef (k choix)

— ou commencer par choisir le chef (n choix) puis les $k-1$ sous-chefs restants ($\binom{n-1}{k-1}$ choix).

Exercice 6 Plaçons-nous dans un quadrillage $\mathbb{Z} \times \mathbb{Z}$. On commence à l'origine et on ne s'autorise que des déplacements de un pas vers la droite ou un pas vers le haut ($+(1,0)$ ou $+(0,1)$). Combien de chemins différents pouvons-nous prendre pour aller jusqu'au point (m,n) ?

Solution de l'exercice 6 Au total il faudra faire exactement m pas vers la droite (et n pas vers le haut). Pour déterminer un chemin il suffit donc de choisir parmi les $n+m$ pas que l'on doit faire les m qui seront vers la droite. Le nombre de chemins est donc $\binom{n+m}{m}$ ($= \binom{n+m}{n}$).

- Pavages et coloriages -

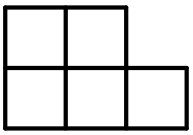
Pour les exercices de pavage, il y a en général deux situations possibles : soit le pavage demandé est réalisable et il faut en trouver un qui marche, soit il ne l'est pas et on peut le démontrer avec un coloriage astucieux. En voici quelques exemples :

Exercice 7 On a un échiquier 8×8 auquel il manque deux coins opposés. Peut-on en paver toutes les cases avec des dominos 2×1 ?

Exercice 8 Une salle de bain est pavée avec des dalles de type 2×2 et 1×4. Une dalle s'est brisée mais il ne nous reste qu'une dalle de l'autre type. Peut-on réarranger les dalles de façon à remplacer la dalle brisée avec une nouvelle dalle de l'autre type ?

Exercice 9 Un tetramino est une figure formée de 4 carrés (pensez à Tetris). Trouvez le nombre m de tetraminos distincts (on dit que deux tetraminos sont identiques si on peut les superposer en les faisant pivoter mais sans les retourner). Est-il possible de paver un rectangle $4 \times m$ avec un tetramino de chaque sorte ?

Exercice 10 Soit m un nombre entier. Un rectangle de taille $5 \times m$ peut-il être pavé par le pentamino ci-dessous ou son symétrique ?



Solution de l'exercice 7 Si l'on colorie notre échiquier en noir et blanc comme un vrai échiquier, on s'aperçoit que deux coins opposés sont de la même couleur. Or un domino couvre exactement une case noire et une case blanche. On ne peut donc pas paver l'échiquier avec les dominos.

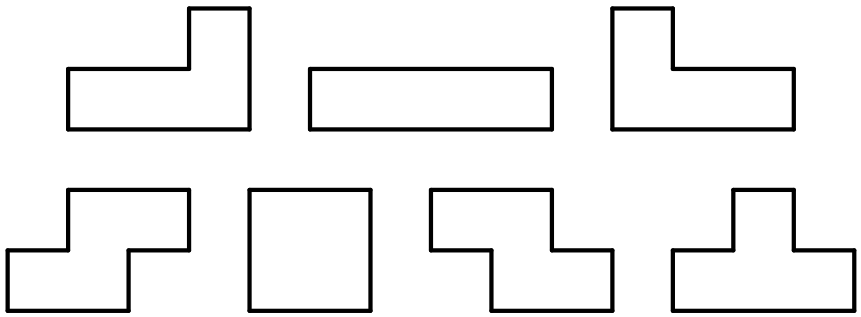
Solution de l'exercice 8 Deux types de coloriages sont possibles pour montrer que l'on ne peut pas remplacer notre dalle brisée :

— On colorie la première ligne en carrés bleus et rouges en commençant par bleu, la deuxième en noir et blanc en commençant par noir. Ensuite on continue avec des lignes alternées bleu-rouge et noir-blanc en commençant toujours par bleu et noir respectivement. Alors les dalles 2×2 couvrent exactement un carré de chaque couleur. Une dalle 4×1 couvre 2 carrés d'une couleur et 2 d'une autre.

— On découpe notre quadrillage en carrés 2×2 dont on colorie en noir la dalle du coin inférieur droit. Alors une dalle carrée recouvre exactement une dalle noire alors qu'une dalle 4×1 en recouvre 0 ou 2.

Ainsi, les deux types de dalles ne sont pas interchangeables.

Solution de l'exercice 9 Il est facile de vérifier qu'il y a 7 pièces différentes au Tetris :



Ensuite, passons au pavage d'un rectangle 4×7. Si on colorie les cases en échiquier, on se retrouve avec 14 cases blanches et 14 noires. Tous les tetraminos recouvrent 2 cases noires et 2 blanches, quelle que soit la manière de les mettre, sauf le T, qui recouvre 3 blanches et 1 noire ou 3 noires et 1 blanche. Il est donc impossible de faire le pavage.

Solution de l'exercice 10

— Dans le cas où m est pair on peut facilement construire un pavage en associant les pentaminos deux à deux.
— Lorsque m est impair, si on colorie une case par carré de 2×2 (comme dans la deuxième solution de l'exercice 2), on obtient $m-1$ cases colorées dans notre rectangle. Or chaque pentamino en recouvre exactement une et on devrait utiliser m pentaminos pour couvrir tout le rectangle. Un tel pavage n'est donc pas possible lorsque m est impair.

3 mercredi 19 matin : Clara Ding

Principe des tiroirs

Si on cherche à ranger $n+1$ chaussettes dans n tiroirs, on sait qu'au moins un tiroir contient au moins deux chaussettes. Ainsi, si on cherche a ranger $n+1$ objets dans n ensembles, au moins un des ensembles contiendra au moins 2 objets. Plus généralement, si on cherche à ranger au moins $kn+1$ objets dans n ensembles, on sait qu'au moins un des ensembles contient au moins $k+1$ objets.

Exercice 1 Sachant qu'un humain a moins de 300000 cheveux et qu'il y a 3000000 de parisiens, au moins deux parisiens ont le même nombre de cheveux. On peut même préciser qu'il existe 10 parisiens au moins ayant le même nombre de cheveux. S'il existait 3000001 parisiens ayant chacun au plus 300000 cheveux, on pourrait affirmer qu'au moins 11 d'entre eux ont le même nombre de cheveux.

Exercice 2 Dans un stage de n personnes, certaines se connaissent et pas d autres. On dit que si A connait B, alors B connait A. Montrez que l on peut trouver 2 stagiaires differents qui connaissent le meme nombre de personnes dans le stage.

Solution de l'exercice 1

Les tiroirs seront le nombre de connaissances de chaque personnes, qui peut donc varier de 0 a $n-1$. Cependant, il y a n tiroirs pour n personnes, ce qui ne nous convient pas pour appliquer le principe des tiroirs. Mais on remarque qu il ne peut pas y avoir quelqu un dans le tiroir de 0 connaissances et quelqu un dans le tiroir de $n-1$ connaissances simultanement. En effet, s

il y avait quelqu un qui ait $n-1$ connaissances, il connait donc tout le monde, et donc tout le monde le connait, et donc tout le monde a au moins une connaissance. Ainsi, personne n est dans le tiroir a 0 connaissances. Ainsi, au plus $n-1$ tiroirs sont remplis, sachant qu on a n personnes, au moins 2 personnes sont dans le meme tiroir et ont donc le meme nombre de connaissances.

Exercice 3 On choisit 55 entiers distincts entre 1 et 99. Peut-on trouver parmi ces entiers 2 dont la différence est 9 ?

Solution de l'exercice 2 La question demande de trouver deux éléments vérifiant une même propriété, il faut donc penser immédiatement au principe des tiroirs. Il nous faut choisir des tiroirs tels que, si deux éléments sont dans le tiroir, alors leur différence est 9. On veut donc des tiroirs du style : $(1, 10)$. Regardons combien de tels tiroirs on peut construire. On commence par :

$$(1, 10), (2, 11), (3, 12), \ldots, (8, 17), (9, 18).$$

Ensuite, on ne peut pas mettre le tiroir $(10, 19)$, car 10 est déjà dans le tiroir $(1, 10)$. On continue donc par le tiroir $(19, 28)$, et ainsi de suite. Cette construction permet de grouper les entiers en tiroirs par paquets de 18. On peut donc grouper tous les entiers inférieurs à $18 \cdot 5 = 90$ en 45 tiroirs. Il nous reste les 9 entiers compris entre 91 et 99, que l'on ne peut plus grouper par paires. Ce n'est pas grave, on crée simplement un nouveau tiroir pour chacun de ces entiers. On a $45 + 9 = 54$ tiroirs, 55 entiers, il y en a donc deux dans le même tiroir, et leur différence est forcément égale à 9.

Exercice 4 Les points du plan sont coloriés de telle sorte que chaque point soit rouge ou bleu. Montrer que pour tout réel $x > 0$, il existe une couleur telle qu'on puisse trouver deux points de cette couleur distants de x.

Solution de l'exercice 3 On prend trois points qui forment un triangle equilatéral de côté x. Il y a 3 points qui peuvent être de deux couleurs différentes. Il y a donc au moins deux points de la même couleur.

Exercice 5 Montrer qu'un polyèdre convexe possède toujours deux faces qui ont le même nombre d'arêtes. (Un polyèdre est convexe s'il n'a pas de "renfoncement" ou, plus formellement, si pour tout couple de points situés à l'intérieur du polyèdre, le segment reliant ces deux points est entièrement situé à l'intérieur du polyèdre).

Solution de l'exercice 4 On doit montrer que deux objets vérifient ensemble une propriété, il faut donc penser au principe des tiroirs. La façon naturelle de faire est de prendre comme chaussettes les faces du polynôme, et comme tiroirs les nombres d'arêtes de chacune des faces. Ainsi, si on a deux chaussettes dans le même tiroir (par exemple deux faces dans le tiroir "3"), alors ces deux faces auront le même nombre d'arêtes (dans notre exemple, ce seront des triangles). Il faut maintenant essayer de compter les chaussettes et les tiroirs.

Supposons que la face du polyèdre ayant le plus d'arêtes en possède m. Alors, les tiroirs utiles seront les tiroirs $(3, 4, 5 \ldots, m)$: il y en a $m-2$. Pour conclure, il nous suffit de prouver que le polyèdre a plus de $m-1$ faces. Regardons une face à m arêtes. Cette face a exactement m faces voisines (c'est la que l'on utilise l'hypothèse de convexité), ce qui termine.

Exercice 6 On place 51 points dans un carré de côté 1, de manière quelconque. Montrer qu'on peut trouver un cercle de rayon $\frac{1}{7}$ contenant au moins trois d'entre eux (le cercle peut déborder le carré).

Solution de l'exercice 5 Pour appliquer le principe des tiroirs et prouver que l'un des n tiroirs contient au moins 3 points, il faut que $51 > 2n$ donc $n \leq 25$. Or il est facile de partager le carré en 25 carrés de côté $\frac{1}{5}$. Pour chacun des côtés communs à deux carrés, il faut convenir auquel des carrés on le rattache, de sorte qu'on ait une réelle partition du carré en sous-ensembles disjoints. Chaque point appartient à un petit carré, donc il existe un petit carré contenant au moins trois points. Reste à voir qu'il existe un cercle de rayon $\frac{1}{7}$ contenant ce carré, car la diagonale du carré, $\frac{\sqrt{2}}{5}$ est inférieure au diamètre du cercle $\frac{2}{7}$.

Exercice 7 On choisit dix entiers quelconques de deux chiffres, donc entre 10 et 99. Montrer que parmi eux, on peut trouver deux sous-ensembles disjoints d'entiers de même somme.

Solution de l'exercice 6
Combien peut-on trouver de sous-ensembles de notre ensemble de dix entiers ? Pour chacun des dix entiers, on peut le choisir ou ne pas le choisir, ce qui constitue dix choix binaires indépendants. Il y a donc $2^{10} = 1024$ sous-ensembles possibles. Et combien y a-t-il de sommes distinctes d'éléments d'un tel sous-ensemble ? En tout cas moins que mille. La plus grande somme possible est : $99+98+...+90 < 1000$, et la plus petite est 10. Donc deux sous-ensembles A et B auront même somme. Rien ne prouve qu'ils sont disjoints, mais ils sont distincts, et s'ils ont une intersection non vide C, en retirant de chacun d'eux les éléments de l'intersection, les sous-ensembles restants deviendront disjoints, et ils auront encore même somme car chaque somme sera diminuée de la somme des éléments de l'intersection.

Exercice 8 On considère 5 points à coordonnées entières $P_1, \ldots, P_5$ dans le plan. Montrer qu'il existe un point à coordonnée entière sur un des segments $]P_i, P_j[$.

Solution de l'exercice 7 On ecrit $P_i = (x_i, y_i)$, avec $x_i, y_i \in \mathbb{Z}$ les coordonnees du point P_i. La "parite" du couple (x_i, y_i) peut prendre $2^2 = 4$ valeurs : (P,P), (P,I), (I,P), (I,I) (P pour pair et I pour impair). Par principe des tiroirs, au moins deux des points P_i et P_j sont de meme parite. On considere alors le milieu de $[P_i, P_j]$, aui est bien a coordonnees entieres.

Exercice 9 Montrez que parmi $n+1$ nombres de l'ensemble $\{1, 2, \ldots, 2n\}$, on peut en trouver 2 dont l'un divise l'autre.

Solution de l'exercice 8
Chaque nombre de l'ensemble $\{1, 2, \ldots, 2n\}$ peut s'ecrire sous la forme de $2^k(2s+1)$, ou s est compris entre 0 et $n-1$. Il y a donc n possibilites pour s. Sachant que nous avons $n+1$ nombres de l ensemble, d'apres le principe des tiroirs, nous pourrons en trouver deux tel que l un s ecrit $2^k(2s+1)$ et l'autre $2^{k'}(2s+1)$, pour un meme s. Ainsi, il est clair que parmi ces deux nombres, l'un divise l'autre.

Il est conseillé de chercher les exercices qui suivent après un cours d'arithmétique.

Exercice 10 Montrez que pour tout n, parmi $n+1$ entiers quelconques $a_1, a_1, \ldots, a_n$, on peut en trouver deux a_i et a_j tels que $a_i - a_j$ soit divisible par n.

Solution de l'exercice 9 On classe les nombres dans les n classes modulo n : $\{kn\}, \{kn+1\}, \ldots \{kn+(n-1)\}$. Au moins une classe contient au moins deux entiers, donc leur différence est divisible par n.

Exercice 11 Montrez que pour tout n, il existe un multiple de n d'au plus n chiffres, tous egaux a 0 ou 1.

Solution de l'exercice 10 Ici, les tiroirs seront les restes de la division par n, et les objets, des nombres dont la différence s'écrive seulement avec des 0 et des 1. Plus précisément, choisissons pour objets les nombres : $a_0 = 0, a_1 = 1, a_2 = 11, a_3 = 111, \ldots, a_n = 11\ldots,1$ qui s'écrivent avec $0, 1, 2, \ldots, n$ chiffres 1. Il y a $n+1$ objets, et leurs restes de la division par n peuvent prendre n valeurs distinctes : $0, 1, \ldots, n-1$. Donc deux de ces nombres auront même reste de la division par n : $a_i = nq_i + r$ et $a_j = nq_j + r$, et leur différence (en supposant $i > j$) : $a_i - a_j = n(q_i - q_j)$ sera divisible par n. Or cette différence s'écrira avec $(i-j)$ fois le chiffre 1 suivis de j fois le chiffre 0, ce qui est conforme à l'énoncé.

Exercice 12 Démontrer que parmi 2015 nombres entiers arbitraires, on peut trouver des nombres dont la somme est divisible par 2015.

Solution de l'exercice 11 Notons $a_1, \ldots, a_{2015}$ les entiers en question et considérons les sommes $s_i = a_1 + a_2 + \cdots + a_i$ (pour $1 \leq i \leq 2015$). Si l'une d'elles est divisible par 2015, c'est gagné. Sinon, d'après le principe des tiroirs, il existe deux sommes, disons s_i et s_j (avec $i < j$), qui ont le même reste dans la division euclidienne par 2015. Dans ce cas, $s_j - s_i$ convient.

Exercice 13 On considère dix entiers quelconques, $a_1, a_2, ...a_{10}$. Montrer qu'on peut choisir, parmi $\{-1, 0, 1\}$, dix nombres $b_1, b_2, ...b_{10}$ non tous nuls tels que : $b_1a_1 + b_2a_2 + ... + b_{10}a_{10}$ soit divisible par 1000.

Solution de l'exercice 12 Cet exercice s'apparente à celui sur les dix entiers entre 10 et 99. Considérons toutes les sommes possibles $c_1a_1 + c_2a_2 + ... + c_{10}a_{10}$ où $c_1, c_2, ...c_{10}$ sont choisis parmi $\{0, 1\}$. Il y en a $2^{10} = 1024$, car chaque c_i peut être choisi indépendamment parmi deux valeurs. Les restes des divisions par 1000 de ces sommes peuvent prendre 1000 valeurs distinctes (les trois derniers chiffres du nombre s'il est positif), de 0 à 999. Donc parmi ces 1024 sommes, nécessairement deux au moins auront même reste de la division par 1000, ce qui signifie que leur différence sera divisible par 1000. Or une différence de deux sommes du type $c_1a_1 + ... + c_{10}a_{10}$ avec $c_i = 0$ ou 1 est précisément une somme du type $b_1a_1 + b_2a_2 + ... + b_{10}a_{10}$ avec $b_i = -1, 0$ ou 1.

La recurrence

La récurrence est un principe de raisonnement mathématique, utile dans de nombreux domaines, notamment en combinatoire et en arithmétique.
Elle s'appuie sur l'idée que l'on peut parcourir l'ensemble des entiers naturels $\mathbb{N}$ de la manière suivante : on part de 0, puis on va en $0+1=1$, puis en $1+1=2$, puis en $2+1=3\ldots$ et ainsi de suite, à chaque fois qu'on se trouve en un entier donné n (autrement dit, à chaque fois qu'on se place au rang n), on peut aller à l'entier suivant, qui sera $n+1$.
Le raisonnement par récurrence vise à répondre à une question du type : "**Montrer que la propriété $P(n)$ est vraie pour tout entier naturel n.**" Il consiste en 3 étapes :

1. L'initialisation : On montre que la propriété $P(0)$ est vraie.
2. L'hérédité : On montre que, si n est un entier naturel tel que $P(n)$ est vraie, alors $P(n+1)$ est vraie aussi.
3. La conclusion : On en conclut que $P(n)$ est vraie pour tous les entiers naturels.

Si on sait monter sur la première marche d'un escalier et qu'on sait monter d'une marche à la suivante, alors on peut gravir tout l'escalier. Telle est l'idée du raisonnement par récurrence ou la n-ième marche correspond à la propriété au rang n, donc $P(n)$.

Exercice 14 Pour un entier $n \geq 1$, soit $P(n)$ la propriété "$1 + 2 + \cdots + n = \frac{n(n+1)}{2}$". Montrons que $P(n)$ est vraie pour tout entier $n \geq 1$ par récurrence sur n.

- (Initialisation) Il est clair que $P(1)$ est vérifiée.
- (Hérédité) Supposons $P(n)$ vérifié. Montrons $P(n+1)$. En utilisant l'hypothèse de récurrence, on a

$$\begin{aligned} 1 + 2 + \cdots + (n+1) &= (1 + 2 + \cdots + n) + (n+1) \\ &= \frac{n(n+1)}{2} + (n+1) \\ &= \frac{n(n+1) + 2(n+1)}{2} \\ &= \frac{(n+1)(n+2)}{2} \end{aligned}$$

On en déduit que $P(n)$ est vérifiée pour tout entier $n \geq 1$.

Exercice 15 Montrer que

$$1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

Solution de l'exercice 13 Pour un entier $n \geq 1$, soit $P(n)$ la propriété

$$"1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}".$$

Montrons que $P(n)$ est vérifiée pour tout entier $n \geq 1$ par récurrence sur n.

- (Initialisation) Il est clair que $P(1)$ est vérifiée.
- (Hérédité) Supposons $P(n)$ vérifiée. Montrons $P(n+1)$. En utilisant l'hypothèse de récurrence, on a

$$\begin{aligned} 1^2 + 2^2 + \cdots + (n+1)^2 &= \left(1^2 + 2^2 + \cdots + n^2\right) + (n+1)^2 \\ &= \frac{n(n+1)(2n+1)}{6} + (n+1)^2 \\ &= \frac{(n+1)(n(2n+1) + 6(n+1))}{6} \\ &= \frac{(n+1)(2n^2 + 7n + 6)}{6} \\ &= \frac{(n+1)(n+2)(2n+3)}{6}. \end{aligned}$$

On en déduit que $P(n)$ est vérifiée pour tout entier $n \geq 1$.

Remarques. Il existe de nombreuses variantes du raisonnement par récurrence. Notamment :

- **Récurrence à partir d'un certain rang.**
  Pour montrer qu'une propriété $P(n)$ est vraie pour tout n supérieur ou égal à un entier k donné (qui ne vaut pas forcément 0) :
  - ▷ Initialisation : on vérifie que la propriété $P(k)$ est vraie.
  - ▷ Hérédité : on suppose qu'il existe un entier naturel $n \geq k$ tel que la propriété $P(n)$ est vraie. On montre qu'alors la propriété $P(n+1)$ est aussi vraie.
- **Récurrence forte.**
  Pour montrer qu'une propriété $P(n)$ est vraie pour tout n, quand $P(n)$ ne suffit pas à prouver $P(n+1)$ pour l heredite, on peut aussi utiliser le fait que P est vraie pour tous les rangs inférieurs à n afin de montrer que $P(n+1)$ est vraie. Cela paraît logique. Si on démontre une propriété P de proche en proche, quand on veut la prouver au rang 100, on sait déjà qu'elle est vraie aux rangs allant de 1 à 99, donc on peut utiliser tout cela dans notre preuve du rang 100. On aura :
  - ▷ Initialisation : on vérifie que la propriété $P(0)$ est vraie.
  - ▷ Hérédité : on suppose qu'il existe un entier naturel n tel que les propriétés $P(0), P(1), \ldots, P(n)$ sont toutes vraies. On montre qu'alors la propriété $P(n+1)$ est aussi vraie.

Exercices

Exercice 16 Montrer que pour tout $n \geq 4$, on a : $2^n \geq n^2$.

Solution de l'exercice 14
Montrons que $P(n)$ est vérifiée pour tout entier $n \geq 4$ par récurrence sur n.

- (Initialisation) On voit que $P(4)$ est vérifiée.
- (Hérédité) Supposons $P(n)$ vérifiée. Montrons $P(n+1)$. En utilisant l'hypothèse de récurrence, on a
$$2^{n+1} \geq 2 \cdot 2^n \geq 2n^2.$$
Il suffit donc de montrer que $2n^2 \geq (n+1)^2$. Pour cela, on écrit
$$2n^2 - (n+1)^2 = n^2 - 2n - 1 = (n-1)^2 - 2,$$
qui est bien positif car $n - 1 \geq 3$.

On en déduit que $P(n)$ est vérifiée pour tout entier $n \geq 4$. Ainsi, $2^n \geq n^2$ pour tout $n \geq 4$.

Exercice 17 Montrer que
$$1 + \frac{1}{4} + \frac{1}{9} + \cdots + \frac{1}{n^2} < 2.$$

Indication : On pourra montrer par recurrence que
$$1 + \frac{1}{4} + \frac{1}{9} + \cdots + \frac{1}{n^2} \leq 2 - \frac{1}{n}.$$

Solution de l'exercice 15 Soit $P(n)$ la propriete "$1 + \frac{1}{4} + \frac{1}{9} + \cdots + \frac{1}{n^2} \leq 2 - \frac{1}{n}$". Il est evident que $P(1)$ est vrai. Supposons $P(n)$ vraie, et montrons que $P(n+1)$ vraie. On a :

$$\begin{aligned} 1+\frac{1}{4}+\frac{1}{9}+\cdots+\frac{1}{n^2}+\frac{1}{(n+1)^2} &\leq 2-\frac{1}{n}+\frac{1}{(n+1)^2} \\ &= 2-\frac{n^2+n+1}{n(n+1)^2} \end{aligned}$$

Il reste a voir si $\frac{n^2+n+1}{n(n+1)^2} \geq \frac{1}{(n+1)^2} \Leftrightarrow n^2+1 \geq 0$, ce qui est bien vrai et donc l heredite marche bien.
On a donc montre par recurrence que pour tout n : $1+\frac{1}{4}+\frac{1}{9}+\cdots+\frac{1}{n^2} \leq 2-\frac{1}{n}$. Donc on a bien : $1+\frac{1}{4}+\frac{1}{9}+\cdots+\frac{1}{n^2} < 2$ et c est gagne.

Exercice 18 Dans un certain pays, deux villes sont toujours reliées soit par une ligne aérienne, soit un canal navigable (à double sens). Montrer qu'il est possible de choisir un moyen de transport, tel que, en partant de n'importe quelle ville, on puisse atteindre n'importe quelle autre ville uniquement à l'aide de ce moyen de transport.

Solution de l'exercice 16 Notons n le nombre de villes. Soit $P(n)$ la propriete : « Pour toute configuration de n villes, il existe un moyen de transport vérifiant les conditions requises. »

- (Initialisation) $P(2)$ est vérifiée.
- (Hérédité) Soit $n \geq 2$ un entier et supposons que $P(n)$ est vraie. Montrons que $P(n+1)$ est satisfaite. Considérons A une ville quelconque et appliquons la propriété $P(n)$ à la configuration des n villes restantes. Sans perte de généralité, supposons que c'est l'avion qui convient. Alors : soit il existe une ligne aérienne reliant A à une autre ville, auquel cas l'avion convient, soit A est relié à toutes les autres villes par un canal, auquel cas le bateau convient. Dans les deux cas, l heredite est verifiee.

Exercice 19 Soit x un nombre réel non nul tel que $x+\frac{1}{x}$ soit un entier. Montrer que pour tout $n \in \mathbb{N}$, $x^n+\frac{1}{x^n}$ est un entier.

Solution de l'exercice 17

Le principe de cet exercice est le suivant : on veut obtenir $x^{n+2}+\frac{1}{x^{n+2}}$ à partir des $x^k+\frac{1}{x^k}$ précédents par des opérations, qui conservent le caractère entier des nombres (addition, soustraction, multiplication).

Or, on constate que :

$$\left(x^{n+1}+\frac{1}{x^{n+1}}\right)\left(x+\frac{1}{x}\right) = x^{n+2}+x^n+\frac{1}{x^n}+\frac{1}{x^{n+2}} \qquad (\star)$$

A partir de cela, il suffit de supposer que $x^n+\frac{1}{x^n}$ et $x^{n+1}+\frac{1}{x^{n+1}}$ sont des entiers pour passer la même propriété à $x^{n+2}+\frac{1}{x^{n+2}}$.

Donc on rédige notre récurrence ainsi : soit, pour tout $n \in \mathbb{N}$, la propriété $P(n)$: « $x^n+\frac{1}{x^n}$ est un entier ».

L'initialisation doit être faite pour $n=0$ et $n=1$. Or $x^0+\frac{1}{x^0}=2$ est entier et $x+\frac{1}{x}$ aussi, par hypothèse de l'énoncé.

On passe donc à l'hérédité, en supposant qu'il existe $n \in \mathbb{N}$ tel que $P(n)$ et $P(n+1)$ sont toutes les deux vraies. Alors, d'après $(*)$, $P(n+2)$ est aussi vraie. Ceci conclut par principe de récurrence.

Remarque. D'un point de vue technique, il s'agit ici d'un schéma de récurrence double, qui est un cas simplifié de récurrence forte. C'est pourquoi il faut initialiser au deux premiers rangs (avec un seul rang, on ne peut pas encore déclencher l'hérédité).

Exercice 20 On trace n cercles dans le plan tels que deux cercles ne soient jamais tangents. Montrer que l'on peut colorier les régions du plan ainsi délimitées de deux couleurs (bleu et rouge par exemple) de telle façon que deux régions séparées par un arc de cercle soient de couleurs différentes.

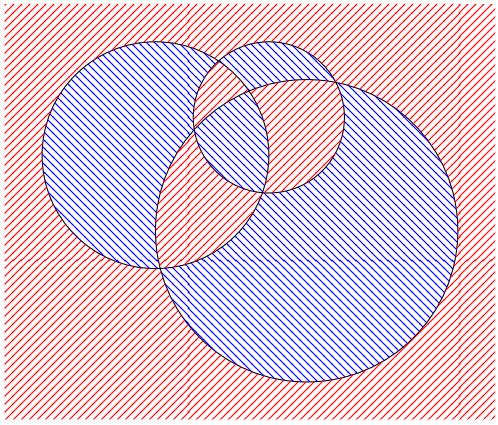


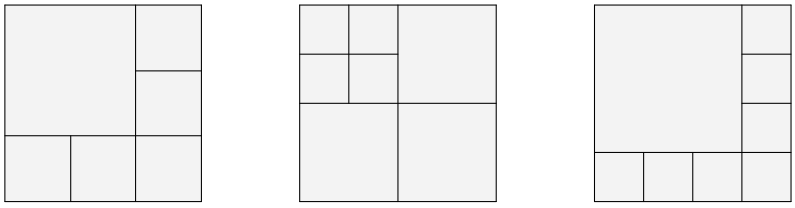
FIGURE.– Exemple de coloriage possible pour $n = 3$ cercles

Solution de l'exercice 18 Nous allons faire la démonstration par récurrence sur n. Pour $n = 1$, il suffit de colorier l'intérieur du cercle en rouge et l'extérieur en bleu.

Maintenant supposons que pour n cercles il est toujours possible de trouver un bon coloriage. Prenons $n+1$ cercles et mettons-en un de côté et oublions le pour l'instant. Il en reste n, donc par hypothèse de récurrence on peut trouver un bon coloriage. Maintenant rajoutons le cercle oublié et faisons la manipulation suivante : on change alors la couleur de chaque région à l'intérieur de notre cercle, et on garde la couleur initiale pour les autres régions.
Verifions que le coloriage ainsi obtenu est bon : c'est gagné quand on regarde deux régions séparées par un arc du cercle oublié (grâce au changement qu'on a fait), mais aussi quand on regarde deux régions séparées par un arc d'un autre cercle (par hypothèse de récurrence).

Exercice 21 Montrer que pour tout $n > 5$ il est possible de découper un carré en n carrés plus petits. Montrer qu'il est impossible pour $n = 2$ et $n = 3$.

Solution de l'exercice 19 Soit $\mathcal{P}(n)$ la propriété : "il est possible de découper un carré en n petits carrés". On remarque que si on sait découper un carré en n carré, alors il est facile de découper un carré en $n+3$ carrés : il suffit de découper en 4 un carré du découpage d'origine. Cela regle donc l'heredite, et il suffit de montrer que l'on peut decouper le carre en 6, 7, et 8 petits carres, ce qui est bien possible comme le montrent les figures ci-dessous.



Voyons comment rédiger cette récurrence plus proprement : on initialise en prouvant que le découpage est possible aux rangs 6, 7 et 8. Maintenant, soit n plus grand que 8, supposons que le découpage est possible à tous les rangs compris entre 6 et n. Alors en particulier le découpage est possible au rang $n-2$ (car comme $n \geq 8$, $n-2 \geq 6$), et en découpant en 4 un carré du découpage en $n-2$ carrés, on obtient un découpage en $n+1$ carrés, ce qui clôt la récurrence.

Pour montrer que c'est impossible pour 2 ou 3, utilisons le principe des tiroirs. Supposons que l'on ait un découpage en 3 (ou 2) carrés, alors par principe des tiroirs un de ces 3 (ou 2) carrés comporte 2 des sommets du carré d'origine, contradiction.

Exercice 22 Soit $n \geq 1$ un entier, et soient $a_1, \ldots, a_n$ des entiers naturels non nuls tels que pour tout i, $a_i \leq i$, et tels que leur somme $a_1 + \ldots + a_n$ soit paire. Monter qu'il existe un choix de signes dans l'expression

$$a_1 \pm a_2 \pm \ldots \pm a_n$$

tel que le total fasse 0.

Solution de l'exercice 20 On va raisonner par récurrence double sur n. Pour $n = 1$ il n'y a rien à vérifier. Pour $n = 2$, on a nécessairement $a_1 = a_2 = 1$, d'où le résultat. Supposons que la conclusion soit vraie pour tous les entiers inférieurs ou égaux à un certain n, et considérons des entiers $a_1, \ldots a_{n+1}$ vérifiant les conditions de l'énoncé. Si on a $a_n = a_{n+1}$, la somme $a_1 + \ldots + a_{n-1}$ est paire, et on peut appliquer l'hypothèse de récurrence aux entiers $a_1, \ldots, a_{n-1}$. En combinant le choix de signes obtenu avec $+a_n - a_{n+1}$ on a le résultat. Supposons donc maintenant que $a_n \neq a_{n+1}$, et considérons la suite $a_1, \ldots, a_{n-1}, |a_n - a_{n+1}|$ (la valeur absolue est là afin que le dernier élément de la suite soit un entier naturel non nul). La somme des éléments de cette suite est de même parité que $a_1 + \ldots + a_{n+1}$. De plus, puisque $1 \leq a_n \leq n$ et $1 \leq a_{n+1} \leq n+1$, on a $|a_n - a_{n+1}| \leq n$. Nous pouvons donc appliquer l'hypothèse de récurrence à cette suite, pour obtenir un choix de signes annulant l'expression

$$a_1 \pm a_1 \pm \ldots \pm a_{n-1} \pm |a_n - a_{n-1}|$$

. On adapte le dernier signe selon si $|a_n - a_{n-1}|$ est égal à $a_n - a_{n-1}$ ou à $a_{n+1} - a_n$ pour conclure.

Exercice 23 Dans un polygone convexe à $n \geq 4$ sommets on trace des diagonales de sorte que deux quelconques d'entre elles ne s'intersectent pas (sauf peut-être aux extrémités). Montrer qu'il existe deux sommets non adjacents du polygone dont ne part aucune diagonale.

Solution de l'exercice 21 Nous allons raisonner par récurrence sur le nombre de sommets. Pour $n = 4$ c'est clair. Supposons que ce soit vrai pour tous les polygones à n sommets, et considérons un polygone à $n+1$ sommets. Si aucune diagonale n'a été tracée, on a fini. Sinon, choisissons l'une des diagonales tracées, et appelons A et B ses extrémités. Elle coupe le polygone en deux plus « petits »polygones convexes de strictement moins de $n+1$ sommets, et chaque autre diagonale choisie appartient à seulement un de ces deux « petits »polygones, vu qu'elle ne peut intersecter la diagonale $[AB]$. Si l'un de ces deux « petits »polygones est un triangle, on a déjà un sommet non utilisé et il reste à en trouver un autre. Par hypothèse de récurrence, dans l'autre plus « petit »polygone, il existe deux sommets adjacents non utilisés. Or A et B sont des sommets adjacents de ce « petits »polygone, donc par le principe des tiroirs, un des sommets non utilisé n'est ni A ni B donc c'est gagné. Si aucun des « petits »polygones n'est un triangle, il existe deux sommets non adjacents non utilisés dans chacun d'eux. Comme avant,

A et B sont des sommets adjacents dans chacun de ces deux « petits »polygones. Donc par le principe des tiroirs, dans chaque « petit »polygone, il existe au moins un sommet non utilisé différent de A et B, et donc aussi non utilisé dans le grand polygone et c'est gagné aussi.

Exercice 24

Soit n un entier supérieur ou égal à 2. On place $2n$ points dans l'espace, et on trace n^2+1 segments entre ces points. Montrer que l'on a tracé au moins un triangle.

Solution de l'exercice 22

L'initialisation se fait pour $n=2$: on a 4 points et 5 segments. Or, il existe exactement 6 segments distincts reliant 4 points. Donc on a oublié de tracer exactement un segment, notons-le $[AB]$. Si C et D sont nos deux autres points, les triangles ACD et BCD sont complets.

Maintenant, on fixe $n \in \mathbb{N}, n \geq 2$ et on se place dans une configuration à $2n+2$ points et $(n+1)^2+1$ segments. Soit $[AB]$ l'un de ces segments, et C_i l'un des $2n$ points restants (avec $1 \leq i \leq 2n$). Si, pour un certain i, les segments $[AC_i]$ et $[BC_i]$ sont tous les deux tracés, alors on a tracé le triangle ABC_i et c'est gagné.

Sinon, cela veut dire que, pour chaque valeur de i, au plus l'un des deux segments $[AC_i]$ ou $[BC_i]$ est tracé. Cela donne au plus $2n$ segments reliant A ou B à un des points restants. Si l'on efface alors les points A et B et tous les segments dans lesquels ces deux points interviennent, il nous reste alors au moins $(n+1)^2+1-(2n+1) = n^2+1$ segments et $2n$ points. Dans cette configuration, on a tracé, par hypothèse de récurrence, au moins un triangle, et donc c'est aussi gagné.

2 Groupe B : logique et stratégies de base

1 mardi 18 matin : logique, Nicolas Segarra

L'objectif de ce cours est d'étudier la construction des assertions et les différents types de raisonnements que l'on rencontre en logique.
Par exemple, quelle(s) est (sont) la (les) différence(s) entre les deux propositions suivantes : « si Nathalie boit du café, alors elle est en forme » et « Nathalie boit du café si et seulement si elle est en forme » ? Parmi ces deux propositions, laquelle vous semble la plus vraisemblable ? Maintenant, imaginons que la proposition : « si Nathalie boit du café, alors elle est en forme » est vraie. Qu'en est-il pour la proposition suivante : « si Nathalie n'est pas en forme, alors elle ne boit pas de café » ?
Nous répondrons à ces questions tout au long de ce cours.

Commençons par une énigme intéressante : trois logiciens se rendent dans un bar. Le barman leur demande : « trois bières ? » Le premier logicien répond : « je ne sais pas », le deuxième logicien répond : « je ne sais pas » et le troisième répond : « oui ». La question est ici de savoir pourquoi le troisième logicien répond « oui », pourquoi le troisième logicien est sûr que le barman va servir trois bières.
Voilà la solution : le premier logicien ne peut pas savoir si les deux autres logiciens veulent une bière. Si le premier logicien ne voulait pas de bière, il aurait répondu « non » car alors le barman aurait dû servir au maximum deux bières. Donc, pour montrer aux deux autres logiciens qu'il veut une bière, il répond simplement : « je ne sais pas ».

Pour le deuxième logicien, c'est le même raisonnement : il ne connaît pas la réponse du troisième. Ce dernier par contre a toutes les cartes en main pour donner une réponse précise au barman car il a bien compris que les deux premiers logiciens souhaitaient boire une bière et comme il en veut une, il est en mesure de répondre pour les trois.

Maintenant, échaufons-nous avec quelques exercices !

I) Exercices d'échauffement.

Exercice 1 Alice vagabonde dans la forêt de l'oubli où elle est incapable de se souvenir du jour de la semaine. Elle rencontre le lion et la licorne. Le lion ment les lundi, mardi et mercredi et dit la vérité les autres jours tandis que la licorne ment uniquement les jeudi, vendredi et samedi.
« Hier était un jour où je mentais » dit le lion.
« Hier était un jour où je mentais » dit la licorne.

Question : Quel jour sommes-nous aujourd'hui ?

Solution de l'exercice 1 Le jour cherché ne peut pas être lundi, mardi ni mercredi. Prenons le cas du lundi (les deux autres jours sont éliminés de manière analogue) : si nous sommes lundi, alors la licorne dit la vérité et le lion ment. Donc la licorne a raison en disant que le jour précédent, elle mentait. Mais, le jour précédent le lundi est dimanche et le dimanche, la licorne dit la vérité donc le jour cherché ne peut pas être lundi (ceci contredit le fait que la licorne ait raison !).
On élimine de la même manière le vendredi, le samedi et le dimanche (en analysant ce que le lion dit cette fois) donc nous sommes jeudi. On peut d'ailleurs vérifier la cohérence des phrases du lion et de la licorne le jeudi pour vérifier que notre raisonnement est bon !

Exercice 2 Messieurs Boulanger, Pâtissier et Fleuriste sont trois amis qui ont chacun un (et un seul) métier différent parmi les suivants : boulanger, pâtissier et fleuriste. Mais chacun d'eux n'exerce pas forcément le métier correspondant à son nom. Sur les informations qui suivent, une seule est vraie :
- Monsieur Pâtissier n'est pas boulanger.
- Monsieur Fleuriste n'est pas pâtissier.
- Monsieur Pâtissier est pâtissier.
- Monsieur Fleuriste n'est pas boulanger.

Question : Quels sont les métiers exercés par les 3 amis ?

Solution de l'exercice 2 Etudions les quatre cas :
1er cas : la première proposition est vraie. Alors, Monsieur Pâtissier n'est pas boulanger et les autres propositions sont fausses donc Monsieur Fleuriste est pâtissier (par la proposition 2 qui est fausse) et boulanger (d'après la proposition 4 qui est fausse) : ceci est impossible car chaque protagoniste enseigne un seul métier.

2ème cas : Monsieur Fleuriste n'est pas pâtissier. Donc Monsieur Pâtissier est boulanger (d'après la première proposition qui est fausse) et Monsieur Fleuriste est aussi boulanger (par la 4ème proposition qui est fausse). C'est impossible car les trois protagonistes exercent des

métiers différents.

3ème cas : Monsieur Pâtissier est pâtissier. Donc la proposition 1 est fausse donc Monsieur Pâtissier exerce deux métiers, ce qui est impossible.

4ème cas : Monsieur Fleuriste n'est pas boulanger. Des propositions 1 et 2 (qui sont fausses), on déduit que : Monsieur Pâtissier est boulanger et Monsieur Fleuriste est pâtissier. Le point 3 n'entre pas en contradiction avec ce qui précède. Finalement, Monsieur Boulanger est fleuriste.

Le quatrième cas est le seul cas possible donc les métiers des trois protagonistes sont ceux énoncés dans le dernier cas.

Exercice 3 Messieurs Lenoir, Leblanc et Lerouge sont professeurs de sport dans une grande école. Chacun enseigne trois spécialités parmi : tennis, judo, foot, basket et rugby. Certaines spécialités sont enseignées par deux personnes, jamais par trois personnes.
- Monsieur Lenoir n'enseigne pas le tennis.
- Monsieur Leblanc est le seul à enseigner le judo.
- Monsieur Lerouge enseigne le foot.
- Monsieur Leblanc n'enseigne pas le basket.

Question : Quels professeurs enseignent quelles spécialités ?

Solution de l'exercice 3 A partir des informations de l'énoncé, on peut déjà élaborer le tableau ci-dessous. On écrira « oui » ou « non » dans la case en position (i, j) selon que le personnage i enseigne ou n'enseigne pas la discipline j.

	Tennis	Judo	Foot	Basket	Rugby
Monsieur Lenoir	non	non			
Monsieur Leblanc		oui		non	
Monsieur Lerouge		non	oui		

Comme chaque professeur enseigne trois spécialités, on en déduit que Monsieur Lenoir enseigne le foot, le basket et le rugby.
De plus, une spécialité ne peut pas être enseignée par 3 personnes donc Monsieur Leblanc ne peut pas enseigner le foot (celui-ci étant déjà enseigné par Monsieur Lenoir et par Monsieur Lerouge). Donc Monsieur Leblanc enseigne le tennis et le rugby en plus du judo.
On en déduit alors que Monsieur Lerouge ne peut pas enseigner le rugby donc il enseigne le tennis et le basket en plus du foot. Le tableau ci-dessous résume les spécialités enseignées par chacun des professeurs.

	Tennis	Judo	Foot	Basket	Rugby
Monsieur Lenoir	non	non	oui	oui	oui
Monsieur Leblanc	oui	oui	non	non	oui
Monsieur Lerouge	oui	non	oui	oui	non

II) Définitions et vocabulaire.

Définition. Une assertion (ou proposition) est un énoncé mathématique qui peut être vrai ou faux.

Exemples.

1) $4 \in \mathbb{N}$ est une proposition vraie.
2) $2 < 15$ est une proposition vraie.
3) $0 = 1$ est une proposition fausse.
4) "$1 + 2$" n'est en revanche pas une proposition.

Dans la suite du cours, A et B désigneront deux propositions.

Définition. La négation d'une proposition A est une proposition que l'on peut définir à l'aide de la table de vérité suivante :

A	non A
V	F
F	V

.

Exemple. Soient x un réel et A l'assertion : ($x > 0$). Alors, non A est l'assertion : ($x \leq 0$).

Définition. Pour A et B deux assertions, la disjonction (exprimée par le mot « ou ») de A et B est donnée par la table de vérité suivante :

A	B	A ou B
V	V	V
V	F	V
F	V	V
F	F	F

.

Remarque. L'assertion : (A ou non A) est toujours vraie.

Définition. La conjonction (exprimée par le mot « et ») de deux assertions A et B est donnée par la table de vérité suivante :

A	B	A et B
V	V	V
V	F	F
F	V	F
F	F	F

.

Remarque. L'assertion : (A et non A) est toujours fausse.

Définition. On définit l'implication entre deux propositions A et B (« A implique B » que l'on note $A \Rightarrow B$) à l'aide de la table de vérité suivante :

A	B	$A \Rightarrow B$
V	V	V
V	F	F
F	V	V
F	F	V

.

Remarques. 1) La troisième ligne de la table de vérité ci-dessus peut paraître peu naturelle. On peut l'expliquer en se convainquant que $A \Rightarrow B$ revient à dire : non A ou B.
On voit bien alors que si A est fausse et B est vraie alors non A ou B donne vrai ou vrai donc vrai !

2) Lorsque $A \Rightarrow B$ est vraie, on peut dire :

- A implique B.
- Si A alors B.
- Pour B, il suffit A.
- Pour A, il faut B.
- A est une condition suffisante pour B.
- B est une condition nécessaire pour A.

Exemples. Voici des exemples d'implications vraies.

1) $ABCD$ est un carré $\Rightarrow$ $ABCD$ est un rectangle.<
2) $x \in \mathbb{N} \Rightarrow x \in \mathbb{Z}$.
3) $1 + 1 = 2 \Rightarrow \sqrt{2}$ est irrationnel.
Ce dernier exemple peut sembler étrange, car on se demande quel est le rapport entre les deux assertions. Mais il n'est en fait pas nécessaire qu'il existe un rapport ou une causalité, puisqu'il suffit que les deux propositions A et B soient vraies (ou toutes les deux fausses) pour que l'implication $A \Rightarrow B$ soit vraie.

Définition. Soient A et B deux propositions. On dit que A est équivalente à B (ou que A équivaut à B) et on note $A \Leftrightarrow B$, si A implique B et B implique A.

Remarques. 1) Voici la table de vérité pour $A \Leftrightarrow B$:

A	B	$A \Rightarrow B$	$B \Rightarrow A$	$A \Leftrightarrow B$
V	V	V	V	V
V	F	F	V	F
F	V	V	F	F
F	F	V	V	V

.

On remarque que $A \Leftrightarrow B$ est vraie lorsque les deux propositions A et B sont toutes les deux vraies ou toutes les deux fausses. Autrement dit, lorsqu'elles ont la même valeur logique.

2) Lorsque $A \Leftrightarrow B$ est vraie, on peut dire :
- A si et seulement si B.
- Pour A, il faut et il suffit B.
- A est une condition nécessaire et suffisante pour B.

Exemples. Voici des exemples d'équivalences vraies.

1) $\text{non}(\text{non}\, A) \Leftrightarrow A$.
2) Soit x un nombre réel. On a $3x + 3 = 6 \Leftrightarrow x = 1$.

Définitions avec des quantificateurs. Soient E un ensemble et $A(x)$ une assertion dépendant de $x \in E$.

1) On définit l'assertion $(\forall\, x \in E,\, A(x))$ comme étant vraie si et seulement si $A(x)$ est vraie pour tout élément x de E.
2) On définit l'assertion $(\exists\, x \in E,\, (A(x))$ comme étant vraie si et seulement s'il existe au moins un élément x de E pour lequel $A(x)$ est vraie.

Exemples. Voici deux exemples d'assertions vraies, définies à l'aide de quantificateurs.

1) $(\forall\, x \in \mathbb{N},\, x \geq 0)$; 2) $(\exists\, x \in \mathbb{R},\, x^2 = 5)$.

Remarques. 1) On peut se convaincre que :
a) $\text{non}(\forall\, x \in E,\, A(x)) \Leftrightarrow \exists\, x \in E,\, \text{non}\, A(x)$.
b) $\text{non}(\exists\, x \in E,\, A(x)) \Leftrightarrow \forall\, x \in E,\, \text{non}\, A(x)$.

2) Lorsque plusieurs quantificateurs sont employés, on ne peut les permuter et obtenir une assertion équivalente que lorsqu'ils sont du même type. En général, avec de gros guillemets, $\forall\exists \not\Leftrightarrow \exists\forall$.

Exercice 4 Soient A et B deux assertions. Montrer les équivalences suivantes :

1) $\text{non}(A$ **et** $B) \Leftrightarrow (\text{non}\, A)$ **ou** $(\text{non}\, B)$.
2) $\text{non}(A$ **ou** $B) \Leftrightarrow (\text{non}\, A)$ **et** $(\text{non}\, B)$.
3) $\text{non}(A \Rightarrow B) \Leftrightarrow A$ **et** $(\text{non}\, B)$.

Solution de l'exercice 4 On démontre ces équivalences à l'aide de tables de vérité.

1)

A	B	non A	non B	A et B	non$(A$ et $B)$	$(\text{non}\, A)$ ou $(\text{non}\, B)$
V	V	F	F	V	F	F
V	F	F	V	F	V	V
F	V	V	F	F	V	V
F	F	V	V	F	V	V

.

2)

A	B	non A	non B	A ou B	non$(A$ ou $B)$	$(\text{non}\, A)$ et $(\text{non}\, B)$
V	V	F	F	V	F	F
V	F	F	V	V	F	F
F	V	V	F	V	F	F
F	F	V	V	F	V	V

.

3)

A	B	non B	$A \Rightarrow B$	non$(A \Rightarrow B)$	A et $(\text{non}\, B)$
V	V	F	V	F	F
V	F	V	F	V	V
F	V	F	V	F	F
F	F	V	V	F	F

.

Exercice 5 Les assertions suivantes sont-elles vraies ?

1. $\forall\, x \in \mathbb{R},\, x^2 + 4x + 3 \neq 0$.
2. $\exists\, x \in \mathbb{N},\, x \in \mathbb{D}$.
3. $\forall\, x \in \mathbb{R},\, x > 4 \Rightarrow x \geq 4,1$.
4. $\exists\, n \in \mathbb{Z},\, \forall\, x \in \mathbb{R},\, n < x \leq n + 1$.

Solution de l'exercice 5

1. Pour montrer que cette assertion est fausse, on va montrer que sa négation est vraie.
On a : $\text{non}(\forall\, x \in \mathbb{R},\, x^2+4x+3 \neq 0) \Leftrightarrow \exists\, x \in \mathbb{R},\, x^2+4x+3=0$. Cette dernière proposition est vraie car $(-1)^2+4\times(-1)+3=0$.
Ainsi, la proposition : $(\forall\, x \in \mathbb{R},\, x^2+4x+3 \neq 0)$ est fausse.

2. Cette assertion est vraie. En effet, $0 \in \mathbb{N}$ et $0 \in \mathbb{D}$.

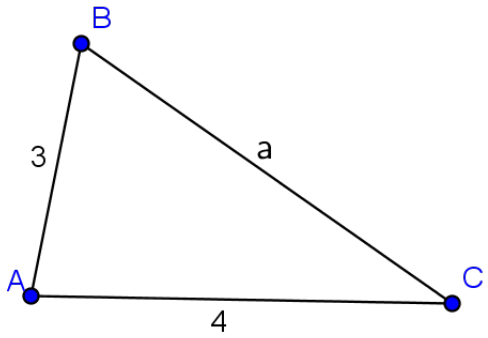
3. Montrons que cette assertion est fausse.
On a : $\text{non}(\forall\, x \in \mathbb{R},\, x>4 \Rightarrow x \geq 4,1) \Leftrightarrow \exists\, x \in \mathbb{R},\, x>4$ et $x<4,1$.
Cette dernière assertion est vraie car $x=4,05$ convient (on a bien : $4<4,05<4,1$).

4. Montrons que cette assertion est fausse.
$\text{non}(\exists\, n \in \mathbb{Z}, \forall\, x \in \mathbb{R},\, n<x\leq n+1) \Leftrightarrow \forall\, n \in \mathbb{Z}, \exists\, x \in \mathbb{R}, \text{non}(x>n$ et $x \leq n+1)$.
$\text{non}(\exists\, n \in \mathbb{Z}, \forall\, x \in \mathbb{R},\, n<x\leq n+1) \Leftrightarrow \forall\, n \in \mathbb{Z}, \exists\, x \in \mathbb{R}, x \leq n$ ou $x>n+1$.
Pour cette dernière proposition, $x=n+2>n+1$ convient et ceci conclut la démonstration.

III) Différents types de raisonnements.

Démontrer une implication. En général, pour prouver que $A \Rightarrow B$, on suppose que A est vraie et on essaie de démontrer que B est alors vraie.

Exemple. Montrons que (ABC est rectangle en A) $\Rightarrow a=5$.



Supposons que ABC est rectangle en A. D'après le théorème de Pythagore, on a : $a^2=3^2+4^2=25$. Donc $a=-5$ ou $a=5$. Mais a est un nombre positif car c'est une longueur donc $a=5$.

Démontrer une équivalence. On peut dans des cas très simples procéder par équivalences successives. Mais en général, il est préférable de raisonner par double implication : on montre une implication puis sa réciproque.

Raisonnement par contraposée. Pour prouver une implication non démontrable directement : $(A \Rightarrow B)$, on peut raisonner par contraposée, c'est-à-dire montrer que : $(\text{non}\, B \Rightarrow \text{non}\, A)$. La table de vérité suivante permet de démontrer que $(A \Rightarrow B) \Leftrightarrow (\text{non}\, B \Rightarrow \text{non}\, A)$:

A	B	non A	non B	$A \Rightarrow B$	non $B \Rightarrow$ non A
V	V	F	F	V	V
V	F	F	V	F	F
F	V	V	F	V	V
F	F	V	V	V	V

.

L'implication : $(\text{non } B \Rightarrow \text{non } A)$ est appelée : implication contraposée de l'implication $(A \Rightarrow B)$.

Raisonnement par l'absurde. Pour démontrer qu'une assertion A est vraie, on peut raisonner par l'absurde. On suppose que A est fausse et on tente d'aboutir à une contradiction. On conclut alors qu'il était absurde de supposer A fausse donc que A est vraie.

Exemple. Soit $n \in \mathbb{Z}$. Montrons que n ne peut pas être pair et impair à la fois.

On raisonne par l'absurde. On suppose alors que n est pair et impair à la fois. Alors il existe deux entiers k et k' tels que $n = 2k = 2k' + 1$. Donc on a : $2(k - k') = 1$ donc $k - k' = \dfrac{1}{2}$. Comme k et k' sont des entiers, $k - k'$ est un entier mais $\dfrac{1}{2}$ n'est pas un entier. Donc on obtient une contradiction. Ainsi, n ne peut pas être pair et impair à la fois.

Raisonnement par disjonction de cas. Parfois, il est pertinent d'étudier tous les cas possibles pour démontrer un résultat. Ce raisonnement est le raisonnement par disjonction de cas. Il a été mis en oeuvre dans les exercices 1 et 2.

Preuve de $(\forall\, x \in E,\, A(x))$. On procède de la manière suivante. On se donne un x quelconque de E et on démontre que $A(x)$ est vraie. L'élément x est quelconque et on n'a imposé aucune condition sur cet élément donc on a démontré que $A(x)$ est vraie pour tout $x \in E$.

Exemple. Montrons que $\forall\, x \in \mathbb{R}$, $(x-2)^2 + (x+3)^2 - 2x \geq 13$.

Soit $x \in \mathbb{R}$. On écrit : $(x-2)^2 + (x+3)^2 - 2x = x^2 - 4x + 4 + x^2 + 6x + 9 - 2x = 2x^2 + 13$ (on se souvient des identités remarquables !).
Comme, $2x^2 \geq 0$, $2x^2 + 13 \geq 13$ donc on a bien $\forall\, x \in \mathbb{R}$, $(x-2)^2 + (x+3)^2 - 2x \geq 13$.
Preuve de $(\exists\, x \in E,\, A(x))$. Pour prouver ce genre de proposition, on peut avoir recours à un théorème d'existence (un théorème assurant l'existence d'au moins un x tel que $A(x)$ soit vraie) ou exhiber un x pour lequel $A(x)$ est vraie.

Exemple. Montrons qu'il existe un entier $p \geq 2$ tel que $2p^2 + 1$ soit premier.

Pour $p = 3$, on a : $2p^2 + 1 = 2 \times 9 + 1 = 19$ et 19 est premier. Donc on a bien montré l'existence d'un entier $p \geq 2$ tel que $2p^2 + 1$ soit premier.

Exercice 6 On suspecte Elise, Fred et Gaétan d'avoir commis un vol. Nous avons à leur sujet les informations suivantes :
- si Gaétan n'est pas coupable alors Fred est coupable.
- Si Elise n'est pas coupable alors Gaétan est coupable.
- Si Gaétan est coupable alors Elise l'est aussi.

- Si Elise est coupable alors Fred ne l'est pas.

Question : Quel est ou quels sont le ou les coupable(s) ?

Solution de l'exercice 6

Les 4 propositions données ci-dessus doivent être vraies simultanément. On va alors montrer à l'aide des propositions 2 et 3 qu'Elise est nécessairement coupable. Raisonnons par l'absurde : supposons qu'Elise n'est pas coupable. Alors par la proposition 2, Gaétan est coupable. Donc par la proposition 3, Elise est coupable. Ceci contredit l'hypothèse de départ. Donc Elise est coupable.
Comme Elise est coupable, Fred n'est pas coupable d'après la proposition 4. On en déduit par la contraposée de la première implication que Gaétan est coupable.
Conclusion : les coupables de ce vol sont Elise et Gaétan.

IV) Exercices supplémentaires.

Exercice 7
1) Soit $p \in \mathbb{Z}$. Montrer que si p^2 est pair alors p est pair.
2) Montrer que $\sqrt{2}$ est irrationnel.

Solution de l'exercice 7

1) Montrons cette proposition en raisonnant par contraposée : supposons que p est impair. Alors, il existe un entier k tel que $p = 2k+1$. On a : $p^2 = (2k+1)^2 = 4k^2+4k+1 = 2(2k^2+2k)+1$ et $2k^2 + 2k \in \mathbb{Z}$ donc p^2 est impair. On a montré que si p est impair alors p^2 est impair donc on a le résultat par contraposée.

2) Raisonnons par l'absurde : supposons alors que $\sqrt{2}$ est un nombre rationnel. Alors, il existe deux entiers a et b premiers entre eux et $b \neq 0$ tels que : $\sqrt{2} = \dfrac{a}{b}$. On a alors en élevant au carré : $2 = \dfrac{a^2}{b^2}$ donc $a^2 = 2b^2$ d'où a^2 est pair et ainsi a est pair (par la proposition démontrée précédemment).
L'entier a est pair donc il existe un entier k tel que : $a = 2k$. On a alors : $a^2 = 4k^2 = 2b^2$ soit : $b^2 = 2k^2$. Donc b^2 est pair ainsi b est pair.
Mais il est impossible que les entiers a et b soient tous les deux pairs car ceci contredit le fait qu'ils soient premiers entre eux !
Donc $\sqrt{2}$ est un nombre irrationnel.

Exercice 8 Démontrer les propositions suivantes :

1. $\forall\, x \in \mathbb{R}$, $x^2 - 8x + 17 > 0$.
2. $\forall\, x \in \mathbb{R}$, $(x+2)^2 - (x-3)^2 \geq 0 \Rightarrow x \geq \dfrac{1}{2}$.
3. $\exists\, n \in \mathbb{N}$, $11 | 6n^2 - 7$.

Solution de l'exercice 8 1. On a : $x^2-8x+17 = (x-4)^2+1$. Comme $(x-4)^2 \geq 0$, $(x-4)^2+1 \geq 1$ donc pour tout réel x, $x^2 - 8x + 17 > 0$.
2. On suppose que $(x+2)^2 - (x-3)^2 \geq 0$. On écrit : $(x+2)^2 - (x-3)^2 = 5(2x-1)$ (troisième

identité remarquable).

Ainsi, on a : $5(2x-1) \geq 0$ donc $2x-1 \geq 0$ (car $5>0$). Donc $x \geq \frac{1}{2}$.

3. Pour $n=5$, $6n^2-7 = 6\times 25 - 7 = 141 = 11\times 13$. Donc on a bien montré qu'il existe au moins un entier naturel n tel que 11 divise $6n^2-7$.

2 mardi 18 après-midi : Cécile Gachet

Introduction. Ce cours donne des exercices d'applications du principe de récurrence simple, puis en présente quelques variantes : récurrence double ou plus généralement d'ordre $k \in \mathbb{N}^*$, récurrence forte et récurrence descendante. Pour finir, le principe voisin de la descente infinie est rapidement exposé.

Commençons donc par quelques exercices, pour vérifier que tout va bien avec la récurrence simple :

Exercice 1 Soit n un entier naturel. Donner une formule explicite de la somme $0+1+2+...+n$.

Solution de l'exercice 1 L'initialisation pour $n=0$ est déjà faite (voir le choix judicieux de a, b, c).

Supposons maintenant qu'il existe un entier naturel n tel que $u_n = \frac{n(n+1)}{2}$. Alors :

$$u_{n+1} = u_n + (n+1) = \frac{n(n+1)}{2} + n + 1 = \frac{(n+1)(n+2)}{2}.$$

donc $\mathcal{P}_{n+1}$ est vraie, ce qui conclut par principe de récurrence.

Exercice 2 Soit $n \geq 1$ un entier. On trace n cercles dans le plan. Montrer qu'on peut colorier chaque région du plan ainsi délimitée avec exactement deux couleurs (bleu et rouge en l'occurrence) de manière à ce que deux régions séparés par un arc de cercle soient toujours de couleur différente.

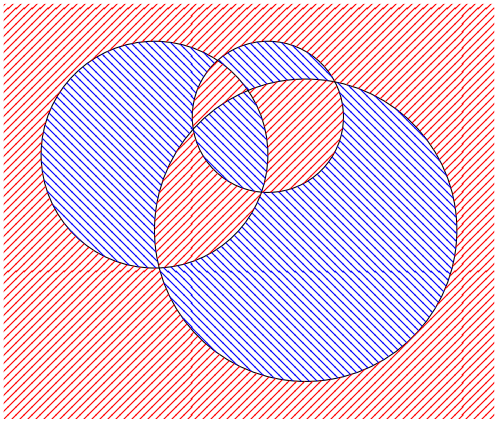


FIGURE.– Exemple de coloriage possible pour $n=3$ cercles

Solution de l'exercice 2 Si l'on n'a qu'un seul cercle, on colorie l'intérieur d'une couleur arbitraire, l'extérieur de l'autre couleur et c'est gagné.

Si on peut toujours colorier n cercles comme voulu, qu'en est-il de $n+1$ cercles ? Pour colorier les régions comme voulu, on oublie tout d'abord un cercle : il en reste alors n, et on

peut colorier les régions correspondantes comme voulu, par hypothèse de récurrence. Puis on rajoute le cercle oublié. Il coupe en deux certaines régions coloriées : on change alors la couleur de chaque région coloriée à l'intérieur de notre cercle, et on garde la couleur initiale pour les autres régions.

Alors, on a bien colorié toutes nos régions comme voulu ! En effet, c'est gagné quand on regarde deux régions séparées par un arc du cercle oublié (grâce au changement qu'on a fait), mais aussi quand on regarde deux régions séparées par un arc d'un autre cercle (par hypothèse de récurrence).

Subtilités d'initialisation. Lorsqu'on montre une propriété ($\mathcal{P}_n$ pour tout $n \in \mathbb{N}$ par récurrence simple, on initialise généralement à $n = 0$. Toutefois, l'hérédité : $\mathcal{P}_n \Longrightarrow \mathcal{P}_{n+1}$ doit alors être montrée pour tout $n \geq 0$.

Ainsi, si l'argument de l'hérédité ne « s'enclenche »qu'à partir d'un certain entier N, on doit initialiser la récurrence à $n = N$, et vérifier à la main que $\mathcal{P}_n$ est aussi vraie pour les rangs que la récurrence ne couvre pas, autrement dit pour $n \in [\![0, N-1]\!]$.

De même, si on ne veut montrer une propriété qu'à partir d'un certain rang N, on initialise à $n = N$ (et on n'a pas besoin de vérifier la propriété aux rangs précédents, puisque rien n'est demandé pour ces rangs...) !

Exercice 3 Montrons que toute boîte de crayons de couleur ne contient que des crayons de la même couleur.

On fait l'initialisation pour $n = 1$: une boîte contenant un seul crayon de couleur ne contint forcément que des crayons de la même couleur.

Pour l'hérédité, supposons qu'il existe un entier n tel que toute boîte contenant n crayons ne contienne que des crayons de la même couleur.

Prenons alors une boîte de $n+1$ crayons. Les n premiers crayons de cette boîte sont tous de la même couleur, et les n derniers crayons sont aussi tous de la même couleur. Donc tous les crayons de notre boîte sont de la même couleur.

Par principe de récurrence, on peut bien conclure que, pour tout entier $n \geq 1$, n'importe quelle boîte contenant n crayons ne contient en fait que des crayons de la même couleur ; autrement dit, n'importe quelle boîte de crayons de couleur ne contient que des crayons de la même couleur.

Maintenant, trouvez l'erreur !

Solution de l'exercice 3 La propriété à montrer est évidemment fausse pour $n = 2$, et dès lors l'hérédité ne peut pas se propager.

Mais pourquoi ce cas $n = 2$ n'est-il pas écarté par la « preuve » ? En fait, l'hérédité suppose implicitement qu'il y a au moins un crayon qui soit dans les n premiers et dans les n derniers. Or, si $n = 1$, dans une boîte de 2 crayons de couleurs, ce n'est pas le cas !

Le principe de récurrence admet de nombreuses variantes.

Récurrence double, récurrence d'ordre k. Pour montrer qu'une propriété $\mathcal{P}_n$ est vraie pour tout $n \in \mathbb{N}$, on ne peut pas toujours déduire $\mathcal{P}_n$ de $\mathcal{P}_{n+1}$ directement. En particulier, on peut avoir besoin de supposer propriété vraie sur plusieurs rangs dans l'hérédité...On recourt alors à une récurrence double, ou d'ordre 2, si l'on montre la propriété à un rang donné en

la supposant vraie aux 2 rangs précédents, voire une récurrence d'ordre k (remplacer 2 par k dans l'explication précédente).

Attention, il faut initialiser en conséquence !

Une récurrence d'ordre k se rédige donc de la façon suivante :

- ▷ Initialisation : on vérifie, pour tout $n \in [\![0, k-1]\!]$, que la propriété $\mathcal{P}_n$ est vraie.
- ▷ Hérédité : on suppose qu'il existe un entier naturel $n \geq k$ tel que les propriétés $\mathcal{P}_{n-k}$, $\mathcal{P}_{n-k+1}$, …, $\mathcal{P}_{n-1}$ sont vraies. On montre qu'alors la propriété $\mathcal{P}_n$ est aussi vraie.

Exercice 4 Soit $(F_n)_{n\in\mathbb{N}}$ la suite de Fibonacci définie par $F_0 = 0, F_1 = 1$ et, pour tout $n \in \mathbb{N}$, $F_{n+2} = F_{n+1} + F_n$.

Soient $\varphi = \frac{1+\sqrt{5}}{2}, \psi = \frac{1-\sqrt{5}}{2}$. On peut remarquer que $\varphi^2 = \varphi + 1$ et $\psi^2 = \psi + 1$.

Montrer que, pour tout $n \in \mathbb{N}$, $F_n = \frac{\varphi^n - \psi^n}{\sqrt{5}}$.

Solution de l'exercice 4 La suite de Fibonacci est définie par une relation de récurrence d'ordre 2 : pour en calculer un terme, on a besoin des deux termes précédents.

On s'engage donc dans une récurrence double. Pour l'hérédité, en supposant la formule exacte pour un certain n et $n+1$, on obtient, en sommant,

$$\begin{aligned} F_{n+2} &= F_{n+1} + F_n \\ &= \frac{\varphi^{n+1} - \psi^{n+1}}{\sqrt{5}} + \frac{\varphi^n - \psi^n}{\sqrt{5}} \\ &= \frac{\varphi^n(\varphi+1) - \psi^n(\psi+1)}{\sqrt{5}} \\ &= \frac{\varphi^{n+2} - \psi^{n+2}}{\sqrt{5}} \end{aligned}$$

Il ne reste plus qu'à initialiser pour $n = 0$ et $n = 1$ et c'est gagné !

Comme la suite de Fibonacci est une suite récurrente d'ordre 2 (on déduit un terme des deux précédents), la récurrence double est une méthode adaptée pour l'étudier.

Plus généralement, lorsqu'une suite (u_n) est définie par la donnée de ses k premiers termes et une relation permettant de déduire un terme des k termes précédents, il faut souvent penser à faire une récurrence d'ordre k pour étudier la suite.

Certains exercices de dénombrement ramènent des phénomènes à des suites récurrentes déjà connues.

Ainsi, une façon expéditive de les aborder consiste à montrer une relation de récurrence sur ce qu'ils énumèrent. En faisant les petits cas, on comprend ensuite l'initialisation, et on montre facilement par une récurrence d'ordre adapté que ce qu'on compte coïncide avec la suite voulue pour tout entier $n \in \mathbb{N}$.

Exercice 5 Pour tout $n \in \mathbb{N}$, on note u_n le nombre de manières de paver un quadrillage de taille $2 \times n$ à l'aide de dominos de taille 2×1. Donner une formule pour u_n.

Solution de l'exercice 5 Pour les petites valeurs, on calcule :

n	0	1	2	3	4	5	6	7	8	9	10
u_n	1	1	2	3	5	18	13	21	34	55	89

Cela nous rappelle la suite de Fibonacci…On conjecture même que $u_n = F_{n+1}$, pour tout $n \in \mathbb{N}$. Reste à trouver une relation de récurrence sur u_n : si c'est la même relation de récurrence que la suite de Fibonacci, c'est gagné ! (on montre alors par récurrence double que les deux suites sont égales, grâce à leur relation de récurrence commune)

On considère le domino qui recouvre le coin supérieur gauche de la grille : soit il est horizontal, soit il est vertical.

- s'il est vertical, alors il pave la première colonne du quadrillage ; donc paver un tel quadrillage de taille $2 \times n$ revient à paver un quadrillage normal de taille $2 \times (n-1)$: cela fait u_{n-1} possibilités.
- s'il est horizontal, alors le coin inférieur gauche de la grille doit également être pavé par un domino horizontal ; ainsi, les deux premières colonnes du quadrillage sont pavées, et paver un tel quadrillage de taille $2 \times n$ revient donc à paver un quadrillage normal de taille $2 \times (n-2)$: cela fait u_{n-2} possibilités.

On a donc $u_{n-1} + u_{n-2}$ possibilités pour paver un quadrillage de taille $2 \times n$, c'est-à-dire que $u_n = u_{n-1} + u_{n-2}$ pour tout $n \geq 2$: c'est la fameuse relation de récurrence qu'on cherchait !

Récurrence forte. Pour montrer qu'une propriété $\mathcal{P}_n$ est vraie pour tout n, lorsqu'on ne sait pas déduire systématiquement la propriété à rang donné d'un certain nombre k de propriétés précédentes (fixé à l'avance comme ordre d'une récurrence hypothétique), on peut aussi procéder ainsi :

- ▷ Initialisation : on vérifie que la propriété $\mathcal{P}_0$ est vraie.
- ▷ Hérédité : on suppose qu'il existe un entier naturel n tel que les propriétés $\mathcal{P}_0, \mathcal{P}_1, \ldots, \mathcal{P}_n$ sont toutes vraies. On montre qu'alors la propriété $\mathcal{P}_{n+1}$ est aussi vraie.

Introduisons l'exercice suivant : dans la vie de tous les jours, on écrit les nombres en base 10 : on utilise les chiffres de 0 à 9, et la place du chiffre correspond à la puissance de 10 par lequel il faut le multiplier pour savoir en quoi il contribue au nombre. Par exemple, 42 en base dix vaut $4 \times 10^1 + 2 \times 1$. Dans cette base, deux nombres s'écrivant différemment sont forcément différents : on dit qu'il y a unicité de la décomposition dans cette base.

De même, tout nombre s'écrit de façon unique en base 2 : par exemple, comme $42 = 1 \times 2^5 + 0 \times 2^4 + 1 \times 2^3 + 0 \times 2^2 + 1 \times 2 + 0 \times 1$, 42 en base 10 vaut 101010 en base 2.

On définit de même la base de Fibonacci, où les chiffres autorisés sont 0 et 1, et où la place d'un chiffre correspond au rang, dans la suite de Fibonacci, du nombre de Fibonacci par lequel on multiplie. Dans cette base, on n'a pas l'unicité de décomposition : par exemple, 011 et 100 en base de Fibonacci valent tous les deux 3 en base 10. Plus généralement, on peut toujours remplacer deux chiffres 1 consécutifs par deux 0 en ajoutant 1 dans la colonne suivante (car $F_{n+2} = F_{n+1} + F_n$).

On dit qu'une décomposition en base de Fibonacci est valide si elle ne contient pas deux 1 consécutifs.

Exercice 6

Théorème de Zeckendorf. Tout entier $N \in \mathbb{N}$ possède une unique décomposition valide en base Fibonacci.

Solution de l'exercice 6 L'entier 0 admet bien-sûr une unique décomposition valide en base de Fibonacci.

Maintenant, soit $N \in \mathbb{N}^*$. Soit $n \geq 2$ l'unique entier tel que $F_n \leq N < F_{n+1}$. En notant $N = F_n + (N - F_n)$, on « commence »à décomposer N, en mettant un 1 dans la colonne correspondant à F_n. C'est un bon début ! En effet, $N - F_n$ est strictement inférieur à N : quitte à faire une récurrence forte, on peut supposer qu'il existe une décomposition valide de $N - F_n$ dans la base de Fibonacci.

Or $0 \leq N - F_n < F_{n+1} - F_n = F_{n-1}$: en prenant la décomposition de $N - F_n$ et en ajoutant 10 devant, on trouve bien une décomposition valide de N !

Pour l'unicité, ça marche aussi par récurrence forte : en effet, si on ne met pas un 1 pour F_n dans la décomposition de N, on obtiendra, quoiqu'on fasse, quelque chose de trop petit, car $F_{n-1} + F_{n-3} + \ldots < F_n$ (il faut ajouter 1 au membre de gauche pour obtenir le membre de droite). Donc on commence par un 1, ensuite il y a forcément un 0 (voir la première moitié de la preuve), et ensuite la décomposition de $N - F_n$ est unique par hypothèse de récurrence, donc c'est gagné !

Récurrence descendante. On préfère ce type de récurrence pour montrer une propriété sur un ensemble fini d'entiers, en particulier lorsque celle-ci est difficile à initialiser en 0. En effet, comme son nom l'indique, cette méthode permet, partant d'une propriété vraie à un certain rang N, de redescendre aux propriétés de rang inférieur.

Pour montrer qu'une propriété $\mathcal{P}_n$ est vraie pour tout n tel que $0 \leq n \leq N$ (où $N \in \mathbb{N}$ est un rang fixé) :

- ▷ Initialisation : on vérifie que la propriété $\mathcal{P}_N$ est vraie.
- ▷ Hérédité : on suppose qu'il existe un entier naturel $1 \leq n \leq N$ tel que la propriété $\mathcal{P}_n$ est vraie. On montre qu'alors la propriété $\mathcal{P}_{n-1}$ est aussi vraie.

Exercice 7 Montrer que pour tout entier $N \geq 2$,

$$\sqrt{2\sqrt{3\sqrt{4\sqrt{\ldots\sqrt{(N-1)\sqrt{N}}}}}} < 3.$$

Indication. *Montrer, par récurrence sur m, que pour tout $N \geq 2$ et pour tout m tel que $2 \geq m \geq N$,*

$$\sqrt{m\sqrt{(m+1)\sqrt{\ldots\sqrt{N}}}} < m + 1.$$

Solution de l'exercice 7 L'indication propose certes de montrer un résultat plus général que l'exercice en lui-même, mais cette version généralisée a un avantage : elle permet de jouer assez finement sur l'entier m.

Soit un entier N fixé. On note, pour tout entier m tel que $2 \leq m \leq N$, $\mathcal{P}_m$ la propriété : « $\sqrt{m\sqrt{(m+1)\sqrt{\ldots\sqrt{N}}}} < m + 1$ ».

Une initialisation en $m = 2$ n'est pas envisageable (c'est la propriété qu'on veut avoir à la fin), nous allons donc procéder par récurrence descendante.

Pour $m = N$, il s'agit de prouver que $\sqrt{N} < N + 1$. Or, $(N + 1)^2 = N^2 + 2N + 1 > N$, d'où l'initialisation.

Maintenant, supposons qu'il existe un entier m tel que $3 \leq m \leq N$ et que :

$$\sqrt{m\sqrt{(m+1)\sqrt{...\sqrt{N}}}} < m+1.$$

Il s'agit de montrer que $\mathcal{P}_{m-1}$ est vraie, soit :

$$\sqrt{(m-1)\sqrt{m\sqrt{(m+1)\sqrt{...\sqrt{N}}}}} < m.$$

Comme $m-1 > 0$, l'hypothèse de récurrence donne :

$$(m-1)\sqrt{m\sqrt{(m+1)\sqrt{...\sqrt{N}}}} < (m-1)(m+1) = m^2 - 1 < m^2,$$

d'où l'on déduit :

$$\sqrt{(m-1)\sqrt{m\sqrt{(m+1)\sqrt{...\sqrt{N}}}}} < \sqrt{m^2-1} < \sqrt{m^2} = m$$

et donc c'est gagné pour l'hérédité !

Ainsi, par principe de récurrence, notre propriété est vraie pour tout N et pour tout $m \in [\![2, N]\!]$. A fortiori, elle est vraie pour tout N dans le cas où $m = 2$.

Principe de la descente infinie. L'idée de cette méthode, dérivée de (et même en fait équivalente à) la récurrence, est la suivante : toute suite d'entiers naturels strictement décroissante est finie.

Ainsi, pour montrer qu'un problème dépendant d'entiers naturels n'admet pas de solution, on peut aussi, en supposant qu'il admette un certain entier positif n pour solution, construire un entier naturel n_1 strictement inférieur à n qui soit aussi solution.

Dès lors, en itérant cette construction, on obtient une suite infinie strictement décroissante d'entiers naturels, ce qui est absurde !

La descente infinie est une méthode très utile en arithmétique (couplée notamment avec la paramétrisation des triplets pythagoriciens) et peut également servir en combinatoire.

Exercice 8 Montrer que $\sqrt{2}$ est irrationnel.

Solution de l'exercice 8 On procède par descente infinie : soient $p, q \in (\mathbb{N}^*)^2$ tels que $\sqrt{2} = \frac{p}{q}$, autrement dit $2q^2 = p^2$. Donc 2 divise p^2, donc 2 divise p (car le produit de deux nombres impairs est impair, donc si p était impair, on aurait p^2 impair, contradiction !).

On peut poser $p = 2q_1$ avec $q_1 \in \mathbb{N}^*$ et alors $2q_1^2 = q^2$, d'où $q_1 < q$. En posant $p_1 = q$, on obtient donc un nouveau couple d'entiers naturels (p_1, q_1) solution de la même équation que (p, q), et $q_1 < q$.

Ainsi, par descente infinie, cette équation n'admet aucune solution. Donc $\sqrt{2}$ est irrationnel.

3 mercredi 19 matin : Victor Quach

Principe des tiroirs

Le principe des objets peut s'énoncer de la manière suivante :

Si l'on range $n+1$ chaussettes dans n tiroirs, alors au moins un tiroir contient au moins deux chaussettes.

Plus généralement, on a la version suivante :

Si l'on range k chaussettes dans n tiroirs, alors au moins un tiroir contient au moins $\lceil \frac{k}{n} \rceil$ chaussettes.

La démonstration se fait très simplement en raisonnant par l'absurde.

Exercice 1 Paris est une ville qui contient 2 300 000 habitants. Il y a au plus 500 000 cheveux sur la tête d'un parisien. Montrer qu'il existe au moins 5 parisiens qui ont le même nombre de cheveux.

Solution de l'exercice 1 Pour tiroirs, on choisit le nombre de cheveux, pour chaussettes, on choisit les parisiens. D'après le principe des tiroirs, il y a au moins $\lceil \frac{2300000}{500} \rceil$ parisiens qui ont le même nombre de cheveux.

Exercice 2 Lors d'une soirée, chaque invité serre la main d'un certain nombre d'autres invités. Montrer qu'il existe deux personnes qui ont serré le même nombre de mains.

Solution de l'exercice 2 On appelle n le nombre d'invités. On choisit pour chaussettes les invités et pour tiroirs le nombre de mains serrées par chaque personne. Il semble que cela n'aboutit pas car le nombre de mains serrés par une personne peut aller de 0 à $n-1$, soit n tiroirs. Toutefois, les tiroirs 0 et $n-1$ ne peuvent pas être non vides tous les deux (si une personne serre la main à tout le monde, chacun a serré la main à au moins une personne). Cela permet de conclure.

Exercice 3 L'ensemble des points du plan est colorié en jaune ou en rouge. Montrer que pour tout réel strictement positif il existe une couleur telle qu'on puisse trouver deux points de cette couleur distants de x.

Solution de l'exercice 3 Soit $x \in \mathbb{R}$. Dans un triangle équilatéral de côté x, on peut appliquer le principe des tiroirs aux sommets, dont deux sont donc de la même couleur.

Exercice 4 Soit n un entier. Montrer que parmi $n+1$ entiers quelconques $a_0, a_1, \dots a_n$, on peut en trouver deux a_i et a_j ($i \neq j$) tels que $a_i - a_j$ soit divisible par n.

Solution de l'exercice 4 Pour tiroirs, on utilise le reste du nombre dans la division euclidienne par n. Puisqu'il y a $n+1$ nombres, deux d'entre eux ont le même reste. Cela conclut.

Exercice 5 Soit n un entier. Soient $a_1, \dots a_n$ n entiers quelconques. Montrer qu'il existe un sous-ensemble non vide de $\{a_1, \dots, a_n\}$ dont la somme des éléments est divisible par n.

Solution de l'exercice 5 Notons $S_1 = a_1, S_2 = a_1 + a_2, \dots S_n = a_1 + \dots + a_n$ les sommes partielles (qui correspondent donc aux sous-ensembles $\{a_1\}, \{a_1, a_2\}, \dots, \{a_1, \dots, a_n\}$). Si l'une de ses sommes est divisible par n, l'exercice est résolu. Sinon, on considère pour n chaussettes ces sommes et pour $n-1$ tiroirs les restes modulo n. Il y a alors $i < j$ deux indices tels que $S_j - S_i$ est divisible par n. Alors l'ensemble $\{a_{i+1}, \dots, a_j\}$ convient.

Exercice 6 Montrer que parmi six stagiaires, on peut toujours en choisir trois tels que deux à deux ils se connaissent ou que deux à deux ils ne se connaissent pas.

Solution de l'exercice 6 Choisissons un stagiaire. D'après le principe des tiroirs, parmi les cinq autres, on peut choisir trois tels qu'il les connaît tous les trois ou qu'il n'en connaît aucun des trois. Pour fixer les idées, disons qu'il les connaît. Si deux parmi ces trois-là se connaissent, c'est gagné. Sinon, c'est que ces trois-là forment un groupe de trois personnes qui ne se connaissent pas deux à deux. Cela conclut.

Exercice 7 L'ensemble des points du plan est colorié en jaune ou en rouge. Montrer qu'il existe une couleur telle que pour tout réel x strictement positif on puisse trouver deux points de cette couleur distants de x.

Solution de l'exercice 7 Raisonnons par l'absurde en supposant qu'on puisse trouver des distances x et y telles que deux points rouges ne soient jamais distants de x et deux points bleus ne soient jamais distants de y. Il existe alors un point rouge ; notons le A. Considérons ensuite un triangle isocèle ABC tel que $AB = AC = x$ et $BC = y$. Ainsi, B et C doivent être bleu. Or ces deux points sont distants de y, ce qui est contradictoire. Notre supposition de départ était donc fausse, ce qui conclut.

Exercice 8 Soit x un irrationnel positif. Montrer qu'il existe une infinité de fractions $\frac{p}{q}$ telles que $|x - \frac{p}{q}| < \frac{1}{q^2}$.

Solution de l'exercice 8 Pour un réel y, on note $\{y\} = y - \lfloor y \rfloor$ la partie fractionnaire de y. Soit n un entier naturel à fixer plus tard (qui permettra de fixer la précision de notre approximation). Considèrons les $n+1$ chaussettes définies par $0, \{x\}, \ldots, \{nx\}$ que l'on répartit en les n tiroirs $[\frac{r}{n}, \frac{r+1}{n}[$ où r est un entier entre 0 et $n-1$. Il existe donc deux indices $0 \leq k < l \leq n$ tels que $\{kx\}$ et $\{lx\}$ soient dans le même tiroir. On a alors $|lx - kx| < \frac{1}{n}$. En notant $p = \lfloor lx \rfloor - \lfloor kx \rfloor$, on trouve : $|(l-k)x - p| < \frac{1}{n}$. On pose alors $q = l - k$, $q \leq n$, ce qui permet d'écrire : $|x - \frac{p}{q}| < \frac{1}{nq} \leq \frac{1}{q^2}$. Ceci prouve l'existence d'une approximation de x par un rationnel avec une précision $\frac{1}{n}$. Pour n suffisamment grand, cela impose une meilleure approximation que celle précédemment trouvée. En réitérant, on exhibe ainsi une infinité de solutions.

Principe de l'extremum

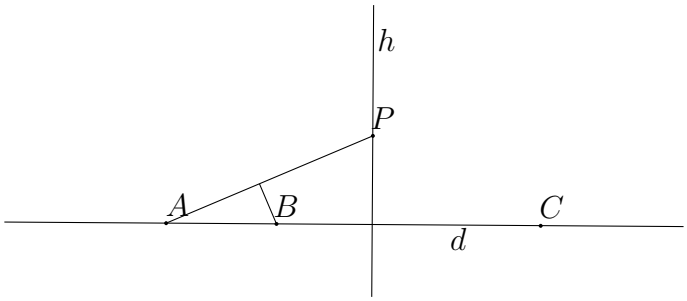
On utilise en fait deux principes de l'extremum.
— Tout ensemble fini non vide de réels contient admet un plus petit élément
— Tout ensemble non vide d'entiers positifs admet un plus petit élément.

Plus généralement, lorsqu'on considère une nombre fini d'objets, il peut être intéressant de les ordonner.

Exercice 9 Soit S un ensemble fini de points du plan tel que si deux points appartiennent à S, alors il en existe un troisième appartenant à la droite formée par ces deu$x$ points. Montrer que l'ensemble S est formé de points alignés.

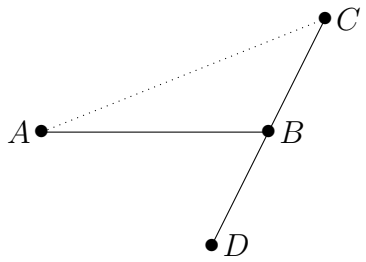
Solution de l'exercice 9 Supposons par l'absurde que ce ne soit pas le cas. Parmi les couples (d, P) formées d'une droite d passant par deux points de S et un point P de S qui n'est pas sur d, il en existe un qui minimise la distance de P à d. Soit h la perpendiculaire à d passant par P. Elle divise d, qui contient par hypothèse trois points S, en deux demi-droites. D'après

le principe des tiroirs, il y en a une qui contient deux points de S. Si on note A le plus éloigné et B le plus proche des h, la distance de B à (AP) est inférieure strictement à la distance de P à d, ce qui fournit la contradiction voulue.



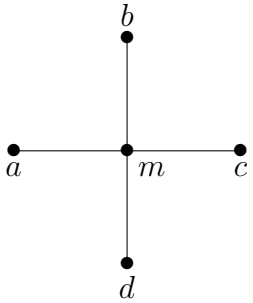
Exercice 10 On se donne des points dans le plan tels que chaque point soit le milieu de deux autres. Montrer que les points sont en nombre infini.

Solution de l'exercice 10 On suppose par l'absurde qu'il n'y a qu'un nombre fini de points. On considère un couple de points (A, B) tel que la distance AB soit maximale. B est par hypothèse le milieu de deux points qu'on nommera C et D. On a alors $AC > AB$ ou $AD > AB$, ce qui contredit la maximalité de AB. Conclusion, les points sont bien en nombre infini.



Exercice 11 On affecte une valeur entière positive ou nulle à chaque point à coordonnées entières du plan de sorte que chaque valeur soit la moyenne de ses quatre voisines. Montrer que toutes les valeurs sont égales.

Solution de l'exercice 11 Les valeurs étant des entiers naturels, on peut considérer m la plus petite de ces valeurs. On se place un point ayant cette valeur. On note a, b, c et d les valeurs de ses voisins.



On a par hypothèse $m = (a+b+c+d)/4$, et m étant la valeur minimale, elle est inférieure ou égale aux quatre autres. Si l'une des quatre valeurs, disons a, est strictement supérieure à m, on a :

$$m = \frac{a+b+c+d}{4} > \frac{m+b+c+d}{4} \geqslant \frac{m+m+m+m}{4} = m,$$

et donc $m > m$, ce qui est absurde. On a donc nécessairement $m = a = b = c = d$. En chacun des voisins peut s'appliquer ce même raisonnement, et on prouve de proche en proche que les valeurs sont égales à m en tout point.

Exercice 12 Étant donnés $2n+1$ nombres tels que n d'entre eux sont toujours inférieurs à la somme des $n+1$ autres. Montrer qu'ils sont tous positifs.

Solution de l'exercice 12 On ordonne les réels selon $a_1 \leq \cdots \leq a_{2n+1}$. L'hypothèse permet d'écrire $a_1 + a_2 + \cdots + a_n + 1 \geq a_{n+2} + \cdots + a_{2n+1}$. Cela se réécrit encore : $a_1 \geq (a_{n+2} - a_2) + \cdots + (a_{2n+1} - a_1)$. Chaque parenthèse étant positive, cela conclut.

Exercice 13 Étant donnés 7 entiers distincts strictement positifs dont la somme vaut 100, montrer qu'on peut en choisir trois dont la somme est supérieure ou égale à 50.

Solution de l'exercice 13 On ordonne les entiers selon $a_1 < a_2 < \cdots < a_7$. Supposons que $a_5 + a_6 + a_7 < 50$. Alors nécessairement, $a_5 \leq 15$ (en effet, $16 + 17 + 18 = 51$). Par conséquent, $a_4 \leq 14, a_3 \leq 13, a_2 \leq 12, a_1 \leq 11$, donc $a_1 + a_2 + a_3 + a_4 \leq 50$, et la somme des 7 nombres est inférieure à 50.

Exercice 14 On considère un ensemble fini de personnes. Chacune de personnes a au plus trois ennemis. La relation d'animosité est réciproque. Montrer qu'on peut séparer ces personnes en deux groupes, de sorte que chaque personne ait au plus un ennemi dans son groupe.

Solution de l'exercice 14 Pour chaque répartition en deux groupes 1 et 2, on note N_1 (resp.N_2) le nombre de relations ennemies internes au groupe 1 (resp. 2). Parmi toutes les répartitions, on considère celle qui minimise $N = N_1 + N_2$. Supposons par l'absurde qu'il existe une personne ayant au moins deux ennemis dans son groupe, (disons le groupe 1). Alors, il a au plus un ennemi dans le groupe 2. En le changeant de groupe, N_1 diminue d'au moins 2 et N_2 est augmenté d'au plus 1. Donc N diminue strictement. Contradiction.

Exercice 15 Dans un tournoi, chaque compétiteur rencontre chaque autre compétiteur exactement une fois. Il n'y a pas de match nul. À l'issue de la compétition, chaque joueur fait une liste qui contient les noms des joueurs qu'il a battus, ainsi que les noms des joueurs que ceux-ci a battus. Montrer qu'il existe une liste qui contient les noms de tous les autres joueurs.

Solution de l'exercice 15 Appelons A le partipcipant qui a battu le plus grand nombre d'adversaires. Montrons qu'il a sur sa feuille les noms de tous les autres participants. On suppose par l'absurde que ce n'est pas le cas. Il existe alors un participant B qui a battu A. B a sur sa feuille le nom de A et de tous ceux que A a battus. B a donc battu 1 adversaire de plus que A, ce qui est absurde.

4 mercredi 19 après-midi : Gabriel Pallier

Invariants

Dans de nombreux énoncés mathématiques, on se pose la question de savoir s'il est possible de faire passer un système d'un état à un autre à l'aide d'un ensemble de transformations que l'on s'autorise à lui faire subir.

Voici deux exemples de telles questions :

Exemple 23. Un fou est disposé sur une case d'un échiquier 8×8, et se déplace uniquement en diagonale. Peut-il se rendre dans le coin en bas à gauche ?

Exemple 24. On prend un Rubik's Cube dont on a recolorié chaque petite facette à l'aide d'une couleur au hasard parmi les 6 ; est-il possible de le remonter ?

Dans les deux cas, prouver que c'est possible est (du moins en théorie) peu coûteux. Il suffit en fait de trouver une suite de transformations adéquate : déplacer le fou jusqu'au coin en bas à gauche, ou remonter le Rubik's Cube constitue alors une preuve tout à fait valable. En revanche, prouver que c'est impossible est un problème a priori plus délicat, puisqu'on ne peut en général pas se permettre d'essayer toutes les séquences de transformations !

Afin d'y remédier, le principe d'un raisonnement par invariant consiste à essayer de repérer une propriété ou une quantité qui ne change pas quand on effectue une transformation. Cette propriété ou quantité est appelée un invariant. On énoncera donc le principe des invariants sous la forme suivante :

Principe des invariants *Si une quantité ou une propriété est conservée par certaines transformations, alors il est impossible de passer d'une situation à une autre où la quantité ou propriété est différente en utilisant seulement ces transformations.*

Dans la pratique, la difficulté est souvent de trouver un bon invariant (de même que pour le principe des tiroirs, de trouver les bons tiroirs) et comme souvent, c'est en pratiquant qu'on progresse. Reprenons nos deux exemples :

1. Si l'on suppose l'échiquier colorié en noir et blanc, la couleur de la case sur laquelle le fou se situe est un invariant. En particulier, si le fou débute sur une case qui n'est pas de la couleur de $\mathrm{a1}$ (à savoir le noir sur les échiquiers classiques), alors il ne pourra jamais s'y rendre.
2. Le nombre de cases coloriées d'une certaine couleur est un invariant. En particulier, si nous n'avons pas colorié 9 facettes pour chaque couleur, alors on ne pourra pas remonter le Rubik's Cube. Remarquez qu'il existe d'autres invariants. Par exemple, les triplets de couleur présentes sur chaque coin. Si un coin est colorié avec seulement une couleur, alors on ne pourra pas remonter le Rubik's Cube.

Comme le second exemple l'illustre, il peut exister plusieurs invariants pour un même problème. Et ce n'est pas parce qu'un invariant n'arrive pas à distinguer deux configurations, que l'on peut passer de l'une à l'autre : il se peut qu'il existe un autre invariant qui les différencie. En outre, certains invariants sont plus fins que d'autres : I_1 est plus fin que I_2 si tout couple de configuration qui sont différenciées par I_2 le sont aussi par I_1.

Exercice 1 Une feuille de papier est déchirée en trois parties. Ensuite, l'une de ces parties est déchirée de nouveau en trois parties, et ainsi de suite. Peut-on obtenir, en fin de compte, un total de cent parties ?

Solution de l'exercice 1 A chaque fois que l'on déchire un morceau de feuille en trois parties, le nombre total de morceaux de feuilles augmente de 2. En particulier, sa parité est préservée : s'il était pair, il le reste, s'il était impair, il le reste. Puisqu'il y avait 1 morceau de feuille au début, il y a toujours un nombre impair de morceaux de feuille ; on ne peut pas en faire 100.

Exercice 2 Lors d'un congrès international de mathématiques, les participants qui se rencontrent se serrent la main. On appelle personne paire (resp. personne impaire), une personne qui a serré un nombre pair (resp. impair) de mains. Montrer que le nombre de personnes impaires est pair.

Solution de l'exercice 2 Au début, il y a 0 personne impaire. A chaque poignée de main entre deux personnes, le nombre de personnes impaires est augmenté de 2 (s'il s'agissait de deux personnes paires), diminué de 2 (s'il s'agissait s'il s'agissait de deux personnes paires) ou reste inchangé (s'il s'agissait d'une personne paire et d'une personne impaire). Dans tous les cas, il reste pair à la fin.

Dans les exercices précédents, nous avons utilisé un invariant de parité. De nombreux invariants peuvent être vus comme des invariants de parité. C'est le cas par exemple de la couleur des cases parcourues par un fou sur un échiquier (la couleur de la ℓ-ième ligne sur la c-ième colonne est déterminée par la parité de $\ell + c$). On retrouvera des raisonnements s'appuyant sur la parité dans la partie sur les preuves par coloriage.

Exercice 3 On considère le tableau rempli de signes suivants :

$$\begin{array}{cccc} + & + & - & + \\ - & - & + & + \\ + & + & + & + \\ + & - & + & - \end{array}$$

On répète plusieurs fois l'opération qui consigne à choisir une ligne ou une colonne et à en changer tous les signes en leurs opposés. Est-il possible d'atteindre un tableau constitué seulement de signes $-$?

Solution de l'exercice 3 Non, ce n'est pas possible : la parité du nombre de signes $-$ dans le tableau est un invariant, et il est impair au départ. On ne peut donc pas atteindre le nombre de 16 signes $-$. On peut également considérer la parité du nombre de $-$ dans les coins du tableau.

Exercice 4 Les nombres entiers $1 \dots 2015$ sont écrits sur un tableau blanc. A chaque étape, on choisit deux nombres a et b distincts au hasard sur le tableau, que l'on efface et remplace par $|a - b|$. Montrer qu'à la fin, il restera un nombre pair au tableau.

Solution de l'exercice 4 Appelons S_n la somme des nombres écrits au tableau après n étapes. Au départ, nous avons

$$S_0 = \frac{2015 \times 2016}{2} = 2015 \times 1008$$

qui est un grand nombre pair. A chaque étape, a et b sont remplacés par $|a - b|$, qui vaut $a - b$ ou $b - a$; nous savons donc que S_{n+1}vaut $S_n - 2a$ ou $S_n - 2b$. La parité de S_{n+1} est la même que S_n ; finalement le dernier nombre écrit au tableau qui est S_{2014}, est pair comme S_0.

Exercice 5 Est-il possible de répartir les entiers $1, 2, \ldots, 33$ en 11 groupes disjoints de trois éléments chacun, de sorte que dans chaque groupe, l'un des éléments soit la somme des deux autres ?

Solution de l'exercice 5 Non, ce n'est pas possible. Si c'était le cas, la somme des entiers de chaque groupe serait paire ; donc la somme des entiers de 1 à 33 serait paire. Ceci n'est pas le cas puisqu'elle vaut 33×17 qui est impair.

Exercice 6 Dans l'espace, on part d'un ensemble de 7 sommets d'un cube. A chaque étape, on s'autorise à remplacer un point par son symétrique par rapport à l'un des autres points. Peut-on atteindre le 8e sommet de cette façon ?

Solution de l'exercice 6 Supposons que les 7 sommets ont pour coordonnées, dans un repère orthonormé :

$$\begin{array}{ccc} (0,0,0) & (0,0,1) & (0,1,0) \\ (1,0,0) & (1,1,0) & (0,1,1) \\ & (1,0,1) & \end{array}$$

Alors, les nouveaux points obtenus seront toujours à coordonnées entières ; de plus, le symétrique de (x, y, z) par rapport à (a, b, c) étant

$$(x + 2(a - x), y + 2(b - y), z + 2(c - z))$$

la parité des coordonnées est respectée. Un point dont les trois coordonnées sont impaires n'est donc pas atteignable ; c'est en particulier le cas du 8e sommet $(1, 1, 1)$.

Exercice 7 On écrit des signes $+$ et $-$ sur chaque case d'un tableau 8×8. Puis on applique les opérations suivantes : à chaque étape, on choisit un carré de taille 3×3 ou 4×4 et on inverse tous les signes présents sur les cases de ce carré. Est-il possible, à partir de n'importe quelle configuration de départ, d'arriver à une configuration où tous les signes sont $+$?

Solution de l'exercice 7 On ne peut pas se contenter de compter la parité du nombre de $-$, puisque celle-ci peut être changée quand on inverse les signes sur un carré 3×3. En revanche, remarquons que tout carré 3×3 rencontre la troisième ou la sixième colonne, et touche un nombre pair de cases sur le reste du tableau. On considère donc comme invariant, la parité du nombre de $-$ dans le tableau qui ne sont pas sur la 3e ou la 6e colonne.

Exercice 8 * On considère les triplets de nombres réels. A chaque étape, on s'autorise à effectuer l'une des trois transformations suivantes :

$$(x, y, z) \to \begin{cases} \left(\frac{x+y}{\sqrt{2}}, \frac{x-y}{\sqrt{2}}, z\right) \\ \left(x, \frac{y+z}{\sqrt{2}}, \frac{y-z}{\sqrt{2}}\right) \\ \left(\frac{z+x}{\sqrt{2}}, y, \frac{z-x}{\sqrt{2}}\right) \end{cases}$$

Peut-on passer de $t_1 = (1, -1, 1)$ à $t_2 = (2, 0, 0)$?

Solution de l'exercice 8 Posons

$$f(x, y, z) = x^2 + y^2 + z^2$$

Alors, f est invariante par les transformations du problème :

$$\begin{aligned}\left(\frac{x+y}{\sqrt{2}}\right)^2+\left(\frac{x-y}{\sqrt{2}}\right)^2+z^2 &= \frac{x^2}{2}+\frac{y^2}{2}+\sqrt{2}xy+\frac{x^2}{2}+\frac{y^2}{2}-\sqrt{2}xy+z^2\\ &= x^2+y^2+z^2\end{aligned}$$

Les deux autres vérifications sont les mêmes, à permutation circulaire près. Or

$$\begin{aligned}f(1,-1,1) &= 3\\ f(2,0,0) &= 4\end{aligned}$$

Donc on ne peut pas passer de t_1 à t_2. Le choix de f peut paraître excessivement astucieux, mais il s'éclaircit un peu quand on raisonne en termes géométriques : les triplets sont les points de l'espace (rapporté à un repère orthonormé direct) et les transformations correspondent alors à des rotations d'angle $\pi/2$ autour des 3 axes. En particulier, la distance à l'origine est inchangée sous ces transformations.

Monovariants

Le principe des monovariants est une variante du principe des invariants :

Principe des monovariants *Si une quantité réelle croît (resp. décroît) au sens large par certaines transformations, alors il est impossible de passer d'une situation à une autre où la quantité ou propriété est strictement plus petite (resp. plus grande) en utilisant seulement ces transformations.*

Exercice 9 Neuf cellules d'un diagramme de taille 10×10 sont infectées. A chaque étape, une cellule est infectée si elle l'était déjà ou bien si elle possédait deux voisines au moins infectées (parmi les 4 cellules adjacentes).

(a) Est-ce que l'infecton peut se répandre partout ?

(b) Combien de cellules infectées au départ faut-il pour répandre l'infection partout ?

Solution de l'exercice 9

(a) Non, ce n'est pas possible. Remarquer que le périmètre de la zone délimitée par les cellules infectées décroît au sens large à chaque étape. Au départ, il est d'au plus $9\times 4=36$, et ne peut pas attendre 40.

(b) D'après la question (a) il faut déjà au moins 10 cellules infectées. On place 10 cellules le long d'une diagonale. On vérifie qu'alors l'infection peut se répandre partout.

Exercice 10 Sur une ligne, on écrit 1000 entiers relatifs. Puis, en-dessous de chaque entier, on écrit le nombre d'occurrences de cet entier dans la liste (par exemple, si 13 apparaît 5 fois, on écrit 5 en-dessous des nombres 13). Puis, on réitère le procédé. Montrer qu'au bout d'un certain temps, toutes les lignes sont identiques.

Solution de l'exercice 10 A partir de la deuxième liste, tous les entiers en question sont des nombres d'occurrences. Donc le nombre situé en-dessous de a est plus grand que a. Si l'on considère les nombres d'une même colonne, ils sont croissants quand on descend la colonne (éventuellement, à l'exception du premier). Puisque toute suite croissante et majorée d'entiers

est constante à partir d'un certain rang, il existe une ligne ℓ_i à partir de laquelle les nombres de la i-ème colonne sont tous les mêmes. On pose alors

$$\ell = \max(\ell_1, \dots \ell_{1000})$$

et on vérifie que toutes les lignes sont identiques à partir de la ℓ-ième.

Symétrie

Le pincipe de symétrie est un cas particulier du principe des invariants, où la propriété conservée est une symétrie du problème :

Principe de symétrie *Si une configuration admet une symétrie, et si cette symétrie est préservée par certaines transformations, alors il est impossible de passer d'une situation symétrique à une autre non symétrique en utilisant seulement ces transformations*

Exercice 11 On se donne un damier de taille 7×7. Sur chaque case est posé un jeton ; et les cases sont repérées par les coordonnées (x, y) où x et y varient dans $\{-3, -2, \dots, 3\}$. Deux joueurs jouent tour à tour en respectant les règles suivantes :

— Si le premier joueur retire le jeton en position (x, y), il doit également retirer les jetons en positions $(y, -x)$, $(-x, -y)$ et $(-y, x)$

— Si le deuxième joueur retire le jeton en position(x, y), il doit également retirer les jetons en positions $(-x, y)$, $(-x, -y)$ et $(x, -y)$

Si l'un des deux joueurs atteint la situation où il reste un seul jeton en position $(0, 1)$, alors il a gagné. L'un des deux joueurs peut-il gagner ?

Solution de l'exercice 11 Au départ, la confguration des jetons admet une symétrie centrale : (x, y) contient un jeton si et seulement si $(-x, -y)$ contient un jeton. Les opérations des deux joueurs respectent cette symétrie. Conclusion, aucun des deux joueurs ne peut gagner.

Coloriages

Nous avons vu dans le cours sur le raisonnement par récurrence qu'il existe F_8 manières de paver un rectangle 8×2. En conséquence, on conçoit qu'il existe énomrmément de manières de paver un échiquier 8×8. Si l'on retire un coin à l'échiquier, un pavage n'est plus possible ainsi qu'on le montre à l'aide d'un invariant de parité. Mais que se passe-t-il si l'on retire deux coins opposés ? L'exercice suivant, qui répond à cette question, constitue le prototype du raisonnement par coloriages.

Exercice 12 On retire le coin en bas à gauche et le coin en haut à droite sur un échiquier 8×8. Est-il possible de recouvrir les cases restantes à l'aide de 31 dominos 2×1 ?

Solution de l'exercice 12 Colorions les cases comme celles d'un échiquier classique. Alors on constate qu'il reste 32 cases blanches pour 32 noires. Or un domino recouvre exactement une case blanche et une case noire. Un tel pavage n'est donc pas possible.

Exercice 13 Est-il possible de parcourir le labyrinthe suivant en entrant par E, sortant par S et en passant une seule fois par chaque case ?

Solution de l'exercice 13 Non, ce n'est pas possible. Colorions le labyrinthe comme un échiquier ; si un parcours des 36 cases du labyrinthe existe et débute par une case noire, il doit terminer par une case blanche. Or E et S sont de la même couleur.

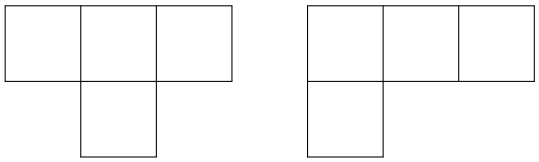


FIGURE 1 – tetraminos T et L

Exercice 14 Un sol rectangulaire est pavés de carreaux de tailles 2×2 et 1×4. Si l'on casse l'un des carreaux, peut-on le remplacer par un carreau de l'autre type (quitte à déplacer tous les autres) ?

Solution de l'exercice 14 Non, ce n'est pas possible. On peut le démontrer à l'aide d'un coloriage à quatre couleurs ; on peut colorier les cases du rectangle à l'aide de quatre couleurs comme sur le tableau suivant (où les couleurs sont dénotées par les nombres $1 \dots 4$) :

$$\begin{array}{ccccccc} 1 & 2 & 1 & 2 & 1 & \cdots \\ 3 & 4 & 3 & 4 & 3 & \cdots \\ 1 & 2 & 1 & 2 & 1 & \cdots \\ 3 & 4 & 3 & 4 & 3 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{array}$$

On remarque alors qu'un carré 2×2 recouvre forcément une case de chaque couleur, tandis qu'un carreau 1×4 recouvre deux cases de deux couleurs, de sorte que si c est le nombre de carreaux 2×2 et n_i le nombre de cases de la couleur i alors on a les congruences

$$n_i \equiv c[2]$$

pour tout i. Si l'on change la parité de c, alors le carrelage devient impossible.

Exercice 15 De combien de manières différentes un damier 10×10 peut-il être recouvert par 25 tétraminos en T ?

Solution de l'exercice 15 C'est un question un peu piégeuse, on ne peut pas le faire ! Montrons ceci à l'aide d'un invariant de parité. Si le damier est bicoloré, les tetraminos recouvrent chacun 3 cases d'une couleur et 1 de l'autre. Si l'on note n (resp. b) le nombre de tetraminos qui recouvrent 3 cases noires (resp. blanches) alors on a les équations

$$3n + b = 50$$

$$n + b = 25$$

Soustrayons la deuxième ligne à la première : nous obtenons $2n = 25$, ce qui est absurde.

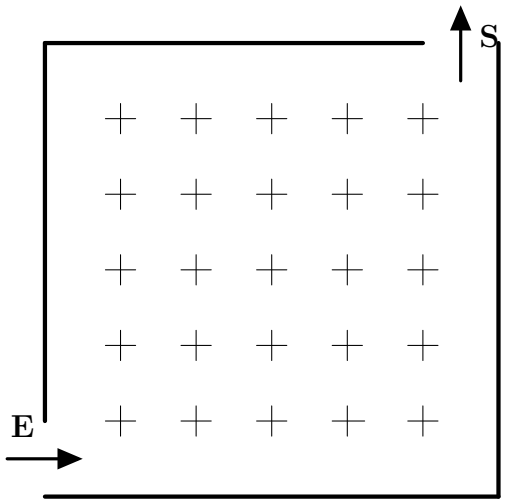


FIGURE 2 – Labyrinthe

Exercice 16 Dans le plan, on considère un pentagone dont tous les sommets sont à coordonnées entières, et dont les longueurs des côtés sont impaires. Montrer que son périmètre est pair.

Solution de l'exercice 16 On commence par colorier chaque point (x, y) de $\mathbb{Z}^2$ à l'aide de bleu ou de rouge, selon la parité de $x + y$. Ensuite, remarquons que si $[AB]$ est un côté du pentagone, alors la longueur $l = AB$ est paire si A et B sont de la même couleur, impaire si A et B sont de couleurs différentes. Ceci découle du théorème de Pythagore :

$$l \equiv l^2 = (x_A - x_B)^2 + (y_A - y_B)^2 \equiv (x_A - x_B) + (y_A - y_B) \pmod{2}$$

Quand on fait un tour du pentagone, on revient sur un point de la même couleur qu'au début. Ceci permet de conclure.

un dernier exercice pour finir...

L'exercice suivant demande de connaître la notion de limite d'une suite.

Exercice 17 On part de deux nombres réels a et b. On pose $x_0 = a$, $y_0 = b$, puis à chaque étape :

$$\begin{aligned} x_{n+1} &= \frac{x_n + y_n}{2} \\ y_{n+1} &= \frac{2x_n y_n}{x_n + y_n} \end{aligned}$$

Montrer que les suites (x_n) et (y_n) admettent une limite commune ℓ (c'est-à-dire ; s'approchent arbitrairement près de ℓ quand n est assez grand), que l'on exprimera en fonction de a et b.

Solution de l'exercice 17 La quantité $x_n y_n$ est un invariant, et vaut donc ab pour tout n. Admettons un instant que x et y tendent vers une limite ℓ. Alors on en déduit par passage à la limite

$$x_n y_n = \ell^2 = ab$$

Soit $\ell = \sqrt{ab}$. D'après l'inégalité arithmético-géométrique, nous avons pour tout n

$$y_n < \sqrt{ab} < x_n$$

et il suffit donc de montrer que $x_n - y_n$ tend vers 0 (c'est-à-dire : devient arbitrairement petit) quand n tend vers $+\infty$. Or, on calcule

$$\begin{aligned} x_{n+1} - y_{n+1} &= \frac{x_n + y_n}{2} - \frac{2x_n y_n}{x_n + y_n} \\ &= \frac{(x_n + y_n)^2 - 4x_n y_n}{2(x_n + y_n)} \\ &= \frac{(x_n - y_n)^2}{2(x_n + y_n)} \\ &< \frac{(x_n - y_n)^2}{2(x_n - y_n)} = \frac{1}{2}(x_n - y_n) \end{aligned}$$

De sorte que par une récurrence, $x_n - y_n < \frac{1}{2^n}(a - b)$. On en déduit que x_n et y_n tendent vers ℓ.

3 Groupe C : géométrie

1 mardi 18 matin : Victor Quach

Exercice 1 Deux cercles Γ_1 et Γ_2 se coupent en A et B. Une tangente commune à ces deux cercles les coupent respectivement en C et D. Montrer que (AB) coupe $[CD]$ en son milieu

Solution de l'exercice 1 Soit M le point d'intersection de (AB) et (CD). M est sur l'axe radical de Γ_1 et Γ_2, d'où $MC^2 = MD^2$, c'est ce qu'on voulait.

Exercice 2 Montrer que les hauteurs d'un triangle sont concourantes.

Solution de l'exercice 2 L'orthocentre peut être vu comme centre radical des trois cercles de diamètre chacun des côtés, dont les axes radicaux deux-à-deux forment les hauteurs.

Exercice 3 Soient A, B, C et D quatre points distincts alignés dans cet ordre. Soient Γ_1 et Γ_2 Les cercles de diamètres respectifs $[AC]$ et $[BD]$, qui s'intersectent en X et Y. On considère O un point arbitraire sur (XY) qui ne soit pas sur la droite originelle. (CO) recoupe Γ_1 en M, (BO) recoupe Γ_2 en N. Montrer que $(AM), (DN)$ et (XY) sont concourantes.

Solution de l'exercice 3 Le point O est sur l'axe radical de Γ_1 et Γ_2, donc $\overline{OM} \cdot \overline{OC} = \overline{OB} \cdot \overline{ON}$, ce qui fournit la cocyclicité de M, N, B et C.

Pour conclure, remarquons qu'il suffit de prouver que les points M, N, A et D sont cocycliques : le point de concours dont on cherche à prouver l'existence ne serait alors rien d'autre que le centre radical de ce cercle avec Γ_1 et Γ_2.

On écrit donc les égalités suivantes modulo π :

$$\begin{aligned}
(ND, AD) &= (ND, BD) \\
&= (ND, BN) + (BN, BD) && \text{(relation de Chasles)} \\
&= -\frac{\pi}{2} + (BN, BC) && (B,C,D \text{ alignés}) \\
&= -\frac{\pi}{2} + (MN, MC) && (M,N,B,C \text{ alignés}) \\
&= (MC, MA) + (MN, MC) && (AMC \text{ rectangle en } M) \\
&= (MN, MA)
\end{aligned}$$

Cela conclut.

Exercice 4 Soit ABC un triangle et M le milieu de $[BC]$. Les points D et E sont respectivement les pieds des hauteurs issues de B et C. On note X et Y les milieux respectifs de $[EM]$ et $[DM]$. (XY) coupe la parallèle à (BC) passant par A en T. Montrer que $TA = TM$.

Solution de l'exercice 4 La droite (DE) étant antiparallèle à (BC) par rapport aux droites (AB) et (AC), elle est également antiparallèle à (TA) par rapport à ces mêmes droites. Ainsi, en notant Γ le cercle circonscrit à ADE, la droite (TA) est tangente à Γ (se prouve également par chasse aux angles).

Le cercle de dianètre $[BC]$ admet M pour centre et passe par E et D. Une chasse aux angles montre alors que (MD) et (ME) sont tangentes à Γ.

Les points X et Y ont alors même puissance par rapport au cercle Γ et au cercle réduit au point M (le cercle de centre M et de rayon nul). Le point T appartient donc aussi à l'axe radical de ces cercles, ce qui permet d'écrire $TA^2 = TM^2$.

Exercice 5 Le cercle inscrit du triangle ABC touche les côtés $[AC]$ et $[AB]$ en E et F. Les droites (BE) et (CF) se coupent en G. Les points R et S sont tels que $BCER$ et $BCSF$ soient des parallélogrammes. Montrer que $GR = GS$.

Solution de l'exercice 5 Introduisons le cercle exinscrit à ABC associé à A. Il est tangent aux côtés $[BC], [AC], [AB]$ en respectivement T, U, V. Les résultats classiques permettent d'écrire $CT^2 = y^2 = BF^2$ et $FV^2 = (y+z)^2 = BC^2$. Puis, en utilisant le parallélogramme $BCSF$, $CT^2 = CS^2$ et $FV^2 = FS^2$. Ainsi, (FC) est l'axe radical du cercle exinscrit et du point S. De la même façon, (DE) est l'axe radical du cercle exinscrit et du point R. Le point G est donc centre radical de ces cercles, d'où $GR^2 = GS^2$.

Exercice 6 Soient A_1, A_2, A_3, A_4 sont quatre points non cocyliques. On note O_1 le centre du cercle circonscrit à $A_2A_3A_4$ et r_1 son rayon. On définit par permutation circulaire $O_2, O_3, O_4, r_1, r_2, r_3$ et r_4. Montrer que $\frac{1}{O_1A_1^2 - r_1^2} + \frac{1}{O_2A_2^2 - r_2^2} + \frac{1}{O_3A_3^2 - r_3^2} + \frac{1}{O_4A_4^2 - r_4^2} = 0$

Solution de l'exercice 6 Notons X le point d'intersection de (A_1A_3) et (A_2A_4) et a_1, a_2, a_3, a_4 les longueurs algébriques $\overline{XA_1}, \overline{XA_2}, \overline{XA_3}, \overline{XA_4}$ respectivement.

Alors

$$\sum_\sigma \frac{1}{O_1A_1^2 - r_1^2} = \sum_\sigma \frac{1}{(a_1 + a_3)(a_1 - \frac{a_2a_4}{a_3})} = \sum_\sigma \frac{a_3}{(a_1 + a_3)(a_1a_3 - a_2a_4)} = 0$$

2 mardi 18 après-midi : Thomas Budzinski

- Introduction -

Question philosophique : qu'est-ce que la géométrie ? L'étude de certaines figures en termes d'angles, de distances... ? La distance d'une figure donnée au bord du tableau ne nous intéresse pourtant pas. L'étude de certaines propriétés de certaines figures ? Certes, mais comment définir exactement ces propriétés ? Qu'est-ce qui distingue la propriété pertinente « A, B et C sont alignés » et la propriété inintéressante « (AB) est perpendiculaire au bord du tableau » ? Ou, moins caricaturalement, la propriété « $AB = 1$ cm », moyennement intéressante de la plupart des points de vue mathématiques.

Un moyen pertinent de définir ces propriétés est : « l'ensemble des propriétés invariantes par une certaine classe de transformations ». Par exemple, si on veut s'intéresser aux distances, on peut considérer les propriétés invariantes par isométries (translations, rotations, réflexions...) ; si on veut s'intéresser aux rapports de longueurs, aux angles, on peut considérer les propriétés invariantes par similitudes ; si on veut s'intéresser au parallélisme, aux milieux, on peut considérer les propriétés invariantes par transformation affines ; si on veut s'intéresser aux alignements, aux points harmoniques, on peut considérer les propriétés invariantes par transformation projective (voir cours avancé).

Il est donc naturel de tenter de comprendre en profondeur ces transformations. Nous considérerons ici les similitudes directes.

- Cours -

Définition 25. On appelle similarité toute transformation (i.e. fonction bijective) du plan qui conserve les angles orientés, c'est-à-dire telle que pour tous points A, B et C, si on note A', B' et C' leurs images, on a $(\vec{A'B'}, \vec{A'C'}) = (\vec{AB}, \vec{AC})$. De manière équivalente, une similarité envoie les triangles sur des triangles directement semblables.

Remarques 26.
- L'équivalence entre conservation des angles orientés et des triangles directement semblables n'est pas immédiatement évidente pour les triangles plats. Toutefois, étant donné trois points A, B et C alignés, pour montrer que le rapport AB/AC est conservé, il suffit de considérer un point P en dehors de la droite et de considérer les triangles ABP et ACP, prouvant que les rapports AB/AP et AP/AC seront conservés. Une astuce du même genre permettra de toujours mettre de côté ce genre de cas résiduels. C'est un bon exercice pour le lecteur pointilleux de remplir les trous...
- On connaît déjà bon nombre de similarités. Translations, rotations, homothéties et similitude directes (voir définition 33) sont des similarités. De plus, il est évident que la composition de deux similarités est une similarité.
- Le terme « similarité » est un anglicisme qu'on utilisera seulement dans ce cours. Le terme approprié est similitude directe, mais cela induit une confusion avec la notion propre au plan de la définition 33. Le théorème 34 en devient d'ailleurs particulièrement limpide...

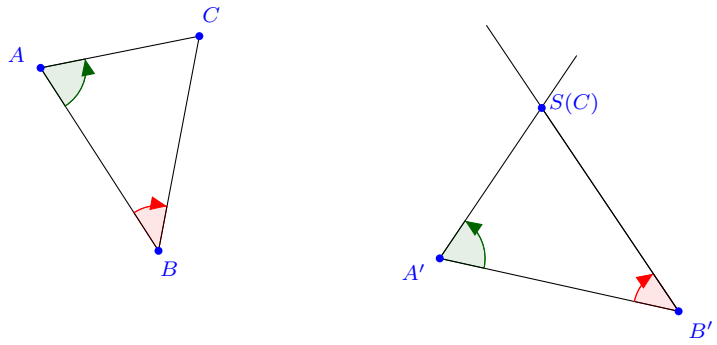
Théoréme 27. Étant donnés quatre points $A \neq B$ et $A' \neq B'$, il existe une unique similarité s telle que :

$$\begin{array}{rcccc} s & : & A & \longmapsto & A' \\ & & B & \longmapsto & B'. \end{array}$$

Démonstration. On pourrait raisonner directement dans l'esprit du théorème 34, mais la preuve naturelle a son intérêt.

Unicité :

Montrons que pour tout point C du plan, cette condition fixe l'image de C par S. On suppose $C \notin (AB)$. Par conservation des angles orientés, l'image de C doit être sur la droite formant en B' un angle $(\vec{BA}, \vec{BC})$ avec le vecteur $\vec{B'A'}$. De même, elle doit être sur la droite formant en A' un angle $(\vec{AB}, \vec{AC})$ avec $\vec{A'B'}$. L'intersection de ces deux droites, uniquement déterminée, est donc le point recherché.



Existence :

On va exhiber une similarité avec cette propriété en composant différentes similarités classiques (translations, rotations, homothéties...) de manière à s'approcher de plus en plus du but souhaité.

Dans un premier temps, afin d'envoyer déjà A sur A', on utilise la translation t de vecteur $\overrightarrow{AA'}$:

$$\begin{array}{rcccc} t & : & A & \longmapsto & A' \\ & & B & \longmapsto & B''. \end{array}$$

On utilise ensuite la rotation ρ de centre A' et d'angle $\widehat{B''A'B'}$:

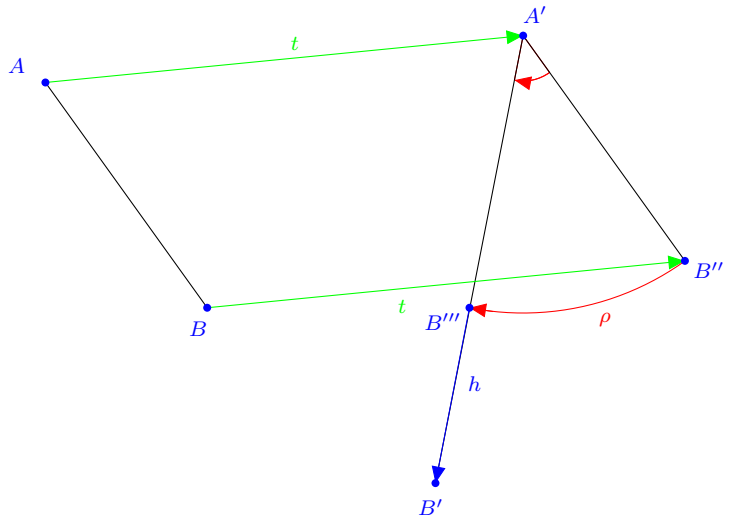
$$\begin{array}{rcccc} \rho & : & A' & \longmapsto & A' \\ & & B'' & \longmapsto & B'''. \end{array}$$

Comme par construction $B''' \in (A'B')$, on peut finalement utiliser l'homothétie h de centre A' et de rapport $A'B'/A'B'''$:

$$\begin{array}{rcccc} h & : & A' & \longmapsto & A' \\ & & B''' & \longmapsto & B'. \end{array}$$

□

Finalement, $S = h \circ \rho \circ t$ convient par construction.



Remarquons que les homothéties ou les rotations peuvent également être définies comme les transformations conservant certaines grandeurs ou propriétés. Cependant, la définition usuelle avec le centre est plus explicite et plus utilisable dans les exercices. On va donc s'intéresser à la notion de centre chez les similarités.

Définition 28. On appelle centre d'une similarité un point fixe de cette similarité.

Exemple 29. Une translation de vecteur non nul n'a aucun centre, une rotation ou une homothétie en a un et la transformation identité admet tous les points du plan comme centre.

Remarques 30.
— L'unicité du théorème précédent appliquée au cas $A = A'$ et $B = B'$ montre que, hormis l'identité, toute similarité a au plus un point fixe.
— Il n'est pas évident a priori que toute similarité a un centre. Cela découle du théorème suivant.

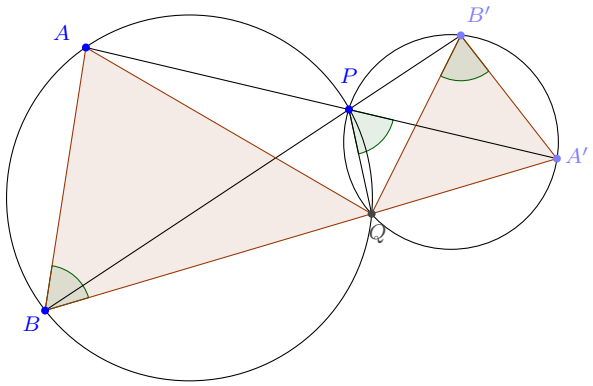
Le théorème suivant, essentiel, montre que l'on connaît bien le centre d'une similitude :

Théoréme 31. Soit A, B, A' et B' supposés en position générale (un couple ne peut être obtenu à partir de l'autre par translation ou homothétie). Soit P le point d'intersection de (AA') et (BB'). Soit $\mathcal{C}_1$ et $\mathcal{C}_2$ les cercles circonscrits à PAB et $PA'B'$ et Q leur deuxième point d'intersection.

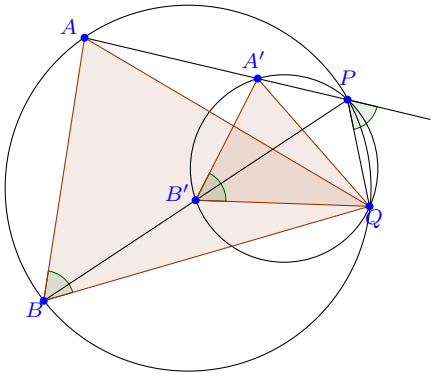
Alors, Q est le centre de la similitude envoyant A et B sur A' et B'.

Démonstration. Soit s l'unique similitude envoyant A et B sur A' et B'. On cherche à montrer que s envoie Q sur lui-même. D'après la démonstration de l'unicité de cette similitude, il suffit de vérifier que ABQ et $A'B'Q$ sont directement semblables. On procède par chasse aux angles. Il suffit de montrer que $\widehat{ABQ} = \widehat{A'B'Q}$, l'égalité $\widehat{BAQ} = \widehat{B'A'Q}$ se montrant de manière similaire :

$\widehat{ABQ} = 180° - \widehat{APQ} = \widehat{A'PQ} = \widehat{A'B'Q}$. □



Remarques 32.
— Si les points ne sont pas en position générale, la construction marche toujours en considérant que deux droites parallèles se coupent « à l'infini » et que le cercle passant par A, B et l'infini n'est autre que la droite (AB).
— Bien sûr, il faudrait écrire cette démonstration en termes d'angles orientés. Ce que le lecteur pointilleux est invité à faire. Il est d'ailleurs important de se familiariser avec les deux configurations :



On remarque de plus en utilisant les triangles semblables de la démonstration précédente que la composée d'une rotation d'angle $\widehat{AQA'} = \widehat{BQB'}$ et d'une homothétie de rapport $QA'/QA = QB'/QB$, toutes deux de centre Q, envoie A sur A' et B sur B'.

Définition 33. Une similitude directe de centre Q est la composée d'une rotation de centre Q et d'une homothétie de centre Q. Elle est caractérisée par son angle de rotation et son facteur de dilatation.

Grâce à l'unicité dans le théorème 27 on a donc le théorème important suivant :

Théoréme 34. Toute similarité est soit une translation soit une similitude directe.

Remarque 35. À ce stade, on peut se demander pourquoi on n'a pas commencé le cours en

donnant la définition 33, ce qui nous aurait épargné le besoin de prouver le théorème 34. Un avantage de la définition 25 est qu'elle rend trivial le fait que la composée de deux similitudes directes est une similitude directe, ce qui n'est pas évident avec 33.

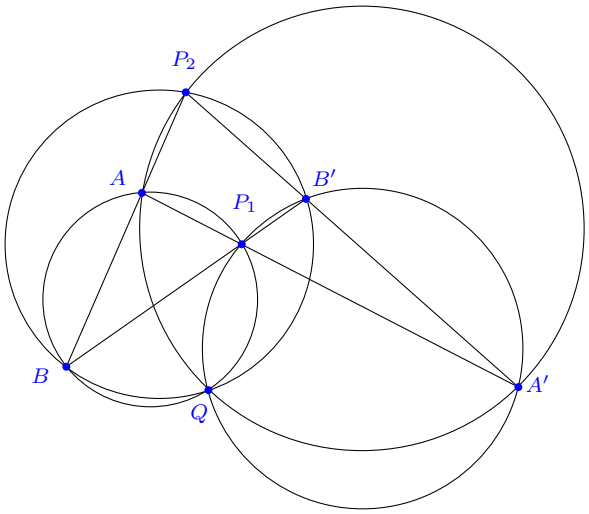
De plus, on voit toujours dans la même figure grâce aux mêmes triangles semblables que la similitude directe de centre Q, d'angle $\widehat{AQB} = \widehat{A'QB'}$ et de rapport $QB/QA = QB'/QA'$ envoie A sur B et A' sur B'. En laissant au lecteur le cas particulier des homothéties, on obtient le théorème important suivant :

Théoréme 36. Si une similitude directe envoie A sur A' et B sur B', alors la similitude envoyant A sur B et A' sur B' a même centre.

En appliquant le théorème 31 aux deux similitudes précédentes, on obtient le résultat bien connu suivant, qui (pour l'intersection des cercles) se démontre également par chasse aux angles (exercice !) :

Théoréme 37. Soit A, B, A' et B' en position générale. Soit $P_1 = (AA') \cap (BB')$ et $P_2 = (AB) \cap (A'B')$. Alors les cercles circonscrits à P_1AB, $P_1A'B'$, P_2AA' et P_2BB' sont concourants en un point Q, appelé point de Miquel du quadrilatère complet $AA'BB'$.

Il est le centre de la similitude directe envoyant A sur A' et B sur B' ainsi que de celle envoyant A sur B et A' sur B'.



Remarque 38. On considérera essentiellement ce point comme centre des similitudes directes précédentes. Mais il est également d'une importance primordiale en géométrie projective unidimensionnelle complexe en tant que centre de l'involution échangeant les 6 sommets du quadrilatère complet (pour comprendre la phrase précédente ... allez au club de mathématiques discrètes de Lyon !).

Remarque 39. Il peut souvent être intéressant de regarder les similitudes d'un point de vue complexe : il s'agit en fait juste des fonctions affines.

Terminons ce cours par un mot sur les similitudes indirectes :

Définition 40. Un similitude indirecte est une transformation du plan qui envoie chaque

angle orienté sur son opposé.

Exemple 41. Les symétries axiales sont des similitudes indirectes. La composée d'une symétrie axiale avec une similitude directe est une similitude indirecte.

Les similitudes indirectes conservent de nombreuses propriétés : rapports de longueur, angles non orientés, alignement, cocyclicité, parallélisme, orthogonalité... Elles sont cependant moins intéressantes que les similitudes directes car beaucoup n'admettent pas de centre (considérer par exemple la composée d'une symétrie axiale et d'une translation parallèle à son axe). Les puissants théorèmes 31 et 36 n'ont donc pas d'analogue pour les similitudes indirectes.

- Conseils pour les exercices : -

Voici quelques conseils généraux qui peuvent servir dans les exercices qui suivent et dans bien d'autres :

— Les exercices où un point varie et où on cherche à déterminer le lieu d'un autre point ou bien à montrer qu'un autre point reste fixe font souvent appel à des transformations.
— N'oubliez pas la chasse aux angles, qui permet souvent de « démarrer » un exercice, par exemple en trouvant deux triangles semblables.
— Quand vous trouvez deux triangles semblables (éventuellement plats), intéressez-vous à la similitude qui envoie l'un sur l'autre : existe-t-il d'autres points dont on connaît bien l'image ? Si la similitude est directe, peut-on trouver son centre ?
— L'apparition des figures du théorème 31 doit donner envie d'introduire des similitudes !
— Quand cette figure apparaît, n'oubliez pas que vous avez en fait trouvé deux similitudes directes intéressantes de même centre : celle qui envoie A sur A' et B sur B', et celle qui envoie A sur B et A' sur B'. Essayez les deux et utilisez celle qui paraît la plus utile.

- Exercices -

Dans tous les exercices, les points sont ou ne sont pas supposés en position générale (à la discrétion du lecteur pointilleux !). Face à un exercice où les points ne sont pas en position générale mais où les techniques de ce cours semblent prometteuses, une bonne stratégie est de dire que, par un argument de continuité (en considérant les points de l'exercice comme des fonctions continues quand écrits en analytique), on peut les supposer en position générale.

Exercice 1 Soit $ABCD$ un quadrilatère, E et F sur $[AD]$ et $[BC]$ respectivement tels que $AE/ED = BF/FC$. Soit $S = (EF) \cap (AB)$ et $T = (EF) \cap (CD)$.

Montrer que les cercles circonscrits aux triangles SAE, SBF, TCF et TDE sont concourants.

Exercice 2 Soient Γ_1 et Γ_2 deux cercles qui se coupent en deux points A et D. La tangente à Γ_1 en A recoupe Γ_2 en B, et la tangente à Γ_2 en A recoupe Γ_1 en C. Soit $E \in [AB)$ tel que $BE = AB$, et F la deuxième intersection de $[AC)$ avec le cercle circonscrit Ω à ADE. Montrer que $AC = AF$.

Exercice 3 Soit $ABCD$ un quadrilatère avec $AD = BC$ et P l'intersection de ses diagonales. Soit F et E des points variables sur les segments $[AD]$ et $[BC]$ respectivement de manière

à avoir $BE = DF$. On pose R et Q les points d'intersections de (EF) avec (AC) et (BD) respectivement.

Montrer que le cercle circonscrit à PQR a un deuxième point fixe quand E et F varient.

Exercice 4 Soit ABC un triangle inscrit dans un cercle Γ, P un point variable sur le l'arc AB qui ne contient pas C. Soient I et J les centres des cercles inscrits des triangles ACP et BCP respectivement. On considère Q le point d'intersection de Γ et du cercle circonscrit au triangle PIJ.

Montrer que Q reste fixe quand P varie.

Exercice 5 Soit Γ_1 et Γ_2 deux cercles s'intersectant en P et Q. Soit A_1 et B_1 deux points variables sur Γ_1 et A_2 et B_2 les deuxièmes points d'intersection de Γ_2 avec (A_1P) et (B_1P) respectivement. Soit $C = (A_1B_1) \cap (A_2B_2)$.

Montrer que le centre O du cercle circonscrit au triangle CA_1A_2 reste sur un cercle fixe quand A_1 et A_2 varient.

L'exercice suivant est important et souvent utilisé (il faut par contre penser à le redémontrer... ou citer ce poly !).

Exercice 6 Soit $ABCD$ un quadrilatère convexe inscrit dans un cercle de centre O, P le point d'intersection des diagonales et Q le deuxième point d'intersection des cercles circonscrits aux triangles APD et BPC.

Montrer que $\widehat{OQP} = 90°$.

Exercice 7

a) Soit T une similitude directe. Montrer qu'il existe une similitude directe de même centre envoyant tout point M sur le milieu de M et $T(M)$.

b) Soit $ABCD$ un quadrilatère, M et N les milieux de ses diagonales et P leur intersection. Soit O_1 et O_2 les centres des cercles circonscrits de ABP et CDP. Montrer que le milieu du segment $[O_1O_2]$ est le centre du cercle circonscrit de PMN.

Exercice 8 Soient Γ_1 et Γ_2 deux cercles se coupant en deux points A et B. Les tangentes à Γ_1 en A et B se coupent en K. Soit M un point variable sur Γ_1, distinct de A et B. On note P le second point d'intersection de (MA) et Γ_2, C le second point d'intersection de (MK) et Γ_1 et Q le second point d'intersection de (AC) avec Γ_2.

a) Montrer que (PQ) passe par un point fixe quand M varie.

b) Montrer que le milieu de $[PQ]$ est sur la droite (MK).

Exercice 9 Soit ABC un triangle, E et D des points sur les côtés $[AB]$ et $[AC]$ de manière à avoir $BE = CD$. Soit P l'intersection des diagonales du quadrilatère $BEDC$ et Q le deuxième point d'intersection des cercles circonscrits à EPB et DPC. Soit K et L les milieux respectifs de $[BE]$ et $[CD]$ et R le point d'intersection de la perpendiculaire à (QK) passant par K et de la perpendiculaire à (QL) passant par L.

Montrer que :

a) Q est sur la bissectrice de l'angle $\widehat{BAC}$.

b) R est sur le cercle circonscrit au triangle ABC.

Exercice 10 (BMO 2009) Soit ABC un triangle. Une droite parallèle à (BC) coupe $[AB]$ en M et $[AC]$ en N. Soit P le point d'intersection de (BN) et (CM). Les cercles circonscrits à BMP et CNP se recoupent en Q.

Montrer que $\widehat{PAB} = \widehat{QAC}$.

Exercice 11 Soit ABC un triangle et Γ son cercle circonscrit. On considère trois points A_1, B_1 et C_1 sur les côtés $[BC]$, $[CA]$ et $[AB]$ respectivement. On note A_3, B_3 et C_3 les symétriques de A_1, B_1 et C_1 par rapport aux milieux de leurs côtés respectifs. On note A_2, B_2 et C_2 les deuxièmes points d'intersection de Γ avec les cercles circonscrits à AB_1C_1, BC_1A_1 et CA_1B_1 respectivement.

Montrer que les triangles $A_2B_2C_2$ et $A_3B_3C_3$ sont semblables.

On peut également trouver un type d'exercice légèrement différent à propos du point de Miquel et des similitudes : une figure ou apparaît de manière évidente une similitude directe particulière et son centre. Le théorème 37 permet alors de trouver des points cocycliques.

Exercice 12 Soit $ABCDE$ un pentagone convexe vérifiant les relations $\widehat{BAC} = \widehat{CAD} = \widehat{DAE}$ et $\widehat{CBA} = \widehat{DCA} = \widehat{EDA}$. Soit $P = (BD) \cap (CE)$.

Montrer que la droite (AP) coupe le segment $[CD]$ en son milieu.

Exercice 13 Soit $ABCDEF$ un hexagone inscriptible vérifiant $AB = CD = EF$. Soit $Z = (AC) \cap (BD)$, $X = (CE) \cap (DF)$ et $Y = (EA) \cap (FB)$.

Montrer que XYZ et BDF sont semblables.

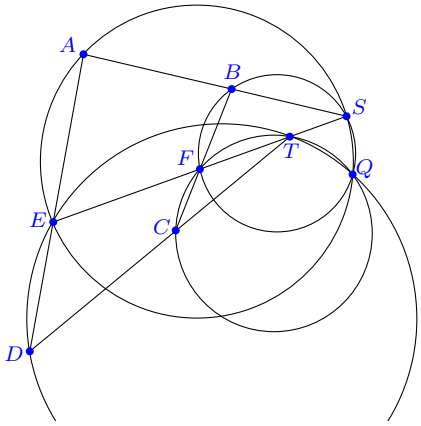
Enfin, comme pour les autres transformations (translation, homothéties, rotations...), il est intéressant de considérer ce que donne la composition de similitudes directes. Afin d'inviter le lecteur curieux à explorer ce champ de possibilités, je conclus sur un exercice dans cette direction.

Exercice 14 Soit Γ_1, Γ_2 et Γ_3 trois cercles avec $\{A, B\} = \Gamma_1 \cap \Gamma_2$, $\{C, D\} = \Gamma_2 \cap \Gamma_3$ et $\{E, F\} = \Gamma_3 \cap \Gamma_1$. On considère P_1 sur Γ_1 et on note P_2 le deuxième point d'intersection de (P_1A) et Γ_2, P_3 le deuxième d'intersection de (P_3C) et Γ_3, P_4 le deuxième point d'intersection de (P_3E) et Γ_1, P_5 le deuxième point d'intersection de (P_4B) et Γ_2, P_6 le deuxième point d'intersection de (P_5D) et Γ_3 et enfin P_7 le deuxième point d'intersection de (P_6F) et Γ_1.

Montrer que $P_7 = P_1$.

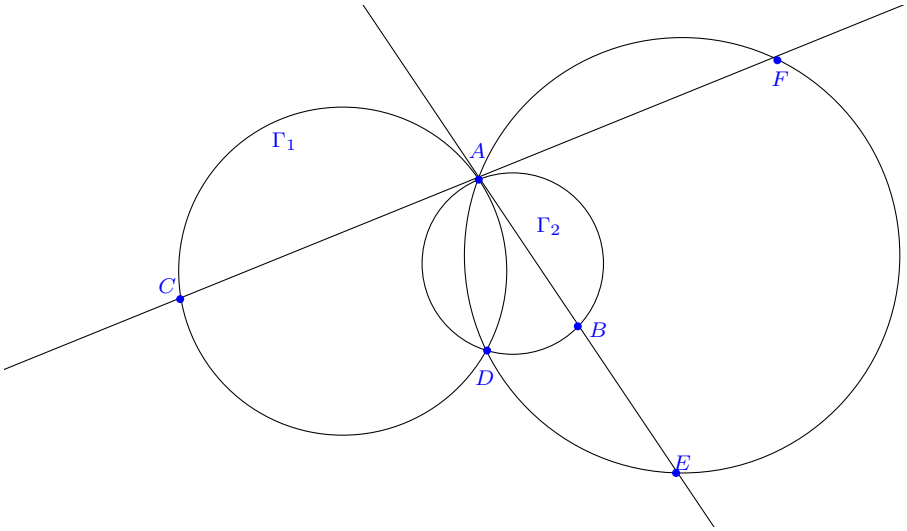
- Solutions -

Solution de l'exercice 1



D'après l'égalité sur les rapports de longueur, la similitude directe envoyant A sur B et D sur C envoie également E sur F. En utilisant le théorème 37 pour les couples de points $(E, D) \mapsto (F, C)$, on obtient que son centre est sur les cercles circonscrits à TCF et TDE. En l'utilisant sur les couples de points $(A, E) \mapsto (B, F)$, ce centre est également sur les cercles circonscrits à SAE et SBF. D'où la conclusion.

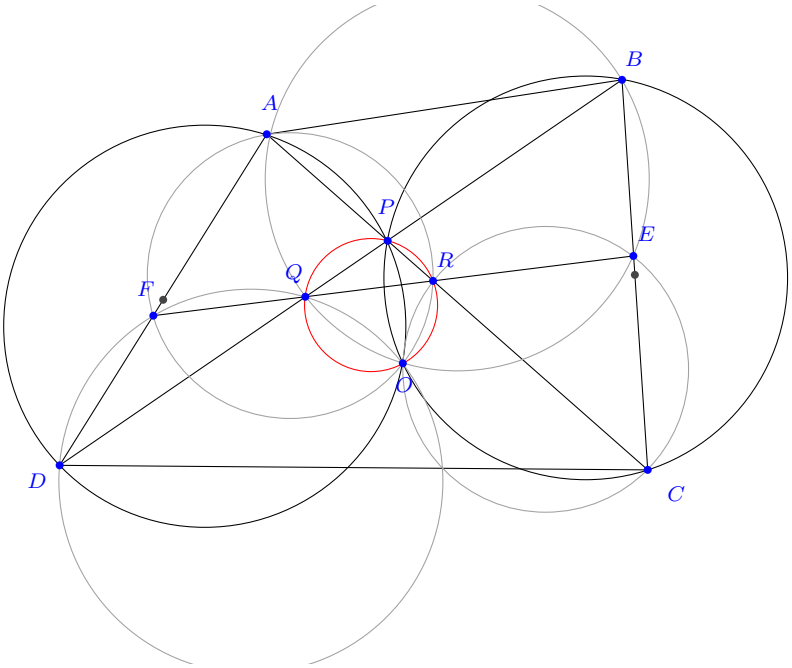
Solution de l'exercice 2



D'après la construction du centre d'une similitude appliquée aux cercles Γ_1 et Γ_2, D est le centre de la similitude directe s_1 qui envoie C sur A et A sur B. En regardant les cercles Γ_1 et Ω, D est le centre de la similitude directe qui envoie C sur F et A sur E, donc le centre de la similitude directe s_2 qui envoie C sur A et F sur E.

Or, comme il existe une unique similitude directe de centre D qui envoie C sur A (car le rapport est forcément $\frac{DA}{DC}$ et l'angle forcément $\widehat{ADC}$), on a $s_1 = s_2$, donc on a une similitude qui envoie C sur A, A sur B et F sur E. Comme B est le milieu de $[AE]$, on en déduit que A est le milieu de $[CF]$.

Solution de l'exercice 3

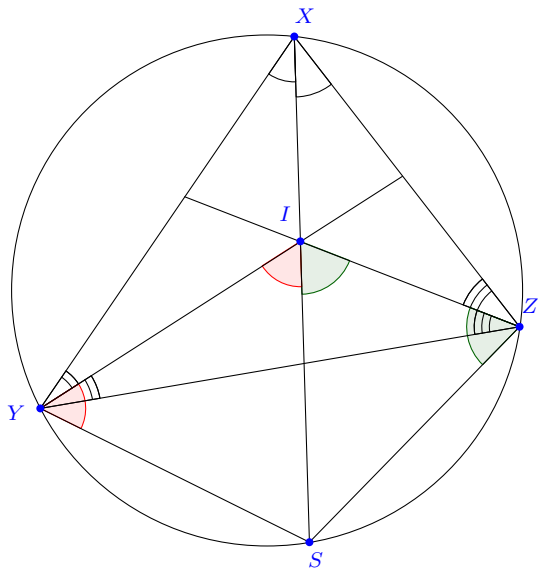


Il existe clairement en utilisant les égalités de longueur une similitude envoyant les points A, F et D sur les points C, E et B respectivement.

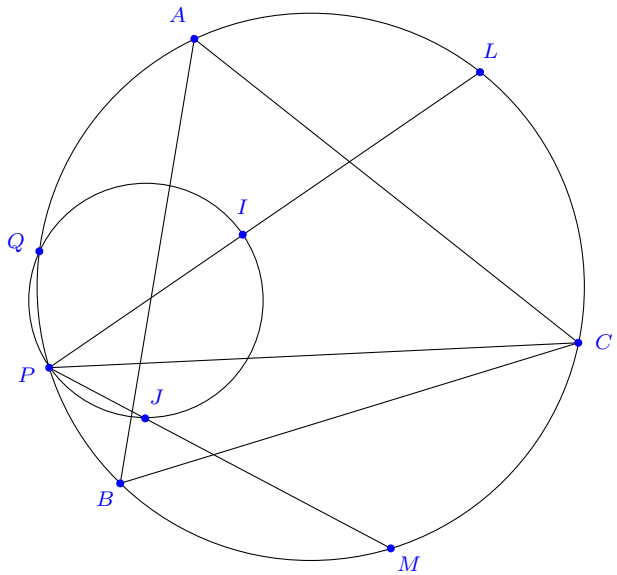
Il est naturel d'introduire son centre O et quelques dessins peuvent nous convaincre que c'est vraisemblablement le point recherché. En utilisant successivement le théorème principal pour les couples $(A, F) \mapsto (C, E)$, $(F, D) \mapsto (E, B)$ et $(D, A) \mapsto (B, C)$, on sait que O est sur le cercle circonscrit aux triangles ARF, ERC, FQD, BQE, APD et BPC. En particulier (en utilisant les deux derniers triangles), il est fixe. Il est donc suffisant (et probablement raisonnablement aisé au vu de tous les autres cercles...) de démontrer que O, P Q et R sont cocycliques.

Or, le théorème de Miquel appliqué au quadrilatère $AFPQ$ prouve qu'il suffit de démontrer que O est sur le cercle circonscrit à ARF, DPA et DFQ. D'où la conclusion.

Solution de l'exercice 4 On rappelle le théorème du pôle Sud, visiblement pertinent dans cet exercice et démontrable grâce à une chasse aux angles élementaire (exercice !).



Si XYZ est un triangle inscrit dans un cercle $\mathcal{C}$, I son centre du cercle inscrit et S le deuxième point d'intersection de (XI) avec $\mathcal{C}$. Alors, S est le milieu de l'arc YZ et, plus précisément, $SY = SI = SZ$.

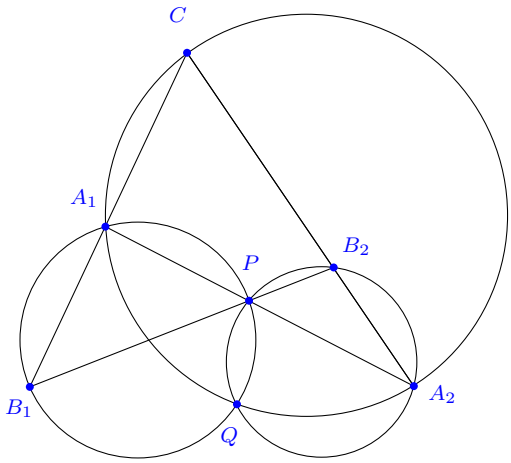


On est dans la situation classique avec deux cercles qui s'intersectent, on connaît bien un des points d'intersection et c'est l'autre qui nous intésse. On cherche donc à compléter le quadrilatère. De manière naturelle, on introduit donc les points fixes L et M, milieux respectifs des petits arcs AC et BC. D'après le théorème du pôle Sud, P, I et L ainsi que P, J et M sont alignés.

D'après le théorème 37, Q est le centre de la similitude S envoyant I sur J et L sur M. (Comme toujours se pose la question de quelle similitude choisir : pourquoi pas celle envoyant

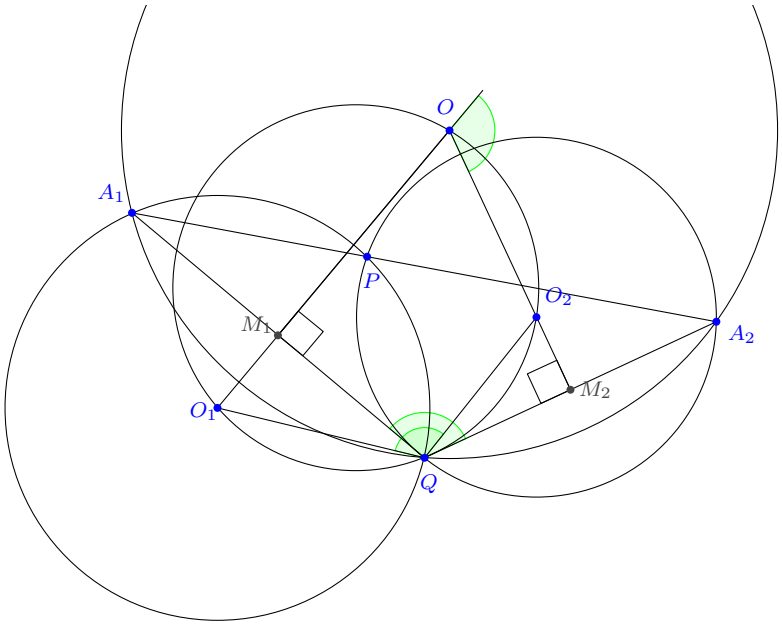
I sur L et J sur M ? Et comme souvent la réponse sera qu'on connaît mieux la première similitude parce que l'on maîtrise bien les longueurs impliquées.) Cette similitude envoyant le point fixe L sur le point fixe M, pour prouver qu'elle est fixe (et donc Q également), il suffit de montrer que son angle de rotation et son rapport de dilatation sont fixes (un petit dessin convaincra le lecteur sceptique...). Or, l'angle vaut $\widehat{LQM}$ qui est fixe d'après le théorème de l'angle inscrit et le rapport de dilatation vaut JM/IL qui vaut CM/CL d'après le théorème du pôle Sud, d'où la conclusion.

Solution de l'exercice 5



On voit qu'on est naturellement dans une situation du type théorème de Miquel dans le quadrilatère $A_1B_1A_2B_2$. En particulier, le cercle circonscrit à CA_1A_2 passe par Q.

Cette remarque est positive pour de nombreuses raisons : on se rend compte que les points B_1 et B_2 sont inutiles (O peut être défini comme le centre du cercle circonscrit à A_1QA_2), ce qui permet de simplifier la figure et de perdre un degré de liberté.



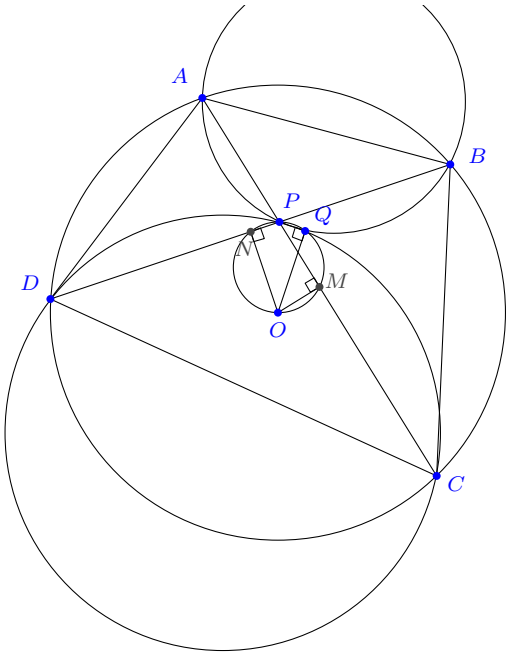
La question naturelle est maintenant : quel va être ce cercle que parcourra O ? Le plus simple est de considérer les cas limites : quand A_1 tend vers Q, A_2 et donc O également. Quand A_1 tend vers P, A_2 tend vers un point de Γ_2 et O devient donc le centre O_2 du cercle Γ_2. De même, quand A_2 tend vers P, O tend vers le centre O_1 de Γ_1.

On cherche donc à montrer que O, O_1, O_2 et Q sont cocycliques. Il faut naturellement travailler avec des angles orientés, mais on s'en passera (exercice...).

Notons M_1 et M_2 les milieux respectifs de $[A_1Q]$ et $[A_2Q]$. En utilisant les angles droits dus aux médiatrices, M_1, O, M_2 et Q sont cocycliques, d'où $\widehat{O_1OO_2} = 180° - \widehat{A_1QA_2}$.

Or, la similitude de centre Q qui envoie A_1 sur A_2 envoie O_1 sur O_2 (d'après par exemple le théorème 37 appliqué à $(A_1, B_1) \mapsto (A_2, B_2)$). D'où $\widehat{A_1QA_2} = \widehat{O_1QO_2}$, ce dont on déduit $\widehat{O_1OO_2} = 180° - \widehat{O_1QO_2}$, et la conclusion par le théorème de l'angle inscrit.

Solution de l'exercice 6 Il est naturel pour obtenir des angles droits de considérer les milieux M et N de $[AC]$ et $[BD]$.

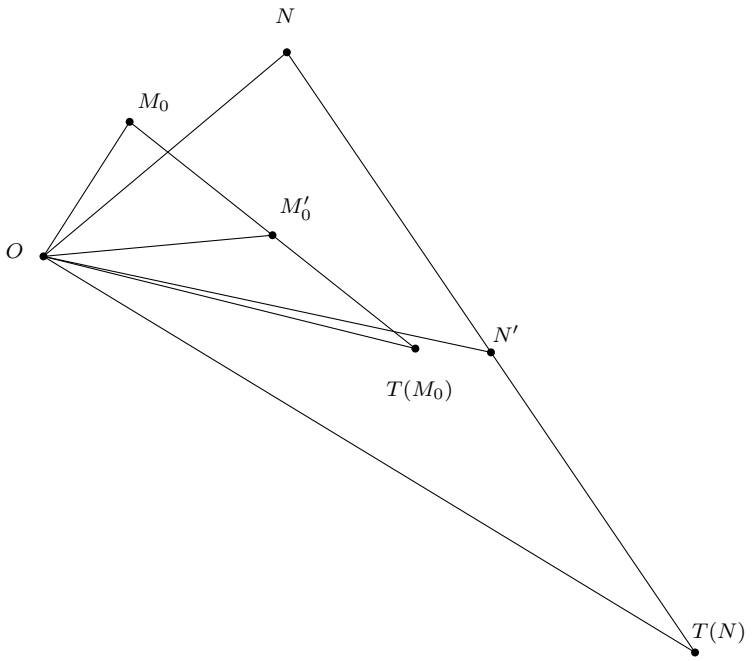


On considère la similitude de centre Q qui envoie A sur B et C sur D. Elle envoie le segment $[AC]$ sur le segment $[BD]$ et en particulier M sur N. En utilisant le théorème 37 avec les couples $(A, M) \mapsto (B, N)$, M, N, P et Q sont cocycliques. Or, en utilisant l'angle droit des médiatrices, il et clair que M, N, P et O sont cocycliques.

D'où finalement M, N, P, Q et O cocycliques et $\widehat{OQP} = 90°$ par le théorème de l'angle inscrit.

Solution de l'exercice 7

a)

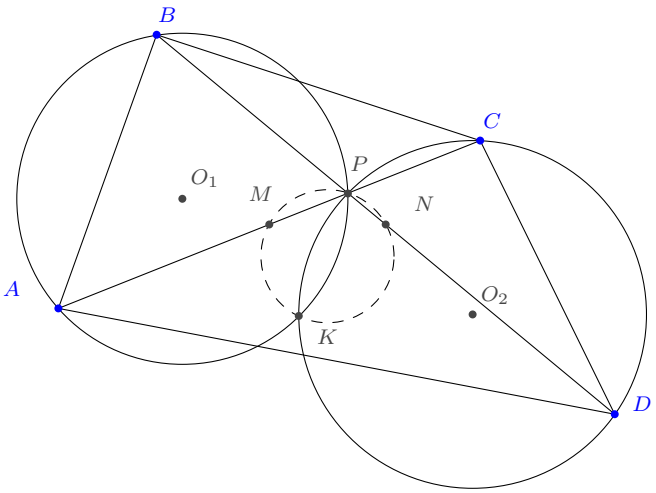


Soit O le centre de la similitude T. Pour un point M, notons M' le milieu de M et de $T(M)$. Fixons un point M_0 (différent de O) et considérons la similitude directe S

de centre O qui envoie M_0 sur M_0'. Soit N un autre point et montrons qu'elle envoie N sur N'. Les triangles $OM_0T(M_0)$ et $ONT(N)$ étant semblables, les triangles OM_0M_0' et ONN' sont semblables. Il existe donc une similitude directe de centre O notée S_2 envoyant M_0 sur M_0' et N sur N'. On en déduit que $S = S_2$, ce qui implique bien que S envoie N sur N'.

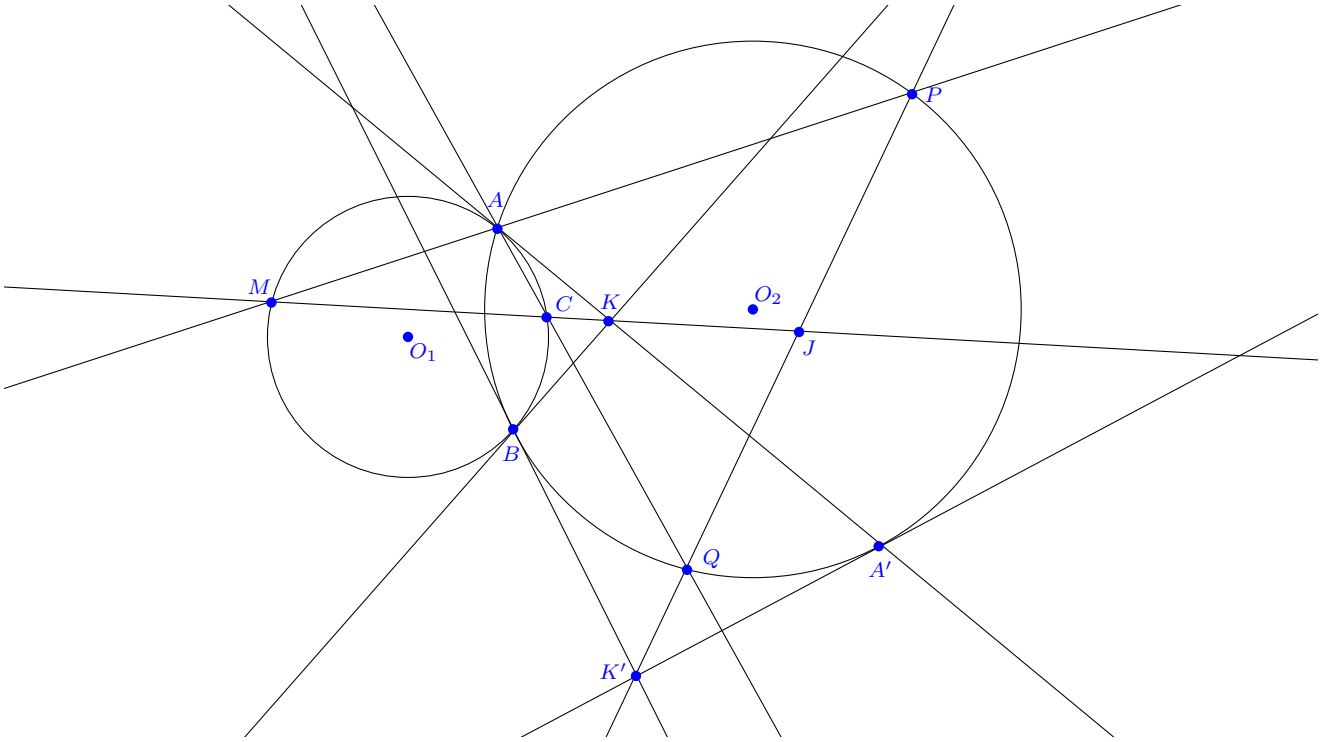
Remarque 42. Il est possible de résoudre facilement cette question en utilisant les nombres complexes. En effet, toute similitude directe f de centre O (où O est l'origine) est de la forme $f(z) = az$ avec a et z deux nombres complexes. Pour résoudre la question, il suffit donc de vérifier que $(z + f(z))/2$ est de cette forme. Comme $(z + f(z))/2 = (1 + a)/2 \cdot z$, $z \to (z + f(z))/2$ est une similitude directe de centre O qui vérifie les conditions de l'énoncé.

b) Soit K l'intersection des cercles circonscrits des triangles ABP et PCD.



On sait que K est le centre de la similitude directe T qui envoie $[AC]$ sur $[BD]$, et donc M sur N et O_1 sur O_2. On en déduit que M, P, N, K sont cocycliques. Considérons la nouvelle similitude S de centre K envoyant tout point U sur le milieu de $[UT(U)]$ (qui existe par (i)). Elle envoie donc A sur M, B sur N et K sur K. Elle envoie donc le cercle circonscrit de ABP sur le cercle passant par M, P, N, K. Comme O_1 est envoyé sur le milieu de $[O_1O_2]$, on en déduit que le milieu de $[O_1O_2]$ est le centre du cercle passant par M, P, N, K.

Solution de l'exercice 8



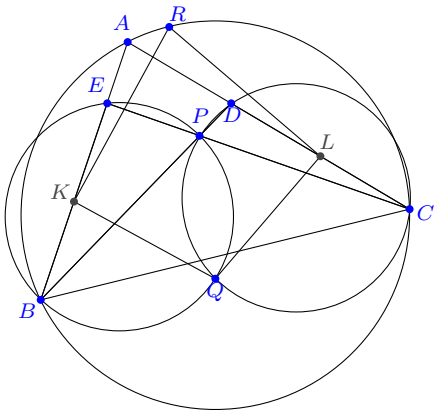
a) D'après la construction du centre d'une similitude, B est le centre d'une similitude directe s qui envoie M sur P, C sur Q, le cercle Γ_1 sur Γ_2. Par conséquent, s envoie (MC) sur (PQ) donc, comme (MC) passe par un point fixe K, (PQ) passe par $s(K)$, noté K'. De plus, on peut construire K' : c'est l'intersection des tangentes à Γ_2 en B et A', où $A' = s(A)$. Or, A' est la seconde intersection de Γ_2 avec la tangente à Γ_1 en A (cela correspond au cas limite de $s(M)$ quand M tend vers A).

b) On note O_1 et O_2 les centres des deux cercles, et J le milieu de $[PQ]$: les angles $\widehat{O_2JK'}$, $\widehat{O_2A'K'}$ et $\widehat{O_2BK'}$ sont droits donc O_2, K', A', B et J sont cocycliques sur le cercle de diamètre $[O'K']$. De plus, en utilisant que BAA' et BKK' sont semblables :

$$\widehat{K'KO_1} = \widehat{K'KB} + \widehat{BKO_1} = \widehat{A'AB} + \frac{1}{2}\widehat{BKA} = \frac{1}{2}\widehat{KAB} + \frac{1}{2}\widehat{BKA} = 90$$

donc K est aussi sur ce cercle.
On a donc $\widehat{BKJ} = 180 - \widehat{BK'J} = 180 - \widehat{BK'P} = 180 - \widehat{BKM}$ donc J, K et M sont alignés, d'où le résultat.

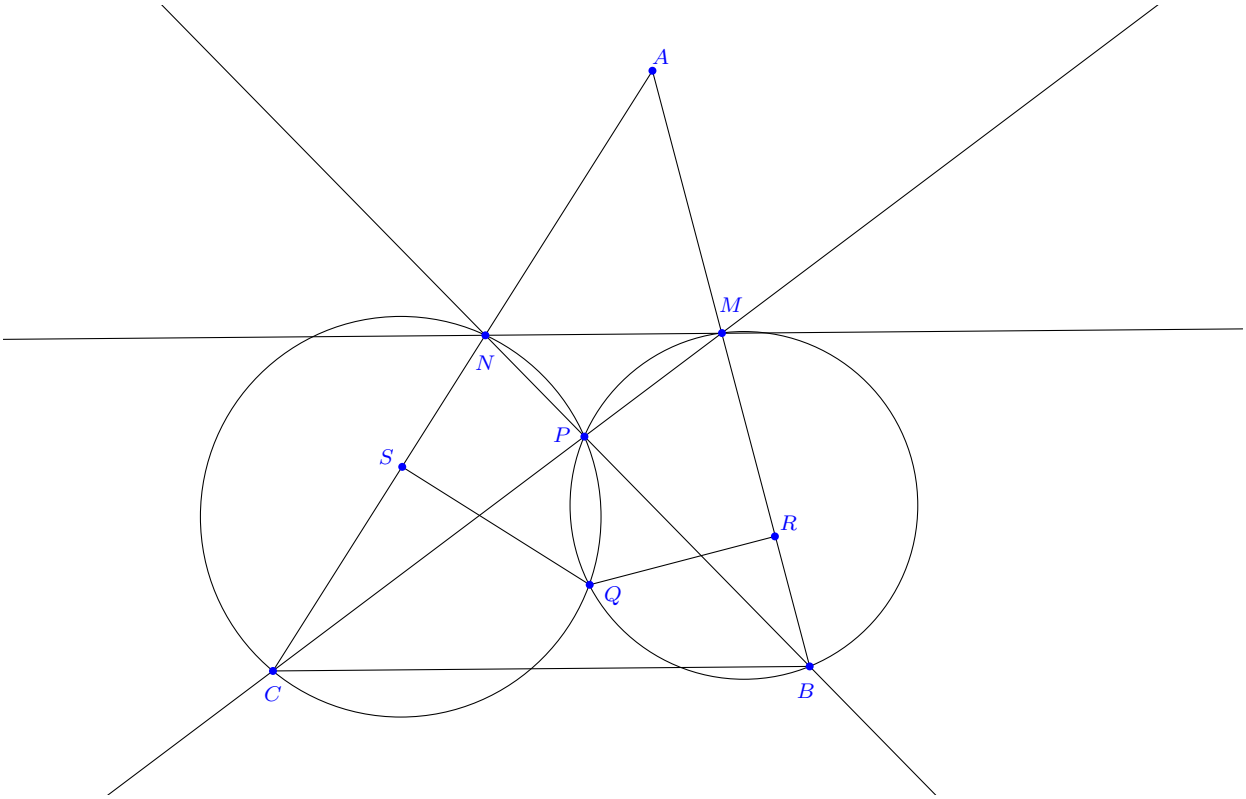
Solution de l'exercice 9



a) Q est le centre de la similitude ρ envoyant B sur D et E sur C. Comme $BE = CD$, son facteur de dilatation est 1 i.e. c'est une rotation. En particulier, en appelant Q_1 et Q_2 les projections de Q sur (AB) et (CD), comme ρ envoie Q_1 sur Q_2, $QQ_1 = QQ_2$, i.e. Q est sur la bissectrice (le lecteur attentif remarquera qu'il faut vérifier que c'est bien la bissectrice intérieure, ce qui se fait facilement par un argument de continuité en regardant le cas extrémal).

b) On remarque dans un premier temps que ρ envoie K sur L. En particulier, $QK = QL$, d'où également $RK = RL$ par Pythagore. De plus, l'angle de la rotation est $\widehat{KQL}$ mais est également, la droite (EB) étant envoyé sur la droite (CD), l'angle entre les droites (BA) et (CA). En particulier, A, K, Q et L sont cocycliques d'après le théorème de l'angle inscrit. Comme il est également clair que K, Q, L et R sont cocycliques, K, Q, L, A et R sont cocycliques.
Le but de l'exercice est donc de montrer que R est le centre de la similitude envoyant K sur L et B sur C. Soit R' le centre de cette similitude. R' comme R est sur le cercle circonscrit à KQL. De plus, comme $KB = LC$, cette similitude est une rotation, d'où, comme pour R, $R'K = R'L$. Ainsi, R et R' font partie des deux points d'intersection de la médiatrice de $[KL]$ et du cercle circonscrit à KAL et un argument fumeux de positionnement (le lecteur pointilleux remarquera que c'est formalisable sans trop de difficulté) montre que c'est en fait les mêmes. D'où la conclusion.

Solution de l'exercice 10



Commençons par nous occuper de P : d'après le théorème de Ceva et celui de Thalès, (AP) est une médiane de ABC, ce qui signifie que $\widehat{PAB}$ ne pourra pas s'exprimer de manière simple. On va donc utiliser de la trigonométrie.

On remarque que Q est le centre de la similitude directe s qui envoie B sur N et M sur C. Pour pouvoir faire des calculs trigonométriques sur $\widehat{QAB}$ et $\widehat{QAC}$, on introduit les projetés orthogonaux R et S de Q sur (AB) et (AC). On a $s(R) = S$ donc $\frac{QS}{QR}$ est égal au rapport de s, soit $\frac{NC}{BM} = \frac{AC}{AB}$ par Thalès. On en déduit $\frac{\sin \widehat{QAC}}{\sin \widehat{QAB}} = \frac{QS/QA}{QR/QA} = \frac{AC}{AB}$.

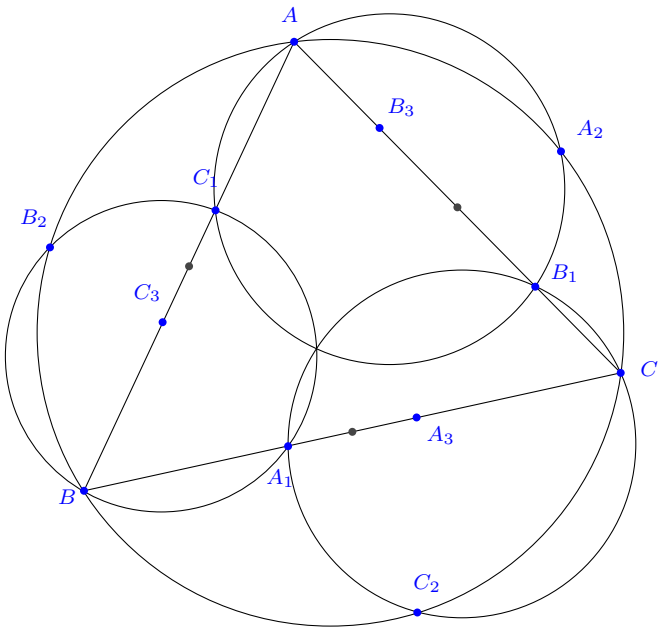
D'un autre côté, si M est le milieu de $[BC]$, on a en utilisant plusieurs fois la loi des sinus :

$$\frac{\sin \widehat{PAB}}{\sin \widehat{PAC}} = \frac{\sin \widehat{MAB}}{\sin \widehat{MAC}} = \frac{\frac{BM}{AM} \sin \widehat{ABM}}{\frac{CM}{AM} \sin \widehat{ACM}} = \frac{\sin \widehat{ABC}}{\sin \widehat{ACB}} = \frac{AC}{AB} = \frac{\sin \widehat{QAC}}{\sin \widehat{QAB}}$$

Autrement dit, $f(\widehat{PAB}) = f(\widehat{QAC})$ avec $f(x) = \frac{\sin x}{\sin(\widehat{BAC} - x)}$. On peut vérifier que cette fonction est strictement croissante, par exemple en la dérivant (exercice), d'où $\widehat{PAB} = \widehat{QAC}$.

Remarque 43. La trigonométrie est une méthode très puissante. Pour passer de formules sur des rapports de sinus (obtenues grâce à la loi des sinus et au théorème de Ceva trigonométrique) à des égalités d'angles, le fait que f soit strictement croissante est très utile et à retenir !

Solution de l'exercice 11



On a visiblement de nombreuses similitudes naturelles dans cette figure et qui dit similitudes dit triangles semblables. Après étude de quelques figures, il semble que l'on puisse montrer que $C_2AB \sim CB_3A_3$.

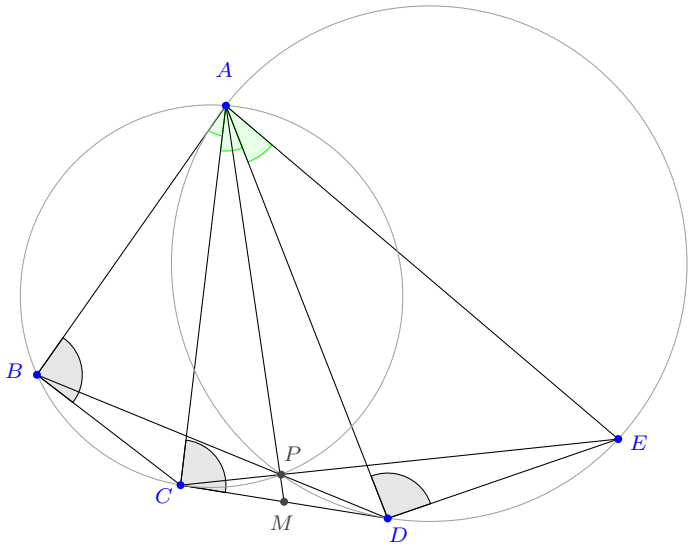
Effectivement, $\widehat{AC_2B} = \widehat{B_3CA_3}$ d'après le théorème de l'angle inscrit. Comme A_3 et B_3 sont plutôt défini en termes de longueur, on cherche également à démontrer que $CB_3/CA_3 = C_2A/C_2B$. Or, le rapport de dilatation de la similitude de centre C_2 envoyant B sur A et A_1 sur B_1 vaut selon la manière de le calculer C_2A/C_2B ou AB_1/BA_1 qui vaut exactement CB_3/CA_3. On a donc bien $C_2AB \sim CB_3A_3$. Cycliquement, on sait que $A_2BC \sim AC_3B_3$ et $B_2CA \sim BA_3C_3$.

On connaît maintenant très bien tous les angles. Philosophiquement, on sait donc qu'il suffit de faire une chasse aux angles. Effectivement :

$$\begin{aligned}\widehat{B_2A_2C_2} &= \widehat{B_2AC_2} = \widehat{BAC_2} + \widehat{B_2AC} - \widehat{BAC} \\ &= \widehat{A_3B_3C} + \widehat{BC_3A_3} - \widehat{BAC} = \widehat{B_3A_3C_3}.\end{aligned}$$

D'où la conclusion en raisonnant cycliquement.

Solution de l'exercice 12

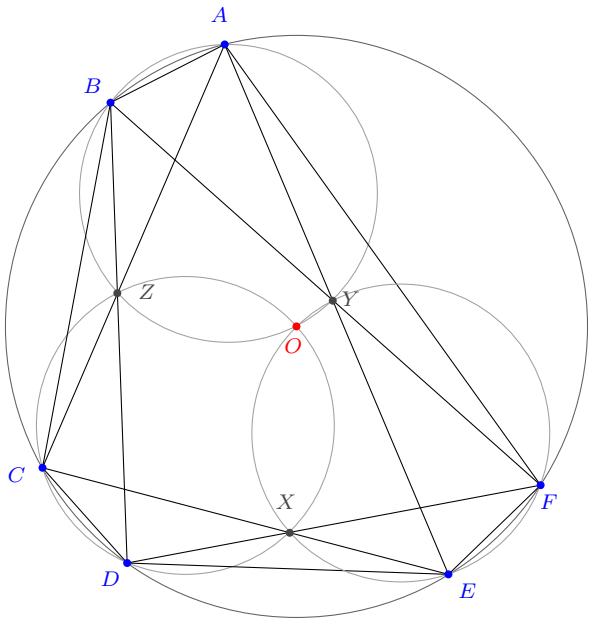


On se rend immédiatement compte qu'il existe une similitude de centre A qui envoie B sur C, C sur D puis D sur E.

Donc, d'après le théorème 37 appliqué au couple de point $(B, D) \mapsto (C, E)$, A est sur le cercle circonscrit Γ_1 à PBC et Γ_2 à PDE. Ici, l'exercice commence à avoir bien la tête d'un exercice utilisant la puissance d'un point. On essaye donc de montrer que Γ_1 est tangent à (CD). Or c'est vrai d'après la récriproque du théorème de l'angle inscrit comme $\widehat{ABC} = \widehat{DCA}$. De même, comme $\widehat{DEA} = 180° - \widehat{EAD} - \widehat{EDA} = 180° - \widehat{CAD} - \widehat{ACD} = \widehat{CDA}$, Γ_2 est également tangent à (CD).

Finalement, en notant $M = (AP) \cap (CD)$, M est sur l'axe radical de Γ_1 et Γ_2 et on peut donc écrire $MC^2 = \mathcal{P}_{\Gamma_1}(M) = \mathcal{P}_{\Gamma_2}(M) = MD^2$ et la conclusion.

Solution de l'exercice 13



On a clairement une rotation (donc une similitude) de centre le centre du cercle O qui envoie A sur B, C sur D et E sur F.

En utilisant le théorème 37 sur le couple $(A, C) \mapsto (B, D)$, A, B, Z et O sont cocycliques. Or, de même, en l'utilisant sur le couple $(A, E) \mapsto (B, F)$, A, B, Y et O sont cocycliques.

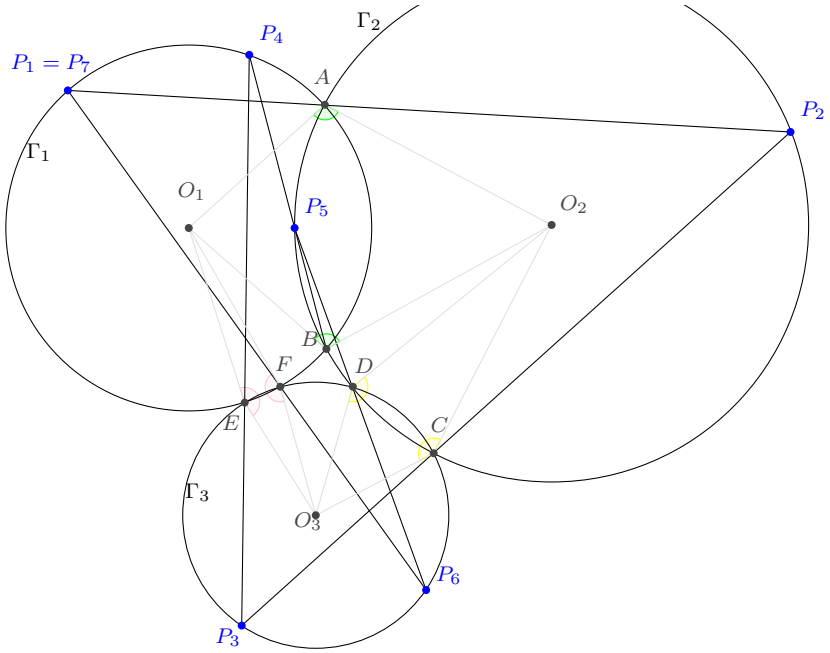
Ainsi, A, B, Z, O, Y sont cocycliques, et de la même manière également C, Z, O, X, D et E, X, O, Y, F.

Encore une fois, philosophiquement parlant, avec tant de cercles on connaît tous les angles, donc une simple chasse aux angles devrait suffire pour terminer. Effectivement :

$$\begin{aligned}
\widehat{ZXY} &= \widehat{ZXO} + \widehat{OXY} \\
&= \widehat{ODZ} + \widehat{OFY} \\
&= \widehat{ODB} + \widehat{OFB} \\
&= \widehat{OBD} + \widehat{OBF} \\
&= \widehat{DBF}.
\end{aligned}$$

On conclut cycliquement.

Solution de l'exercice 14



On considère ϕ_B la similitude de centre B qui envoie P_1 sur P_2 et Γ_1 sur Γ_2. De même, on considère ϕ_D la similitude de centre D qui envoie P_2 sur P_3 et Γ_2 sur Γ_3. on définit de manière similaire ϕ_F, ϕ_A, ϕ_C et ϕ_E.

On note $\Phi = \phi_F \circ \phi_D \circ \phi_B \circ \phi_E \circ \phi_C \circ \phi_A$. On a alors $P_7 = \Phi(P_1)$. Or, l'angle de rotation de Φ vaut $(AO_1, AO_2) + (CO_2, CO_3) + (EO_3, EO_1) + (BO_1, BO_2) + (DO_2, DO_3) + (FO_3, FO_1) = 0$ en éliminant les termes correspondants (voir figure). De même, le facteur de dilatation de Φ vaut $r_2/r_1 \cdot r_3/r_2 \cdot r_1/r_3 \cdot r_2/r_1 \cdot r_3/r_2 \cdot r_1/r_3 = 1$.

Φ est donc l'identité, d'où la conclusion.

3 mercredi 19 matin : Nicolas Ségarra

Pour tout ce cours, si ABC est un triangle, on note $a = BC$, $b = AC$, $c = AB$, $\widehat{A} = \widehat{BAC}$, $\widehat{B} = \widehat{ABC}$ et $\widehat{C} = \widehat{ACB}$. On note S l'aire de ABC, H son orthocentre, G son centre de gravité, I le centre de son cercle inscrit, O le centre de son cercle circonscrit et R le rayon de ce dernier.

I) Produit scalaire.

Rappels sur les vecteurs. Un vecteur du plan $\mathbb{R}^2$ est la donnée d'une direction, d'un sens et d'une longueur (norme). On note $\vec{0}$ le vecteur nul. La norme d'un vecteur est notée $||\vec{u}||$, c'est la longueur du vecteur $\vec{u}$. Deux points A et B du plan définissent un vecteur $\overrightarrow{AB}$. Si O est un point fixé du plan alors, à un vecteur $\vec{u}$, on peut associer de manière unique un point, noté $P_{\vec{u}}$ tel que $\overrightarrow{OP_{\vec{u}}} = \vec{u}$.

Si $(O, \vec{i}, \vec{j})$ est un repère (pas forcément orthogonal ni orthonormal) du plan, on dit que $\begin{pmatrix} x \\ y \end{pmatrix}$

(ou indifféremment (x, y)) sont les coordonnées du vecteur $\vec{u}$ si $\begin{pmatrix} x \\ y \end{pmatrix}$ sont les coordonnées du point $P_{\vec{u}}$ dans le repère $(O, \vec{i}, \vec{j})$. On note alors $\vec{u}\begin{pmatrix} x \\ y \end{pmatrix}$.
Dans le repère $(O, \vec{i}, \vec{j})$, si on a deux vecteurs $\vec{u}\begin{pmatrix} x \\ y \end{pmatrix}$ et $\vec{v}\begin{pmatrix} x' \\ y' \end{pmatrix}$ alors on note $\vec{u} + \vec{v}$ le vecteur de coordonnées $\begin{pmatrix} x + x' \\ y + y' \end{pmatrix}$ et pour tout réel λ, on note $\lambda.\vec{u}$ (ou indifféremment $\lambda\vec{u}$) le vecteur de coordonnées $\begin{pmatrix} \lambda x \\ \lambda y \end{pmatrix}$.
Pour tous points A et B du plan, on a $\overrightarrow{AB} = -\overrightarrow{BA}$ et pour tous points A, B, C du plan, on a : $\overrightarrow{AB} = \overrightarrow{AC} + \overrightarrow{CB}$ (relation de Chasles).

A partir de maintenant, on travaille dans un repère orthonormal du plan $(O, \vec{i}, \vec{j})$.

Définition du produit scalaire. Le produit scalaire de deux vecteurs $\vec{u}\begin{pmatrix} x \\ y \end{pmatrix}$ et $\vec{v}\begin{pmatrix} x' \\ y' \end{pmatrix}$ est le nombre réel noté $\vec{u}.\vec{v}$ (ou $< \vec{u}, \vec{v} >$) défini par : $\vec{u}.\vec{v} = xx' + yy'$.

Conséquences. (1) Pour tout nombre réel λ, $(\lambda\vec{u}).\vec{v} = \vec{u}.(\lambda\vec{v}) = \lambda(\vec{u}.\vec{v})$. Pour cette raison, on note ce nombre $\lambda\vec{u}.\vec{v}$.
(2) Pour tous vecteurs $\vec{u}$, $\vec{v}$ et $\vec{w}$, on a : $\vec{u}.\vec{v} = \vec{v}.\vec{u}$ et $(\vec{u} + \vec{v}).\vec{w} = \vec{u}.\vec{w} + \vec{v}.\vec{w}$.
(3) Pour tout vecteur $\vec{u}\begin{pmatrix} x \\ y \end{pmatrix}$, $\vec{u}.\vec{u} = x^2 + y^2 = ||\vec{u}||^2$. On écrit souvent $\vec{u}^2$ pour désigner ce nombre. (On appelle cela : carré scalaire de $\vec{u}$).
(4) Si $\vec{u}$ ou $\vec{v}$ est nul alors $\vec{u}.\vec{v} = 0$. Attention, la réciproque est fausse : considérer les vecteurs $\vec{u}\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ et $\vec{v}\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ par exemple.
(5) Si $\vec{u} = \lambda\vec{v}$ avec $\lambda \in \mathbb{R}$, on a : $\vec{u}.\vec{v} = \lambda||\vec{v}||^2$.

Remarque. On utilisera souvent la 3ème conséquence pour écrire : $\overrightarrow{AB}^2 = \overrightarrow{AB}.\overrightarrow{AB}$ et pour pouvoir utiliser le calcul vectoriel (notamment la relation de Chasles).

Théorème : autres expressions du produit scalaire. Soient $\vec{u}$ et $\vec{v}$ deux vecteurs. On a :
(1) $\vec{u}.\vec{v} = \dfrac{1}{2}\left(||\vec{u} + \vec{v}||^2 - ||\vec{u}||^2 - ||\vec{v}||^2\right)$.
(2) Lorsque $\vec{u}$ et $\vec{v}$ sont non nuls, $\vec{u}.\vec{v} = ||\vec{u}||.||\vec{v}||.\cos(\vec{u}, \vec{v})$, où $(\vec{u}, \vec{v})$ est l'angle orienté entre les vecteurs $\vec{u}$ et $\vec{v}$.

Une conséquence importante de l'assertion (1) est que le produit scalaire ne dépend pas de la base orthonormée choisie.

Démonstration. Pour (1), écrivons :
$||\vec{u} + \vec{v}||^2 = (\vec{u} + \vec{v}).(\vec{u} + \vec{v}) = \vec{u}.\vec{u} + \vec{v}.\vec{v} + 2\vec{u}.\vec{v} = ||\vec{u}||^2 + ||\vec{v}||^2 + 2\vec{u}.\vec{v}$. Le résultat en découle.
Pour (2), plaçons-nous dans le repère orthonormé direct $(O, \vec{i}, \vec{j})$ où $\vec{i} = \dfrac{\vec{u}}{||\vec{u}||}$ (on a vu que (1)

implique que le produit scalaire ne dépend pas de la base orthonormée choisie). Alors, en notant $\alpha = (\vec{u}, \vec{v})$, on a : $\vec{u}\begin{pmatrix} ||\vec{u}|| \\ 0 \end{pmatrix}$ et $\vec{v}\begin{pmatrix} ||\vec{v}||\cos(\alpha) \\ ||\vec{v}||\sin(\alpha) \end{pmatrix}$. Ainsi, $\vec{u}.\vec{v} = ||\vec{u}||.||\vec{v}||.\cos(\alpha)$ d'où le résultat.

Remarque. L'intérêt du théorème précédent est d'exprimer le produit scalaire de manière « purement géométrique », c'est-à-dire sans faire intervenir les coordonnées.

Propriétés. Soient $\vec{u}$ et $\vec{v}$ deux vecteurs. On a :
(1) $(\vec{u} - \vec{v})^2 = \vec{u}^2 - 2\vec{u}.\vec{v} + \vec{v}^2$.
(2) $(\vec{u} + \vec{v})(\vec{u} - \vec{v}) = \vec{u}^2 - \vec{v}^2$.

Preuve. Laissée en exercice.

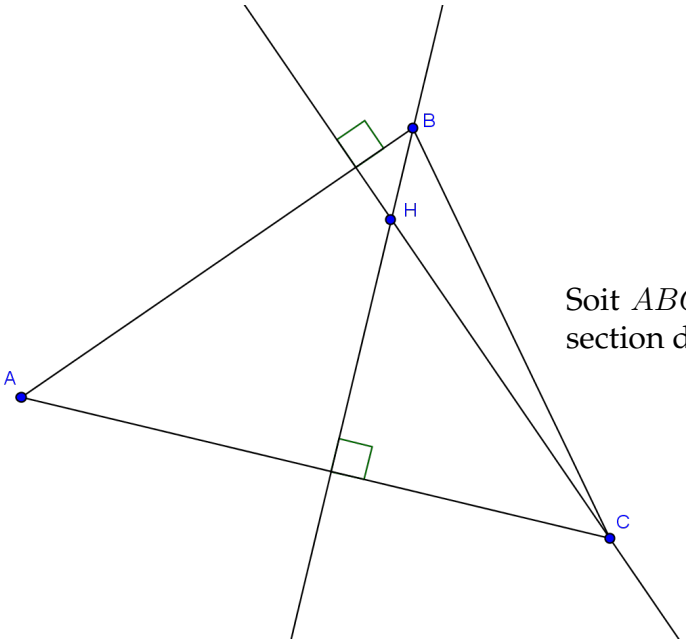
Théorème. Deux vecteurs $\vec{u}$ et $\vec{v}$ sont orthogonaux si et seulement si $\vec{u}.\vec{v} = 0$.

Démonstration. D'après le théorème de Pythagore, $\vec{u}$ et $\vec{u}$ sont orthogonaux si et seulement si $||\vec{u} + \vec{v}||^2 = ||\vec{u}||^2 + ||\vec{v}||^2$. D'après le théorème précédent, cela équivaut à $\vec{u}.\vec{v} = 0$.
Propriété. Soient A, B, C, D des points du plan avec $A \neq B$ et $C \neq D$. Les droites (AB) et (CD) sont perpendiculaires si et seulement si $AC^2 + BD^2 = AD^2 + BC^2$.

Démonstration. On a : $AC^2 + BD^2 - AD^2 - BC^2 = (\overrightarrow{AB} + \overrightarrow{BC})^2 + (\overrightarrow{BA} + \overrightarrow{AD})^2 - AD^2 - BC^2 = 2\overrightarrow{AB}.\overrightarrow{AB} + 2\overrightarrow{AB}.\overrightarrow{BC} + 2\overrightarrow{BA}.\overrightarrow{AD} = 2\overrightarrow{AB}.(\overrightarrow{AB} + \overrightarrow{BC} - \overrightarrow{AD}) = 2\overrightarrow{AB}.\overrightarrow{DC}$. Ainsi, les droites (AB) et (CD) sont perpendiculaires si et seulement si $\overrightarrow{AB}.\overrightarrow{DC} = 0$, ce qui équivaut à $AC^2 + BD^2 - AD^2 - BC^2 = 0$: ce qui permet de conclure.

Exercice 1. A l'aide du produit scalaire, démontrer que les trois hauteurs d'un triangle sont concourantes.

Solution de l'exercice 1.



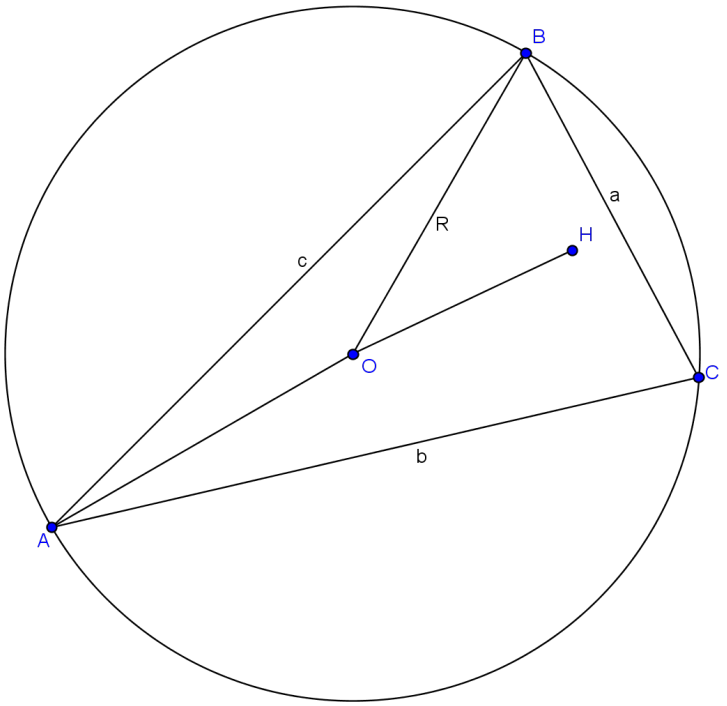
Soit ABC un triangle. Soit H le point d'intersection des hauteurs issues des points B et C.

Montrons que $\overrightarrow{AH}.\overrightarrow{BC} = 0$. On sait que $\overrightarrow{BH}.\overrightarrow{AC} = 0$ et que $\overrightarrow{CH}.\overrightarrow{AB} = 0$. En utilisant le fait que : $\overrightarrow{BH}.\overrightarrow{AC} = 0$, on peut écrire : $0 = (\overrightarrow{BC}+\overrightarrow{CH}).(\overrightarrow{AB}+\overrightarrow{BC}) = \overrightarrow{BC}.\overrightarrow{AB}+\overrightarrow{BC}.\overrightarrow{BC}+\overrightarrow{CH}.\overrightarrow{BC} = \overrightarrow{BC}.(\overrightarrow{AB} + \overrightarrow{BC} + \overrightarrow{CH}) = \overrightarrow{BC}.\overrightarrow{AH}$. Donc on a bien : $\overrightarrow{AH}.\overrightarrow{BC} = 0$.

Exercice 2. Soit ABC un triangle.

1) Prouver que $\overrightarrow{OA}.\overrightarrow{OB} = R^2 - \dfrac{c^2}{2}$.
2) Prouver que $\overrightarrow{OH} = \overrightarrow{OA} + \overrightarrow{OB} + \overrightarrow{OC}$.
3) Prouver que $OH^2 = 9R^2 - a^2 - b^2 - c^2$.

Solution de l'exercice 2.



1) Pour résoudre cette question, on peut utiliser la relation suivante : $\vec{u}.\vec{v} = \frac{1}{2}(||\vec{u}||^2 + ||\vec{v}||^2 - ||\vec{u} - \vec{v}||^2)$, relation se démontrant de la même manière qu'une autre expression du produit scalaire donnée dans un théorème précédent.
On a alors : $\overrightarrow{OA}.\overrightarrow{OB} = \frac{1}{2}(||\overrightarrow{OA}||^2 + ||\overrightarrow{OB}||^2 - ||\overrightarrow{OA} - \overrightarrow{OB}||^2) = \frac{1}{2}(R^2 + R^2 - ||\overrightarrow{BA}||^2) = R^2 - \frac{c^2}{2}$.
2) Soit H' le point tel que : $\overrightarrow{OH'} = \overrightarrow{OA} + \overrightarrow{OB} + \overrightarrow{OC}$.
On a : $\overrightarrow{AH'}.\overrightarrow{BC} = (\overrightarrow{AO} + \overrightarrow{OH'}).\overrightarrow{BC} = \overrightarrow{AO}.\overrightarrow{BC} + \overrightarrow{OH'}.\overrightarrow{BC} = \overrightarrow{AO}.\overrightarrow{BC} + (\overrightarrow{OA} + \overrightarrow{OB} + \overrightarrow{OC}).\overrightarrow{BC} = \overrightarrow{OB}.\overrightarrow{BC} + \overrightarrow{OC}.\overrightarrow{BC} = 0$ (en écrivant : $\overrightarrow{BC} = \overrightarrow{BO} + \overrightarrow{OC}$). On montre de la même manière que $\overrightarrow{BH'}.\overrightarrow{AC} = 0$ donc H' appartient à deux hauteurs du triangle ABC donc $H' = H$.
3) On écrit : $OH^2 = \overrightarrow{OH}^2 = (\overrightarrow{OA} + \overrightarrow{OB} + \overrightarrow{OC})^2$. En développant et en utilisant les relations : $\overrightarrow{OA}.\overrightarrow{OB} = R^2 - \frac{c^2}{2}$, $\overrightarrow{OB}.\overrightarrow{OC} = R^2 - \frac{a^2}{2}$ et $\overrightarrow{OA}.\overrightarrow{OC} = R^2 - \frac{b^2}{2}$, on obtient le résultat.

II) Quelques applications du produit scalaire.

Propriété : identité du parallélogramme. Soit $ABCD$ un parallélogramme. Alors $AC^2 + BD^2 = 2(AB^2 + AD^2)$.

Preuve. En prenant $\vec{u} = \overrightarrow{AB}$ et $\vec{v} = \overrightarrow{AD}$, ceci provient du fait que : $(\vec{u}+\vec{v})^2+(\vec{u}-\vec{v})^2 = 2(\vec{u}^2+\vec{v}^2)$.

Géométrie analytique. Le produit scalaire est également utile en géométrie analytique pour montrer que deux vecteurs sont orthogonaux ou pour calculer les coordonnées de divers points lorsque de l'orthogonalité est mise en jeu.

(1) On munit le plan d'un repère orthonormal. Soient A, B, C trois points distincts du plan. Comment trouver l'équation de la perpendiculaire à (AB) passant par C ?
Un point $M\begin{pmatrix}x\\y\end{pmatrix}$ appartient à cette droite si et seulement si $\overrightarrow{CM}.\overrightarrow{AB} = 0$. Ainsi, si $A\begin{pmatrix}x_A\\y_A\end{pmatrix}$, $B\begin{pmatrix}x_B\\y_B\end{pmatrix}$ et $C\begin{pmatrix}x_C\\y_C\end{pmatrix}$, alors la droite perpendiculaire à (AB) passant par C peut être caractérisée par l'équation : $(x - x_C)(x_B - x_A) + (y - y_C)(y_B - y_A) = 0$.

(2) Deux droites de coefficients directeurs respectifs k et k' sont perpendiculaires si et seulement si $kk' = -1$. On rappelle que pour une droite d'équation $ax + by + c = 0$, le vecteur de coordonnées $(-b, a)$ est un vecteur directeur de cette droite et que le vecteur de coordonnées (a, b) est un vecteur normal à cette droite (i.e : un vecteur orthogonal à tous les vecteurs directeurs de la droite).

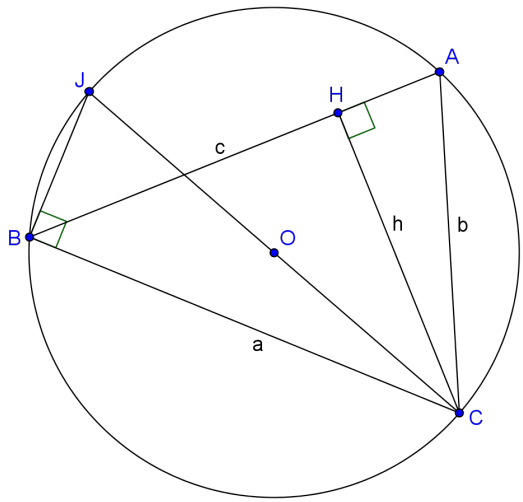
III) Relations métriques et trigonométriques dans un triangle.

Théorème d'Al-Kashi. Soit ABC un triangle. On a : $a^2 = b^2 + c^2 - 2bc\cos\widehat{A}$.

Démonstration. On écrit : $a^2 = \overrightarrow{BC}^2 = (\overrightarrow{BA} + \overrightarrow{AC})^2 = BA^2 + 2\overrightarrow{BA}.\overrightarrow{AC} + AC^2 = b^2 + c^2 - 2\overrightarrow{AB}.\overrightarrow{AC} = b^2 + c^2 - 2bc\cos\widehat{A}$.

Loi des sinus. On a : $\dfrac{a}{\sin\widehat{A}} = \dfrac{b}{\sin\widehat{B}} = \dfrac{c}{\sin\widehat{C}} = 2R = \dfrac{abc}{2S}$.

Démonstration.



L'aire S du triangle peut être calculée en choisissant le côté $[AB]$ comme base et h comme hauteur, on obtient alors :
$S = \dfrac{c \times h}{2} = \dfrac{c \times b\sin\widehat{A}}{2} = \dfrac{1}{2}bc\sin\widehat{A}$.

Ainsi, l'aire S du triangle peut être exprimée de l'une de ces trois façons selon le côté que l'on choisit comme base :
$S = \dfrac{1}{2}bc\sin\widehat{A} = \dfrac{1}{2}ac\sin\widehat{B} = \dfrac{1}{2}ab\sin\widehat{C}$.

En multipliant par $\dfrac{2}{abc} \neq 0$ (et bien sûr, a, b et c sont non nuls), on obtient :

$\dfrac{2S}{abc} = \dfrac{\sin\widehat{A}}{a} = \dfrac{\sin\widehat{B}}{b} = \dfrac{\sin\widehat{C}}{c}$.

En prenant l'inverse de chaque membre, on obtient (en ayant : $S \neq 0$, $\sin\widehat{A} \neq 0$, $\sin\widehat{B} \neq 0$ et $\sin\widehat{C} \neq 0$) :

$\dfrac{a}{\sin\widehat{A}} = \dfrac{b}{\sin\widehat{B}} = \dfrac{c}{\sin\widehat{C}} = \dfrac{abc}{2S}$.

Introduisons maintenant le point J tel que $[CJ]$ soit un diamètre du cercle circonscrit au triangle ABC. Le triangle BCJ est inscrit dans un cercle en ayant un diamètre du cercle pour côté (le côté $[CJ]$) donc CBJ est rectangle en B. On a alors : $\sin\widehat{BJC} = \dfrac{a}{2R}$. De plus, par le théorème de l'angle inscrit, $\widehat{BJC} = \widehat{A}$ donc $\sin\widehat{A} = \dfrac{a}{2R}$ ainsi, $\dfrac{a}{\sin\widehat{A}} = 2R$.

Théorème de la médiane. Soient ABC un triangle et I le milieu de $[AB]$. On a :

(1) $AC^2 + BC^2 = 2IC^2 + \dfrac{1}{2}AB^2$.

(2) $AC^2 - BC^2 = 2\overrightarrow{CI}.\overrightarrow{BA}$.

(3) $\overrightarrow{CA}.\overrightarrow{CB} = CI^2 - \dfrac{1}{4}AB^2$.

Démonstration. Pour (1), on écrit :

$AC^2 + BC^2 = \overrightarrow{AC}^2 + \overrightarrow{BC}^2 = (\overrightarrow{AI} + \overrightarrow{IC})^2 + (\overrightarrow{BI} + \overrightarrow{IC})^2 = AI^2 + 2(\overrightarrow{AI} + \overrightarrow{BI}).\overrightarrow{IC} + BI^2 + 2IC^2$.

Comme on a : $\overrightarrow{AI} + \overrightarrow{BI} = \vec{0}$ et $AI = BI = \dfrac{1}{2}AB$, on obtient la relation énoncée.

Les preuves des deux autres assertions sont similaires et sont laissées en exercice.

Relations trigonométriques. Soit x un nombre réel.

$\cos(-x) = \cos(x)$	$\sin(-x) = -\sin(x)$.
$\cos(\pi - x) = -\cos(x)$	$\sin(\pi - x) = \sin(x)$.
$\cos(\pi + x) = -\cos(x)$	$\sin(\pi + x) = -\sin(x)$.
$\cos\left(\frac{\pi}{2} - x\right) = \sin(x)$	$\sin\left(\frac{\pi}{2} - x\right) = \cos(x)$.
$\cos\left(\frac{\pi}{2} + x\right) = -\sin(x)$	$\sin\left(\frac{\pi}{2} + x\right) = \cos(x)$.
$\cos^2 x + \sin^2 x = 1$.	

Remarque. Ces relations peuvent être aisément vérifiées à l'aide d'un cercle trigonométrique.

Théorème (formules d'addition et de duplication trigonométriques). Soient a et b deux nombres réels.

(1) $\cos(a - b) = \cos(a)\cos(b) + \sin(a)\sin(b)$.
$\cos(a + b) = \cos(a)\cos(b) - \sin(a)\sin(b)$.

(2) $\sin(a - b) = \sin(a)\cos(b) - \cos(a)\sin(b)$.
$\sin(a + b) = \sin(a)\cos(b) + \cos(a)\sin(b)$.

(3) $\cos(2a) = \cos^2 a - \sin^2 a = 2\cos^2(a) - 1 = 1 - 2\sin^2 a$.
$\sin(2a) = 2\sin(a)\cos(a)$.

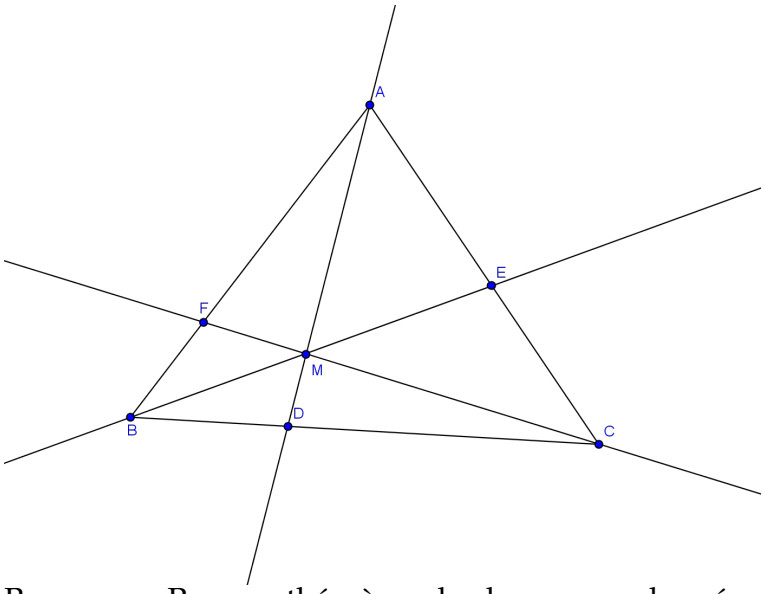
Pour a tel que : $2a \neq \frac{\pi}{2} + k\pi$, $k \in \mathbb{Z}$ et $\tan^2(a) \neq 1$, $\tan(2a) = \frac{2\tan a}{1-\tan^2 a}$.

(4) Pour $a-b$ tel que $a - b \neq \frac{\pi}{2} + k\pi$, $k \in \mathbb{Z}$ et $\tan(a)\tan(b) \neq -1$

$\tan(a-b) = \frac{\tan(a) - \tan(b)}{1 + \tan(a)\tan(b)}$.

Démonstration. Pour (1), introduisons les points U et V de coordonnées $U\begin{pmatrix}\cos a\\ \sin a\end{pmatrix}$ et $V\begin{pmatrix}\cos b\\ \sin b\end{pmatrix}$.
Ainsi, $b-a$ est l'angle (modulo 2π) orienté $(\overrightarrow{OU}, \overrightarrow{OV})$. Comme $OU = OV = 1$, on obtient, en calculant de deux manières différentes le produit scalaire $\overrightarrow{OU}.\overrightarrow{OV}$, $\cos(a-b) = \overrightarrow{OU}.\overrightarrow{OV} = \cos(a)\cos(b) + \sin(a)\sin(b)$.
On déduit la seconde relation de la première en prenant $-b$ à la place de b.
Pour (2), on écrit : $\sin(a+b) = \cos\left(\frac{\pi}{2} - a - b\right)$ et on utilise (1).
Finalement, (3) et (4) sont des conséquences de (1) et (2) laissées en exercice.

Théorème de Ceva.



Soient ABC un triangle et D, E, F des points distincts des sommets et appartenant respectivement aux segments $[BC]$, $[CA]$ et $[AB]$. Les droites (AD), (BE) et (CF) sont concourantes si et seulement si $\frac{\overline{DB}}{\overline{DC}}.\frac{\overline{EC}}{\overline{EA}}.\frac{\overline{FA}}{\overline{FB}} = 1$.

Remarque. Pour ce théorème, les longueurs données sont des longueurs algébriques (éventuellement négatives).

Démonstration.

On note $\mathscr{A}_{ABC}$ l'aire du triangle ABC et d'une manière analogue pour les autres triangles.

Sens direct : notons h la longueur de la hauteur relative au côté $[BD]$ du triangle MDB. On a : $\mathscr{A}_{MDB} = \frac{DB \times h}{2}$ et $\mathscr{A}_{MDC} = \frac{DC \times h}{2}$.
Notons maintenant h' la longueur de la hauteur relative au côté $[BD]$ du triangle ABD. On a : $\mathscr{A}_{ABD} = \frac{DB \times h'}{2}$ et $\mathscr{A}_{ADC} = \frac{DC \times h'}{2}$.

De plus, $\mathscr{A}_{MAB} = \mathscr{A}_{ABD} - \mathscr{A}_{MBD} = \dfrac{DB \times (h' - h)}{2}$ et $\mathscr{A}_{MAC} = \mathscr{A}_{ADC} - \mathscr{A}_{MDC} = \dfrac{DC \times (h' - h)}{2}$ donc $\dfrac{\mathscr{A}_{MAB}}{\mathscr{A}_{MAC}} = \dfrac{DB}{DC}$.

Par un raisonnement analogue, on a : $\dfrac{\mathscr{A}_{MBC}}{\mathscr{A}_{MBA}} = \dfrac{EC}{EA}$ et $\dfrac{\mathscr{A}_{MCA}}{\mathscr{A}_{MCB}} = \dfrac{FA}{FB}$. Le produit des trois rapports est bien égal à 1.

Réciproque : les droites (AD) et (BE) ne sont pas parallèles donc elles sont sécantes en un point M. La droite (CM) coupe le segment $[AB]$ en F'. D'après le raisonnement précédent, on a : $\dfrac{DB}{DC}.\dfrac{EC}{EA}.\dfrac{F'A}{F'B} = 1$. Comme $\dfrac{DB}{DC}.\dfrac{EC}{EA}.\dfrac{FA}{FB} = 1$, on obtient, après simplification : $\dfrac{FA}{FB} = \dfrac{F'A}{F'B}$. Or, il n'existe qu'un seul point sur un segment qui divise celui-ci selon un rapport donné donc $F = F'$. Ainsi, le point M appartient à la droite (CF).

IV) Exercices supplémentaires.

Exercice 3. Soient ABC un triangle, D, E et F trois points distincts des sommets et appartenant respectivement à $[BC]$, $[CA]$ et $[AB]$. Montrer que les droites (AD), (BE) et (CF) sont concourantes si et seulement si $\dfrac{\sin\widehat{BAD}}{\sin\widehat{CAD}}.\dfrac{\sin\widehat{ACF}}{\sin\widehat{BCF}}.\dfrac{\sin\widehat{CBE}}{\sin\widehat{ABE}} = 1$.

Solution de l'exercice 3. Appliquons la loi des sinus dans les triangles BAD et ADC,

on obtient : $\dfrac{BD}{\sin\widehat{BAD}} = \dfrac{AD}{\sin\widehat{B}}$ et $\dfrac{DC}{\sin\widehat{DAC}} = \dfrac{AD}{\sin\widehat{C}}$ donc $\dfrac{BD}{DC} = \dfrac{\sin\widehat{BAD}}{\sin\widehat{DAC}} \times \dfrac{\sin\widehat{C}}{\sin\widehat{B}}$.

On raisonne de la même manière pour les autres rapports et on montre que :

$$\frac{BD}{DC}.\frac{ED}{EA}.\frac{FA}{FB} = \frac{\sin\widehat{BAD}}{\sin\widehat{CAD}}.\frac{\sin\widehat{ACF}}{\sin\widehat{BCF}}.\frac{\sin\widehat{CBE}}{\sin\widehat{ABE}}.$$

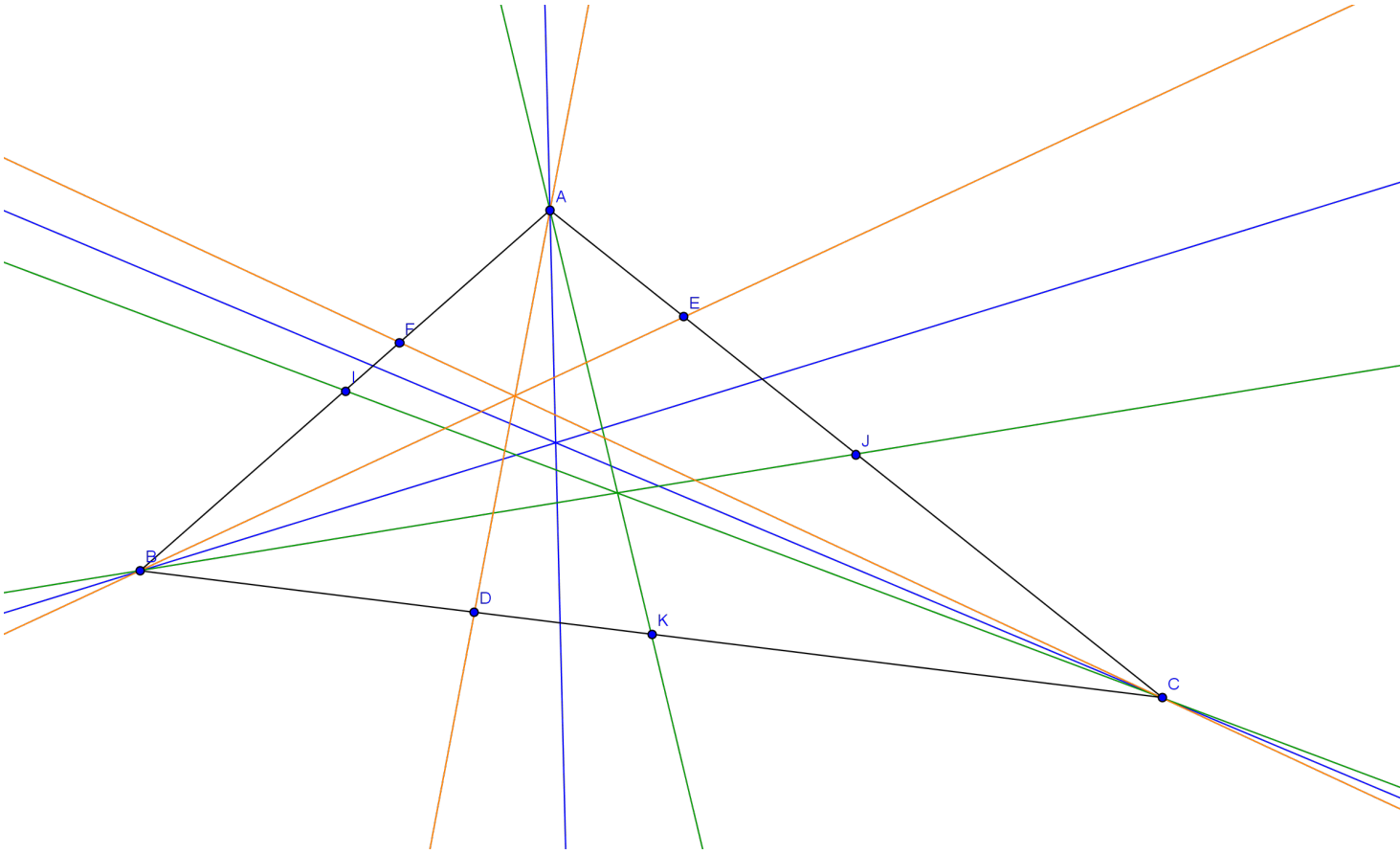
Le théorème de Ceva classique est donc équivalent à ce théorème de Ceva trigonométrique !

Exercice 4.

On se donne un triangle ABC. Soit K le milieu de $[BC]$. La droite (AK) est alors une médiane du triangle ABC. On construit la droite symétrique de la droite (AK) par rapport à la bissectrice de l'angle $\widehat{A}$. Cette dernière droite coupe le segment $[BC]$ en D. La droite (AD) est une symédiane du triangle ABC. On construit de la même manière manière les deux autres symédianes du triangle ABC. Montrer que les symédianes sont concourantes.

Solution de l'exercice 4.

On appelle I le milieu du segment $[AB]$ et J le milieu de $[AC]$. La symédiane issue de C coupe le segment $[AB]$ au point F et la symédiane issue de B coupe le segment $[AC]$ en E. Faisons tout d'abord une belle figure pour y voir plus clair. On a représenté les médianes en vert, les bissectrices en bleu et les symédianes en orange.



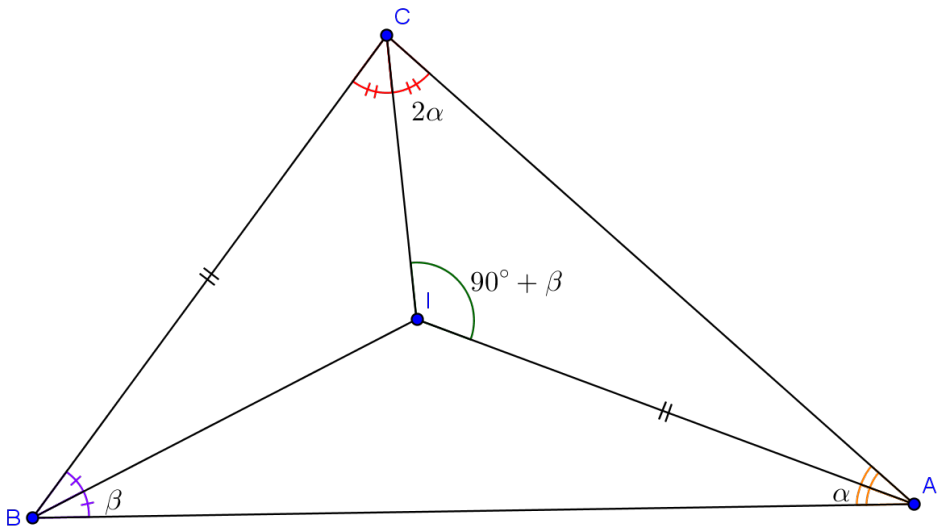
Les médianes : (AK), (BJ) et (CI) du triangle ABC sont concourantes donc par le théorème de Ceva trigonométrique, on a : $\frac{\sin\widehat{BAK}}{\sin\widehat{CAK}}.\frac{\sin\widehat{ACI}}{\sin\widehat{BCI}}.\frac{\sin\widehat{CBJ}}{\sin\widehat{ABJ}}=1$.

De plus, on a (car la symétrie axiale conserve les angles) : $\widehat{BAK}=\widehat{CAD}$ et $\widehat{CAK}=\widehat{BAD}$, $\widehat{ACI}=\widehat{BCF}$ et $\widehat{BCI}=\widehat{ACF}$, $\widehat{CBJ}=\widehat{ABE}$ et $\widehat{ABJ}=\widehat{CBE}$.

Donc on obtient : $\frac{\sin\widehat{CAD}}{\sin\widehat{BAD}}.\frac{\sin\widehat{BCF}}{\sin\widehat{ACF}}.\frac{\sin\widehat{ABE}}{\sin\widehat{CBE}}=1$ puis par passage à l'inverse : $\frac{\sin\widehat{BAD}}{\sin\widehat{CAD}}.\frac{\sin\widehat{ACF}}{\sin\widehat{BCF}}.\frac{\sin\widehat{CBE}}{\sin\widehat{ABE}}=1$. Ainsi, par le théorème de Ceva trigonométrique, les symédianes du triangle ABC sont concourantes.

Exercice 5. Soient ABC un triangle non plat et I le centre de son cercle inscrit. On suppose que $AI=BC$ et que $\widehat{ICA}=2\widehat{IAC}$. Quelle est la valeur de $\widehat{ABC}$?

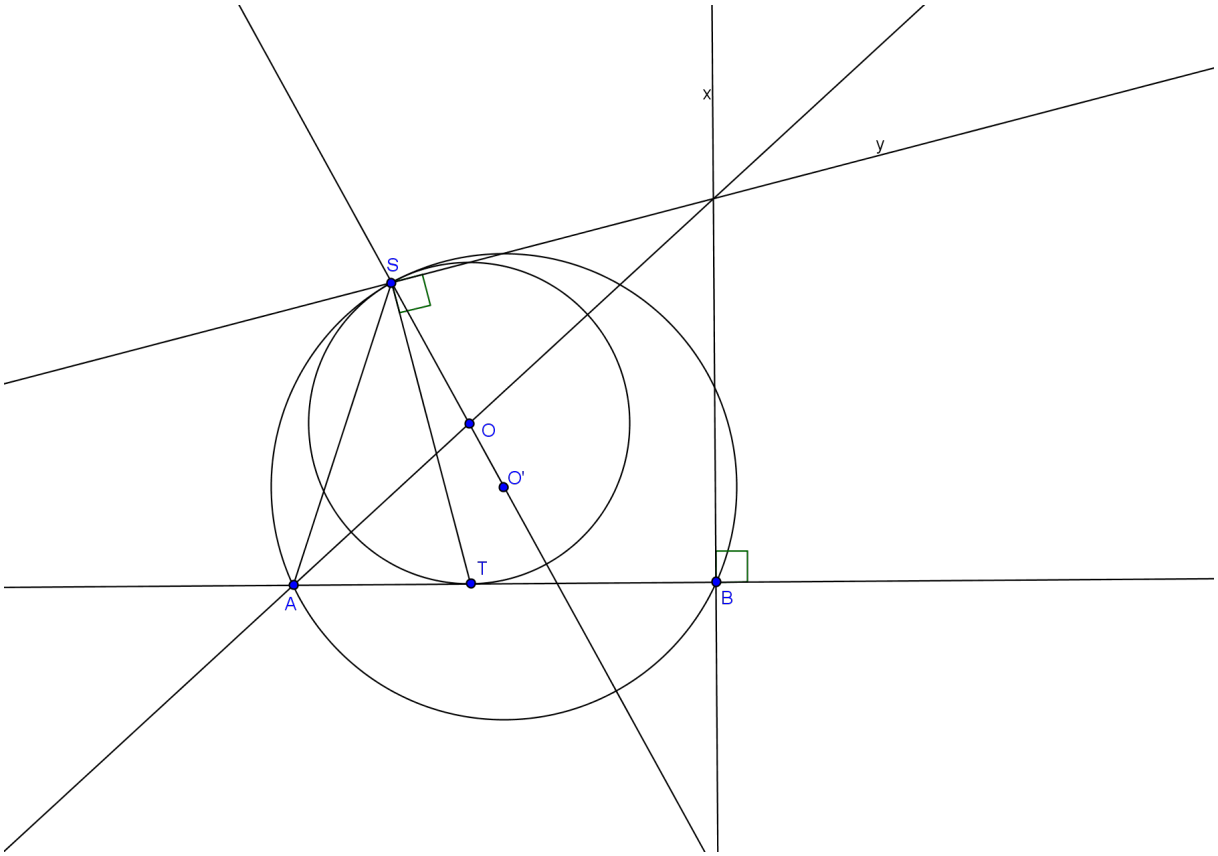
Solution de l'exercice 5. Notons α l'angle $\widehat{IAB}$ et β l'angle $\widehat{IBA}$. Par hypothèse, $\widehat{ICA}=2\alpha$.



On vérifie (en utilisant que la somme des angles d'un triangle est égale à 180°) que : $\beta = 90^\circ - 3\alpha$ et $\widehat{CIA} = 90^\circ + \beta$. On utilise la loi des sinus dans les triangles AIC et ABC et on obtient : $\dfrac{AI}{\sin(2\alpha)} = \dfrac{AC}{\sin(90^\circ + \beta)}$ et $\dfrac{AC}{\sin(2\beta)} = \dfrac{BC}{\sin(2\alpha)}$.
Par hypothèse, $AI = BC$ donc : $\dfrac{AC}{AI} \times \sin(2\alpha) = \sin(90^\circ + \beta) = \sin(2\beta)$.
D'après les propriétés de la fonction sinus, si deux angles x et y ont une mesure comprise entre 0°et 180°et que $\sin x = \sin y$ alors $x = y$ ou $x = 180^\circ - y$. Regardons les deux cas :
1) si $90^\circ + \beta = 2\beta$ alors $\beta = 90^\circ$et alors $\widehat{ABC} = 180^\circ$. Ceci est impossible car le triangle ABC est non plat.
2) Si $90^\circ + \beta = 180^\circ - 2\beta$ alors $\beta = 30^\circ$et $\widehat{ABC} = 60^\circ$. Ainsi, $\widehat{ABC} = 60^\circ$.

Exercice 6. Deux cercles Γ_1 et Γ_2 sont tangents en un point S avec Γ_1 à l'intérieur de Γ_2. On note O le centre de Γ_1. Une corde $[AB]$ de Γ_2 est tangente à Γ_1 en T. Montrer que (AO), la perpendiculaire à (AB) passant par B et la perpendiculaire à (ST) passant par S sont concourantes.

Solution de l'exercice 6.



On note (Bx) la perpendiculaire à (AB) passant par B et (Sy) la perpendiculaire à (ST) passant par S. Montrons que les droites (AO), (Bx) et (Sy) sont concourantes. Pour obtenir le résultat grâce au théorème de Ceva trigonométrique, on doit montrer que :

$$\frac{\sin \widehat{BAO}}{\sin \widehat{SAO}} . \frac{\sin \widehat{ASy}}{\sin \widehat{BSy}} . \frac{\sin \widehat{SBx}}{\sin \widehat{ABx}} = 1.$$

On sait que $\sin \widehat{ABx} = 1$. Notons O' le centre du cercle Γ_2 et h l'homothétie de centre S et de rapport $\lambda = \dfrac{SO'}{SO}$. On a : $h(O) = O'$ et $h(\Gamma_1) = \Gamma_2$. Comme $T \in \Gamma_1$, $h(T) \in \Gamma_2$ et les points S, T et $h(T)$ sont alignés. Donc $h(T)$ est le point d'intersection de la droite (ST) et du cercle Γ_2, différent du point S. L'image de la droite (OT) par l'homothétie h est la droite $(h(O)h(T)) = (O'h(T))$. Cette dernière droite est parallèle à la droite (OT). Or, $(OT) \perp (AB)$ donc $(O'h(T)) \perp (AB)$. Ainsi, la droite $(O'h(T))$ est la médiatrice du segment $[AB]$ donc $h(T)A = h(T)B$ donc le triangle $Ah(T)B$ est isocèle en $h(T)$. Dès lors, la droite $(O'h(T))$ est également la bissectrice intérieure de l'angle $\widehat{Ah(T)B}$ donc $\widehat{Ah(T)O'} = \widehat{O'h(T)B}$.
De plus, on a : $O'A = O'h(T) = O'B$ donc $\widehat{O'Ah(T)} = \widehat{O'h(T)A}$ et $\widehat{O'Bh(T)} = \widehat{O'h(T)B}$ ainsi, $\widehat{O'Ah(T)} = \widehat{O'Bh(T)}$.
Finalement, $\widehat{AO'h(T)} = 180 - 2 \times \widehat{O'Ah(T)} = 180 - 2 \times \widehat{O'Bh(T)} = \widehat{BO'h(T)}$.
Or, $\widehat{AST} = \dfrac{\widehat{AO'h(T)}}{2}$ et $\widehat{TSB} = \dfrac{\widehat{BO'h(T)}}{2}$ donc $\widehat{AST} = \widehat{TSB}$.
On a : $\widehat{ASy} = \widehat{AST} + 90°$et $\widehat{BSy} = 90° - \widehat{TSB} = 90° - \widehat{AST} = 180° - \widehat{ASy}$.

Ainsi, $\sin \widehat{ASy} = \sin \widehat{BSy}$ donc il reste à montrer :

$$\frac{\sin \widehat{BAO}}{\sin \widehat{SAO}} . \sin \widehat{SBx} = 1.$$

Or, $\sin \widehat{BAO} = \dfrac{OT}{AO} = \dfrac{OS}{AO}$. D'après la loi des sinus dans le triangle ASO, on a : $\dfrac{OS}{\sin \widehat{SAO}} = \dfrac{AO}{\sin \widehat{ASO}}$. Donc $\sin \widehat{BAO} = \dfrac{\sin \widehat{SAO}}{\sin \widehat{ASO}}$.
Montrons maintenant que $\widehat{ASO} = \widehat{SBx}$. On a : $\widehat{ASO} = \widehat{ASO'} = \dfrac{1}{2}(\pi - \widehat{AO'S}) = \dfrac{\pi}{2} - \widehat{SBA} = \widehat{SBx}$ d'où le résultat.

4 mercredi 20 après-midi : Jean-Louis Tu

Orthocentre

Exercice 1 Soit H l'orthocentre de ABC, M le milieu de $[BC]$, A' le point diamétralement opposé de A sur le cercle circonscrit Γ et H' le symétrique de H par rapport à (BC). Montrer que M est le milieu de $[HA']$, que $H' \in \Gamma$ et que H' et A' sont symétriques par rapport à la médiatrice de $[BC]$. De plus, (AO) et (AH) sont symétriques par rapport à la bissectrice de $\widehat{A}$.

Exercice 2 Soit O le centre du cercle circonscrit, H l'orthocentre de ABC, et A', B', C' les symétriques de H par rapport à $(BC), (CA)$ et (AB). Montrer que les parallèles à $(OA), (OB), (OC)$ passant par A', B', C' respectivement sont concourantes.

Exercice 3 On fixe une corde $[BC]$ d'un cercle. Le point A se déplace sur l'un des arcs BC. Déterminer le lieu de l'orthocentre de ABC.

Exercice 4 Montrer que $AH^2 + BC^2 = 4OA^2$.

Exercice 5 Soit ABC un triangle acutangle, et O le centre du cercle circonscrit ω. Soit D le point de (BC) tel que $\widehat{BAD} = \widehat{OAC}$. Soit E le second point d'intersection de ω avec (AD). Si M, N, P sont les milieux de $[BE], [OD]$ et $[AC]$, montrer que M, N, P sont colinéaires.

Exercice 6 Soit ABC un triangle acutangle et Γ son cercle circonscrit. On note H l'orthocentre. Soit K un point de Γ sur l'arc ne contenant pas A. Soit L le symétrique de K par rapport à (AB), et M le symétrique de K par rapport à (BC). Soit E le second point d'intersection de Γ avec le cercle BLM. Montrer que les droites (KH), (EM) et (BC) sont concourantes.

Point de contact du cercle inscrit et exinscrit

Exercice 7 Montrer que si X et Z sont les points de contacts des cercles inscrit et exinscrit dans l'angle $\widehat{A}$ avec (BC), alors (AZ) passe par le point diamétralement opposé à X.

Exercice 8 Soit C un cercle, d une tangente à C, et M un point de d. Déterminer le lieu des points P tels qu'il existe $Q, R \in d$ tels que M soit le milieu de $[QR]$, et tel que C soit le cercle inscrit à PQR.

Exercice 9 Soit $ABCD$ un trapèze isocèle avec $(AB) \parallel (CD)$. Le cercle inscrit ω au triangle (BCD) rencontre (CD) en E. Soit F un point sur la bissectrice intérieure à $\widehat{DAC}$ tel que $(EF) \perp (CD)$. Le cercle (ACF) rencontre (CD) en C et G. Montrer que AFG est isocèle.

Exercice 10 Le cercle A-exinscrit (O) de ABC touche (BC) en M. Les points D et E sont sur $[AB]$ et $[AC]$ de sorte que $(DE) \parallel (BC)$. Le cercle inscrit (O_1) de ADE touche (DE) en N. Si $BO_1 \cap DO = F$ et $CO_1 \cap EO = G$, montrer que le milieu de $[FG]$ est sur MN.

Point de Miquel

Exercice 11 Montrer que si ABC est un triangle, $D \in (BC)$, $E \in (CA)$ et $F \in (AB)$, alors les cercles AEF, BFD et CDE sont concourants. De plus, le point commun M appartient au cercle ABC si et seulement si D, E, F sont alignés.

Exercice 12 Soit A, B, C un triangle. Montrer que lorsqu'un point D varie sur (AB) et qu'un point E varie sur (CD), le second point d'intersection entre les cercles ADE et CBE reste sur un cercle fixe.

Exercice 13 Les points P et Q sont sur les diagonales $[AC]$ et $[BD]$, respectivement, d'un quadrilatère $ABCD$ tel que $\frac{AP}{AC} + \frac{BQ}{BD} = 1$. La droite (PQ) rencontre les côtés $[AD]$ et $[BC]$ aux points M et N. Montrer que les cercles AMP, BNQ, DMQ, et CNP sont concourants.

Solution de l'exercice 1 Chasse aux angles.

Solution de l'exercice 2 Chasse aux angles : ces trois droites sont les hauteurs de $A'B'C'$.

Solution de l'exercice 3 $\overrightarrow{AH} = \overrightarrow{OB} + \overrightarrow{OC}$ est constant donc H décrit un arc de cercle.

Solution de l'exercice 4 Soit M le milieu de $[BC]$. On a $AH^2 = 4OM^2 = 4(OB^2 - BM^2)$.

Solution de l'exercice 5 D est le pied de la hauteur $[AH]$. Il suffit de montrer que $MDPO$ est un parallélogramme. Or, $\overrightarrow{MD} = \frac{1}{2}\overrightarrow{BH} = \overrightarrow{OP}$.

Solution de l'exercice 6 Soit c_2 le symétrique de Γ par rapport à (AB), c_3 le symétrique de Γ par rapport à (BC), alors H est sur c_2 et c_3. Soit $(AH) \cap \Gamma = P$, alors P est le symétrique de H par rapport à BC, donc $D = (HK) \cap (PM)$ appartient à (BC). On pose $(PM) \cap \Gamma = E'$.

Par symétrie on a $(MB, MH) = -(KB, KP) = -(AB, AP) = \pi/2 + \beta$, $(LB, LH) = (AB, AH) = \pi/2 - \beta$, $(BL, BM) = (BL, BA) + (BA, BM) = -(BK, BA) + (BA, BM) = (BA, BC) + (BC, BK) + (BA, BM) = -2\beta$ donc $(MH, LH) = (MH, MB) + (BM, BL) + (BL, LH) = 0$, donc L, H, M sont colinéaires. On a donc $(E'B, E'M) = (E'B, E'P) = (AB, AP) = \pi/2 - \beta = (LB, LH) = (LB, LM)$ donc $EMBL$ est cyclique, ainsi $E = E'$.

Solution de l'exercice 7 Utiliser l'homothétie de centre A qui envoie un cercle sur l'autre.

Solution de l'exercice 8 Soit E le point de contact entre C et d, et F le symétrique de E par rapport à M. Soit E' le point diamétralement opposé à E. Nécessairement, P appartient à $(E'F)$.

Réciproquement, si $P \in (E'F)$, on définit Q et R...

Solution de l'exercice 9 F est le centre du cercle exinscrit dans l'angle A de ADC. Une chasse aux angles montre que $\widehat{FAG} = \widehat{FGA} = 90° - \widehat{DCA}/2$.

Solution de l'exercice 10 D'après Desargues pour les triangles BFD et CGE, on a $(DE) \parallel (FG) \parallel (BC)$. Soient X, Y, Z les milieux de $[DE], [BC], [MN]$. Soient $P = (OM) \cap (DE)$, $Q = (O_1N) \cap (BC)$, $V = AN \cap BC$, W le point diamétralement opposé à M sur (O). V est le point de contact du cercle inscrit de ABC avec (BC) donc Y est le milieu de $[VM]$. Or, A, N, V, W sont colinéaires, donc O, Y, Z aussi. De même pour O_1, X, Z. D'après Desargues pour O_1XN et YOM,$(O_1Y), (OX), (MN)$ sont concourantes. Or, le milieu de $[M, N]$ est sur (OX) et (O_1Y).

Solution de l'exercice 11 Chasse aux angles.

Solution de l'exercice 12 Point de Miquel pour DBC et $A \in (BD)$, $B \in [BC]$ et $E \in (CD)$.

Solution de l'exercice 13 Soit E l'intersection de (AC) et (BD). D'après Miquel, les cercles AMP, DMQ, EPQ, EAD sont concourants, ainsi que BNQ, CNP, EPQ, EBC. Il reste à montrer que EPQ, EAD, EBC sont concourants. Soit F le second point d'intersection des cercles EBC, EAD. Alors F est le centre de la similitude directe s qui envoie $[BD]$ sur $[CA]$. Comme $\frac{AP}{AC} = \frac{DQ}{BD}$, s envoie Q sur P et D sur A, donc F appartient au cercle EPQ.

4 Groupe D : arithmétique

1 mardi 18 matin : Igor Kortchemski

NB. Des exercices supplémentaires par rapport à ce qui a été vu pendant la séance ont été rajoutés dans la section 2, ainsi que la méthode (très utile) de Dan Scwharz.

Première partie

La première partie de la séance a consisté à revoir quelques outils de bases et réflexes à avoir à travers d'exercices.

Exercice 1 Trouver tous les entiers $n \geq 1$ tels que $3^{n-1} + 5^{n-1}$ divise $3^n + 5^n$.

Exercice 2 Trouver tous les entiers $a, b \geq 1$ tels que les deux quantités

$$\frac{a^2 + b}{b^2 - a} \qquad \text{et} \qquad \frac{b^2 + a}{a^2 - b}$$

soient des nombres entiers.

Exercice 3 Trouver le reste de la division euclidienne de $6^{83} + 8^{83}$ par 49.

Exercice 4 Trouver les deux derniers chiffres de 1032^{1032}.

Exercice 5 Soit p un nombre premier. Montrer que tout diviseur premier de $2^p - 1$ est strictement plus grand que p.

Exercice 6 Soient p, q, r des nombres premiers tels que p soit impair et divise $q^r + 1$. Montrer que $2r$ divise $p - 1$ ou p divise $q^2 - 1$.

Exercice 7 Trouver tous les entiers $x, y \geq 1$ tels que $x^3 - y^3 = xy + 61$.

Deuxième partie

Pour résoudre des équations diophantiennes, on a souvent recours à des congruences en considérant l'équation modulo N. Mais quel modulo N choisir ?

— s'il y a des puissances p-ième avec p premier, essayez $N = p^2$, p^3, etc.

En effet, si a n'est pas divisible par p, d'après le théorème d'Euler, $a^{p^{k-1}(p-1)} \equiv 1 \mod p^k$, de sorte que $(a^p)^{p^{k-2}(p-1)} \equiv 1 \mod p^k$, ce qui limite le nombre de valeurs prises par a^p modulo p^k.

— lorsqu'il intervient une puissance n-ième (avec n un entier connu), il peut être utile de choisir pour N un nombre premier congru à 1 modulo n.

En effet, dans ce cas, $a^{N-1} \equiv 1 \mod N$ d'après le petit théorème de Fermat, de sorte que $(a^n)^{\frac{N-1}{n}} \equiv 1 \mod N$, ce qui limite le nombre de valeurs prises par a^n modulo N.

— lorsqu'il intervient une puissance n-ième (où n est l'inconnue), disons a^n, il peut être utile de choisir $N = a^k$ (avec k supérieur à la plus grande solution supposée).

— lorsqu'il intervient une puissance n-ième (où n est l'inconnue), disons a^n, il peut être utile de choisir pour N un diviseur pas trop grand de $a^k - 1$ pour un certain entier k.

En effet, si on sait que n est congru à nombre fixé modulo un certain m (ou bien prend un nombre de valeurs limitées modulo m), il peut être judicieux de trouver N tel que l'ordre de a modulo N vaut m, ou bien divise m, ou bien soit un multiple de m. Dans les deux premiers cas, N divise $a^m - 1$, et dans le dernier cas N divise $a^k - 1$ avec k multiple de N.

En effet, dans les deux premiers cas, a^n est alors constant modulo N, et dans le troisième cas, a^n prend un nombre de valeurs limitées modulo N.

Il peut aussi être utile d'utiliser le fait que si $a^k \equiv 1 \mod N$ et si ω est l'ordre de a modulo N, alors $a^\omega - 1$ divise $a^k - 1$.

– Pour les équations de type $a^x = b^y + c$ (avec a, b, c connus et x et y connus) ayant un nombre fini de solutions, on considère (x_0, y_0) la "plus grande", en supposant $x > x_0, y > y_0$ on la retranche à l'équation originelle pour obtenir $a^{x_0}(a^{x-x_0} - 1) = b^{y_0}(b^{y-y_0} - 1)$. Quand a et b sont premiers entre eux, on a alors a^{x_0} qui divise $b^{y-y_0} - 1$. Si ω est l'ordre de b modulo a^{x_0}, on en déduit que $b^\omega - 1$ divise $b^{y-y_0} - 1$ et donc divise $a^{x-x_0} - 1$. On trouve alors un diviseur premier sympathique de $b^\omega - 1$ et on continue de proche en proche (on peut aussi partir du fait que b^{y_0} divise a^{x-x_0}) jusqu'à aboutir à une contradiction. C'est la méthode de *Dan Schwarz* (qui revient grosso modo à ce qui précède, mais donne peut-être plus facilement les bons modulos à considérer).

Exercice 8 Soient $m, n \geq 1$ des entiers. Montrer que $3^m + 3^n + 1$ n'est pas un carré parfait.

Exercice 9 Trouver tous les entiers $x, y \geq 1$ tels que $3^x - 2^y = 7$.

Exercice 10 Trouver tous les entiers $x, y \in \mathbb{Z}$ tels que $15x^2 - 7y^2 = 9$.

Exercice 11 Montrer que quel que soit $n > 1$, $n^5 + 7$ n'est pas un carré.

Exercice 12 Trouver tous les entiers $n \geq 1$ tels que $2^n + 12^n + 2014^n$ soit un carré parfait.

Exercice 13 Existe-t-il des nombres rationnels positifs ou nuls x, y et z tels que $x^5 + 2y^5 + 5z^5 = 11$?

Exercice 14 Montrer que 19^{19} ne peut pas s'écrire comme la somme d'un cube et d'une puissance quatrième de nombres entiers.

Exercice 15 Trouver tous les entiers $x, y \geq 1$ tels que $x^5 = y^2 + 4$.

Exercice 16 Trouver tous les entiers $a, y \geq 1$ tels que $3^{2a-1} + 3^a + 1 = 7^y$.

Exercice 17 Trouver tous les entiers $a, b \geq 1$ tels que les deux nombres $a^5b + 3$ et $ab^5 + 3$ soient des cubes de nombres entiers.

Exercice 18 Trouver tous les entiers $n, m, r \geq 1$ tels que $n^5 + 49^m = 1221^r$.

Exercice 19 Trouver tous les entiers $a \geq 1$ tels que l'entier $1 - 8 \cdot 3^a + 2^{a+2}(2^a - 1)$ soit un carré parfait.

Exercice 20 Trouver tous les entiers $x, y \geq 0$ tels que $2^x = 3^y + 5$.

Exercice 21 Trouver tous les entiers $m, n \geq 0$ tels que $3^m - 7^n = 2$.

Exercice 22 Trouver tous les entiers $k, n, m \geq 0$ tels que $5^n - 3^k = m^2$.

Exercice 23 Trouver tous les entiers $a, b, c, d \geq 1$ tels que $4^a \cdot 5^b - 3^c \cdot 11^d = 1$.

Exercice 24 Trouver tous les nombres entiers $x, y \geq 1$ tels que $7^x = 3^y + 4$.

Exercice 25 Trouver tous les entiers $x, y \geq 0$ tels que $33^x + 31 = 2^y$.

Exercice 26 Trouver tous les entiers $x, y \geq 1$ tels que $2^x + 3 = 11^y$.

Exercice 27 Trouver tous les entiers $x, y \geq 1$ tels que $2^x - 5 = 11^y$.

Troisième partie

Les exercices suivants, un peu plus exotiques, n'ont pas été abordés pendant la séance.

Exercice 28 Soient $m, n \geq 3$ deux entiers impairs. Montrer que $2^m - 1$ ne divise pas $3^n - 1$.

Exercice 29 Soient a et b deux entiers strictement positifs avec $(a, b) \neq (1, 1)$ et tels que $ab - 1$ divise $a^2 + b^2$. Montrer que $a^2 + b^2 = 5ab - 5$.

Exercice 30 Soient a et b deux entiers positifs impairs tels que $2ab+1$ divise a^2+b^2+1. Montrer que $a = b$.

Exercice 31 Trouver tous les entiers $n \geq 1$ tels que 2^n-1 soit divisible par 3 et tels que $(2^n-1)/3$ divise $4m^2 + 1$ pour un certain entier $m \geq 1$.

Exercice 32 Soient $a > b > 1$ deux entiers avec b impair. Soit n un entier strictement positif. On suppose que b^n divise $a^n - 1$. Montrer que $a^b > 3^n/n$.

Solution des exercices

<u>*Solution de l'exercice 1*</u> (Manipulations algébriques, utilisant le fait que si $a \mid b$, alors $a \mid b + ka$ pour tout entier relatif k)

Soit $n \geq 1$ tel que $3^{n-1} + 5^{n-1} \mid 3^n + 5^n$. Alors

$$3^{n-1} + 5^{n-1} \mid 5(3^{n-1} + 5^{n-1}) - 3^n + 5^n = 2 \cdot 3^{n-1}.$$

Or $3^{n-1} + 5^{n-1} > 2 \cdot 3^{n-1}$ pour $n \geq 2$, donc $3^{n-1} + 5^{n-1}$ ne divise pas $2 \cdot 3^{n-1}$ pour $n \geq 2$. Réciproquement, on vérifie que $n = 1$ convient.

<u>*Solution de l'exercice 2*</u> (Ordres de grandeurs, utilisant le fait que si $b \geq 1$ et $a \mid b$, alors $a \leq b$)

Soient $a, b \geq 1$ vérifiant les conditions de l'énoncé, et, par symétrie, supposons $b \geq a$. Alors $a^2 + b \geq b^2 - a$ et $b^2 + a \geq a^2 - b$, ce qui s'écrit également

$$(a - b + 1)(a + b) \geq 0, \qquad (b - a + 1)(a + b) \geq 0.$$

On en déduit que $a = b$ ou $a = b - 1$.

Premier cas : $a = b$. Alors $a^2 - a \mid a^2 + a$. Or $\frac{a^2+a}{a^2-a} = \frac{a+1}{a-1} = 1 + \frac{2}{a-1}$. On en déduit les solutions $(a, b) = (2, 2), (3, 3)$.

Deuxième cas : $a = b - 1$. Dans ce cas, $\frac{a^2+b}{b^2-a} = 1$, et

$$\frac{b^2 + a}{a^2 - b} = \frac{(a+1)^2 + a}{a^2 - a - 1} = \frac{a^2 + 3a + 1}{a^2 - a - 1} = 1 + \frac{4a + 2}{a^2 - a - 1}.$$

Or

$$4a + 2 \geq a^2 - a - 1 \qquad \Longleftrightarrow \qquad a^2 - 5a - 3 \leq 0.$$

Comme $a^2 - 5a - 3$ est négatif pour $a = 5$ et positif pour $a = 6$, on en déduit que $a \leq 5$, et on vérifie que réciproquement seuls $a = 1, 2$ conviennent.

On trouve finalement $(a, b) = (1, 2), (2, 1), (2, 3), (3, 2), (2, 2), (3, 3)$ comme solutions.

<u>*Solution de l'exercice 3*</u> (Théorème d'Euler et manipulations d'inverses modulo un entier)

On note ϕ la fonction indicatrice d'Euler, et on remarque que $\phi(49) = \phi(7^2) = 7^2 - 7 = 42$. Ainsi, $6^{84} \equiv 1 \mod 49$ et $8^{84} \equiv 1 \mod 49$. Ainsi, en notant x^{-1} l'inverse de x modulo 49 lorsque x est premier avec 49, on a

$$\begin{aligned} 6^{83} + 8^{83} &\equiv (6^{84}) \cdot 6^{-1} + (8^{84}) \cdot 8^{-1} \mod 49 \\ &\equiv 6^{-1} + 8^{-1} \mod 49. \end{aligned}$$

En factorisant par $6^{-1}8^{-1}$, on obtient :

$$\begin{aligned} 6^{-1} + 8^{-1} &\equiv (6 + 8)6^{-1}8^{-1} \mod 49 \\ &\equiv 14 \cdot 48^{-1} \mod 49 \\ &\equiv 14 \cdot (-1) \mod 49 \\ &\equiv 35 \mod 49. \end{aligned}$$

La réponse est donc 35.

<u>*Solution de l'exercice 4*</u> (Théorème chinois)

De manière équivalente d'après le théorème chinois, on calcule 1032^{1032} modulo 4, puis modulo 25. Tout d'abord, il est clair que $1032^{1032} \equiv 0 \mod 4$. Ensuite,

$$1032^{1032} \equiv 7^{1032} \equiv (-1)^{516} \equiv 1 \mod 25.$$

On en déduit aisément que $1032^{1032} \equiv 76 \mod 100$.

<u>*Solution de l'exercice 5*</u> (Ordre multiplicatif)

Soit q un diviseur premier de $2^p - 1$. Soit ω l'ordre de 2 modulo q. Alors ω divise p, de sorte que $\omega = 1$ ou $\omega = p$. Dans le premier cas, on aurait $2 \equiv 1 \mod q$, absurde. Donc $\omega = p$. Or, d'après le petit théorème de Fermat, $2^{q-1} \equiv 1 \mod q$. Donc p divise $q - 1$, de sorte que $q - 1 \geq p$, ce qui implique que $q > p$.

<u>*Solution de l'exercice 6*</u> (Ordre multiplicatif)

Comme p divise $q^r + 1$, il divise également $q^{2r} - 1$. Ainsi, en notant ω l'ordre de q modulo p, on a $\omega \mid 2r$. Comme p est impair, il ne peut pas diviser $q^r - 1$. Ainsi $\omega \in \{1, 2, 2r\}$.

Cas 1 : $\omega = 1$. Dans ce cas, p divise $q - 1$, et donc p divise bien $q^2 - 1$.

Cas 2 : $\omega = 2$. Dans ce cas, p divise $q^2 - 1$.

Cas 3 : $\omega = 2r$. Dans ce cas, d'après le petit théorème de Fermat, $q^{p-1} \equiv 1 \mod p$, et donc $2r$ divise $p-1$.

Ceci conclut.

Solution de l'exercice 7 (Ordres de grandeur)

Soient (x, y) une solution. On a clairement $x > y$, et $(x-y)(x^2+xy+y^2) = xy+61$. On en déduit que $x^2+xy+y^2 \leq xy+61$, et donc $2y^2 < x^2+y^2 < 61$, de sorte que $y \leq 5$. On vérifie aisément que, réciproquement, seul $y = 5$ donne la solution $(6, 5)$.

Solution de l'exercice 8

On travaille modulo 8 : on remarque que $3^m + 3^n + 1$ est congru à 3, 5 ou 7 modulo 8. Or un carré est congru à 0, 1 ou 4 modulo 8, ce qui conclut.

Solution de l'exercice 9

On vérifie que $y = 1$ donne la solution $x = 2$, et que $y = 2$ ne donne pas de solution. On suppose donc $y \geq 3$. Il judicieux de travailler modulo 8 : on doit avoir $3^x \equiv 7 \mod 8$. Or une puissance de 3 n'est jamais congrue à 7 modulo 8, ce qui conclut.

Solution de l'exercice 10 Modulo 3, on voit que $3 \mid y$, puis que $3 \mid x$. En écrivant $y = 3y'$ et $x = 3x'$, on obtient $15x'^2 - 7y'^2 = 1$. On arrive alors à une contradiction modulo 3 car 2 n'est pas un carré modulo 3.

Solution de l'exercice 11 On a affaire à une puissance 5 connue ; on regarde donc modulo 11 : $n^5 + 7$ peut être congru 6, 7 ou 8 modulo 11, mais on vérifie qu'un carré n'est jamais congru à ces nombres modulo 11.

Solution de l'exercice 12 Regardons l'expression modulo 3 : $2^n + 12^n + 2014^n \equiv (-1)^n + 1 \mod 3$. Comme un carré n'est jamais congru à 2 modulo 3, on en déduit que n est impair. Regardons ensuite l'expression modulo 7 :

$$2^n + 12^n + 2014^n \equiv 2^n + (-2)^n + 5^n \equiv 5^n \mod 7$$

car n est impair. Lorsque n est impair, 5^n ne peut être congru qu'à 3, 5 ou 6 modulo 7. Or un carré est congru à $0, 1, 2$ ou 4 modulo 7. Il n'existe donc pas d'entiers $n \geq 1$ tels que $2^n + 12^n + 2014^n$ soit un carré parfait.

Solution de l'exercice 13 Nous allons montrer qu'il n'existe pas de tels rationnels x, y, z. On raisonne par l'absurde en supposant qu'il en existe. Soit d le plus petit dénominateur commun de x, y et z. On peut alors écrire $x = \frac{a}{d}$, $y = \frac{b}{d}$ et $z = \frac{c}{d}$ pour certains entiers a, b et c. L'équation que l'on cherche à résoudre devient alors :

$$a^5 + 2b^5 + 5c^5 = 11d^5.$$

Comme nous avons affaire à des puissances cinquièmes, il est judicieux d'étudier cette équation modulo 11. Une recherche exhaustive (ou l'utilisation du petit théorème de Fermat) montre qu'une puissance 5-ième est congrue à 0, 1 ou -1 modulo 11. On en déduit que la congruence $a^5 + 2b^5 + 5c^5 \equiv 0 \pmod{11}$ implique que a, b et c sont tous les trois multiples de 11. Ainsi, $a^5 + 2b^5 + 5c^5$ est divisible par 11^5, d'où on déduit que d est lui aussi divisible par 11. Les fractions $\frac{a}{d}$, $\frac{b}{d}$ et $\frac{c}{d}$ peuvent donc, toutes les trois, être simplifiées par 11. Ceci contredit la minimalité de d et termine la démonstration.

Solution de l'exercice 14

On a affaire à des puissances troisièmes et quatrièmes (exposants connus). D'après ce qu'on a vu, il est judicieux de considérer un nombre premier p congru à 1 modulo 3 et congru à 1 modulo 4, par exemple $p = 13$. On voit qu'effectivement, modulo 13, un cube est congru à $0, 1, 5, 8, 12$ et une puissance quatrième à $0, 1, 3, 9$. Or

$$19^{19} \equiv (6^{12}) \cdot 6^7 \equiv (6^2)^3 \cdot 6 \equiv (-3)^3 \cdot 6 \equiv 7 \mod 13.$$

Or il n'est pas possible de former un entier congru à 7 modulo 13 en additionnant un entier choisi dans $\{0, 1, 5, 8, 12\}$ avec un entier choisi dans $\{0, 1, 3, 9\}$. Ceci conclut.

Solution de l'exercice 15 On a affaire à des puissances 5 et 2 (exposants connus). D'après ce qu'on a vu, il est judicieux de considérer un nombre premier p congru à 1 modulo 5 et congru à 1 modulo 2, par exemple $p = 11$. On voit qu'effectivement, modulo 11, une puissance cinquième est congrue à $0, 1, 10$ et un carré à $0, 1, 3, 4, 5, 9$. Or il n'est pas possible de former un entier congru à 4 modulo 11 en soustrayant à un entier choisi dans $\{0, 1, 10\}$ un entier choisi dans $\{0, 1, 3, 4, 5, 9\}$. Ceci conclut.

Solution de l'exercice 16 Tout d'abord, $(a, y) = (1, 1)$ est solution. On suppose donc que $a, y \geq 2$. En regardant modulo 9 et en utilisant le fait que l'ordre de 7 modulo 9 vaut 3, on obtient que $y \equiv 0 \mod 3$. On cherche donc p tel que l'ordre de 7 modulo p vaut 3. Dans ce cas, on doit avoir $p \mid 7^3 - 1$ et on voit que $p = 19$ convient. Ainsi, $3^{2a-1} + 3^a + 1 \equiv 1 \mod 19$. (Alternativement, on aurait pu direcement dire que comme 3 divise y, 19 divise $7^3 - 1$ qui divise $7^y - 1$).

Donc $19 \mid 3^{a-1} + 1$, donc $3^{a-1} \equiv 18 \mod 19$. Or l'ordre de 3 modulo 9 vaut 18. On en déduit que $a \equiv 10 \mod 18$.

On cherche donc ensuite p tel que l'ordre de 3 modulo p vaut 18 ou, pour simplifiser, divise 18 si possible. On trouve que $p = 7$ convient (l'ordre de 3 modulo 7 vaut 6). Modulo 7, on a donc $3^{19} + 3^{10} + 1 \equiv 0 \mod 7$, ce qui est absurde.

Solution de l'exercice 17 Supposons que a^5b+3 et ab^5+3 soient tous les deux des cubes. D'après ce qu'on a vu, il est judicieux de considérer l'équation modulo 9. Tout d'abord, il est clair que 3 ne divise ni a, ni b. Or un cube non divisible par 3 est congru à 1 ou 8 modulo 9. Ainsi, a^5b et ab^5 sont congrus à 5 ou 7 modulo 9. Leur produit est donc congru à 4, 7 ou 8 modulo 9. Or $a^5b \cdot ab^5 = (ab)^6 \equiv 1 \mod 9$ d'après le théorème d'Euler. Absurde.

Solution de l'exercice 18 On va montrer qu'il n'y a pas de solutions. Tout d'abord, il est clair que n est pair. Modulo 8, on voit que r est pair. Écrivons donc $r = 2s$. L'équations se réécrit alors $n^5 = (1221^s - 7^m)(1221^s + 7^m)$. Comme le PGCD de $1221^s - 7^m$ et de $1221^s + 7^m$ vaut 2, deux cas de figure se présentent.

Cas 1. $1221^s - 7^m = 2x^5$ et $1221^s + 7^m = 16y^5$ avec $x, y \geq 1$ entiers. Alors $1221^s = x^5 + 8y^5$ et $7^m = 8y^5 - x^5$. Comme on a affaire à des puissances 5-ièmes, il est judicieux de considérer l'équation modulo 11. Comme une puissance 5-ième est congrue 0, 1 ou -1 modulo 11, de $0 \equiv 1221^s \equiv x^5 + 8y^5 \mod 11$, on voit que 11 divise x et y, ce qui contredit le fait que $7^m = 8y^5 - x^5$.

Cas 2. $1221^s - 7^m = 16x^5$ et $1221^s + 7^m = 2y^5$ avec $x, y \geq 1$ entiers. Comme dans le premier cas, on trouve que $1221^s = 8x^5 + y^5$ et $7^m = y^5 - 8x^5$. Modulo 11, on trouve encore que 11 divise à la fois x et y, ce qui est absurde.

Solution de l'exercice 19 La quantité $1 - 8 \cdot 3^a + 2^{a+2}(2^a - 1)$ est égale à $(2^{a+1} - 1)^2 - 2^3 \cdot 3^a$. On remarque que c'est un carré pour $a = 3$ (elle vaut $9 = 3^2$) et $a = 5$ (elle vaut $2045 = 25^2$) mais pas pour $a \in \{1, 2, 4, 6, 7, 8\}$. On suppose dorénavant $a \geq 9$.

Supposons que $1-8\cdot 3^a+2^{a+2}(2^a-1)$ soit un carré, c'est-à-dire, puisque cette quantité est impaire, qu'il existe un entier impair k tel que

$$(2^{a+1}-1)^2-2^3\cdot 3^a=(2k+1)^2. \tag{III.1}$$

Ainsi

$$(2^{a+1}-1)^2-(2k+1)^2=2^3\cdot 3^a, \tag{III.2}$$

soit encore $(2^a-k-1)(2^a+k)=2\cdot 3^a$. Il existe alors un entier $b\geq 0$ tel que l'une des deux situations suivantes se produit (en discutant selon la parité de k) :

Cas 1. On a $2^a+k=2\cdot 3^b$ et $2^a-k-1=3^{a-b}$.

Cas 2. On a $2^a+k=3^b$ et $2^a-k-1=2\cdot 3^{a-b}$.

Traitons d'abord le cas 1. On a $2k+1=2\cdot 3^b-3^{a-b}$, et donc $b\geq a-b$. De plus, $2^{a+1}-1=3^{a-b}+2\cdot 3^b$. Donc

$$2^{a+1}-1=3^{a-b}(1+2\cdot 3^{2b-a}).$$

Comme $a\geq 9$, on a $a-b\geq 3$, de sorte que 3^3 divise $2^{a+1}-1$. Or l'ordre de 2 modulo 3^3 vaut 18. Donc $a\equiv 17 \mod 18$. Il est donc naturel de considérer l'équation modulo 19 car alors 2^{a+1} est constant modulo 19, et vaut 1 (alternativement, $19\mid 2^{18}-1\mid 2^{a+1}-1$). Donc

$$(2^{a+1}-1)^2-2^3\cdot 3^a\equiv (1-1)^2-2^3\cdot 13\equiv 10 \mod 19.$$

Alors, par (III.1), $(2k+1)^{18}\equiv 10^9=18 \mod 19$, ce qui contredit le petit théorème de Fermat.

Traitons le cas 2. On a $2k+1=3^b-2\cdot 3^{a-b}$, et donc $b\geq a-b$. De plus, $2^{a+1}-1=3^b+2\cdot 3^{a-b}$. Donc

$$2^{a+1}-1=3^{a-b}(3^{2b-a}+2),$$

et on conclut comme dans le premier cas.

Il n'y a donc pas de solution $a\geq 9$. En conclusion, les seules solutions sont 3 et 5.

<u>*Solution de l'exercice 20*</u> Pour $x\leq 5, y\leq 3$, on trouve les solutions $(x,y)=(3,1)$ et $(x,y)=(5,3)$. On suppose donc $x\geq 6$ et $y\geq 4$.

Il est naturel de commencer par regarder modulo $3^4, 3^5, ..., 2^6, 2^7, ...$ On regarde modulo 2^6 : l'ordre de 3 modulo 64 vaut 16. On trouve donc que $y\equiv 11 \mod 16$. Pour rendre 3^y constant, il est naturel de regarder modulo $p=17$, car alors $3^y+5\equiv 3^{11}+5\equiv 12 \mod 17$. Or on vérifie que les puissances de 2 ne valent jamais 12 modulo 17. Ceci montre qu'il n'y a pas d'autres solutions.

<u>*Solution de l'exercice 21*</u> On vérifie qu'il n'y a qu'une seule solution pour $m\leq 2$: $(m,n)=(2,1)$. On suppose donc que $m\geq 3$ et $n\geq 2$. On applique la méthode de Dan Schwarz en réécrivant l'équation sous la forme

$$3^2(3^{m-2}-1)=7(7^{n-1}-1).$$

Ainsi $3^2\mid 7^{n-1}-1$. Or l'ordre de 7 modulo 3^2 vaut 3. Donc $19\mid 7^3-1\mid 7^{n-1}-1$, de sorte que $19\mid 3^{m-2}-1$.

Or l'ordre de 3 modulo 19 vaut 18. Donc $37\mid 3^{18}-1\mid 3^{m-2}-1$, de sorte que $37\mid 7^{n-1}-1$.

Or l'ordre de 7 modulo 37 vaut 9. Donc $3^3\mid 7^9-1\mid 7^{n-1}-1$, de sorte que $3^3\mid 3^2(3^{m-2}-1)$. C'est absurde, il n'y a donc pas d'autres solutions.

<u>*Solution de l'exercice 22*</u> Modulo 4, on voit que k est pair. Modulo 3, on voit que n est pair. Écrivons donc $k=2p$ et $n=2q$. Ainsi, $(5^q-m)(5^q+m)=9^p$. Ccomme 5^q-m et 5^q+m sont

premiers entre eux, on a $5^q + m = 9^v$ et $5^q - m = 9^u$ avec $v > u \geq 0$. Alors $2 \cdot 5^q = 9^v + 9^u$, ce qui force $u = 0$. Ainsi, $2 \cdot 5^q = 9^p + 1$.

Si $q = 0$, $p = 0$ donne une solution. On suppose donc $q > 0$. Modulo 5, on voit que p est impair. Écrivons donc $p = 2r + 1$, de sorte que $2 \cdot 5^q = 3^{4r+2} + 1$. La valeur $q = 1$ donne la solution $p = 1$. Supposons donc $q \geq 2$. Comme l'ordre de 3 modulo 25 vaut 20, on a $8 = 3^2 - 1 \mid 3^{20} - 1 \mid 3^{4r+2} - 1$, ce qui est absurde.

Les seules solutions sont donc $(n, k, m) = (0, 0, 0)$ et $(n, k, m) = (2, 2, 4)$.

Remarque. À partir de $2 \cdot 5^q = 9^p + 1$, on aurait pu invoquer le théorème de Zsigmondy qui implique, lorsque $p \geq 2$, l'existence d'un nombre premier s tel que s divise $9^p + 1$ mais pas $9 + 1$.

Solution de l'exercice 23 On va montrer que la seule solution est $(a, b, c, d) = (1, 2, 2, 1)$.

Modulo 4, on a $3^{c+d} \equiv 3 \mod 4$, ce qui implique $c + d$ est impair.

Modulo 3, on trouve que b est impair. Écrivons $b = 2n$ avec $n \geq 1$.

Modulo 8, en utilisant le fait que $c + d$ est impair et b est pair, on trouve que $4^a \equiv 4 \mod 8$, ce qui implique $a = 1$.

Ainsi, $3^c \cdot 11^d = 4 \cdot 5^{2n} - 1$, ou encore $(2 \cdot 5^n - 1)(2 \cdot 5^n + 1) = 3^c \cdot 11^d$. Comme $2 \cdot 5^n - 1$ et $2 \cdot 5^n + 1$ sont premiers entre eux, deux cas de figure se présentent.

Cas 1. $2 \cdot 5^n - 1 = 3^c$ et $2 \cdot 5^n + 1 = 11^d$. Le cas $n = 1$ donne la solution $c = 2$ et $d = 1$. On suppose donc $n \geq 2$ et $d \geq 2$. L'ordre de 11 modulo 25 vaut 5, donc $3 \mid 11^{20} - 1 \mid 11^d - 1 = 2 \cdot 5^n$, ce qui est absurde.

Cas 2. $2 \cdot 5^n - 1 = 11^d$ et $2 \cdot 5^n + 1 = 3^c$. Le cas $n = 1$ ne donne pas de solutions, on suppose donc $n \geq 1$ et $c \geq 1$. L'ordre de 3 modulo 25 vaut 20, donc $3^2 - 1 \mid 3^{20} - 1 \mid 3^c - 1 = 2 \cdot 5^n$, ce qui est absurde.

Solution de l'exercice 24

Tout d'abord $(x, y) = (1, 1)$ est une solution, et il n'y a pas de solution pour $y = 2$. On suppose donc $y \geq 3$ par la suite.

Première solution. Réécrivons l'équation en utilisant la méthode de Dan Scwharz :

$$7(7^{x-1} - 1) = 3(3^{y-1} - 1).$$

L'ordre de 3 modulo 7 vaut 6. Donc $13 \mid 3^6 - 1 \mid 3^{y-1} - 1$, de sorte que $13 \mid 7^{x-1} - 1$.

Or l'ordre de 7 modulo 13 vaut 12. Donc $3^2 \mid 7^{12} - 1 \mid 7^{x-1} - 1$. Donc 3^2 divise $3(3^{y-1} - 1)$, absurde.

Deuxième solution. On a affaire à des puissances 7^x et 3^y inconnues. D'après ce qu'on a vu, il est judicieux de travailler modulo $7, 7^2, ..., 3, 3^2, ...$

En regardant modulo 7, on voit que y est impair. Puis, en regardant modulo 4, on voit que x est impair. Ensuite, modulo 5, on voit que x et y sont congrus à 1 modulo 4. Modulo 9, on trouve que x est congru à 2 modulo 3. D'après le théorème chinois, on en déduit que x est congru à 5 modulo 12. Donc, comme $7^{12} \equiv 1 \mod 13$, on en déduit que 7^x est congru à 11 modulo 13. Or, comme $y \equiv 1 \mod 4$, 3^y est congru à 1, 3 ou 9 modulo 13. Contradiction.

Troisième solution. Modulo 27, on a $7^x \equiv 4 \mod 27$. Or l'ordre de 7 modulo 27, noté ω, vaut 9. En effet, 27 divise $7^{18} - 1$ d'après le petit théorème de Fermat, de sorte ω divise 18. On vérifie que 27 ne divise pas $7^9 + 1$. Ainsi ω divise 9 et on vérifie que $\omega = 9$. Comme $7^8 \equiv 4 \mod 27$, on trouve que $x \equiv 8 \mod 9$.

Ainsi, x est constant modulo 9. D'après ce qu'on a vu, il peut être judicieux de trouver N tel que l'ordre de 7 modulo N soit 9. On a

$$7^9 - 1 = (7^3 - 1)(7^6 + 7^3 + 1) = (2 \cdot 3^2 \cdot 19) \cdot (3 \cdot 37 \cdot 1063).$$

On prend donc $N = 37$. Comme 37 ne divise pas $7^3 - 1$, l'ordre de 7 modulo 37 vaut bien 9. Ainsi, $7^x \equiv 7^8 \equiv 12 \mod 37$.

En regardant modulo 8, on voit que y est impair. Or 3^{2k+1} peut être congru à $3, 27, 21, 4, 36, 28, 30, 11$ ou 25 modulo 37, mais pas à 12. Ceci conclut.

Solution de l'exercice 25 Tout d'abord, $(x, y) = (0, 5)$ et $(x, y) = (1, 6)$ sont solutions. On suppose donc que $x \geq 2$ et $y \geq 7$. On applique la méthode de Dan Schwarz en réécrivant l'équation

$$3 \cdot 11(3^{x-1} - 1) = 2^6(2^{y-6} - 1).$$

Donc $2^6 \mid 3^{x-1} - 1$. Or l'ordre de 3 modulo 2^6 vaut 16. Donc $3^{16} - 1 \mid 3^{x-1} - 1$. Donc $193 \mid 3^{16} - 1 \mid 2^{y-6} - 1$. Mais l'ordre de 2 modulo 193 vaut 96, donc $3^2 \mid 2^{96} - 1 \mid 2^{y-6} - 1$. Donc $3^2 \mid 3 \cdot 11(3^{x-1} - 1)$, ce qui force $x = 1$ et conclut.

Solution de l'exercice 26 On vérifie tout d'abord que pour $x \leq 4$, seul $x = 3$ donne la solution $y = 1$. On suppose donc que $x \geq 5$ dans la suite.

Première solution. Appliquons la méthode Dan Schwarz en réécrivant l'équation sous la forme

$$2^3(2^{x-3} - 1) = 11 \cdot (11^{y-1} - 1).$$

Donc 11 divise $2^{x-3} - 1$. Or l'ordre de 2 modulo 11 vaut 10. Donc $13 \mid 2^{10} - 1 \mid 2^{x-3} - 1$, de sorte que $13 \mid 11^{y-1} - 1$.

Or l'ordre de 11 modulo 13 vaut 12. Donc $2^4 \mid 11^{12} - 1 \mid 11^{y-1} - 1$. Donc $2^4 \mid 2^3 \cdot (2^{x-3} - 1)$, ce qui est absurde.

Deuxième solution. Considérons l'équation modulo $2^5 = 32$. On a $11^y \equiv 3 \mod 32$. On vérifie que $11^7 \equiv 3 \mod 32$ et que l'ordre de 11 modulo 32 vaut 8. Ainsi, $y \equiv 7 \mod 8$.

Considérons l'équation modulo 11. On a $2^x \equiv 8 \mod 11$. On vérifie que l'ordre de 2 modulo 11 vaut 10, de sorte que $x \equiv 3 \mod 10$.

D'après ce qu'on a vu, il est judicieux de considérer l'équation modulo un nombre premier p tel que l'ordre de 11 modulo p vaut (ou divise) 8. Or

$$11^8 - 1 = (11^4 + 1)(11^2 + 1)(11 - 1)(11 + 1) = (2 \cdot 7321) \cdot (2 \cdot 61) \cdot (2 \cdot 5) \cdot (2^2 \cdot 3).$$

Prenons donc $p = 61$. L'ordre de 11 modulo 61 vaut alors 4, et $11^y \equiv 50 \mod 61$.

Or 2^x est de la forme $8 \cdot 2^{10k} \equiv 8 \cdot 48^k \mod 61$. Supposons qu'il existe un entier $k \geq 1$ tel que $8 \cdot 48^k \equiv 50 \mod 61$, ou encore, comme 23 est l'inverse de 8 modulo 61, que $48^k \equiv 52 \mod 61$. Or les puissances de 48 ne valent que $48, 47, 60, 14, 14$ et 1 modulo 61. Ceci conclut.

Troisième solution. En commencçant comme dans la deuxième solution, on aurait pu ensuite essayer de considérer l'équation modulo un nombre premier p tel que l'ordre de 11 modulo p est un multiple de 8. Pour cela, on remarque que 17 divise $11^8 + 1$, de sorte que l'ordre de 11 modulo 17 vaut 16. On vérifie que modulo 17 on obtient bien une contradiction.

Solution de l'exercice 27 Tout d'abord, $(x, y) = (4, 1)$ est solution. On suppose que $y \geq 2, x \geq 4$. On applique la méthode de Dan Schwarz en réécrivant l'équation

$$2^4(2^{x-4} - 1) = 11(11^{y-1} - 1).$$

Donc $2^4 \mid 11^{y-1} - 1$. Or l'ordre de 11 modulo 2^4 vaut 4. Donc $61 \mid 11^4 - 1 \mid 11^{y-1} - 1$, de sorte que $61 \mid 2^{x-4} - 1$. Mais l'ordre multiplicatif de 11 modulo 2^4 vaut 4. Donc $61 \mid 11^4 - 1 \mid 11^{y-1} - 1$. Or l'ordre de 2 modulo 61 vaut 60, donc $41 \mid 2^{60} - 1 \mid 2^{x-4} - 1$, de sorte que $41 \mid 11^{y-1} - 1$. Or l'ordre multiplicatif de 11 modulo 41 vaut 40, on a $2^5 \mid 11^{40} - 1 \mid 11^{y-1} - 1$, de sorte que $2^5 \mid 2^4(2^{x-4} - 1)$. Ceci est absurde et montre qu'il n'y a pas d'autres solutions.

Solution de l'exercice 28 (Réciprocité quadratique)

Soit p un diviseur premier impair de $3^n - 1$ (en particulier $p \neq 3$). Alors p divise $3^{n+1} - 3$. Comme $n + 1$ est pair, cela implique que 3 est un carré modulo p, c'est-à-dire que $\left(\frac{3}{p}\right) = 1$ (en utilisant le symbole de Legendre). D'après la loi de réciprocité quadratique,

$$\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{\frac{3-1}{2}\cdot\frac{p-1}{2}}.$$

Premier cas : $p \equiv 1 \mod 3$. Alors p est un carré modulo 3. D'après la loi de réciprocité quadratique, $(-1)^{(p-1)/2} = 1$. Donc $(p-1)/2$ est pair. Ainsi, $p \equiv 1 \mod 12$.

Deuxième cas : $p \equiv 2 \mod 3$. Alors p n'est pas un carré modulo 3. D'après la loi de réciprocité quadratique, $(-1)^{(p-1)/2} = -1$. Donc $(p-1)/2$ est impair. Ainsi, $p \equiv -1 \mod 12$.

On en déduit que tous les diviseurs de $3^n - 1$ sont congrus à 1 ou -1 modulo 12. Or $m \geq 3$ étant impair, on vérifie que $2^m - 1 \equiv 5 \mod 12$. Ceci conclut.

Solution de l'exercice 29 (Vieta Jumping)

Supposons par l'absurde que $\frac{a^2+b^2}{ab-1} = k$ avec $k \neq 5$. Parmi tous les couples (a, b) d'entiers strictement positifs tels que $a \geq b$ et $\frac{a^2+b^2}{ab-1} = k$, choisissons-en un minimisant la somme $a + b$, et notons le (a_1, b_1). On voit aisément que $a_1 \neq b_1$; en particulier $a_1 \geq b_1 + 1$.

Traitons déjà le cas $b_1 = 1$: alors $a-1$ divise a^2+1, et donc $a-1$ divise $a^2+1-(a+1)(a-1) = 2$. Donc $a = 2$ ou $a = 3$, ce qui donne $k = 5$ dans tous les cas, absurde. Ainsi, $b_1 \geq 2$.

Considérons le polynôme $P(x) = x^2 - x(kb_1) + b_1^2 + k = 0$. Par définition, $P(a_1) = 0$. Notons a_2 la seconde racine réelle de P.

Étape 1 : a_2 est entier. En effet, d'après les formules de Viète, $a_2 = kb_1 - a_1$.

Étape 2 : a_2 est strictement positif. En effet, d'après les formules de Viète, $a_2 = \frac{b_1^2+k}{a_1}$, ce qui prouve que $a_2 > 0$.

Étape 3 : $a_2 < a_1$. En effet, d'après les formules de Viète, $a_2 = \frac{b_1^2+k}{a_1}$. Or

$$a_2 < a_1 \iff b_1^2 + k < a_1^2 \iff \frac{a_1^2 + b_1^2}{a_1 b_1 - 1} < (a_1 - b_1)(a_1 + b_1) \iff a_1(b_1 a_1^2 - 2a_1 - b_1^3) > 0.$$

Or le polynôme $Q(x) = b_1 x^2 - 2x - b_1^3$ atteint son minimum en $x = 1/b_1$. On en déduit que $Q(a_1) \geq Q(b_1 + 1) = 2b_1^2 - b_1 - 2$, qui est strictement positif car $b_1 \geq 2$.

On a donc également $\frac{a_2^2+b_1^2}{a_2 b_1 - 1} = k$ avec $a_2 + b_1 < a_1 + b_1$, absurde.

Solution de l'exercice 30 (Vieta Jumping)

Supposons par l'absurde que $a \neq b$, et écrivons $k = \frac{a^2+b^2+1}{2ab+1}$. Clairement $k \neq 1$ car $a \neq b$. Parmi tous les couples (a, b) d'entiers impairs strictement positifs tels que $a \geq b$ et $k = \frac{a^2+b^2+1}{2ab+1}$, choisissons-en un minimisant la somme $a + b$, et notons le (a_1, b_1). Comme $k \neq 1$, on a $a_1 \neq b_1$.

Considérons le polynôme $P(x) = x^2 - 2b_1kx + b_1^2 - k + 1 = 0$. Par définition, $P(a_1) = 0$. Notons a_2 la seconde racine réelle de P.

Étape 1 : a_2 est un entier. En effet, d'après les formules de Viète, $a_2 = 2b_1k - a_1$.

Étape 2 : a_2 est impair et strictement positif. Le fait que a_2 soit impair découle de l'égalité $a_2 = 2b_1k - a_1$. Comme $a_2^2+b_1^2+1 = k(2a_1a_2+1)$, si $a_2 \leq -1$, on aurait $a_2^2+b_1^2+1 \leq k(1-2a_1) < 0$, absurde.

Étape 3 : $a_2 < a_1$. En effet, d'après les formules de Viète, $a_2 = \frac{b_1^2-k+1}{a_1}$. Ainsi,

$$a_2 < a_1 \iff b_1^2 - k + 1 < a_1^2 \iff b_1^2 - a_1^2 + 1 < \frac{a_1^2 + b_1^2 + 1}{2a_1b_1 + 1} \iff 2a_1(a_1 - b_1)(a_1 + a_1b_1 + b_1^2) > 0,$$

ce qui est le cas.

On a donc également $k = \frac{a_2^2+b_1^2+1}{2a_2b_1+1}$ avec $a_2 + b_1 < a_1 + b_1$, absurde.

Solution de l'exercice 31 (Nombres de Fermat, théorème chinois)

On montre que n est une puissance de 2.

Comme 3 divise $2^n - 1$, n est pair. On écrit $n = 2k$. La condition de l'énoncé se réécrit donc $\frac{4^k-1}{3} \mid 4m^2 + 1$.

Tout d'abord, montrons que ceci est vrai pour $k = 2^r$. On écrit

$$\frac{4^k - 1}{3} = \frac{4^{2^r} - 1}{3} = (4^{2^{r-1}} + 1)(4^{2^{r-2}} + 1) \cdots (4 + 1).$$

Pour prouver qu'il existe m tel que $4m^2 + 1$ est divisible par ce produit, nous allons utiliser le théorème chinois, en remarquant que $4^{2^a} = 2^{2^{a+1}} + 1 = F_{a+1}$ est le $a + 1$-ième nombre de Fermat. Il est bien connu que les nombres de Fermat sont deux à deux premiers entre eux (ceci découle par exemple de la formule $F_r = F_{r-1}F_{r-2} \cdots F_0 + 2$ qu'on prouve par récurrence). Il suffit donc de prouver que le système de congruences

$$\begin{aligned}
4m^2 + 1 &\equiv 0 \mod 4 + 1 \\
4m^2 + 1 &\equiv 0 \mod 4^2 + 1 \\
&\vdots \\
4m^2 + 1 &\equiv 0 \mod 4^{2^{r-2}} + 1 \\
4m^2 + 1 &\equiv 0 \mod 4^{2^{r-1}} + 1
\end{aligned}$$

admet une solution pour m. Or $4^{2^a} + 1 = 4(2^{2^a-1})^2 + 1$ pour $a \geq 0$, de sorte qu'une solution de $m^2 + 1 \equiv 0 \mod 4^{2^a} + 1$ est $m \equiv 2^{2^a-1} \mod 4^{2^a} + 1$. Ceci montre que le résultat voulu est vrai lorsque k (et donc n) est une puissance de 2.

Ensuite, supposons que k n'est pas une puissance de 2 en écrivant $k = p2^r$ avec $r \geq 0$ et $p \neq 1$ impair et soit m un entier tel que $\frac{4^k-1}{3} \mid 4m^2+1$. Nous allons aboutir à une contradiction. De même,

$$\frac{4^{2^r p} - 1}{3} = \frac{(4^{2^{r-1}p} + 1)(4^{2^{r-3}p} + 1) \cdots (4^p + 1)(4^p - 1)}{3}.$$

Comme $\frac{4^{2^r p}-1}{3}$ divise $4m^2+1$, $(4^p-1)/3$ divise également $4m^2+1$. Cependant, comme p est impair, $3 \mid 2^p+1$, et on peut écrire $(4^p-1)/3 = (2^p-1)\cdot((2^p+1)/3)$. On en déduit que $2^p-1 \mid 4m^2+1$.

Comme $p>1$ est impair, $2^p-1 \equiv 3 \mod 4$. Il existe donc un diviseur premier impair de 2^p-1 congru à 3 modulo 4 ; notons le q. Alors q divise $(2m)^2+1$, donc -1 est un carré modulo 4.

Solution de l'exercice 32 (Ordre, théorème LTE)

Il suffit de résoudre l'exercice pour b premier. En effet, si c'est le cas, si b n'est pas premier et q est un diviseur premier de b, alors $q^n \mid a^n-1$, et donc $a^b > a^q > 3^n/n$.

Supposons donc $b=p$ premier (impair), et notons ω l'ordre de a modulo p. D'après le petit théorème de Fermat, $\omega \mid p-1$. Donc $\omega \leq p-1$.

Comme $p \mid a^n-1$, $\omega \mid n$. Écrivons donc $n=\omega n_1$. D'après le théorème LTE, en notant v_p la valuation p-adique,

$$v_p(a^n-1) = v_p((a^\omega)^{n_1}-1) = v_p(a^\omega-1)+v_p(n_1) \geq n$$

car $p^n \mid a^n-1$.

Maintenant, comme $\omega \leq p-1$,

$$a^p > a^\omega - 1 \geq p^{v_p(a^\omega-1)} \geq p^{n-v_p(n_1)} = \frac{p^n}{p^{v_p(n_1)}} \geq \frac{p^n}{n_1} = \frac{\omega p^n}{n} \geq \frac{3^n}{n}$$

car $p^n \geq 3^n$.

2 mardi 18 après-midi : Xavier Caruso

Il s'agit d'un cours-TD dont l'objectif est de présenter les corps finis ainsi que quelques applications que ceux-ci peuvent avoir en arithmétique et en combinatoire. Durant la séance, les élèves ont été invités à réfléchir par eux-mêmes à tous les exemples qui ont été posés sous forme d'exercice.

Congruences dans la suite de Fibonacci

On rappelle que la suite de Fibonacci est définie par :

$$F_0 = 0, \quad F_1 = 1, \quad F_n = F_{n-1} + F_{n-2} \text{ pour } n \geq 2.$$

Étant donné un nombre premier p, on se propose d'étudier l'ensemble I_p des indices n pour lesquels F_n est un multiple de p. Un premier résultat classique — qu'il est bon de connaître et savoir redémontrer — est le suivant.

Proposition 44. Il existe un entier strictement positif a_p tel que I_p soit l'ensemble des multiples de a_p.

Démonstration. Commençons par démontrer qu'il existe un indice $a > 0$ tel que F_a soit multiple de p. Par le principe des tiroirs, il existe deux entiers i et j avec $i > j$ tels qu'on ait simultanément :

$$F_i \equiv F_j \pmod p \quad \text{et} \quad F_{i+1} \equiv F_{j+1} \pmod p. \tag{III.3}$$

On peut alors « remonter » ces congruences à $a = 0$ en inversant la relation de récurrence $F_n = F_{n-1} + F_{n-2}$. Plus précisément, cette dernière relation entraîne qu'un terme de la suite de Fibonacci est déterminé par les deux qui le suivent puisque l'on a $F_{n-2} = F_n - F_{n-1}$. Ainsi des relations (III.3), on déduit que $F_{i-1} \equiv F_{j-1} \pmod{p}$. Par récurrence, on arrive à $F_{i-j} \equiv F_0 = 0 \pmod{p}$. Comme $i - j > 0$, on conclut, comme souhaité, à l'existence d'un multiple de p non nul parmi les termes de la suite de Fibonacci.

Soit a_p le plus petit entier strictement positif tel que F_{a_p} soit multiple de p. Le terme suivant F_{a_p+1} n'est, lui, pas un multiple de p. En effet, si c'est le cas, en reprenant l'argument du paragraphe précédent, on trouverait que $F_1 = 1$ est multiple de p, ce qui n'est pas le cas. En posant $\lambda = F_{a_p+1}$, on démontre facilement par récurrence sur n que :

$$F_{a_p+n} \equiv \lambda \cdot F_n \pmod{p}.$$

Ceci, combiné à la minimalité de a_p, permet de conclure. □

Remarque 45. La démonstration ci-dessus fait fortement penser à celle de l'existence de l'ordre d'un élément dans $(\mathbb{Z}/p\mathbb{Z})^\times$. Comme nous le verrons par la suite, cette ressemblance est tout sauf fortuite.

On se propose maintenant d'étudier plus précisément ce nombre a_p. Pour cela, l'idée consiste à utiliser un analogue modulo p de la formule explicite

$$F_n = \frac{1}{\sqrt{5}} \cdot \left(\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right). \tag{III.4}$$

Bien sûr, le problème est qu'*a priori*, le symbôle $\sqrt{5}$ n'a pas de sens dans $\mathbb{Z}/p\mathbb{Z}$. Tout l'objectif de ce qui va suivre est de lui en donner un.

Lorsque $p = 2$, on obtient facilement $a_p = 3$ par le calcul. *À partir de maintenant, on supposera toujours que* $p > 2$.

Un premier cas facile. C'est celui où il existe un élement $\omega \in \mathbb{Z}/p\mathbb{Z}$ tel que $\omega^2 = 5$. Ceci se produit, par exemple, lorsque $p = 11$: on vérifie alors que $\omega = 4$ convient. Pour le moment, on se s'attarde par davantage sur cette hypothèse mais on y reviendra longuement par la suite.

On note $\bar{F}_n \in \mathbb{Z}/p\mathbb{Z}$ la classe de F_n modulo p. Supposant l'existence de ω et $p \neq 5$, la formule (III.4) admet un analogue modulo p qui s'écrit simplement :

$$\bar{F}_n = \omega^{-1} \cdot \left(\left(\frac{1+\omega}{2} \right)^n - \left(\frac{1-\omega}{2} \right)^n \right). \tag{III.5}$$

On rappelle que p est supposé impair, de sorte que la division par 2 est bien définie dans $\mathbb{Z}/p\mathbb{Z}$. Comment démontre-t-on cette formule ? Simplement en recopiant la démonstration de la formule usuelle (III.4) : on vérifie qu'elle est valide pour $n = 0$ et $n = 1$ puis on l'établit pour tout n par récurrence (en utilisant la relation $\omega^2 = 5$ bien entendu).

Remarque 46. Lorsque $p = 5$, on a $\omega = 0$ et la formule (III.5) n'a pas de sens. On dispose malgré tout d'une formule explicite pour $\bar{F}_n$ qui est $\bar{F}_n = 3^{n-1}n$ (la démonstration se fait également par récurrence). À partir de là — ou, plus simplement, en calculant les premiers $\bar{F}_n$ à la main — on déduit directement que $a_5 = 5$.

En supposant toujours que $p \neq 5$, on déduit de l'expression (III.5) que F_n est multiple de p si, et seulement si :

$$\left(\frac{1+\omega}{2}\right)^n = \left(\frac{1-\omega}{2}\right)^n$$

ce qui se réécrit encore, en remarquant que $\omega \neq 1$ (puisque $\omega^2 = 5 \neq 1$) :

$$\left(\frac{1+\omega}{1-\omega}\right)^n = 1.$$

Autrement dit, l'entier a_p n'est autre que l'ordre multiplicatif de l'élément $\frac{1+\omega}{1-\omega}$ de $\mathbb{Z}/p\mathbb{Z}$. En particulier, on déduit du petit théorème de Fermat que a_p est un diviseur de $p-1$ ou, si l'on préfère, que $F_{p-1} \equiv 0 \pmod{p}$.

L'autre cas. Il reste à traiter le cas où 5 n'est pas un carré modulo p. L'idée est alors d'ajouter artificiellement à $\mathbb{Z}/p\mathbb{Z}$ une racine carrée de 5, de la même manière qu'on ajoute une racine carrée de -1 à $\mathbb{R}$ pour obtenir $\mathbb{C}$. Concrètement, on considère l'ensemble $\mathbb{F}_{p^2}$ des expressions de la forme :

$$a + \omega b \quad \text{avec} \quad a, b \in \mathbb{Z}/p\mathbb{Z}.$$

Ces expressions s'addtionnent de la manière évidente et se multiplient en se rappelant que $\omega^2 = 5$:

$$(a+\omega b)\cdot(c+\omega d) = (ac+5bd) + \omega\cdot(ad+bc).$$

De même que dans $\mathbb{C}$, la méthode de la quantité conjuguée permet de montrer que tout élément non nul dans $\mathbb{F}_{p^2}$ a un inverse :

$$\frac{1}{a+\omega b} = \frac{a-\omega b}{a^2-5b^2} = \frac{a}{a^2-5b^2} + \omega\cdot\frac{-b}{a^2-5b^2}.$$

Dans l'expression ci-dessus, le dénominateur ne s'annule pas car on a supposé que 5 n'est pas un carré modulo p. (En effet, si le dénominateur s'annulait, 5 serait le carré de $\frac{a}{b} \in \mathbb{Z}/p\mathbb{Z}$.) À présent, on démontre exactement comme dans la partie précédente que la formule :

$$\bar{F}_n = \omega^{-1}\cdot\left(\left(\frac{1+\omega}{2}\right)^n - \left(\frac{1-\omega}{2}\right)^n\right)$$

vaut dans $\mathbb{F}_{p^2}$ et, par suite, que F_n est multiple de p si, et seulement si :

$$\left(\frac{1+\omega}{1-\omega}\right)^n = 1.$$

On est ainsi amené à étudier l'ordre multiplicatif des éléments de $\mathbb{F}_{p^2}$. *Grosso modo*, tout se passe comme dans $\mathbb{Z}/p\mathbb{Z}$, comme le précise la proposition suivante.

Proposition 47. Soit x un élément non nul de $\mathbb{F}_{p^2}$.

1. Il existe un entier strictement $\mathrm{ord}(x)$ tel que $x^k = 1$ si et seulement si k est multiple de $\mathrm{ord}(x)$.
2. On a $x^{p^2-1} = 1$; autrement dit $\mathrm{ord}(x)$ est un diviseur de p^2-1.

Remarque 48. La propriété 2 est l'analogue du petit théorème de Fermat.

Démonstration. La première assertion se démontre de la manière habituelle. Puisque $\mathbb{F}_{p^2}$ est un ensemble fini, d'après la principe de tiroirs, il existe deux entiers $i > j$ tels que $x^i = x^j$. En simplifiant par x^j, on obtient $x^{i-j} = 1$. On définit à présent $\mathrm{ord}(x)$ comme le plus petit entier strictement positif tel que $x^{\mathrm{ord}(x)} = 1$. On a alors $x^{\mathrm{ord}(x)+k} = x^k$ pour tout k, ce qui permet de conclure.

On démontre à présent la deuxième assertion. Pour cela, une possibilité consiste à remarquer que la multiplication par x permute les éléments de $\mathbb{F}_{p^2}^\times = \mathbb{F}_{p^2} \setminus \{0\}$. On a donc :

$$\prod_{y \in \mathbb{F}_{p^2}^\times} y = \prod_{y \in \mathbb{F}_{p^2}^\times} xy = x^{p^2-1} \cdot \prod_{y \in \mathbb{F}_{p^2}^\times} y$$

d'où on déduit $x^{p^2-1} = 1$ en simplifiant par $\prod_{y \in \mathbb{F}_{p^2}^\times} y$ qui n'est pas nul. □

Dans notre situation, le petit théorème de Fermat implique que a_p est un diviseur de $p^2 - 1$. En fait, on peut être plus précis et démontrer que a_p est même un diviseur de $p + 1$. Pour cela, on note $\rho = \frac{1+\omega}{1-\omega}$ et on vérifie que ρ est solution de l'équation de degré 2 :

$$x^2 - 3x + 1 = 0. \tag{III.6}$$

En élevant l'égalité $\rho^2 - 3\rho + 1 = 0$ à la puissance p, on obtient $\rho^{2p} - 3\rho^p + 1 = 0$ étant donné, d'une part, que $(a + b)^p = a^p + b^p$ dans $\mathbb{F}_{p^2}$ (puisque les autres termes de développement du binôme de Newton sont multiples de p) et, d'autre part, que $3^p = 3 \pmod p$ par le petit théorème de Fermat. Ainsi ρ^p est aussi une solution de (III.6). Par ailleurs $\rho^p \neq \rho$. En effet, l'équation polynômiale $x^p = x$ a au plus p solutions dans $\mathbb{F}_{p^2}$ qui sont exactement les éléments de $\mathbb{Z}/p\mathbb{Z}$ d'après le petit théorème de Fermat. Or, du fait que $\omega \notin \mathbb{Z}/p\mathbb{Z}$, on déduit que $\rho = \frac{3+\omega}{2}$ n'est pas non plus dans $\mathbb{Z}/p\mathbb{Z}$. En résumé, ρ et ρ^p sont les deux solutions de l'équation (III.6). On en déduit que leur produit vaut 1, c'est-à-dire que $\rho^{p+1} = 1$. Autrement dit, l'ordre de ρ est un diviseur de $p + 1$ et on a bien démontré que a_p divise $p + 1$.

La loi de réciprocité quadratique. On vient de démontrer, qu'en mettant à part les cas $p = 2$ et $p = 5$:

- si 5 est un carré modulo p, alors a_p divise $p - 1$, tandis que
- si 5 n'est pas un carré modulo p, alors a_p divise $p + 1$.

Telle qu'elle est formulée, la condition qui apparaît sur p ne semble pas facile à manipuler : naïvement, il semblerait que l'on ait besoin d'énumérer tous les éléments de $\mathbb{Z}/p\mathbb{Z}$ et de tester, pour chacun d'eux, si son carré est 5. Heureusement, on dispose de critères bien plus efficaces pour répondre à cette question. Le premier que l'on peut citer est le critère d'Euler.

Théoréme 49 (Critère d'Euler)**.** Soit p un nombre premier impair et soit a un élément non nul de $\mathbb{Z}/p\mathbb{Z}$. Alors a est un le carré d'un élément de $\mathbb{Z}/p\mathbb{Z}$ si, et seulement si $a^{(p-1)/2} = 1$.

Démonstration. On remarque tout d'abord que si a est le carré de $b \in (\mathbb{Z}/p\mathbb{Z})^\times$, alors $a^{(p-1)/2} = b^{p-1} = 1$ par le petit théorème de Fermat. Pour la réciproque, on considère le sous-ensemble $A \subset (\mathbb{Z}/p\mathbb{Z})^\times$ formé des carrés et le sous-ensemble $B \subset (\mathbb{Z}/p\mathbb{Z})^\times$ formé des solutions de l'équation $x^{(p-1)/2} = 1$. On vient de démontrer que $A \subset B$. Par ailleurs, B étant constitué des solutions d'une équation polynômiale de degré $\frac{p-1}{2}$, on a $\mathrm{card}\, B \leq \frac{p-1}{2}$. D'autre part, étant donné que, pour $a \in \mathbb{Z}/p\mathbb{Z}$, l'équation $x^2 = a$ a au plus deux solutions, l'ensemble A compte

au moins $\frac{p-1}{2}$ éléments. Ainsi :

$$\text{card } B \leq \frac{p-1}{2} \leq \text{card } A.$$

Comme on a, en outre, l'inclusion $A \subset B$, on en déduit que $A = B$ et le théorème est démontré. □

Remarque 50. Par des méthodes similaires, on peut démontrer plus généralement que $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ est une puissance k-ième si, et seulement si :

$$a^{\frac{p-1}{\text{PGCD}(p-1,k)}} = 1.$$

En particulier, si k est premier avec $p-1$, tout élément de $\mathbb{Z}/p\mathbb{Z}$ est une puissance k-ième.

Le second critère qu'on souhaite énoncer — et qui aboutit, dans notre situation, à une condition très simple de congruence — est la loi de réciprocité quadratique. Étant donnés deux nombres premiers distincts p et q, on définit le symbole de Legendre $\left(\frac{p}{q}\right)$ par :

$$\begin{aligned} \left(\tfrac{p}{q}\right) &= 1 \quad && \text{si } p \text{ est un carré modulo } q \\ &= -1 && \text{sinon.} \end{aligned}$$

Théoréme 51 (Loi de réciprocité quadratique)**.** Étant donnés deux nombres premiers impairs p et q, on a :

$$\left(\tfrac{p}{q}\right) \cdot \left(\tfrac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

Nous n'incluons pas la démonstration de la loi de réciprocité quadratique dans ce texte pour ne pas l'allonger de manière démesurée.

La loi de réciprocité quadratique appliquée avec $q = 5$ implique, qu'étant donné un nombre premier $p \notin \{2, 5\}$, 5 est un carré modulo p si, et seulement si p est un carré modulo 5. Il est immédiat de vérifier que cette dernière condition est elle-même équivalente à $p \equiv 1$ ou $4 \pmod 5$ (on rappelle que l'on suppose que p est premier avec 5). On obtient ainsi le théorème suivant.

Théoréme 52. Soit (F_n) la suite de Fibonacci et soit p un nombre premier. On note a_p le plus petit entier n pour lequel p divise F_n. Alors :

- pour $p = 5$, on a $a_5 = 5$,
- si $p \equiv 1$ ou $4 \pmod 5$, alors a_p divise $p - 1$,
- si $p \equiv 2$ ou $3 \pmod 5$, alors a_p divise $p + 1$.

La théorie des corps finis

Dans la partie précédente, pour les besoins de l'exercice, on a construit une *extension* de $\mathbb{Z}/p\mathbb{Z}$ en ajoutant une racine carrée manquante. Dans le cas des nombres réels, une fois ajoutée une racine carrée de -1, le processus se termine car l'ensemble de nombres obtenu $\mathbb{C}$ est algébriquement clos. Dans le cas de $\mathbb{Z}/p\mathbb{Z}$, les choses sont plus complexes : d'une part, comme on va le voir, il existe des équations « irréductibles » sans solution de tout degré > 1 et, d'autre part, on ne peut jamais obtenir un corps algébriquement après ajout d'un nombre fini de nouveaux éléments. Le but de ce paragraphe est de complètement clarifier ces phénomènes.

À partir de maintenant, on fixe un nombre premier p et on pose $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Construction générale d'une extension de $\mathbb{F}_p$. Dans le partie précédente, nous avions expliqué comment ajouter une racine carrée de 5 à $\mathbb{F}_p$ (pour $p \equiv 2$ ou $3 \pmod 5$). Notre objectif, ici, est d'étendre cette construction à l'ajout d'un élément ω qui est solution d'une équation polynomiale de degré arbitraire. On considère donc

$$P(x) = x^n + a_{n-1}x^n + \cdots + a_1 x + a_0$$

un polynôme unitaire à coefficients dans $\mathbb{F}_p$ que l'on suppose *irréductible*[1]. En particulier P n'a pas de racine dans $\mathbb{F}_p$ dès que $n > 1$ (en effet, dans le cas contraire, il serait divisible par $x - a$ en notant a la racine présumée).

On souhaite construire un corps[2] $\mathbb{F}_p[\omega]$ qui serait obtenu en ajoutant à $\mathbb{F}_p$ une racine ω de P. Si un tel objet existe, il doit contenir toutes les puissances de ω, et plus généralement toutes les expressions de la forme $Q(\omega)$ où Q est un polynôme à coefficients dans $\mathbb{F}_p$. Dès lors que Q est de degré au moins n, on peut utiliser la contrainte $P(\omega) = 0$ pour se ramener à un polynôme de degré inférieur. Par contre, cette réduction ne fonctionne pas si Q est de degré strictement plus petit que n. Pour cette raison, on est amené à définir $\mathbb{F}_p[\omega]$ comme l'ensemble des expressions formelles de la forme :

$$Q(\omega) = c_0 + c_1\omega + c_2\omega^2 + \cdots + c_{n-1}\omega^{n-1} \quad \text{avec} \quad c_0, \ldots, c_{n-1} \in \mathbb{F}_p$$

(la lettre Q désigne ainsi un polynôme à coefficients dans $\mathbb{F}_p$ de degré au plus $n-1$). De telles expressions s'additionnent de la manière évidente et se multiplient à l'aide de la relation $P(\omega) = 0$. En termes plus élaborés, le produit des expressions formelles $Q_1(\omega)$ par $Q_2(\omega)$ est défini comme étant $R(\omega)$ où R est le reste de la division euclidienne de Q_1Q_2 par P.

Le calcul de l'inverse est plus subtil mais néanmoins faisable. Soit $Q(\omega)$ un élément de $\mathbb{F}_p[\omega]$ que l'on suppose non nul (*i.e.* le polynôme Q n'est pas le polynôme nul). Cette dernière hypothèse assure que P et Q sont premiers entre eux puisque P est irréductible et de degré n. Ainsi, par le théorème de Bézout, il existe des polynômes U et V à coefficients dans $\mathbb{F}_p$ tels que $PU + QV = 1$. Ceci permet de mener le calcul suivant :

$$\frac{1}{Q(\omega)} = \frac{V(\omega)}{Q(\omega)V(\omega)} = \frac{V(\omega)}{P(\omega)U(\omega) + Q(\omega)V(\omega)} = V(\omega).$$

L'introduction de $P(\omega)$ est tout à fait légitime puisque, par construction, cette quantité est nulle dans $\mathbb{F}_p[\omega]$.

En bref, on a construit un ensemble $\mathbb{F}_p[\omega]$ qui contient manifestement $\mathbb{F}_p$ et, sur celui-ci, on a défini une addition, une multiplication et une division par les éléments non nuls. Le cardinal de cet ensemble que p^n (il y a p choix pour chacun des n coefficients c_i). De même que dans le cas de $\mathbb{F}_p$ et de $\mathbb{F}_{p^2}$, il est possible de définir et d'étudier l'ordre multiplicatif d'un élément de $\mathbb{F}_p[\omega]$. Précisément, on a la proposition suivante qui est l'exact analogue de la proposition 47 et qui se démontre de la même manière.

Proposition 53. Soit x un élément non nul de $\mathbb{F}_p[\omega]$.

1. Il existe un entier strictement positif $\mathrm{ord}(x)$ tel que $x^k = 1$ si et seulement si k est multiple de $\mathrm{ord}(x)$.

1. On étudiera plus en détails les polynômes irréductibles sur $\mathbb{F}_p$ dans le prochain paragraphe. Pour l'instant, on suppose simplement qu'un tel polynôme nous est donné.

2. C'est-à-dire un ensemble muni des opérations d'addition et de multiplication, dans lequel tout élément non nul est inversible.

2. On a $x^{p^n-1} = 1$; autrement dit $\mathrm{ord}(x)$ est un diviseur de $p^n - 1$.

Le corollaire 54 ci-après est une reformulation de la propriété 2 de la proposition ci-dessus. Toutefois, il a l'avantage de ne pas exclure le cas $x = 0$ et, pour cette raison, est souvent plus agréable à manipuler.

Corollaire 54. Tout élément x de $\mathbb{F}_p[\omega]$ vérifie $x^{p^n} = x$.

Proposition 55. Il existe dans $\mathbb{F}_p[\omega]$ un élément non nul d'ordre $p^n - 1$.

Démonstration. Montrons tout d'abord que, s'il existe dans $\mathbb{F}_p[\omega]$ un élément x d'ordre s et un élément x d'ordre t, alors il existe un élément d'ordre $\mathrm{PPCM}(s,t)$. Si s et t sont premiers entre eux, alors $z = \frac{x}{y}$ convient. En effet, de $z^k = 1$, on déduit $x^k = y^k$ puis, en élevant cette égalité à la puissance s, que t divise sk. Par le lemme de Gauss, t divise k. On démontre de même que s divise k. Ainsi st divise k et l'ordre de z est au moins égal à st. Par ailleurs, on a clairement $z^{st} = 1$, ce qui démontre que $\mathrm{ord}(z) = st$.

Si on ne suppose plus maintenant que s et t sont premiers entre eux, en décomposant s et t en facteurs premiers, on démontre tout d'abord que $\mathrm{PPCM}(s,t)$ peut s'écrire comme le produit de deux nombres *premiers entre eux* s' et t' tels que s' divise s et t' divise t. Les éléments $x' = x^{s/s'}$ et $y' = y^{t'/t}$ sont alors respectivement d'ordre s' et t'. D'après la première partie de la démonstration, il s'ensuit que $z' = \frac{x'}{y'}$ est d'ordre $s't' = \mathrm{PPCM}(s,t)$. Notre assertion est ainsi démontrée.

On considère, à présent, l'entier e défini comme le PPCM de l'ordre de tous les éléments non nuls de $\mathbb{F}_p[\omega]$. D'après ce qui précède, il existe un élément d'ordre e dans $\mathbb{F}_p[\omega]$. Il suffit donc de montrer que $e = p^n - 1$. On a déjà clairement $e \leq p^n - 1$. Par ailleurs, de la définition de e, il résulte que $x^e = 1$ pour tout élément non nul x de $\mathbb{F}_p[\omega]$. Ceci n'est pas possible si $e < p^n - 1$ car une équation algébrique de degré e a, au plus, e solutions. □

La proposition 55 détermine complètement la structure de la table de multiplication de $\mathbb{F}_p[\omega]$. En effet, si $g \in \mathbb{F}_p[\omega]$ est d'ordre $p^n - 1$, les g^i pour i variant dans $\{0, 1, \ldots, p^n - 2\}$ sont deux à deux distincts et donc énumèrent tous les éléments non nuls de $\mathbb{F}_p[\omega]$. D'autre part, la multiplication des g^i correspond évidemment simplement à l'addition des exposants modulo $p^n - 1$.

Les polynômes irréductibles sur $\mathbb{F}_p$. À partir de la donnée d'un irréductible P à coefficients dans $\mathbb{F}_p$, on a construit une extension $\mathbb{F}_p[\omega]$ de $\mathbb{F}_p$ en ajoutant à $\mathbb{F}_p$ une racine ω de P. La question se pose ainsi de savoir s'il y a beaucoup de tels polynômes irréductibles. En particulier, y en a-t-il de tout degré ? C'est l'objet de ce paragraphe de répondre à ces questions.

Pour ce faire, la clé est le corollaire 54. En effet, en reprenant les notations du paragraphe précédent, on remarque que la propriété 2 de cette proposition implique que le polynôme $P(x)$ divise $Q(x) = x^{p^n} - x$. En effet, on a $Q(\omega) = 0$ ce qui, en revenant aux définitions, signifie exactement que Q est multiple de P. De manière plus précise, on a la proposition suivante.

Proposition 56. Pour tout entier n, on a :

$$x^{p^n} - x = \prod_{\substack{P \text{ irréd.} \\ \deg P \mid n}} P(x)$$

où la notation signifie que le produit est étendu à tous les polynômes unitaires irréductibles P à coefficients dans $\mathbb{F}_p$ de degré divisant n.

Démonstration. En écrivant la décomposition en facteurs irréductibles de $x^{p^n} - x$, on se rend compte qu'il suffit de démontrer les trois résultats suivants :

1. tout polynôme irréductible de degré divisant n est un diviseur de $x^{p^n} - x$,
2. tout polynôme irréductible dont le degré ne divise pas n n'est pas un diviseur de $x^{p^n} - x$
3. le polynôme $x^{p^n} - x$ n'a pas de facteur irréductible double.

On a déja vu que tout polynôme irréductible de degré n divise $x^{p^n} - x$. La même démonstration permet d'établir le résultat 1.

On considère, à présent, un polynôme irréductible P dont le degré d ne divise pas n. Soit $\mathbb{F}_p[\omega]$ l'extension de $\mathbb{F}_p$ obtenue à partir de P ; on a donc $P(\omega) = 0$. On suppose par l'absurde que P divise $x^{p^n} - x$. Par le premier résultat, P divise également $x^{p^d} - x$ et donc, par un résultat classique, il divise également $x^{p^s} - x$ avec $s = \text{PGCD}(n, d) < d$. Ainsi $\omega^{p^s} = \omega$. Mais, pour tout polynôme Q à coefficients dans $\mathbb{F}_p$, ceci implique :

$$Q(\omega)^{p^s} = Q(\omega^{p^s}) = Q(\omega)$$

la première égalité s'obtenant après avoir remarqué que $(a + b)^p = a^p + b^p$ dans $\mathbb{F}_p[\omega]$ (car les autres coefficients binomiaux sont multiples de p). Autrement dit, tout élément $x \in \mathbb{F}_p[\omega]$ vérifie $x^{p^s} = x$. Mais ceci n'est pas possible car cette dernière équation est une équation polynomiale de degré p^s et ne peut donc avoir strictement plus de p^s solutions.

Il reste finalement à démontrer le résultat 3. On raisonne à nouveau par l'absurde en supposant que le polynôme $x^{p^n} - x$ ait un facteur irréductible double. On pourrait alors écrire :

$$x^{p^n} - x = F(x)^2 \cdot G(x)$$

pour des polynômes F et G avec $\deg F > 1$. Mais, en dérivant l'égalité précédent, on obtiendrait que F divise le polynôme constant -1, ce qui n'est clairement pas possible. □

Soit c_d le nombre de polynômes unitaires irréductibles de degré d sur $\mathbb{F}_p$. En comparant les degrés dans l'égalité de la proposition 56, on obtient les égalités :

$$\forall n \geq 1, \quad \sum_{d|n} d c_d = p^n. \tag{III.7}$$

Les égalités de ce type peuvent s'inverser grâce à ce que l'on appelle la *fonction de Moebius*. Elle est définie par :

$$\begin{aligned} \mu(n) = (-1)^r \quad & \text{si } n = p_1 \cdots p_r \text{ où les } p_i \text{ sont des nombres premiers distincts} \\ = 0 \quad & \text{si } n \text{ est divisible par le carré d'un entier} > 1. \end{aligned}$$

On vérifie que $\sum_{d|n} \mu(n)$ vaut 1 si $n = 1$ et 0. En combinant ceci avec la relation (III.7), on trouve :

$$c_n = \sum_{d|n} \mu(d) \cdot \frac{p^d}{d}.$$

On déduit de cela que c_n est de l'ordre de $\frac{p^n}{n}$; autrement dit, parmi les polynômes unitaires de degré n à coefficients dans $\mathbb{F}_p$, environ un sur n est irréductible [3]. En particulier, on peut démontrer à partir de là qu'il existe des polynômes irréductibles de tout degré sur $\mathbb{F}_p$.

3. Ce résultat est à mettre en parallèle avec le théorème des nombres premiers qui assure que parmi les nombres de n chiffres, il y a une proportion inversement proportionnelle à n de nombres premiers.

La clôture algébrique de $\mathbb{F}_p$. De ce qui précède, il suit que, contrairement à ce qui se passait avec $\mathbb{R}$, il n'est pas possible d'obtenir un corps algébriquement clos en ajoutant une seule valeur supplémentaire ω. Il y a, en fait, deux raisons à cela : la première est l'existence de polynômes irréductibles de tout degré et la seconde est le corollaire 54 qui implique que l'équation $x^{p^n} = x + 1$ n'a pas de solutions dans $\mathbb{F}_p[\omega]$ si ce dernier est de cardinal p^n.

Malgré tout, travailler dans une clôture algébrique de $\mathbb{F}_p$ peut être agréable. Pour l'obtenir, on peut énumérer les polynômes irréductibles à coefficients par $\mathbb{F}_p$ (en les ordonnant selon le degré, par exemple) et ajouter successivement des solutions à chacun d'eux en suivant la méthode présentée précédemment [4]. On aboutit comme ceci, à un nouvel ensemble de nombres noté $\bar{\mathbb{F}}_p$ qui vérifie les deux propriétés suivantes :

- tout élément de $\bar{\mathbb{F}}_p$ est solution d'une équation polynomiale à coefficients dans $\mathbb{F}_p$, et
- tout polynôme à coefficients dans $\bar{\mathbb{F}}_p$ a une racine dans $\bar{\mathbb{F}}_p$.

Un des intérêts de disposer d'une clôture algébrique est qu'elle contient naturellement tous les corps $\mathbb{F}_p[\omega]$ qui ont été construits précédemment. En effet, soit P un polynôme irréductible de degré n à coefficients dans $\mathbb{F}_p$. On note $\mathbb{F}_p[\omega]$ le corps construit à partir de P et $\alpha \in \bar{\mathbb{F}}_p$ une racine de P. On peut alors considérer l'application :

$$\iota : \quad \mathbb{F}_p[\omega] \to \bar{\mathbb{F}}_p, \quad Q(\omega) \mapsto Q(\alpha)$$

(on rappelle que les éléments de $\mathbb{F}_p[\omega]$ sont, par définition, les symbôles $Q(\omega)$ où Q est un polynôme de degré au plus $n-1$). Il est facile de vérifier que celle-ci est compatible aux opérations : on a $\iota(x+y) = \iota(x) + \iota(y)$ et $\iota(xy) = \iota(x)\iota(y)$ pour tous x et y dans $\mathbb{F}_p[\omega]$. De plus, ι est injective. En effet, de $Q(\alpha) = 0$, on déduit que P et Q ne sont pas premiers entre eux, et donc que P divise Q puisque P est irréductible. Ainsi Q doit être le polynôme nul puisqu'il est de degré strictement inférieur à celui de P.

L'application ι dépend du choix de la racine α de P dans $\bar{\mathbb{F}}_p$. Par contre, son image n'en dépend pas comme le précise la proposition suivante.

Proposition 57. L'image de ι est exactement formée des solutions dans $\bar{\mathbb{F}}_p$ de l'équation polynomiale $x^{p^n} = x$.

Démonstration. Pour simplifier les notations, appelons A l'image de ι et B le sous-ensemble de $\bar{\mathbb{F}}_p$ formé des éléments x, solutions de $x^{p^n} = x$. D'après le corollaire 54, on a $A \subset B$. Par ailleurs, on déduit de l'injectivité de ι que le cardinal de A est p^n. Le cardinal de B, quant à lui, est au plus p^n puisque B consiste en les solutions d'une équation polynomiale de degré p^n. La proposition résulte de ces observations. □

Non seulement la proposition 57 implique que l'image de ι ne dépend pas du choix de α mais, mieux encore, elle implique que les images dans $\bar{\mathbb{F}}_p$ de deux extensions $\mathbb{F}_p[\omega_1]$ et $\mathbb{F}_p[\omega_2]$ construites à partir de deux polynômes irréductibles P_1 et P_2 de *même* degré — mais *a priori* différents — coïncident. Autrement dit, vu dans $\bar{\mathbb{F}}_p$, il y a un *unique* corps de cardinal p^n : c'est l'ensemble des solutions de l'équation $x^{p^n} = x$. Ceci justifie que ce corps soit généralement simplement noté $\mathbb{F}_{p^n}$, sans que l'on fasse référence au polynôme irréductible P de degré n qui a été utilisé pour la construction.

4. Il y a malgré tout une mise en garde. En effet, un polynôme qui était initialement irréductible sur $\mathbb{F}_p$ peut se factoriser en produit de plusieurs facteurs sur le corps sur lequel on est en train de travailler. Si cela se produit, il suffit de considérer la factorisation en question et de travailler avec chaque facteur successivement.

Proposition 58. Étant donnés deux entiers m et n, on a :

$$\mathbb{F}_{p^n} \cap \mathbb{F}_{p^m} = \mathbb{F}_{p^d} \quad \text{avec} \quad d = \text{PGCD}(n, m).$$

En particulier, l'inclusion $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m}$ a lieu si, et seulement si n divise m.

Démonstration. La proposition résulte de la proposition 57 et de l'égalité « bien connue » $\text{PGCD}(x^{p^n} - x,\, x^{p^m} - x) = x^{p^d} - x$ (laissée en exercice au lecteur). □

Polynôme minimal et conjugués. Par définition, le *polynôme minimal* d'un élément $\alpha \in \bar{\mathbb{F}}_p$ est le polynôme unitaire $\mu_\alpha \in \mathbb{F}_p[x]$ de plus petit degré qui s'annule en α. Un tel polynôme existe toujours et il est irréductible. En effet, si μ_α pouvait s'écrire comme un produit non trivial PQ, on aurait soit $P(\alpha) = 0$, soit $Q(\alpha) = 0$, ce qui contredirait dans tous les cas la minimalité du degré. Les *conjugués* de α sont, par définition, les autres racines de μ_α dans $\bar{\mathbb{F}}_p$. De manière surprenante, on dispose d'une description très simple des polynômes minimaux et des conjugués dans ce contexte.

Proposition 59. Soit $\alpha \in \bar{\mathbb{F}}_p$. Alors la suite $(\alpha^{p^i})_{i\geq 0}$ est périodique. De plus, si n désigne sa période, on a :

$$\mu_\alpha(x) = (x - \alpha) \cdot (x - \alpha^p) \cdot (x - \alpha^{p^2}) \cdots (x - \alpha^{p^{n-1}}).$$

Autrement dit, le polynôme minimal de α est de degré n et les conjugués de α sont exactement les α^{p^i} pour $i \in \{1, \ldots, n-1\}$.

Remarque 60. Si s est un entier strictement positif, la proposition ci-dessus s'étend à $\mathbb{F}_{p^s}$ comme suit : le polynôme minimal de α sur $\mathbb{F}_{p^s}$ — c'est-à-dire le polynôme de plus petit degré à coefficients dans $\mathbb{F}_{p^s}$ annulant α — est :

$$(x - \alpha) \cdot (x - \alpha^q) \cdot (x - \alpha^{q^2}) \cdots (x - \alpha^{q^{n-1}}).$$

où $q = p^s$ et n est la période de la suite des α^{q^i}.

Démonstration. On appelle provisoirement d le degré de μ_α et on considère le corps $\mathbb{F}_p[\omega]$ construit à partir du polynôme irréductible μ_α. Par le corollaire 54, on obtient $\omega^{p^d} = \omega$ puis, par suite, $\alpha^{p^d} = \alpha$. Ceci démontre la périodicité de la suite $(\alpha^{p^i})_{i\geq 0}$. On remarque à présent que si β est une racine de μ_α, alors il en est de même de β^p. En effet, comme cela a déjà été utilisé à plusieurs reprises, l'égalité $\mu_\alpha(\beta) = 0$ implique $\mu_\alpha(\beta^p) = 0$ par élévation à la puissance p. On en déduit, par une récurrence immédiate, que les α^{p^i} sont tous racines de μ_α. Ainsi μ_α est divisible par le polynôme :

$$P(x) = (x - \alpha) \cdot (x - \alpha^p) \cdot (x - \alpha^{p^2}) \cdots (x - \alpha^{p^{n-1}})$$

puisque les α^{p^i} sont deux à deux distincts pour i variant entre 0 en $n-1$. Il suffit donc de montrer pour conclure que les coefficients de P sont tous dans $\mathbb{F}_p$. Or, ces derniers sont égaux, au signe près, aux fonctions symétriques élémentaires $\sigma_i(\alpha, \alpha^p, \ldots, \alpha^{p^{n-1}})$ pour $i \in \{1, \ldots, n\}$. De plus, on a :

$$\begin{aligned}
\big(\sigma_i(\alpha, \alpha^p, \ldots, \alpha^{p^{n-1}})\big)^p &= \sigma_i(\alpha^p, \alpha^{p^2}, \ldots, \alpha^{p^n}) && \text{par l'argument habituel} \\
&= \sigma_i(\alpha^p, \alpha^{p^2}, \ldots, \alpha^{p^{n-1}}, \alpha) && \text{par la périodicité} \\
&= \sigma_i(\alpha, \alpha^p, \ldots, \alpha^{p^{n-1}}) && \text{par symétrie.}
\end{aligned}$$

Les coefficients de P sont donc tous solutions de l'équation $x^p = x$. D'après la proposition 57, ceci implique qu'ils sont dans $\mathbb{F}_p$, comme souhaité. □

En guise d'application de la proposition précédente, on peut étudier la factorisation des polynômes cyclotomiques sur $\mathbb{F}_p$. On rappelle que les polynômes cyclotomiques Φ_n peuvent être définis par les relations :

$$\forall n \geq 1, \quad X^n - 1 = \prod_{d|n} \Phi_d(x).$$

On a ainsi, par exemple :

$$\begin{aligned}
\Phi_1(x) &= x - 1 \\
\Phi_2(x) &= \tfrac{x^2-1}{\Phi_1(x)} = x + 1 \\
\Phi_3(x) &= \tfrac{x^3-1}{\Phi_1(x)} = x^2 + x + 1 \\
\Phi_4(x) &= \tfrac{x^4-1}{\Phi_1(x)\Phi_2(x)} = x^2 + 1.
\end{aligned}$$

Il suit de la définition ci-dessus que les polynômes cyclotomiques sont tous à coefficients entiers. Ils peuvent donc également être considérés comme des polynômes à coefficients dans $\mathbb{F}_p$. Soit $\omega_n \in \bar{\mathbb{F}}_p$ une racine de Φ_n. On a alors $\omega_n^n = 1$, $\omega_n^k \neq 1$ pour tout entier strictement positif $k < n$ et la factorisation complète de Φ_n s'écrit :

$$\Phi_n(x) = \prod_{k \in (\mathbb{Z}/n\mathbb{Z})^\times} (x - \omega_n^k)$$

où $(\mathbb{Z}/n\mathbb{Z})^\times$ désigne l'ensemble des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$, c'est-à-dire l'ensemble des classes d'entiers k premiers avec n. Par ailleurs, par la proposition 59, les conjugués de ω_n^k sont exactement les $\omega_n^{kp^i}$ pour i variant dans $\mathbb{N}$. Les facteurs irréductibles de Φ_n correspondent donc exactement aux orbites de la multiplication par p agissant sur $(\mathbb{Z}/n\mathbb{Z})^\times$. De la même manière, à partir de la remarque 60, on démontre que les facteurs irréductibles de $\Phi_n(x)$ sur $\mathbb{F}_{p^s}$ correspondent aux orbites de la multiplication par p^s agissant sur $(\mathbb{Z}/n\mathbb{Z})^\times$.

La norme et la trace. La norme (resp. la trace) d'un élement α de $\bar{\mathbb{F}}_p$ est défini comme le produit (resp. la somme) de α et de tous ses conjugués (sur $\mathbb{F}_p$ ou, éventuellement, sur une extension fixée $\mathbb{F}_{p^s}$). Néanmoins, pour avoir de bonnes propriétés, il est préférable de fixer deux extensions $\mathbb{F}_{p^s} \subset \mathbb{F}_{p^{ns}}$. On pose $q = p^s$. Suivant la proposition 59 (voir aussi la remarque 60), on pose pour $\alpha \in \mathbb{F}_{q^n}$:

$$\begin{aligned}
N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) &= \alpha \cdot \alpha^q \cdot \alpha^{q^2} \cdots \alpha^{q^{n-1}} = \alpha^{(q^n-1)/(q-1)} \\
\mathrm{tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) &= \alpha + \alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^{n-1}}.
\end{aligned}$$

On insiste sur le fait que la suite des α^{q^i} peut tout à fait être périodique de période divisant n (*e.g.* pour $\alpha \in \mathbb{F}_q$). Dans ce cas, la norme (resp. la trace) n'est pas le produit (resp. la somme) des conjugués de α mais en est une puissance (resp. un multiple). Quoi qu'il en soit, $N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)$ et $\mathrm{tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)$ sont tous les deux des éléments de $\mathbb{F}_q$. Autrement dit, on dispose d'applications :

$$N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) : \mathbb{F}_{q^n} \to \mathbb{F}_q \quad \text{et} \quad \mathrm{tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) : \mathbb{F}_{q^n} \to \mathbb{F}_q$$

qui vérifient les relations suivantes :

$$N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha\beta) = N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)\cdot N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\beta) \tag{III.8}$$

$$\mathrm{tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha+\beta) = \mathrm{tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) + \mathrm{tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\beta) \tag{III.9}$$

$$\mathrm{tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\lambda\alpha) = \lambda\cdot \mathrm{tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) \tag{III.10}$$

pour tout $\alpha,\beta\in\mathbb{F}_{q^s}$ et $\lambda\in\mathbb{F}_q$. On remarque, par ailleurs, qu'étant donné $y\in\mathbb{F}_q$, l'équation $\mathrm{tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)=y$ est une équation polynomiale de degré q^{n-1} et a donc au plus q^{n-1} solutions. Autrement dit, tout élement de $\mathbb{F}_q$ a au plus q^{n-1} antécédents par l'application $\mathrm{tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}$. Comme les cardinaux de $\mathbb{F}_{q^n}$ et $\mathbb{F}_q$ sont respectivement q^n et q, on en déduit que tout élément de $\mathbb{F}_q$ a exactement q^{n-1} antécédents par $\mathrm{tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}$. De la même manière, on démontre que tout élément non nul de $\mathbb{F}_{q^n}$ a $\frac{q^n-1}{q-1}$ antécédents par l'application $N_{\mathbb{F}_{q^n}/\mathbb{F}_q}$ tandis que 0, lui, a un unique antécédent.

Les relations (III.9)–(III.10) signifient que $\mathrm{tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}$ est une application $\mathbb{F}_q$-linéaire. La proposition suivante énonce une réciproque à cette propriété.

Proposition 61. Soit $f:\mathbb{F}_{q^n}\to\mathbb{F}_q$ une application $\mathbb{F}_q$-linéaire, c'est-à-dire une application vérifiant :

$$f(x+y)=f(x)+f(y) \quad \text{et} \quad f(\lambda x)=\lambda f(x)$$

pour tous $x,y\in\mathbb{F}_{q^n}$ et tout $\lambda\in\mathbb{F}_q$. Alors il existe un unique $a\in\mathbb{F}_{q^n}$ tel que $f(x)=\mathrm{tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(ax)$ pour tout $x\in\mathbb{F}_{q^n}$.

Démonstration. Notons $\mathcal{L}$ l'ensemble des applications $\mathbb{F}_q$-linéaires de $\mathbb{F}_{q^n}$ dans $\mathbb{F}_q$. On dispose d'une application :

$$L:\quad \mathbb{F}_{q^n}\to\mathcal{L},\quad a\mapsto\big(x\mapsto \mathrm{tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(ax)\big).$$

Il s'agit de montrer que L est bijective. Un argument standard d'algèbre linéaire — que nous nous reproduisons pas ici afin de ne pas encore allonger démesurément ce texte — montre que le cardinal de $\mathcal{L}$ est q^n. Il suffit donc de démontrer que L est injective. Par conséquent, on suppose que :

$$\mathrm{tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(ax)=\mathrm{tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(bx) \tag{III.11}$$

pour tout $x\in\mathbb{F}_{q^n}$ et on souhaite démontrer que $a=b$. En posant $c=a-b$, la condition (III.11) se réécrit $\mathrm{tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(cx)=0$ pour tout $x\in\mathbb{F}_{q^n}$. Or, d'après ce que l'on a vu précédemment, il existe un élément $u\in\mathbb{F}_{q^n}$ tel que $\mathrm{tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(u)=1$. Ceci implique que $c=0$ car, dans le cas contraire, on aurait $\mathrm{tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(cx)=1\neq 0$ pour $x=\frac{u}{c}$. Ainsi $a=b$ et la proposition est démontrée. □

Exercice 1 Soit $\alpha\in\mathbb{F}_{q^n}$. Montrer que si $\mathrm{tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha)=0$ alors il existe $\beta\in\mathbb{F}_{q^n}$ tel que $\alpha=\beta^q-\beta$.

Solution de l'exercice 1 On note $A\subset\mathbb{F}_{q^n}$ l'ensemble des éléments de trace nulle et $B\subset\mathbb{F}_{q^n}$ l'ensemble des éléments qui s'écrivent sous la forme $\beta^q-\beta$ pour un certain $\beta\in\mathbb{F}_{q^n}$. On veut démontrer que $A\subset B$. Or, on remarque que l'inclusion réciproque $B\subset A$ est vraie. Pour conclure, il suffit donc de démontrer que $\mathrm{Card}\,A\leq\mathrm{Card}\,B$. On a déjà vu que $\mathrm{Card}\,A=q^{n-1}$. On considère l'application $f:\mathbb{F}_{q^n}\to B$ qui à β associe $\beta^q-\beta$. Tout élément de B a, au plus, q antécédents par f puisque ces antécédents sont les solutions d'une équation polynômiale de degre q. On en déduit que $\mathrm{Card}\,B\geq\frac{q^n}{q}=q^{n-1}=\mathrm{Card}\,A$, comme voulu.

Quelques applications à la combinatoire

La structure des tables d'addition et de multiplication sur les $\mathbb{F}_{p^n}$ est tellement riche et particulière qu'elle permet de construire des ensembles possédant des propriétés combinatoires étonnantes. Dans cette dernière partie, nous présentons — et contemplons — quelques exemples dans cette direction.

Un problème de digicode. Soient n et q deux entiers strictement positifs. On se donne un ensemble E de cardinal q et on se propose de construire une suite $(u_n)_{n\geq 0}$ à valeurs dans E vérifiant les deux propriétés suivantes :

1. la suite $(u_n)_{n\geq 0}$ est périodique de période q^n, et
2. pour tout n-uplet $(a_0, \dots, a_{n-1}) \in q^n$, il existe $i \in \mathbb{N}$ tel que $u_{i+j} = a_j$ pour tout $j \in \{0, \dots n-1\}$.

Autrement dit, on cherche à construire un mot infini sur l'alphabet E qui soit périodique de période q^n et contienne comme sous-mot tout mot de longueur n. Avant de commencer, remarquons que la valeur q^n requise pour la période est minimale : en effet, si la suite (u_n) est périodique de période T, la propriété 2 ne peut être vérifiée qu'au maximum pour T uplets $(a_0, \dots, a_{n-1})$.

On remarque, pour débuter, que si q s'écrit comme le produit de deux entiers premiers entre eux s et t, alors le problème est résolu pour q dès lors qu'on sait le résoudre pour s et t (en conservant le même n). En effet, si l'on sait construire deux suites $(v_n)_{n\geq 0}$ et $(w_n)_{n\geq 0}$ solutions du problème pour les entiers s et t respectivement, alors il est facile de vérifier que la suite $(v_n)_{n\geq 0}$ définie par $u_n = (v_n, w_n)$ est solution du problème pour l'entier q. En décomposant q en facteur premiers, on se ramène au cas où q est une puissance d'un nombre premier, ce qu'on supposera à partir de maintenant.

On peut alors faire entrer dans la machine les corps $\mathbb{F}_q$ et $\mathbb{F}_{q^n}$. On considère un élément $g \in \mathbb{F}_{q^n}$ d'ordre $q^n - 1$ qui existe par la proposition 55. On définit la suite $(u'_n)_{n\geq 0}$ à valeurs dans $\mathbb{F}_q$ par $u'_n = \mathrm{tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(g^n)$. Cette suite est clairement périodique de période $q^n - 1$. Par ailleurs, nous allons démontrer qu'elle vérifie la propriété 2 pour les n-uplets $(a_0, \dots, a_{n-1}) \neq (0, \dots, 0)$. Par un argument de cardinalité, il suffit pour cela de démontrer que :

$$(u'_i, u'_{i+1}, \dots, u'_{i+n-1}) = (u'_j, u'_{j+1}, \dots, u'_{j+n-1}) \tag{III.12}$$

seulement si $i \equiv j \pmod{p^n - 1}$. Or, en revenant aux définitions, on se rend compte que l'égalité (III.12) implique :

$$\mathrm{tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}\big(g^i \cdot Q(g)\big) = \mathrm{tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}\big(g^j \cdot Q(g)\big) \tag{III.13}$$

pour tout polynôme $Q \in \mathbb{F}_q[x]$ de degré au plus $n-1$. En outre, il résulte de la proposition 59 que le polynôme minimal de g est de degré n. En comparant à nouveau les cardinaux, on en déduit que les $Q(g)$ énumèrent tous les éléments de $\mathbb{F}_{q^n}$ lorsque Q parcourt l'ensemble des polynômes sur $\mathbb{F}_q$ de degré au plus $n-1$. L'unicité dans la proposition 61 implique alors que $g^i = g^j$. Comme g est d'ordre $q^n - 1$, on obtient bien $i \equiv j \pmod{q^n - 1}$.

Pour conclure, il reste à ajouter la séquence $(0, 0, \dots, 0)$ mais, pour cela, il suffit de remplacer chaque occurrence de la séquence $(0, \dots, 0, 1)$ avec $n-1$ zéros par la séquence $(0, \dots, 0, 1)$ avec n zéros. Ce qui précède assure que l'on ajoute ainsi un 0 tous les $q^n - 1$ termes, obtenant ainsi une suite périodique de période q^n satisfaisant en outre à la propriété 2.

Un soupçon de géométrie. Il arrive parfois que la géométrie se mèle délicieusement à l'arithmétique pour venir au secours de la combinatoire. Comme mise en bouche, considérons le problème suivant. On cherche à construire deux ensembles finis E et $\mathcal{E} \subset \mathcal{P}(E)$ tels que :

1. tous les éléments de $\mathcal{E}$ (qui sont des parties de E) ont même cardinal,
2. si $A, B \in \mathcal{E}$ avec $A \neq B$, l'intersection $A \cap B$ est un singleton,
3. le nombre de façons d'écrire le singleton $\{x\}$ (pour $x \in E$) comme une intersection $A \cap B$ avec $A, B \in \mathcal{E}$, $A \neq B$ est indépendant de x.

Un premier candidat qui vient à l'esprit lorsqu'on lit la deuxième condition consiste à prendre pour $\mathcal{E}$ un ensemble de droites du plan puisque celles-ci s'intersectent généralement en un point. Toutefois — hormis le fait légèrement embêtant que cela ne fournit pas des ensembles finis — se pose le problème des droites parallèles. Une manière de contourner cette difficulté est de renverser le rôle des points et des droites : on va prendre pour E l'ensemble des droites du plan tandis que $\mathcal{E}$ sera formé des ensembles de la forme

$$E_x = \big\{ \text{droites du plan passant par } x \big\}$$

pour x parcourant le plan. Si x et y sont distincts, l'intersection $E_x \cap E_y$ est alors un singleton qui consiste en l'unique droite qui relie x à y.

Il reste à expliquer comment adapter cette construction pour obtenir des ensembles finis. L'idée est de remplacer $\mathbb{R}$ par l'un des $\mathbb{F}_q$. Plus précisément, on ne travaille avec le plan habituel $\mathbb{R}^2$, mais avec $\mathbb{F}_q^2$ pour un certain $q = p^s$ où p est un nombre premier et s est un entier. Par analogie avec $\mathbb{R}$, une droite de $\mathbb{F}_q^2$ est définie comme un ensemble de la forme :

$$\Delta_{a,b,c} = \big\{ \ (x,y) \in \mathbb{F}_q^2 \quad | \quad ax + by + c = 0 \ \big\}$$

où a, b et c sont des éléments de $\mathbb{F}_q$ tels que $(a,b) \neq (0,0)$. Comme dans le cas réel, on vérifie que deux droites $\Delta_{a,b,c}$ et $\Delta_{a',b',c'}$ coïncident si, et seulement si les vecteurs (a,b,c) et (a',b',c') sont proportionnels. Suivant ce que l'on a dit précédemment, on définit E comme l'ensemble des $\Delta_{a,b,c}$ (pour $a,b,c \in \mathbb{F}_q$ avec $a \neq b$). Par ailleurs, pour $M \in \mathbb{F}_q^2$, on définit E_M comme l'ensemble des $\Delta_{a,b,c}$ contenant le point M et on note $\mathcal{E}$ l'ensemble des E_M ainsi définis. En résolvant des systèmes linéaires, on vérifie facilement que :

- chaque $\Delta_{a,b,c}$ est de cardinal q,
- chaque E_M est de cardinal $q+1$,
- si M et N sont deux points distincts, l'intersection $E_M \cap E_N$ est un singleton : c'est celui dont l'unique élément est la droite (MN).

Les propriétés requises 1 et 2 sont ainsi vérifiées. Par ailleurs, étant donnée une droite $\Delta_{a,b,c} \in E$, un couple (M,N) avec $M \neq N$ vérifie :

$$E_M \cap E_N = \{ \Delta_{a,b,c} \} \tag{III.14}$$

si, et seulement si $\Delta_{a,b,c}$ est la droite (MN) ce qui se produit si, et seulement si M et N sont deux points de $\Delta_{a,b,c}$. Ainsi le nombre de couples (M,N) avec $M \neq N$ solutions de (III.14) est $q(q-1)$ et ne dépend donc pas de la droite $\Delta_{a,b,c}$ considérée.

Le plan projectif sur $\mathbb{F}_q$. Précédemment, afin d'éviter le problème des droites parallèles, on a inversé le rôle des points et des droites. Une autre solution — probablement plus naturelle pour ceux qui connaissent — est de travailler dans le plan projectif.

On rappelle, pour commencer, que le plan projectif réel $\mathbb{P}^2(\mathbb{R})$ est défini comme l'ensemble des droites de l'espace. En travaillant avec des coordonnées, on s'aperçoit que $\mathbb{P}^2(\mathbb{R})$ est aussi l'ensemble des symbôles $[x : y : z]$ avec $x, y, z \in \mathbb{R}^3$, $(x, y, z) \neq (0, 0, 0)$, ces symbôles étant soumis aux relations :

$$[x : y : z] = [\lambda x : \lambda y : \lambda z] \quad \text{pour} \quad (x, y, z) \neq (0, 0, 0) \text{ et } \lambda \neq 0.$$

Une droite de $\mathbb{P}^2(\mathbb{R})$ est alors définie comme un ensemble de points de la forme :

$$D_{a,b,c} = \left\{ [x : y : z] \in \mathbb{P}^2(\mathbb{R}) \quad | \quad ax + by + cz = 0 \right\}$$

pour des réels a, b et c. On remarque, à nouveau, que les droites $D_{a,b,c}$ et $D_{a',b',c'}$ coïncident si, et seulement s'il existe λ non nul tel que $(a', b', c') = (\lambda a, \lambda b, \lambda c)$. Autrement dit, les droites sont paramétrées par les éléments $[a : b : c]$ de $\mathbb{P}^2(\mathbb{R})$... et on voit poindre la dualité entre points et droites qu'on a déjà utilisée précédemment [5] ! Un autre intérêt de travailler avec le plan projectif est que, maintenant, deux droites s'intersectent toujours en un point.

Tout ce que l'on vient de dire s'étend *verbatim* en remplaçant $\mathbb{R}$ par $\mathbb{F}_q$ pour un entier $q = p^s$ où p est un nombre premier et s est un entier strictement positif. Ainsi, revenant au problème qui nous intéresse, on peut prendre $E = \mathbb{P}^2(\mathbb{F}_q)$ et $\mathcal{E} = \left\{ \text{droites de } \mathbb{P}^2(\mathbb{F}_q) \right\}$. À nouveau en résolvant des systèmes linéaires, on vérifie que :

- toute droite de $\mathbb{P}^2(\mathbb{F}_q)$ est de cardinal $q + 1$,
- par chaque point de $\mathbb{P}^2(\mathbb{F}_q)$, il passe exactement $q + 1$ droites,
- par deux points distincts de $\mathbb{P}^2(\mathbb{F}_q)$, il passe une unique droite.

Ces propriétés permettent alors de conclure comme précédemment.

En réalité, la situation actuelle est bien plus riche. En effet, on dispose en outre d'une bijection $f : E \xrightarrow{\sim} \mathcal{E}$ qui envoie un point de coordonnées projective $[a : b : c]$ sur la droite $D_{a,b,c}$. Cette application vérifie en outre la propriété suivante :

$$A \in f(A') \quad \text{si, et seulement si} \quad A' \in f(A)$$

pour $A, A' \in \mathbb{P}^2(\mathbb{F}_q)$. En effet, si $A = [a : b : c]$ et $A' = [a' : b' : c']$, les deux conditions d'appartenance ci-dessus sont équivalentes à la condition algébrique $aa' + bb' + cc' = 0$. Il s'agit d'un cas particulier de la notion de conjugaison dans le plan projectif. Plus généralement, on considère une *forme bilinéaire symétrique*, c'est-à-dire une fonction f de la forme :

$$\begin{aligned} f(x, y, z, x', y', z') = \alpha xx' + \beta yy' + \gamma zz' \\ + \delta(xy' + x'y) + \varepsilon(xz' + x'z) + \zeta(yz' + y'z) \end{aligned}$$

avec $\alpha, \beta, \ldots, \zeta \in \mathbb{F}_q$. L'équation quadratique $f(x, y, z, x, y, z)$ définit une conique $\mathcal{C}$ dans $\mathbb{P}^2(\mathbb{F}_q)$ et on dit que deux points projectifs $A = [x : y : z]$ et $A' = [x' : y' : z']$ sont conjugués par rapport à $\mathcal{C}$ si $f(x, y, z, x', y', z') = 0$. Les points de $\mathcal{C}$ sont donc exactement ceux qui sont conjugués à eux-mêmes. Étant donné un point $A = [x : y : z] \in \mathbb{P}^2(\mathbb{F}_q)$, l'ensemble des points qui lui sont conjugués est une droite qui s'appelle la *polaire* de A par rapport à $\mathcal{C}$. On

5. En un sens, la première construction proposée était donc, elle aussi, projective.

démontre que toute droite de $\mathbb{P}^2(\mathbb{F}_q)$ est la polaire d'un unique point par rapport à $\mathcal{C}$. Ceci établit donc une bijection — qui dépend de $\mathcal{C}$ ou, de manière équivalente, de f — entre les points et les droites de $\mathbb{P}^2(\mathbb{F}_q)$. Bien entendu, cette construction fonctionne pareillement avec $\mathbb{R}$... et elle peut, de fait, être utile dans certains exercices de géométrie !

Les cercles dans $\mathbb{P}^1(\mathbb{F}_{q^2})$. Pour terminer, on étudie la généralisation naturelle du problème précédent que voici. On cherche à construire deux ensembles finis E et $\mathcal{E} \subset \mathcal{P}(E)$ tels que :

1. tous les éléments de $\mathcal{E}$ ont même cardinal,
2. si $A, B, C \in \mathcal{E}$ sont deux à deux disjoints, l'intersection $A \cap B \cap C$ est un singleton,
3. le nombre de façons d'écrire le singleton $\{x\}$ (pour $x \in E$) comme une intersection $A \cap B \cap C$ avec A, B, C deux à deux disjoints est indépendant de x.

Tout à l'heure, on avait exploité le fait que, par deux points distincts, il passe une unique droite. Cette fois-ci, on va naturellement exploiter le fait que, par trois points distincts, il passe un unique cercle. Cette dernière assertion mérite toutefois d'être nuancée car, lorsque les trois points sont alignés, le cercle dégénère en une droite.

Un point de vue agréable sur ces questions est celui de la géométrie projective complexe. On rappelle que $\mathbb{P}^1(\mathbb{C})$ peut être défini naïvement comme $\mathbb{C} \cup \{\infty\}$. Étant donné quatre points $\alpha, \beta, \gamma, \delta \in \mathbb{P}^1(\mathbb{C})$ prenant au moins trois valeurs distinctes, on définit leur *birapport* par la formule :

$$[\alpha, \beta, \gamma, \delta] = \frac{(\alpha - \gamma) \cdot (\beta - \delta)}{(\alpha - \delta) \cdot (\beta - \gamma)} \in \mathbb{P}^1(\mathbb{C})$$

(on vérifie que l'on peut toujours donner un sens à cette formule sous l'hypothèse qui a été faite). On démontre que quatre points sont cocycliques ou alignés si, et seulement si leur birapport (pris dans n'importe quel sens) est dans $\mathbb{P}^1(\mathbb{R}) = \mathbb{R} \cup \{\infty\}$. Il résulte de ceci qu'étant donnés trois points deux à deux distincts $x, y, z \in \mathbb{P}^1(\mathbb{C})$, il existe un unique cercle-ou-droite [6] passant par ces points qui est défini par :

$$\mathcal{C}_{x,y,z} = \big\{\ t \in \mathbb{P}^1(\mathbb{C}) \quad | \quad [x, y, z, t] \in \mathbb{P}^1(\mathbb{R})\ \big\}.$$

Il existe un analogue de cette théorie dans un contexte fini qui s'obtient en remplaçant $\mathbb{R}$ par $\mathbb{F}_q$ et $\mathbb{C}$ par $\mathbb{F}_{q^2}$ pour un entier $q = p^s$ où p est un nombre premier et s est un entier strictement positif. Étant donnés trois points deux à deux distincts $x, y, z \in \mathbb{P}^1(\mathbb{F}_{q^2})$, on définit ainsi le cercle circonscrit au triangle (x, y, z) par :

$$\mathcal{C}_{x,y,z} = \big\{\ t \in \mathbb{P}^1(\mathbb{F}_{q^2}) \quad | \quad [x, y, z, t] \in \mathbb{P}^1(\mathbb{F}_q)\ \big\}.$$

Deux tels cercles $\mathcal{C}_{x,y,z}$ et $\mathcal{C}_{x',y',z'}$ sont confondus si, et seulement si le birapport de quatre points deux à deux distincts quelconques parmi x, y, z, x', y', z' est dans $\mathbb{P}^1(\mathbb{F}_q)$.

Lemme 62. 1. Tout cercle $\mathcal{C}_{x,y,z}$ est de cardinal $q + 1$.

2. Pour $x \in \mathbb{P}^1(\mathbb{F}_{q^2})$, il existe exactement $q \cdot (q + 1)$ cercles passant par x.

Démonstration. Il est facile de vérifier que l'application

$$f : \mathbb{P}^1(\mathbb{F}_{q^2}) \to \mathbb{P}^1(\mathbb{F}_{q^2}), \quad t \mapsto [x, y, z, t]$$

6. On dira simplement « cercle » dans la suite.

est une bijection. Or, par définition, $\mathcal{C}_{x,y,z}$ est l'image réciproque par f de $\mathbb{P}^1(\mathbb{F}_q)$. Ainsi $\mathcal{C}_{x,y,z}$ a le même cardinal que $\mathbb{P}^1(\mathbb{F}_q)$, c'est-à-dire $q+1$.

Un cercle passant par x est défini par la donnée d'un couple (y,z) d'éléments de $\mathbb{P}^1(\mathbb{F}_{q^2})\backslash\{x\}$ avec $y \neq z$. D'autre part, un cercle $\mathcal{C}$ passant par x est obtenu de cette manière à partir de n'importe quel couple (y,z) comme ci-dessus tel que l'on ait en outre $y,z \in \mathcal{C}\backslash\{x\}$. De Card $\mathbb{P}^1(\mathbb{F}_{q^2}) = q^2+1$ et Card $\mathcal{C} = q+1$ (par ce qui précède), on déduit que le nombre de cercles passant par x vaut :

$$\frac{q^2\cdot(q^2-1)}{q\cdot(q-1)} = q\cdot(q+1). \qquad \square$$

On est maintenant en position pour résoudre le problème proposé. On définit E comme l'ensemble des cercles de $\mathbb{P}^1(\mathbb{F}_{q^2})$. Pour tout $x \in \mathbb{P}^1(\mathbb{F}_{q^2})$, l'ensemble des cercles passant par x et on appelle $\mathcal{E}$ l'ensemble des E_x. Par le lemme précédent, chaque E_x a le même cardinal, à savoir $q\cdot(q+1)$. Pour $x,y,z \in \mathbb{P}^1(\mathbb{F}_{q^2})$ deux à deux distincts, l'intersections $E_x \cap E_y \cap E_z$ est un singleton dont l'unique élément est le cercle $\mathcal{C}_{x,y,z}$. Finalement, un singleton $\{\mathcal{C}\}$ (pour $\mathcal{C} \in E$) s'écrit comme une intersection $E_x \cap E_y \cap E_z$ pour exactement $(q+1)\cdot q\cdot(q-1)$ triplets (x,y,z) d'éléments deux à deux distincts de $\mathbb{P}^1(\mathbb{F}_{q^2})$. En effet, puisque x, y et z sont supposés deux à deux distincts, la condition $E_x \cap E_y \cap E_z = \{\mathcal{C}\}$ est équivalente à $x,y,z \in \mathcal{C}$. Le décompte annoncé en découle lorsque l'on se rappelle que $\mathcal{C}$ est de cardinal $q+1$.

3 mercredi 19 matin : Jean-Louis Tu

Principe des tiroirs.

Exercice 1 Montrer que si on choisit $n+1$ nombres de $\{1,2,\ldots,2n\}$, alors deux de ces nombres sont premiers entre eux, et l'un de ces nombres est multiple d'un autre.

Sommes de sous-ensembles.

Exercice 2 Montrer que si A est un ensemble de n entiers, alors il existe une partie non vide $B \subset A$ dont la somme des éléments est divisible par n.

Exercice 3 Etant donné 10 entiers $a_1,\ldots,a_{10}$, montrer qu'il existe $\epsilon_i \in \{-1,0,1\}$ non tous nuls tels que $\sum_i \epsilon_i a_i$ soit divisible par 1000.

Exercice 4 Etant donnés n entiers strictement positifs dont la somme s est $\leqslant 2n-1$, montrer que si $1 \leqslant m \leqslant s$ alors on peut choisir certains de ces entiers dont la somme vaut m.

Exercice 5 (Erdös-Ginzburg-Ziv) Etant donnés $2n-1$ entiers, montrer qu'on peut en choisir n dont la somme est divisible par n.

Sommes de deux ensembles. On note $A+B = \{a+b \mid a \in A,\ b \in B\}$.

Exercice 6 (Cauchy-Davenport.) Si A et B sont deux parties non vides de $\mathbb{Z}/p\mathbb{Z}$ avec p premier, alors $|A+B| \geqslant \min(|A|+|B|-1, p)$.

Exercice 7 Montrer que si $A \subset \mathbb{Z}$ alors $|A+A| \geqslant 2|A|-1$. Quand y a-t-il égalité ?

Exercice 8 On dit que A est sans somme s'il n'existe pas $a,b,c \in A$ non nécessairement distincts tels que $a+b=c$. Quel est le cardinal maximal d'un ensemble sans somme $A \subset \{1,2,\ldots,n\}$?

Exercice 9 (Erdös) Soit $A \subset \mathbb{Z}^*$. Montrer que A contient un sous-ensemble sans somme B tel que $|B| > |A|/3$.

Constructions.

Exercice 10 Montrer que tout entier strictement positif peut s'exprimer comme somme de termes de la forme $2^a 3^b$ tels qu'aucun de ces termes ne soit divisible par un autre.

Exercice 11 Montrer que pour tout $n \geqslant 2$, il existe un ensemble A de n entiers tels que ab soit divisible par $(a-b)^2$ pour tous $a, b \in A$ distincts.

Exercice 12 Montrer que pour tout n il existe une suite arithmétique non constante de longueur n dont tous les termes sont des puissances parfaites.

Exercice 13 (N6, 2001) Est-il possible de trouver 100 entiers naturels inférieurs à 25000 dont les sommes des paires sont toutes distinctes ?

Divers.

Exercice 14 (C2, 2001) Etant donnés des entiers c_i et n impair, soit $S(a) = \sum_{i=1}^n c_i a_i$. Montrer qu'il existe deux permutations distinctes a et b de $\{1, \ldots, n\}$ telles que $S(a) - S(b)$ soit divisible par $n!$.

Exercice 15 (N3, 2007) Etant donnés 10000 entiers non divisibles par 47, montrer qu'on peut choisir un sous-ensemble Y de 2015 nombres tels que $a - b + c - d + e$ ne soit pas divisible par 47 pour tous $a, b, c, d, e \in Y$.

Principe des tiroirs.

Solution de l'exercice 1 a) Deux nombres sont consécutifs. b) Pour tout $a \in \{1, 2, \ldots, 2n\}$ impair, considérer l'intersection de l'ensemble avec $\{a, 2a, 4a, \ldots\}$.

Sommes de sous-ensembles.

Solution de l'exercice 2 Considérer $s_i = a_1 + \cdots + a_i$ et $s_j - s_i$.

Solution de l'exercice 3 Il y a $2^{10} = 1024$ sommes de certains des a_i, deux d'entres-elles ont le même reste modulo 1000.

Solution de l'exercice 4 Récurrence, on retire le plus grand terme $\leqslant m$ (s'il vaut 1 et $s = 2n - 1$ alors tous les termes sont égaux à 1).

Solution de l'exercice 5 Se ramener à n premier. Si $0 \leqslant a_1 \leqslant \cdots \leqslant a_{2n-1} \leqslant n-1$ sont ces entiers, et $b_i = a_{n+i} - a_i$, alors si $b_i \neq 0$, il y a au moins $s+1$ classes mod n de $\sum_{i=1}^n a_i + \sum_{i=1}^s \epsilon_i b_i$ ($\epsilon_i = 0, 1$).

Sommes de deux ensembles.

Solution de l'exercice 6 Récurrence sur $|B|$. Si $A \cap B \neq \emptyset$, comme $A \cap B + A \cup B \subset A + B$ cela conclut si $\emptyset \neq A \cap B \neq B$. On cherche $c \in B - A$ tel que $(A + c) \cap B \neq B$. Si aucun c ne convient alors $(B - B) + A \subset A$ donc $A = \mathbb{Z}/p\mathbb{Z}$.

Solution de l'exercice 7 A est une suite arithmétique (récurrence).

Solution de l'exercice 8 $\lceil n/2 \rceil$. Se ramener à $n = \max A$ et utiliser $|\{a, n-a\} \cap A| \leqslant 1$.

Solution de l'exercice 9 On peut se ramener à $A \subset [-k, k] \setminus \{0\} \subset \mathbb{Z}/p\mathbb{Z}$ avec $p = 3k + 2$ premier. On prend $B = A \cap (x \cdot [k+1, 2k+1])$ avec x aléatoire uniforme. Alors $E[|B|] > |A|/3$.

Constructions.

Solution de l'exercice 10 Récurrence, en distinguant la parité. Si n impair, retrancher la plus grande puissance de 3 qui est $\leqslant n$.

Solution de l'exercice 11 $(a_1, \ldots, a_n) \to (\lambda a_1 \cdots a_n + a_1, \ldots, \lambda a_1 \cdots a_n + a_n, (\lambda + \mu) a_1 \cdots a_n)$ où $\mu = \prod_{i<j}(b_i - b_j)$ où $b_i = a_1 \cdots \widehat{a_i} \cdots a_n$ et $\lambda b_i \equiv -1 \pmod{(\mu b_i - 1)^2}$.

Solution de l'exercice 12 Chercher $(a_1, \ldots, a_n) \mapsto (\lambda^k a_1, \ldots, \lambda^k a_n, \lambda^k (a_n + r))$.

Solution de l'exercice 13 $p = 101$ est premier. On prend $x_n = 2pn + (n^2 \bmod p) \in [(2n)p, (2n + 1)p[$. Si $x_a + x_b = x_c + x_d$ alors $a + b = c + d$ donc $a^2 + b^2 \equiv c^2 + d^2$ donc $\{a, b\} = \{c, d\}$.

Divers.

Solution de l'exercice 14 En raisonnant par l'absurde, calculer $\sum_a S(a) \bmod n!$ de deux manières.

Solution de l'exercice 15 Soit $J = \{-9, -7, -5, \ldots, 7, 9\}$. Cet ensemble satisfait la propriété. Soit A_k l'ensemble des éléments x tels que $kx \bmod 47 \in J$. Alors $\sum_k |A_k| = 100000$ donc l'un des A_k est de cardinal $\geqslant 100000/46 > 2015$.

IV. Deuxième période

Contenu de cette partie

1 Groupe A : algèbre et logique

1 mercredi 19 après-midi : Mathieu Barré

- Manipulations algébriques -

Calculer avec des lettres nécessite de connaître les quelques identités suivantes. Dans ce qui suit, sauf indication contraire, les lettres employées désignent des réels.

Propriétés à retenir

1. Distributivité : $k(a+b) = ka + kb$.
2. Factorisation du rectangle : $ab + bc + cd + da = (a+c)(b+d)$.
3. Si a est positif, $(a^b)^c = (a^c)^b = a^{bc}$.
4. $(a+b)^2 = a^2 + 2ab + b^2$.
5. $(a-b)^2 = a^2 - 2ab + b^2$.
6. $a^2 - b^2 = (a+b)(a-b)$.
7. $(a+b)^3 = a^3 + 3a^2b + 3b^2a + b^3$.
8. $(a-b)^3 = a^3 - 3a^2b + 3b^2a - b^3$.
9. $a^3 - b^3 = (a-b)(a^2 + ab + b^2)$.
10. De façon plus générale, si n est un entier naturel,
$$a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1})$$
11. Binôme de Newton : si n est un entier, alors
$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i}b^i$$

Il faut toujours garder à l'esprit les propriétés précédentes afin de les repérer dans les exercices, en général pour obtenir une forme factorisée.

* * *

Exercice 1

$$1 = 1^{\frac{1}{2}} = ((-1)^2)^{\frac{1}{2}} = (-1)^{2\times\frac{1}{2}} = (-1)^1 = -1$$

Où est l'erreur ?

Exercice 2

Factoriser $n^5 - 5n^3 + 4n$. Que peut-on en conclure en termes de divisibilité ?

Exercice 3

Développer $(a+b)^5$.

Exercice 4

Soient a et b deux réels positifs tels que
$$\frac{a}{a+1} + \frac{b}{b+1} = 1$$

Montrer que

$$\frac{a}{b^2+1} - \frac{b}{a^2+1} = a - b$$

Exercice 5

Calculer la valeur de

$$\frac{2014^4 + 4 \times 2013^4}{2013^2 + 4027^2} - \frac{2012^4 + 4 \times 2013^4}{2013^2 + 4025^2}$$

Exercice 6

Montrer que

$$\frac{43}{44} < \frac{1}{1\sqrt{2}+2\sqrt{1}} + \frac{1}{2\sqrt{3}+3\sqrt{2}} + \cdots + \frac{1}{2014\sqrt{2015}+2015\sqrt{2014}} < \frac{44}{45}$$

- Inégalités -

Les inégalités désignent l'étude de la relation d'ordre entre plusieurs quantités : il s'agit de les comparer, de déterminer lesquels sont les plus grandes, les plus petites...etc.

L'inégalité la plus simple est sans doute le résultat suivant :

Théorème. Un carré est toujours positif. Pour tout réel x, $x^2 \geq 0$.

Ce théorème peut paraître évident à premier abord, mais il s'avère être extrêmement puissant, pour la simple et bonne raison que la plupart des inégalités, aussi sophistiquées soient elles, peuvent se ramener à ce simple fait.

D'autre part, mentionnons l'inégalité des moyennes avec laquelle on peut également faire énormément de choses.

Théorème (inégalité des moyennes)**.** Soient $x_1, \ldots, x_n$ des réels **positifs**. On a

$$\frac{n}{\frac{1}{x_1} + \cdots + \frac{1}{x_n}} \leq \sqrt[n]{x_1 \times \cdots \times x_n} \leq \frac{x_1 + \cdots + x_n}{n} \leq \sqrt{\frac{x_1^2 + \cdots + x_n^2}{n}}$$

Dans l'ordre, ces expressions correspondent aux moyennes harmonique, géométrique, arithmétique et enfin quadratique.

En particulier, on retiendra la deuxième inégalité, dénommée inégalité arithmético-géométrique et abrégée IAG, qui dit en substance que si l'on dispose de n variables positives alors

$$\text{Somme des variables} \geq n \sqrt[n]{\text{Produit des variables}}$$

avec égalité si et seulement si toutes les variables sont égales.

* * *

Exercice 7

Montrer que pour tous réels x et y,

$$5x^2 + y^2 + 4 \geq 4x + 4xy$$

Exercice 8

Montrer que pour tout $x > 0$,

$$x + \frac{1}{x} \geq 2$$

Exercice 9

Montrer que pour tous réels positifs a et b,

$$a^3 + b^3 + a + b \geq 4ab$$

Exercice 10

Montrer que pour tous réels positifs a, b et c, on a $a^2 + b^2 + c^2 \geq ab + bc + ca$ et en déduire que $(a + b + c)^2 \geq 3(ab + bc + ca)$.

Exercice 11

Montrer que pour tous réels positifs x, y et z,

$$x^2 + y^4 + z^6 \geq xy^2 + y^2z^3 + xz^3$$

Exercice 12

Prouver que pour tout $x > 0$,

$$1 + x^{2016} \geq \frac{(2x)^{2015}}{(1 + x)^{2014}}$$

Exercice 13

Soit $m = \min\{x + 2y + 3z, x^3y^2z = 1\}$. Combient vaut m^3 ?

Exercice 14

Montrer que pour tout entier n,

$$\frac{1}{n} + \frac{1}{n+1} + \cdots + \frac{1}{2n-1} \geq n(\sqrt[n]{2} - 1)$$

- Solutions des exercices -

Solution de l'exercice 1 L'erreur réside dans le fait que pour écrire $((-1)^2)^{\frac{1}{2}} = (-1)^{2\times\frac{1}{2}}$, on a utilisé la propriété 3 avec $a = -1$ qui n'est pas positif.

Solution de l'exercice 2

L'idée est d'essayer de faire apparaître des carrés et des différences de carrés pour pouvoir factoriser l'expression proposée.

$$\begin{aligned} n^5 - 5n^3 + 4n &= n(n^4 - 5n^2 + 4) \\ &= n((n^4 - 4n^2 + 4) - n^2) \\ &= n((n^2 - 2)^2 - n^2) \\ &= n(n^2 - n - 2)(n^2 + n - 2) \\ &= (n-2)(n-1)n(n+1)(n+2) \end{aligned}$$

Ainsi, pour tout entier n, $n^5 - 5n^3 + 4n$ est le produit de 5 entiers consécutifs. Parmi ces cinq entiers, au moins l'un d'entre eux sera divisible par 3, au moins un par 5, au moins un par 2 et un autre par 4. De cette façon, $n^5 - 5n^3 + 4n$ sera toujours divisible par $3 \times 5 \times 2 \times 4 = 120$.

Remarque : De façon plus générale, on peut montrer (par exemple avec les coefficients binomiaux ou la formule de Legendre) que le produit de k entiers consécutifs est divisible par $k!$, c'est-à-dire par $1 \times 2 \times 3 \times \cdots \times k$.

Solution de l'exercice 3

En regardant la cinquième ligne du triangle de Pascal (la première ligne étant numérotée zéro), l'application du binôme de Newton donne

$$(a+b)^5 = a^5 + 5a^4b + 10a^3b^2 + 10a^2b^3 + 5ab^4 + b^5$$

Solution de l'exercice 4

Essayons d'y voir plus clair dans la condition de l'énoncé en la simplifiant (car il faut toujours simplifier !) :

$$\frac{a}{a+1} + \frac{b}{b+1} = 1 \Leftrightarrow a(b+1) + b(a+1) = (a+1)(b+1) \Leftrightarrow ab = 1$$

On en déduit alors que

$$\begin{aligned} \frac{a}{b^2+1} - \frac{b}{a^2+1} &= \frac{a(a^2+1) - b(b^2+1)}{(a^2+1)(b^2+1)} \\ &= \frac{(a^3 - b^3) + (a-b)}{a^2b^2 + a^2 + b^2 + 1} \\ &= \frac{(a-b)(a^2 + ab + b^2 + 1)}{(ab)^2 + a^2 + b^2 + 1} \\ &= a - b \text{ après simplification car } ab = 1 \end{aligned}$$

Solution de l'exercice 5

Pour plus de lisibilité, posons $n = 2013$. Notre expression se réécrit

$$\frac{(n+1)^4+4n^4}{n^2+(2n+1)^2} - \frac{(n-1)^4+4n^4}{n^2+(2n-1)^2} = \frac{5n^4+4n^3+6n^2+4n+1}{5n^2+4n+1} - \frac{5n^4-4n^3+6n^2-4n+1}{5n^2-4n+1}$$

Pour simplifier (car il faut toujours simplifier !), essayons de factoriser le numérateur de chaque fraction par son dénominateur. Par exemple, on veut écrire $5n^4+4n^3+6n^2+4n+1 = (5n^2+4n+1)(\dots)$. Dans la parenthèse $(\dots)$, on ne peut avoir que des termes en n^2, n ou n^0. En effet, si on avait une puissance de n supérieure à 3, le développement donnerait une puissance supérieure à 5 non présente au numérateur. Après quelques tâtonnements, on trouve que $5n^4+4n^3+6n^2+4n+1 = (5n^2+4n+1)(n^2+1)$ et de même que $5n^4-4n^3+6n^2-4n+1 = (5n^2-4n+1)(n^2+1)$, d'où la réponse cherchée est zéro.

Remarque : Pour pouvoir trouver de façon systématique la parenthèse $(\dots)$, on peut utiliser le concept de *division polynomiale*. Il s'agit de poser une division euclidienne exactement comme on l'apprend en primaire mais dans laquelle on remplace les nombres par des polynômes, c'est-à-dire des expressions de la forme $\sum a_i x^i$. Ici, cela donne :

$$\begin{array}{rl|l} 5n^4+4n^3+6n^2+4n+1 & & 5n^2+4n+1 \\ \cline{3-3} -\ 5n^4+4n^3+n^2 & & n^2+1 \\ \cline{1-1} 5n^2+4n+1 & & \\ -\ 5n^2+4n+1 & & \\ \cline{1-1} 0 & & \end{array}$$

Solution de l'exercice 6

On cherche à encadrer la somme

$$S = \sum_{i=1}^{2014} \frac{1}{i\sqrt{i+1}+(i+1)\sqrt{i}}$$

Pour simplifier (car il faut toujours simplifier !), on cherche à éliminer les $\sqrt{i}$ et les $\sqrt{i+1}$. Pour ce faire, nous devons multiplier numérateur et dénominateur par une expression contenant $\sqrt{i+1}$ et $\sqrt{i}$. Après quelques essais, on voit que multiplier par $\sqrt{i+1}-\sqrt{i}$ permet de simplifier notre somme. Plus précisément,

$$\begin{aligned}
S &= \sum_{i=1}^{2014} \frac{(\sqrt{i+1}-\sqrt{i})}{(i\sqrt{i+1}+(i+1)\sqrt{i})(\sqrt{i+1}-\sqrt{i})} \\
&= \sum_{i=1}^{2014} \frac{\sqrt{i+1}-\sqrt{i}}{\sqrt{i(i+1)}} \\
&= \sum_{i=1}^{2014} \frac{1}{\sqrt{i}} - \frac{1}{\sqrt{i+1}} \\
&= \frac{1}{\sqrt{1}} - \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} - \frac{1}{\sqrt{3}} + \cdots - \frac{1}{\sqrt{2014}} + \frac{1}{\sqrt{2014}} - \frac{1}{\sqrt{2015}} \\
&= 1 - \frac{1}{\sqrt{2015}}
\end{aligned}$$

Et puisque $44 < \sqrt{2015} < 45$, c'est que $-\frac{1}{44} < -\frac{1}{\sqrt{2015}} < -\frac{1}{45}$. En ajoutant 1 à chaque membre de cette dernière inégalité, on obtient la conclusion cherchée.

Solution de l'exercice 7

On passe tout d'un côté puis on cherche à faire apparaître des carrés grâce aux identités remarquables, pour conclure en utilisant le fait qu'une somme de carrés est toujours positive. On obtient :

$$\begin{aligned}
5x^2+y^2+4-4x-4xy \geq 0 &\Leftrightarrow (x^2-4x+4)+(4x^2-4xy+y^2) \geq 0 \\
&\Leftrightarrow (x-2)^2+(2x-y)^2 \geq 0
\end{aligned}$$

Solution de l'exercice 8 Là encore, on peut transformer cette inégalité en carré positif. En effet,

$$x+\frac{1}{x} \geq 2 \Leftrightarrow x^2+1 \geq 2x \Leftrightarrow (x-1)^2 \geq 0$$

De façon équivalente, l'inégalité arithmético-géométrique donne

$$x+\frac{1}{x} \geq 2\sqrt{x \times \frac{1}{x}} = 2$$

Solution de l'exercice 9

On utilise l'inégalité arithmético-géométrique sur les quatre termes a^3, b^3, a et b :

$$a^3+b^3+a+b \geq 4\sqrt[4]{a^3 \times b^3 \times a \times b} = 4ab$$

Solution de l'exercice 10

Une première solution consiste à tout passer du même côté, à multiplier par 2 puis à remarquer que l'inégalité cherchée est équivalente à

$$(a-b)^2+(b-c)^2+(c-a)^2 \geq 0$$

Sinon, pour conclure avec l'inégalité arithmético-géométrique, il nous faut "découper" notre membre de gauche en sommes de nombres dont le produit se simplifiera lorsqu'on appliquera l'IAG. En effet, pour obtenir par exemple le terme ab, on a appliqué l'IAG à $\frac{a^2+b^2}{2}$. En raisonnant de même avec les termes bc et ca, on trouve comment séparer le membre de gauche en trois pour appliquer l'IAG de la façon suivante :

$$\begin{aligned}\frac{a^2+b^2}{2} &\geq ab\\ \frac{b^2+c^2}{2} &\geq bc\\ \frac{c^2+a^2}{2} &\geq ca\end{aligned}$$

La somme de ces trois inégalités donne alors le résultat.

Pour la seconde partie de l'exercice, on rappelle fort à propos que

$$(a+b+c)^2 = a^2+b^2+c^2+2(ab+bc+ca)$$

Ainsi

$$(a+b+c)^2 \geq 3(ab+bc+ca) \Leftrightarrow a^2+b^2+c^2 \geq ab+bc+ca$$

ce qui vient d'être démontré.

Solution de l'exercice 11

Comme dans l'exercice précédent, on cherche un moyen de découper le membre de gauche en raisonnant sur les exposants du membre de droite, et on trouve

$$\begin{aligned}\frac{x^2+y^4}{2} &\geq xy^2\\ \frac{y^4+z^6}{2} &\geq y^2z^3\\ \frac{z^6+x^2}{2} &\geq z^3x\end{aligned}$$

Une fois encore, on achève la preuve en sommant les trois inégalités ci-dessus.

Solution de l'exercice 12

On veut montrer que

$$(1+x^{2016})(1+x)^{2014} \geq (2x)^{2015}$$

Pour ce faire, appliquons l'inégalité arithmético-géométrique sur chaque parenthèse du membre de gauche. Il vient

$$1+x^{2016} \geq 2\sqrt{1\times x^{2016}} = 2x^{1008}$$

et

$$(1+x)^{2014} \geq (2\sqrt{x})^{2014} = 2^{2014}x^{1007}$$

La multiplication de ces deux inégalités clôt la preuve.

Solution de l'exercice 13

Il s'agit de minimiser la somme $x+2y+3z$ en exploitant la condition $x^3y^2z=1$ grâce à l'IAG. Malheureusement, il n'y a pas de termes en x^3 ni en x^2 dans l'expression $x+2y+3z$. Il nous faut donc découper le terme x en trois termes, de telle sorte que l'application de l'IAG fasse apparaître un terme en x^3 qui devrait se simplifier grâce à l'hypothèse $x^3y^2z=1$. De même, il nous faut séparer le terme $2y$ en deux pour obtenir un exposant deux et laisser le terme $3z$ tel quel car l'exposant 1 correspond déjà. Ainsi, on écrit

$$\begin{aligned} x+2y+3z &= \frac{1}{3}x+\frac{1}{3}x+\frac{1}{3}x+y+y+3z \\ &\geq 6\sqrt[6]{\frac{1}{3}x\times\frac{1}{3}x\times\frac{1}{3}x\times y\times y\times 3z} \text{ d'après l'IAG} \\ &= 6\sqrt[6]{\frac{1}{9}x^3y^2z}=6\sqrt[6]{\frac{1}{9}} \text{ car } x^3y^2z=1 \end{aligned}$$

Attention, il faut encore vérifier que la valeur $6\sqrt[6]{\frac{1}{9}}$ peut être atteinte pour en conclure qu'il s'agit du minimum !. En effet, x, y et z étant positifs, on pourrait très bien dire sans trop de risque que $x+2y+3z\geq 0$, mais 0 n'est pas le minimum pour autant. Ici, en se rappelant du cas d'égalité de l'IAG, on vérifie aisément que prendre $\frac{1}{3}x=y=3z=\sqrt[6]{\frac{1}{9}}$ convient et que par conséquent on a bien $m=6\sqrt[6]{\frac{1}{9}}$, soit $m^3=72$.

Solution de l'exercice 14

$$\begin{aligned} \frac{1}{n}+\frac{1}{n+1}+\cdots+\frac{1}{2n-1}\geq n(\sqrt[n]{2}-1) &\Leftrightarrow \frac{1}{n}+\frac{1}{n+1}+\cdots+\frac{1}{2n-1}+n\geq n\sqrt[n]{2} \\ &\Leftrightarrow \left(1+\frac{1}{n}\right)+\left(1+\frac{1}{n+1}\right)+\cdots+\left(1+\frac{1}{2n-1}\right)\geq n\sqrt[n]{2} \\ &\Leftrightarrow \frac{n+1}{n}+\frac{n+2}{n+1}+\cdots+\frac{2n}{2n-1}\geq n\sqrt[n]{2} \end{aligned}$$

Cette dernière inégalité est vraie d'après l'inégalité arithmético-géométrique puisque

$$\frac{n+1}{n}+\frac{n+2}{n+1}+\cdots+\frac{2n}{2n-1}\geq n\sqrt[n]{\frac{n+1}{n}\times\frac{n+2}{n+1}\times\cdots\times\frac{2n}{2n-1}}=n\sqrt[n]{2}$$

et la démonstration est terminée.

2 jeudi 20 matin : Vincent Bouis

- Inégalité de Cauchy-Schwarz -

Soient a_1, a_2, ..., a_n, b_1, b_2, ..., b_n des réels.
On a alors :

$$(a_1^2+a_2^2+...+a_n^2)(b_1^2+b_2^2+...+b_n^2)\geq(a_1b_1+a_2b_2+...+a_nb_n)^2.$$

- Inégalité des mauvais élèves -

Soient a_1, a_2, ..., a_n des réels, et x_1, x_2, ..., x_n des réels strictement positifs.
On a alors :

$$\frac{a_1^2}{x_1} + \frac{a_2^2}{x_2} + ... + \frac{a_n^2}{x_n} \geq \frac{(a_1 + a_2 + ... + a_n)^2}{x_1 + x_2 + ... + x_n}.$$

- Exercices -

Exercice 1 Soient a_1, a_2, ..., a_n des réels strictement positifs. Montrer que

$$(a_1 + a_2 + ... + a_n)\left(\frac{1}{a_1} + \frac{1}{a_2} + ... + \frac{1}{a_n}\right) \geq n^2.$$

Exercice 2 Montrer l'inégalité des mauvais élèves pour $n = 2$ sans l'inégalité de Cauchy-Scharz.

Exercice 3 Montrer l'inégalité des mauvais élèves dans le cas général sans Cauchy-Scharz.

Exercice 4 [Nesbitt]
Soient a, b, c des réels strictement positifs. Montrer que

$$\frac{a}{b+c} + \frac{b}{c+a} + \frac{c}{a+b} \geq \frac{3}{2}.$$

Exercice 5 Soient a et b des réels positifs. Montrer que

$$8(a^4 + b^4) \geq (a+b)^4.$$

Exercice 6 Soient a, b, c, d des réels strictement positifs. Montrer que

$$\frac{1}{a} + \frac{1}{b} + \frac{4}{c} + \frac{16}{d} \geq \frac{64}{a+b+c+d}.$$

Exercice 7 Soient x, y, z des réels strictement positifs tels que $xyz = 1$. Montrer que

$$\frac{1}{x^3(y+z)} + \frac{1}{y^3(z+x)} + \frac{1}{z^3(x+y)} \geq \frac{3}{2}.$$

Exercice 8 Soient x, y, z des réels strictement positifs. Montrer que

$$\frac{2}{x+y}+\frac{2}{y+z}+\frac{2}{z+x}\geq\frac{9}{x+y+z}$$

Exercice 9 Soient x, y, z des réels strictement positifs. Montrer que

$$\frac{x^2}{(x+y)(x+z)}+\frac{y^2}{(y+z)(y+x)}+\frac{z^2}{(z+x)(z+y)}\geq\frac{3}{4}$$

Exercice 10 Soient a, b, c des réels strictement positifs. Montrer que

$$\frac{a^2+b^2}{a+b}+\frac{b^2+c^2}{b+c}+\frac{c^2+a^2}{c+a}\geq a+b+c$$

Exercice 11 Soient a, b, x, y, z des réels strictement positifs. Montrer que

$$\frac{x}{ay+bz}+\frac{y}{az+bx}+\frac{z}{ax+by}\geq\frac{3}{a+b}.$$

Exercice 12 Soient a, b, c des réels strictement positifs. Montrer que

$$\frac{ab}{a+b}+\frac{bc}{b+c}+\frac{ca}{c+a}\leq\frac{3(ab+bc+ca)}{2(a+b+c)}.$$

Exercice 13

$$\frac{a}{\sqrt{a^2+8bc}}+\frac{b}{\sqrt{b^2+8ca}}+\frac{c}{\sqrt{c^2+8ab}}\geq 1.$$

3 jeudi 20 après-midi : logique, Nicolas Ségarra

L'objectif de ce cours est d'étudier la construction des assertions et les différents types de raisonnements que l'on rencontre en logique.
Par exemple, quelle(s) est (sont) la (les) différence(s) entre les deux propositions suivantes : « si Nathalie boit du café, alors elle est en forme » et « Nathalie boit du café si et seulement si elle est en forme » ? Parmi ces deux propositions, laquelle vous semble la plus vraisemblable ? Maintenant, imaginons que la proposition : « si Nathalie boit du café, alors elle est en forme » est vraie. Qu'en est-il pour la proposition suivante : « si Nathalie n'est pas en forme, alors elle ne boit pas de café » ?

Nous répondrons à ces questions tout au long de ce cours.

Commençons par une énigme intéressante : trois logiciens se rendent dans un bar. Le barman leur demande : « trois bières ? » Le premier logicien répond : « je ne sais pas », le deuxième logicien répond : « je ne sais pas » et le troisième répond : « oui ». La question est ici de savoir pourquoi le troisième logicien répond « oui », pourquoi le troisième logicien est sûr que le barman va servir trois bières.
Voilà la solution : le premier logicien ne peut pas savoir si les deux autres logiciens veulent une bière. Si le premier logicien ne voulait pas de bière, il aurait répondu « non » car alors le barman aurait dû servir au maximum deux bières. Donc, pour montrer aux deux autres logiciens qu'il veut une bière, il répond simplement : « je ne sais pas ».
Pour le deuxième logicien, c'est le même raisonnement : il ne connaît pas la réponse du troisième. Ce dernier par contre a toutes les cartes en main pour donner une réponse précise au barman car il a bien compris que les deux premiers logiciens souhaitaient boire une bière et comme il en veut une, il est en mesure de répondre pour les trois.

Maintenant, échaufons-nous avec quelques exercices !

I) Exercices d'échauffement.
Exercice 1 Alice vagabonde dans la forêt de l'oubli où elle est incapable de se souvenir du jour de la semaine. Elle rencontre le lion et la licorne. Le lion ment les lundi, mardi et mercredi et dit la vérité les autres jours tandis que la licorne ment uniquement les jeudi, vendredi et samedi.
« Hier était un jour où je mentais » dit le lion.
« Hier était un jour où je mentais » dit la licorne.

Question : Quel jour sommes-nous aujourd'hui ?

Solution de l'exercice 1 Le jour cherché ne peut pas être lundi, mardi ni mercredi. Prenons le cas du lundi (les deux autres jours sont éliminés de manière analogue) : si nous sommes lundi, alors la licorne dit la vérité et le lion ment. Donc la licorne a raison en disant que le jour précédent, elle mentait. Mais, le jour précédent le lundi est dimanche et le dimanche, la licorne dit la vérité donc le jour cherché ne peut pas être lundi (ceci contredit le fait que la licorne ait raison !).
On élimine de la même manière le vendredi, le samedi et le dimanche (en analysant ce que le lion dit cette fois) donc nous sommes jeudi. On peut d'ailleurs vérifier la cohérence des phrases du lion et de la licorne le jeudi pour vérifier que notre raisonnement est bon !

Exercice 2

Messieurs Boulanger, Pâtissier et Fleuriste sont trois amis qui ont chacun un (et un seul) métier différent parmi les suivants : boulanger, pâtissier et fleuriste Mais chacun d'eux n'exerce pas forcément le métier correspondant à son nom. Sur les informations qui suivent, une seule est vraie :
- Monsieur Pâtissier n'est pas boulanger.
- Monsieur Fleuriste n'est pas pâtissier.
- Monsieur Pâtissier est pâtissier.
- Monsieur Fleuriste n'est pas boulanger.

Question : Quels sont les métiers exercés par les 3 amis ?

Solution de l'exercice 2 Etudions les quatre cas :

1er cas : la première proposition est vraie. Alors, Monsieur Pâtissier n'est pas boulanger et les autres propositions sont fausses donc Monsieur Fleuriste est pâtissier (par la proposition 2 qui est fausse) et boulanger (d'après la proposition 4 qui est fausse) : ceci est impossible car chaque protagoniste enseigne un seul métier.

2ème cas : Monsieur Fleuriste n'est pas pâtissier. Donc Monsieur Pâtissier est boulanger (d'après la première proposition qui est fausse) et Monsieur Fleuriste est aussi boulanger (par la 4ème proposition qui est fausse). C'est impossible car les trois protagonistes exercent des métiers différents.

3ème cas : Monsieur Pâtissier est pâtissier. Donc la proposition 1 est fausse donc Monsieur Pâtissier exerce deux métiers, ce qui est impossible.

4ème cas : Monsieur Fleuriste n'est pas boulanger. Des propositions 1 et 2 (qui sont fausses), on déduit que : Monsieur Pâtissier est boulanger et Monsieur Fleuriste est pâtissier. Le point 3 n'entre pas en contradiction avec ce qui précède. Finalement, Monsieur Boulanger est fleuriste.

Le quatrième cas est le seul cas possible donc les métiers des trois protagonistes sont ceux énoncés dans le dernier cas.

Exercice 3

Messieurs Lenoir, Leblanc et Lerouge sont professeurs de sport dans une grande école. Chacun enseigne trois spécialités parmi : tennis, judo, foot, basket et rugby. Certaines spécialités sont enseignées par deux personnes, jamais par trois personnes.
- Monsieur Lenoir n'enseigne pas le tennis.
- Monsieur Leblanc est le seul à enseigner le judo.
- Monsieur Lerouge enseigne le foot.
- Monsieur Leblanc n'enseigne pas le basket.

Question : Quels professeurs enseignent quelles spécialités ?

Solution de l'exercice 3 A partir des informations de l'énoncé, on peut déjà élaborer le tableau ci-dessous. On écrira « oui » ou « non » dans la case en position (i, j) selon que le personnage i enseigne ou n'enseigne pas la discipline j.

	Tennis	Judo	Foot	Basket	Rugby
Monsieur Lenoir	non	non			
Monsieur Leblanc		oui		non	
Monsieur Lerouge		non	oui		

Comme chaque professeur enseigne trois spécialités, on en déduit que Monsieur Lenoir en-

seigne le foot, le basket et le rugby.
De plus, une spécialité ne peut pas être enseignée par 3 personnes donc Monsieur Leblanc ne peut pas enseigner le foot (celui-ci étant déjà enseigné par Monsieur Lenoir et par Monsieur Lerouge). Donc Monsieur Leblanc enseigne le tennis et le rugby en plus du judo.
On en déduit alors que Monsieur Lerouge ne peut pas enseigner le rugby donc il enseigne le tennis et le basket en plus du foot. Le tableau ci-dessous résume les spécialités enseignées par chacun des professeurs.

	Tennis	Judo	Foot	Basket	Rugby
Monsieur Lenoir	non	non	oui	oui	oui
Monsieur Leblanc	oui	oui	non	non	oui
Monsieur Lerouge	oui	non	oui	oui	non

II) Définitions et vocabulaire.

Définition. Une assertion (ou proposition) est un énoncé mathématique qui peut être vrai ou faux.

Exemples.

1) $4 \in \mathbb{N}$ est une proposition vraie.
2) $2 < 15$ est une proposition vraie.
3) $0 = 1$ est une proposition fausse.
4) "$1 + 2$" n'est en revanche pas une proposition.

Dans la suite du cours, A et B désigneront deux propositions.

Définition. La négation d'une proposition A est une proposition que l'on peut définir à l'aide de la table de vérité suivante :

A	non A
V	F
F	V

.

Exemple. Soient x un réel et A l'assertion : ($x > 0$). Alors, non A est l'assertion : ($x \leq 0$).

Définition. Pour A et B deux assertions, la disjonction (exprimée par le mot « ou ») de A et B est donnée par la table de vérité suivante :

A	B	A ou B
V	V	V
V	F	V
F	V	V
F	F	F

.

Remarque. L'assertion : (A ou non A) est toujours vraie.

Définition. La conjonction (exprimée par le mot « et ») de deux assertions A et B est donnée

par la table de vérité suivante :

A	B	A et B
V	V	V
V	F	F
F	V	F
F	F	F

.

Remarque. L'assertion : (A et non A) est toujours fausse.

Définition. On définit l'implication entre deux propositions A et B (« A implique B » que l'on note $A \Rightarrow B$) à l'aide de la table de vérité suivante :

A	B	$A \Rightarrow B$
V	V	V
V	F	F
F	V	V
F	F	V

.

Remarques. 1) La troisième ligne de la table de vérité ci-dessus peut paraître peu naturelle. On peut l'expliquer en se convainquant que $A \Rightarrow B$ revient à dire : non A ou B.
On voit bien alors que si A est fausse et B est vraie alors non A ou B donne vrai ou vrai donc vrai !

2) Lorsque $A \Rightarrow B$ est vraie, on peut dire :
- A implique B.
- Si A alors B.
- Pour B, il suffit A.
- Pour A, il faut B.
- A est une condition suffisante pour B.
- B est une condition nécessaire pour A.

Exemples. Voici des exemples d'implications vraies.

1) $ABCD$ est un carré $\Rightarrow$ $ABCD$ est un rectangle.
2) $x \in \mathbb{N} \Rightarrow x \in \mathbb{Z}$.
3) $1 + 1 = 2 \Rightarrow \sqrt{2}$ est irrationnel.
Ce dernier exemple peut sembler étrange, car on se demande quel est le rapport entre les deux assertions. Mais il n'est en fait pas nécessaire qu'il existe un rapport ou une causalité, puisqu'il suffit que les deux propositions A et B soient vraies (ou toutes les deux fausses) pour que l'implication $A \Rightarrow B$ soit vraie.

Définition. Soient A et B deux propositions. On dit que A est équivalente à B (ou que A équivaut à B) et on note $A \Leftrightarrow B$, si A implique B et B implique A.

Remarques. 1) Voici la table de vérité pour $A \Leftrightarrow B$:

A	B	$A \Rightarrow B$	$B \Rightarrow A$	$A \Leftrightarrow B$
V	V	V	V	V
V	F	F	V	F
F	V	V	F	F
F	F	V	V	V

.

On remarque que $A \Leftrightarrow B$ est vraie lorsque les deux propositions A et B sont toutes les deux vraies ou toutes les deux fausses. Autrement dit, lorsqu'elles ont la même valeur logique.

2) Lorsque $A \Leftrightarrow B$ est vraie, on peut dire :
- A si et seulement si B.
- Pour A, il faut et il suffit B.
- A est une condition nécessaire et suffisante pour B.

Exemples. Voici des exemples d'équivalences vraies.

1) $\text{non}(\text{non}\, A) \Leftrightarrow A$.
2) Soit x un nombre réel. On a $3x + 3 = 6 \Leftrightarrow x = 1$.

Définitions avec des quantificateurs. Soient E un ensemble et $A(x)$ une assertion dépendant de $x \in E$.

1) On définit l'assertion $(\forall\, x \in E,\, A(x))$ comme étant vraie si et seulement si $A(x)$ est vraie pour tout élément x de E.
2) On définit l'assertion $(\exists\, x \in E,\, (A(x))$ comme étant vraie si et seulement s'il existe au moins un élément x de E pour lequel $A(x)$ est vraie.

Exemples. Voici deux exemples d'assertions vraies, définies à l'aide de quantificateurs.

1) $(\forall\, x \in \mathbb{N},\, x \geq 0)$; 2) $(\exists\, x \in \mathbb{R},\, x^2 = 5)$.

Remarques. 1) On peut se convaincre que :
a) $\text{non}(\forall\, x \in E,\, A(x)) \Leftrightarrow \exists\, x \in E,\, \text{non}\, A(x)$.
b) $\text{non}(\exists\, x \in E,\, A(x)) \Leftrightarrow \forall\, x \in E,\, \text{non}\, A(x)$.

2) Lorsque plusieurs quantificateurs sont employés, on ne peut les permuter et obtenir une assertion équivalente que lorsqu'ils sont du même type. En général, avec de gros guillemets, $\forall\exists \not\Leftrightarrow \exists\forall$.

Exercice 4 Soient A et B deux assertions. Montrer les équivalences suivantes :

1) $\text{non}(A$ **et** $B) \Leftrightarrow (\text{non}\, A)$ **ou** $(\text{non}\, B)$.
2) $\text{non}(A$ **ou** $B) \Leftrightarrow (\text{non}\, A)$ **et** $(\text{non}\, B)$.
3) $\text{non}(A \Rightarrow B) \Leftrightarrow A$ **et** $(\text{non}\, B)$.

Solution de l'exercice 4 On démontre ces équivalences à l'aide de tables de vérité.

1)

A	B	non A	non B	A et B	non(A et B)	(non A) ou (non B)
V	V	F	F	V	F	F
V	F	F	V	F	V	V
F	V	V	F	F	V	V
F	F	V	V	F	V	V

.

2)

A	B	non A	non B	A ou B	non(A ou B)	(non A) et (non B)
V	V	F	F	V	F	F
V	F	F	V	V	F	F
F	V	V	F	V	F	F
F	F	V	V	F	V	V

.

3)

A	B	non B	$A \Rightarrow B$	non($A \Rightarrow B$)	A et (non B)
V	V	F	V	F	F
V	F	V	F	V	V
F	V	F	V	F	F
F	F	V	V	F	F

.

Exercice 5 Les assertions suivantes sont-elles vraies ?

1. $\forall\, x \in \mathbb{R}$, $x^2 + 4x + 3 \neq 0$.
2. $\exists\, x \in \mathbb{N}$, $x \in \mathbb{D}$.
3. $\forall\, x \in \mathbb{R}$, $x > 4 \Rightarrow x \geq 4,1$.
4. $\exists\, n \in \mathbb{Z}$, $\forall\, x \in \mathbb{R}$, $n < x \leq n + 1$.

Solution de l'exercice 5

1. Pour montrer que cette assertion est fausse, on va montrer que sa négation est vraie.
On a : non($\forall\, x \in \mathbb{R}$, $x^2 + 4x + 3 \neq 0$) $\Leftrightarrow \exists\, x \in \mathbb{R}$, $x^2 + 4x + 3 = 0$. Cette dernière proposition est vraie car $(-1)^2 + 4 \times (-1) + 3 = 0$.
Ainsi, la proposition : ($\forall\, x \in \mathbb{R}$, $x^2 + 4x + 3 \neq 0$) est fausse.

2. Cette assertion est vraie. En effet, $0 \in \mathbb{N}$ et $0 \in \mathbb{D}$.

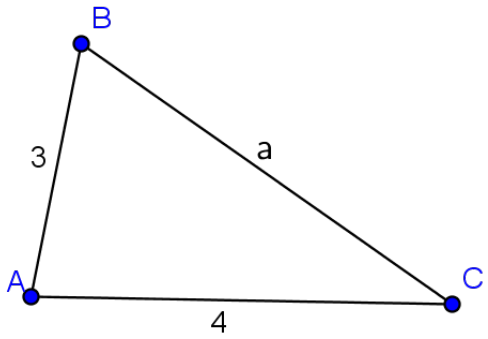
3. Montrons que cette assertion est fausse.
On a : non($\forall\, x \in \mathbb{R}$, $x > 4 \Rightarrow x \geq 4,1$) $\Leftrightarrow \exists\, x \in \mathbb{R}$, $x > 4$ et $x < 4,1$.
Cette dernière assertion est vraie car $x = 4,05$ convient (on a bien : $4 < 4,05 < 4,1$).

4. Montrons que cette assertion est fausse.
non($\exists\, n \in \mathbb{Z}$, $\forall\, x \in \mathbb{R}$, $n < x \leq n + 1$) $\Leftrightarrow \forall\, n \in \mathbb{Z}$, $\exists\, x \in \mathbb{R}$, non($x > n$ et $x \leq n + 1$).
non($\exists\, n \in \mathbb{Z}$, $\forall\, x \in \mathbb{R}$, $n < x \leq n + 1$) $\Leftrightarrow \forall\, n \in \mathbb{Z}$, $\exists\, x \in \mathbb{R}$, $x \leq n$ ou $x > n + 1$.
Pour cette dernière proposition, $x = n + 2 > n + 1$ convient et ceci conclut la démonstration.

III) Différents types de raisonnements.

Démontrer une implication. En général, pour prouver que $A \Rightarrow B$, on suppose que A est vraie et on essaie de démontrer que B est alors vraie.

Exemple. Montrons que (ABC est rectangle en A) $\Rightarrow a = 5$.



Supposons que ABC est rectangle en A. D'après le théorème de Pythagore, on a : $a^2 = 3^2 + 4^2 = 25$. Donc $a = -5$ ou $a = 5$. Mais a est un nombre positif car c'est une longueur donc $a = 5$.

Démontrer une équivalence. On peut dans des cas très simples procéder par équivalences successives. Mais en général, il est préférable de raisonner par double implication : on montre une implication puis sa réciproque.

Raisonnement par contraposée. Pour prouver une implication non démontrable directement : $(A \Rightarrow B)$, on peut raisonner par contraposée, c'est-à-dire montrer que : $(\text{non } B \Rightarrow \text{non } A)$. La table de vérité suivante permet de démontrer que $(A \Rightarrow B) \Leftrightarrow (\text{non } B \Rightarrow \text{non } A)$:

A	B	non A	non B	$A \Rightarrow B$	non $B \Rightarrow$ non A
V	V	F	F	V	V
V	F	F	V	F	F
F	V	V	F	V	V
F	F	V	V	V	V

.

L'implication : $(\text{non } B \Rightarrow \text{non } A)$ est appelée : implication contraposée de l'implication $(A \Rightarrow B)$.

Raisonnement par l'absurde. Pour démontrer qu'une assertion A est vraie, on peut raisonner par l'absurde. On suppose que A est fausse et on tente d'aboutir à une contradiction. On conclut alors qu'il était absurde de supposer A fausse donc que A est vraie.

Exemple. Soit $n \in \mathbb{Z}$. Montrons que n ne peut pas être pair et impair à la fois.

On raisonne par l'absurde. On suppose alors que n est pair et impair à la fois. Alors il existe deux entiers k et k' tels que $n = 2k = 2k' + 1$. Donc on a : $2(k - k') = 1$ donc $k - k' = \dfrac{1}{2}$. Comme k et k' sont des entiers, $k - k'$ est un entier mais $\dfrac{1}{2}$ n'est pas un entier. Donc on obtient une contradiction. Ainsi, n ne peut pas être pair et impair à la fois.

Raisonnement par disjonction de cas. Parfois, il est pertinent d'étudier tous les cas possibles pour démontrer un résultat. Ce raisonnement est le raisonnement par disjonction de cas. Il a été mis en oeuvre dans les exercices 1 et 2.

Preuve de $(\forall\, x \in E,\, A(x))$. On procède de la manière suivante. On se donne un x quelconque

de E et on démontre que $A(x)$ est vraie. L'élément x est quelconque et on n'a imposé aucune condition sur cet élément donc on a démontré que $A(x)$ est vraie pour tout $x \in E$.

Exemple. Montrons que $\forall\, x \in \mathbb{R}$, $(x-2)^2 + (x+3)^2 - 2x \geq 13$.

Soit $x \in \mathbb{R}$. On écrit : $(x-2)^2 + (x+3)^2 - 2x = x^2 - 4x + 4 + x^2 + 6x + 9 - 2x = 2x^2 + 13$ (on se souvient des identités remarquables !).
Comme, $2x^2 \geq 0$, $2x^2 + 13 \geq 13$ donc on a bien $\forall\, x \in \mathbb{R}$, $(x-2)^2 + (x+3)^2 - 2x \geq 13$.
Preuve de $(\exists\, x \in E,\, A(x))$. Pour prouver ce genre de proposition, on peut avoir recours à un théorème d'existence (un théorème assurant l'existence d'au moins un x tel que $A(x)$ soit vraie) ou exhiber un x pour lequel $A(x)$ est vraie.

Exemple. Montrons qu'il existe un entier $p \geq 2$ tel que $2p^2 + 1$ soit premier.

Pour $p = 3$, on a : $2p^2 + 1 = 2 \times 9 + 1 = 19$ et 19 est premier. Donc on a bien montré l'existence d'un entier $p \geq 2$ tel que $2p^2 + 1$ soit premier.

Exercice 6 On suspecte Elise, Fred et Gaétan d'avoir commis un vol. Nous avons à leur sujet les informations suivantes :
- si Gaétan n'est pas coupable alors Fred est coupable.
- Si Elise n'est pas coupable alors Gaétan est coupable.
- Si Gaétan est coupable alors Elise l'est aussi.
- Si Elise est coupable alors Fred ne l'est pas.

Question : Quel est ou quels sont le ou les coupable(s) ?

Solution de l'exercice 6

Les 4 propositions données ci-dessus doivent être vraies simultanément. On va alors montrer à l'aide des propositions 2 et 3 qu'Elise est nécessairement coupable. Raisonnons par l'absurde : supposons qu'Elise n'est pas coupable. Alors par la proposition 2, Gaétan est coupable. Donc par la proposition 3, Elise est coupable. Ceci contredit l'hypothèse de départ. Donc Elise est coupable.
Comme Elise est coupable, Fred n'est pas coupable d'après la proposition 4. On en déduit par la contraposée de la première implication que Gaétan est coupable.
Conclusion : les coupables de ce vol sont Elise et Gaétan.

IV) Exercices supplémentaires.

Exercice 7
1) Soit $p \in \mathbb{Z}$. Montrer que si p^2 est pair alors p est pair.
2) Montrer que $\sqrt{2}$ est irrationnel.

Solution de l'exercice 7

1) Montrons cette proposition en raisonnant par contraposée : supposons que p est impair. Alors, il existe un entier k tel que $p = 2k+1$. On a : $p^2 = (2k+1)^2 = 4k^2+4k+1 = 2(2k^2+2k)+1$ et $2k^2 + 2k \in \mathbb{Z}$ donc p^2 est impair. On a montré que si p est impair alors p^2 est impair donc on a le résultat par contraposée.

2) Raisonnons par l'absurde : supposons alors que $\sqrt{2}$ est un nombre rationnel. Alors, il existe deux entiers a et b premiers entre eux et $b \neq 0$ tels que : $\sqrt{2} = \dfrac{a}{b}$. On a alors en élevant au carré : $2 = \dfrac{a^2}{b^2}$ donc $a^2 = 2b^2$ d'où a^2 est pair et ainsi a est pair (par la proposition démontrée précédemment).
L'entier a est pair donc il existe un entier k tel que : $a = 2k$. On a alors : $a^2 = 4k^2 = 2b^2$ soit : $b^2 = 2k^2$. Donc b^2 est pair ainsi b est pair.
Mais il est impossible que les entiers a et b soient tous les deux pairs car ceci contredit le fait qu'ils soient premiers entre eux !
Donc $\sqrt{2}$ est un nombre irrationnel.

Exercice 8 Démontrer les propositions suivantes :

1. $\forall\, x \in \mathbb{R}$, $x^2 - 8x + 17 > 0$.
2. $\forall\, x \in \mathbb{R}$, $(x+2)^2 - (x-3)^2 \geq 0 \Rightarrow x \geq \dfrac{1}{2}$.
3. $\exists\, n \in \mathbb{N}$, $11 | 6n^2 - 7$.

Solution de l'exercice 8 1. On a : $x^2 - 8x + 17 = (x-4)^2 + 1$. Comme $(x-4)^2 \geq 0$, $(x-4)^2 + 1 \geq 1$ donc pour tout réel x, $x^2 - 8x + 17 > 0$.
2. On suppose que $(x+2)^2 - (x-3)^2 \geq 0$. On écrit : $(x+2)^2 - (x-3)^2 = 5(2x-1)$ (troisième identité remarquable).
Ainsi, on a : $5(2x-1) \geq 0$ donc $2x - 1 \geq 0$ (car $5 > 0$). Donc $x \geq \dfrac{1}{2}$.
3. Pour $n = 5$, $6n^2 - 7 = 6 \times 25 - 7 = 141 = 11 \times 13$. Donc on a bien montré qu'il existe au moins un entier naturel n tel que 11 divise $6n^2 - 7$.

2 Groupe B : algèbre

1 jeudi 20 matin : Xavier Caruso

L'objectif de ce cours est de présenter un panel de méthodes classiques pour la manipulation des expressions algébriques. Un détour par les inégalités est également proposé. Nous commençons par étudier longuement les expressions de degré 2 puis étudions — de manière moins approfondie — les polynômes de degré supérieur.

L'algèbre des expressions de degré 2

Les identités remarquables. Les identités remarquables sont à la base de la manipulation algébrique des expressions de degré 2. Nous les rappelons ci-dessous :

$$(a+b)^2 = a^2 + 2ab + b^2 \tag{IV.1}$$
$$(a-b)^2 = a^2 - 2ab + b^2 \tag{IV.2}$$
$$(a+b)(a-b) = a^2 - b^2. \tag{IV.3}$$

Ces identités sont utiles pour développer mais aussi, et surtout, pour factoriser. Autrement dit, on les utilisera couramment « de la droite vers la gauche » : dans une expression développée, on essaiera de reconnaître — ou de faire apparaître — l'une des trois expressions développées de (IV.1)–(IV.3) et, le cas échéant, on la remplacera par l'expression factorisée en espérant que cela puisse être utile pour la résolution du problème posé.

La résolution de l'équation de degré 2. Un cas d'école où la stratégie esquissée ci-dessus est efficace est celui de la résolution des équations de degré 2. Montrons, pour commencer, comment cela fonctionne sur un exemple : supposons que l'on désire résoudre l'équation :

$$x^2 - 4x + 3 = 0.$$

On ne reconnaît pas directement l'expression développée d'une identité remarquable mais les deux premiers termes $x^2 - 4x$ font penser à $a^2 - 2ab$ (pour $a = x$ et $b = 2$, donc). Malheureusement, nous avons ensuite un 3 au lieu d'un 4. Qu'à cela ne tienne, on fait apparaître arficiellement le 4 qui nous manque en remplaçant 3 par $4 - 1$. L'équation que l'on cherche à résoudre se réécrit ainsi successivement :

$$\begin{aligned} x^2 - 4x + 4 - 1 &= 0 \\ (x-2)^2 - 1 &= 0 \end{aligned}$$

et on peut utiliser à présent la troisième identité remarquable pour terminer la factorisation, obtenant $(x-1)(x-3) = 0$. Les solutions sont donc 1 et 3.

Cette méthode fonctionne pareillement dans le cas de l'équation générale :

$$ax^2 + bx + c = 0 \tag{IV.4}$$

où a, b et c sont des paramètres connus et x est l'inconnue. On suppose que a est non nul : dans le cas contraire, l'équation se réduit à $bx + c = 0$ et on sait déjà la résoudre. Si $a \neq 0$, on commence par diviser par a pour simplifier les calculs à venir :

$$x^2 + \tfrac{b}{a}\, x + \tfrac{c}{a} = 0$$

puis on poursuit la résolution en factorisant comme précédemment :

$$\begin{aligned} x^2 + 2 \cdot \tfrac{b}{2a}\, x + \tfrac{b^2}{4a^2} - \tfrac{b^2-4ac}{4a^2} &= 0 \\ \left(x + \tfrac{b}{2a}\right)^2 - \tfrac{b^2-4ac}{4a^2} &= 0 \end{aligned}$$

À ce stade, nous devons discuter selon le signe de $b^2 - 4ac$:

- s'il est strictement négatif, l'équation n'a pas de solution ;
- s'il est nul, l'équation a une unique solution qui est $\frac{-b}{2a}$;
- s'il est strictement positif, on peut continuer la factorisation ainsi :

$$\left(x + \tfrac{b}{2a} + \tfrac{\sqrt{b^2-4ac}}{2a}\right) \cdot \left(x + \tfrac{b}{2a} - \tfrac{\sqrt{b^2-4ac}}{2a}\right) = 0$$

et on trouve les deux solutions :

$$\frac{-b - \sqrt{b^2 - 4ac}}{2a} \quad \text{et} \quad \frac{-b + \sqrt{b^2 - 4ac}}{2a}. \tag{IV.5}$$

Remarque 63. Lorsque $b^2 - 4ac = 0$, les expressions (IV.5) prennent toutes les deux la valeur $\frac{-b}{2a}$, c'est-à-dire celle de l'unique solution de l'équation. Pour cette raison — et aussi pour d'autres — il est commode dans ce cas de convenir que la solution $\frac{-b}{2a}$ compte double.

Le nombre $b^2 - 4ac$ s'appelle le *discriminant* de l'équation (IV.4) et est généralement noté Δ (lire *delta*). C'est lui qui gouverne la nature des solutions de l'équation : selon son signe, il y a deux racines (cas $\Delta > 0$), une racine double (cas $\Delta = 0$) ou aucune racine (cas $\Delta < 0$).

La somme et le produit des solutions. On se place à présent dans le cas où $\Delta \geq 0$ et on pose

$$x_1 = \frac{-b - \sqrt{b^2 - 4ac}}{2a} \quad \text{et} \quad x_2 = \frac{-b + \sqrt{b^2 - 4ac}}{2a}.$$

Ce sont les deux solutions de l'équation qui se confondent lorsque $\Delta = 0$. Un calcul simple conduit à :

$$x_1 + x_2 = \frac{b}{a} \quad \text{et} \quad x_1 x_2 = \frac{c}{a}. \tag{IV.6}$$

Autrement dit, bien que les solutions de l'équation (IV.4) aient des expressions relativement compliquées, leurs sommes et leurs produits s'expriment simplement. En particulier, les racines carrées disparaissent toutes.

La « disparition des racines carrées » n'est pas un phénomène isolé. En fait, il est possible de démontrer que les racines carrées se simplifient toujours lorsque l'on évalue une expression qui est symétrique en x_1, x_2 (c'est-à-dire qui reste inchangée lorsque l'on permute x_1 et x_2). Par exemple :

$$\begin{aligned} x_1^2 + x_2^2 &= \left(\tfrac{-b-\sqrt{b^2-4ac}}{2a}\right)^2 + \left(\tfrac{-b+\sqrt{b^2-4ac}}{2a}\right)^2 \\ &= \tfrac{b^2 - 2b\sqrt{b^2-4ac} + b^2 - 4ac}{4a^2} + \tfrac{b^2 + 2b\sqrt{b^2-4ac} + b^2 - 4ac}{4a^2} \\ &= \tfrac{b^2 - 2ac}{a^2} \end{aligned}$$

(Pour ce calcul, on aurait pu aussi remarquer que $x_1^2 + x_2^2 = (x_1 + x_2)^2 - 2x_1x_2$ et utiliser les formules pour la somme et le produit des x_i.) Ce phénomène de simplification n'est en outre pas spécifique au degré 2. Nous y reviendrons plus longuement dans la suite lorsque nous étudierons les polynômes de degré supérieur.

Il est intéressant de se rendre compte que les propriétés ci-dessus admettent une réciproque qui s'énonce comme suit : si u et v sont deux nombres réels dont la somme vaut s et le produit vaut p, alors u et v sont les deux solutions — éventuellement confondues — de l'équation

$$x^2 - sx + p = 0. \tag{IV.7}$$

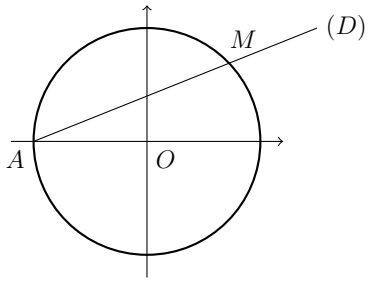
En effet, des équations $u+v = s$ et $uv = p$, on déduit $u(s-u) = p$, c'est-à-dire que u est solution de (IV.7). D'après les formules (IV.6), l'autre solution de équation est $s - u$, c'est-à-dire v.

Un exemple : paramétrisation du cercle. On munit le plan d'un repère orthonormé. Soit $\mathcal{C}$ le cercle de rayon 1 centré à l'origine — qui est parfois appelé le *cercle trigonométrique*. L'équation de ce cercle est $x^2 + y^2 = 1$. On se propose de déterminer une équation paramétrique de ce cercle, c'est-à-dire un système de la forme :

$$\begin{cases} x = f(t) \\ y = g(t) \end{cases}$$

où f et g sont deux fonctions et où, lorsque t parcourt l'ensemble des nombres réels, le point de coordonnées (x, y) correspondant parcourt (presque) tout le cercle C.

Pour cela, une stratégie possible est de fixer un point A sur le cercle puis de déterminer le deuxième point d'intersection M de $\mathcal{C}$ et d'une droite (D) passant par A. Lorsque la droite (D) tourne autour de A, le point M balaye tout le cercle (si on convient que, dans le cas de la droite tangente horizontale, le point M est confondu avec A).



On prend le point A de coordonnées $(0, 1)$ comme sur la figure. En notant t la pente de (D), l'équation de cette dernière est $y = t(x+1)$. En reportant dans l'équation du cercle, on obtient :

$$x^2 + t^2(x + 1)^2 = 1$$

soit encore :

$$(t^2 + 1)x^2 + 2t^2x + (t^2 - 1) = 0.$$

En utilisant les formules de résolution, on trouve $\Delta = 4t^4 - 4(t^2 + 1)(t^2 - 1) = 4$ et les deux solutions de l'équation sont donc :

$$x_1 = \frac{-2t^2 - 2}{2(t^2 + 1)} = -1 \quad \text{et} \quad x_2 = \frac{-2t^2 + 2}{2(t^2 + 1)} = \frac{1 - t^2}{1 + t^2}.$$

On retrouve, sans surprise, la solution -1 qui correspond au point d'intersection A. À vrai dire, sachant cela *a priori*, on aurait pû utiliser plutôt la formule donnant la somme des solutions (IV.6) pour accéder plus rapidement à x_2. Cette remarque justifie également le fait qu'aucune racine carrée n'apparaisse.

Maintenant qu'on a calculé l'abscisse x_2 du point M, on obtient son ordonnée y_2 en reportant dans l'équation de la droite (D) :

$$y_2 = t(x_2 + 1) = \frac{2t}{1 + t^2}$$

puis, une paramétrisation du cercle, comme souhaité. On notera que cette paramétrisation évite le point B car la droite (AB) est verticale et n'a donc pas de pente. Le point B correspond en fait à la limite de la paramétrisation lorsque t tend vers l'infini.

Un des intérêts de la paramétrisation que l'on vient d'obtenir est qu'elle ne fait intervenir que les quatre opérations de base (et pas de racine carrée ou de fonction trigonométrique). Elle peut ainsi être très utile dans un contexte arithmétique. Par exemple, une méthode classique de résolution de l'équation Pythagoricienne $x^2 + y^2 = z^2$ en nombres entiers s'appuie sur cette paramétrisation.

Soulignons enfin que la méthode que nous venons de présenter permet, de la même façon, de trouver un paramétrage de presque[1] toutes les courbes définies par des expressions de degré 2 de la forme[2] :

$$ax^2 + bxy + cy^2 + dx + ey + f = 0 \quad \text{avec} \quad a, b, c, d, e, f \in \mathbb{R}. \tag{IV.8}$$

dès lors que l'on est capable de trouver les coordonnées d'un point sur cette courbe. Les avantages de nature arithmétique sus-mentionnés persistent aussi.

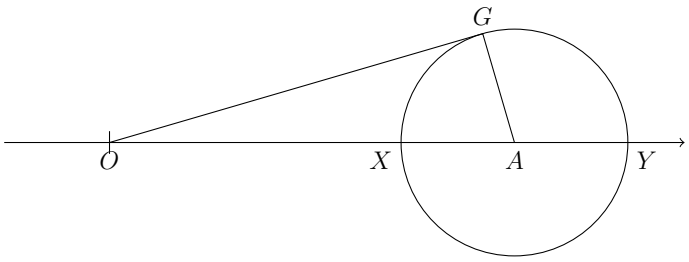
Applications aux inégalités.

Comme on le sait bien, *un carré est toujours positif*. Cette idée simple, combinée à une manipulation intelligente des expressions de degré 2, a des conséquences remarquables. Détaillons-en quelques unes.

L'inégalité arithmético-géométrique. De l'inégalité évidente $(a-b)^2 \geq 0$, on déduit en développant : $a^2 + b^2 \geq 2ab$ pour tous réels a et b. En posant $x = a^2$ et $y = b^2$, on obtient :

$$\frac{x+y}{2} \geq \sqrt{xy} \quad \text{pour tous réels } \textit{positifs } x, y. \tag{IV.9}$$

La quantité de gauche $\frac{x+y}{2}$ est appelée la *moyenne arithmétique* — ou, souvent, plus simplement *moyenne* — des deux nombres x et y tandis que la quantité de droite $\sqrt{xy}$ est leur *moyenne géométrique*. L'inégalité (IV.9) est ainsi généralement appelée l'*inégalité arithmético-géométrique* (en deux variables). Cette inégalité admet une interprétation géométrique intéressante. Sur un demi-axe gradué d'origine O, on place les points X et Y d'abscisse respective x et y. On trace le cercle de diamètre $[XY]$ et l'une des deux droites tangente à ce cercle passant par O. On appelle G le point de tangence et A le milieu de $[XY]$.



L'abscisse du point A est $\frac{x+y}{2}$; autrement dit la longueur OA est égale à la moyenne arithmétique de x et y. Par ailleurs, le triangle OGA est rectangle en G. On en déduit, par le théorème de Pythagore, que :

$$OG^2 = OA^2 - AG^2 = (OA - AG) \cdot (OA + AG) = xy.$$

La longueur OG est donc égale à la moyenne géométrique de x et y. L'inégalité arithméco-géométrique (IV.9) s'interprète ainsi géométriquement comme le fait que l'hypothèse OA du triangle rectangle OAG est plus longue que le côté opposé en l'angle en A.

L'inégalité (IV.9) s'étend à n variables comme suit :

1. La condition est que l'équation (IV.8) ne se factorise pas comme un produit de deux équations de droite.
2. De telles courbes s'appelles des *coniques*.

Proposition 64 (Inégalité arithmético-géométrique)**.** Soient $x_1, \dots, x_n$ des nombres réels positifs. Alors :

$$\frac{x_1 + x_2 + \cdots + x_n}{n} \geq \sqrt[n]{x_1 x_2 \dots x_n}. \tag{IV.10}$$

Notation 65. On rappelle que si x est un nombre réel positif ou nul, $\sqrt[n]{x}$ désigne l'unique nombre réel positif y tel que $y^n = x$.

Démonstration. Appelons (I_n) l'inégalité (IV.10). Nous allons démontrer :

a) si l'inégalité (I_n) est vraie alors (I_{2n}) est aussi vraie, et

b) si l'inégalité (I_{n+1}) est vraie alors (I_n) est aussi vraie.

Ceci nous permettra de conclure par récurrence. En effet, à partir de *a)* et du fait que (I_2) est connue, on déduit que (I_{2^s}) est vraie pour tout entier s. Une récurrence descendante dont l'hérédite est basée sur *b)* permet alors de montrer que (I_n) pour tout entier $n \leq 2^s$. Comme ceci est valable pour tous s, on peut conclure.

Il ne reste donc plus qu'à démontrer *a)* et *b)*. On commence par *a)* : on suppose (I_n) et on cherche à démontrer (I_{2n}). On considère donc $2n$ variables que l'on appelle $x_1, \dots, x_{2n}$. On peut alors écrire :

$$\begin{aligned}
\frac{x_1 + \cdots + x_{2n}}{2n} &= \frac{1}{2} \cdot \left(\frac{x_1 + \cdots + x_n}{n} + \frac{x_{n+1} + \cdots + x_{2n}}{n} \right) \\
&\geq \frac{\sqrt[n]{x_1 \dots x_n} + \sqrt[n]{x_{n+1} \dots x_{2n}}}{2} \\
&\geq \sqrt{\sqrt[n]{x_1 \dots x_n} \cdot \sqrt[n]{x_{n+1} \dots x_{2n}}} = \sqrt[2n]{x_1 \dots x_{2n}}
\end{aligned}$$

la première minoration provenant de notre hypothèse (I_n) — appliquée deux fois — tandis que la seconde n'est autre que l'inégalité arithmético-géométrique en deux variables. On a ainsi démontré (I_{2n}).

On va maintenant démontrer *b)*. On suppose (I_{n+1}) et on considère n variables $x_1, \dots, x_n$. On note $m = \frac{x_1 + \cdots + x_n}{n}$ la moyenne arithmétique des x_i. Si $m = 0$, alors tous les x_i s'annulent et l'inégalité (I_n) est clairement vraie. On suppose donc à partir de maintenant que $m > 0$. La moyenne arithmétique des $(n+1)$ nombres réels $x_1, \dots, x_n, m$ est égale à :

$$\frac{x_1 + \cdots + x_n + m}{n+1} = \frac{nm + m}{n+1} = m.$$

L'inégalité (I_{n+1}) appliquée aux nombres $x_1, \dots, x_n, m$ fournit $m^{n+1} \geq x_1 \dots x_n$. En simplifiant par m, on en déduit $m^n \geq x_1 \dots x_n$, c'est-à-dire (I_n). □

Remarque 66 (Cas d'égalité)**.** En suivant la même stratégie que dans la démonstration ci-dessus, on peut démontrer le rabiot suivant : l'inégalité (IV.10) est une égalité si, et seulement si tous les nombres x_i sont égaux.

Une application classique de l'inégalité arithmético-géométrique est l'inégalité :

$$\frac{x_1}{x_2} + \frac{x_2}{x_3} + \cdots + \frac{x_{n+1}}{x_n} + \frac{x_n}{x_1} \geq n \tag{IV.11}$$

qui est valable pour tous réels strictement positifs $x_1, \dots, x_n$. En effet le produit des fractions qui apparaissent dans le membre de gauche de (IV.11) est 1. Leur moyenne géométrique est

donc égale à 1 et, par suite, d'après l'inégalité arithmético-géométrique, leur moyenne arithmétique est supérieure ou égale à 1. Autrement dit, leur somme est supérieure ou égale à n.

L'inégalité de Cauchy–Schwartz. Une autre application de la positivité des carrés et de la méthode de résolution de l'équation de degré 2 est l'équation de Cauchy–Schwartz qui s'énonce comme suit.

Proposition 67 (Inégalité de Cauchy–Schwartz)**.** Soient $x_1, \dots, x_n$ et $y_1, \dots, y_n$ deux familles de n nombres réels. On a l'inégalité :

$$(x_1y_1 + x_2y_2 + \cdots + x_ny_n)^2 \leq (x_1^2 + x_2^2 + \cdots + x_n^2) \cdot (y_1^2 + x_2^2 + \cdots + y_n^2). \tag{IV.12}$$

Démonstration. L'inégalité est clairement vérifiée si tous les x_i et tous les y_i sont nuls. On suppose donc à partir de maintenant que ce n'est pas le cas. On introduit l'expression suivante

$$A = (tx_1 + y_1)^2 + (tx_2 + y_2)^2 + \cdots + (tx_n + y_n)^2.$$

Elle ne s'annule que si $tx_i + y_i = 0$ pour tout i, ce qui ne peut arriver qu'au plus pour une seule valeur de t. Par ailleurs, en développant, on s'aperçoit que A est une expression de degré 2 en t, à savoir :

$$A = (x_1^2 + x_2^2 + \cdots + x_n^2)t^2 + 2(x_1y_1 + x_2y_2 + \cdots + x_ny_n)t + (y_1^2 + x_2^2 + \cdots + y_n^2).$$

Comme l'équation $A = 0$ a au plus de solution, son discriminant Δ doit être négatif ou nul. Or un calcul donne :

$$\Delta = 4 \cdot \big((x_1y_1 + x_2y_2 + \cdots + x_ny_n)^2 - (x_1^2 + x_2^2 + \cdots + x_n^2) \cdot (y_1^2 + x_2^2 + \cdots + y_n^2)\big).$$

L'inégalité de Cauchy–Schwartz en découle. □

Remarque 68 (Cas d'égalité)**.** En examinant attentivement la démonstration ci-dessous, on s'aperçoit que l'inégalité (IV.12) est une égalité si et seulement si les vecteurs $(x_1, \dots, x_n)$ est $(y_1, \dots, y_n)$ sont colinéaires, c'est-à-dire s'il existe un couple de nombres réels $(\lambda, \mu) \neq (0, 0)$ tels que :

$$\lambda \cdot (x_1, \dots, x_n) + \mu \cdot (y_1, \dots, y_n) = (0, \dots, 0).$$

Un corollaire classique de la proposition 67 est obtenu en prenant $y_i = 1$ pour tout i. Il s'écrit :

$$(x_1 + x_2 + \cdots + x_n)^2 \leq n \cdot (x_1^2 + \cdots + x_n^2) \tag{IV.13}$$

pour toute famille $(x_1, \dots, x_n)$ de nombres réels. En supposant les x_i positifs ou nuls et en prenant la racine carrée de chaque côté dans (IV.13), on obtient :

$$\frac{x_1 + x_2 + \cdots + x_n}{n} \leq \sqrt{\frac{x_1^2 + x_2^2 + \cdots + x_n^2}{n}}. \tag{IV.14}$$

On reconnaît la moyenne arithmétique des x_i dans le membre de gauche. L'expression qui apparaît dans le membre de droite est appelée la *moyenne quadratique* des x_i : c'est la racine carrée de la moyenne des carrés. On vient ainsi de démontrer, comme corollaire de l'inégalité de Cauchy–Schwartz, que la moyenne arithmétique est toujours inférieure à la moyenne quadratique. En combinant cela avec l'inégalité arithmético-géométrique, on obtient :

$$\text{moyenne géométrique} \leq \text{moyenne arithmétique} \leq \text{moyenne quadratique}.$$

Il existe moultes autres inégalités de moyenne. On les détaillera pas davantage dans ce cours mais on renvoie au poly d'inégalités pour de nombreux compléments à ce sujet.

Les polynômes de degré supérieur

Nous allons maintenant étendre certains résultats obtenus précédemment pour le degré 2 aux degrés supérieurs. Ceci nous amènera à introduire et à étudier la notion de *polynôme*.

Généralisation des identités remarquables. La première identité remarquable que nous avions vue pour le degré 2 était $(a+b)^2 = a^2 + 2ab + b^2$. Sa généralisation naturelle aux degrés supérieurs est une formule pour $(a+b)^n$. Pour les premières valeurs de n, on obtient :

$$\begin{aligned}(a+b)^2 &= a^2 + 2ab + b^2\\ (a+b)^3 &= a^3 + 3a^2b + 3ab^2 + b^3\\ (a+b)^4 &= a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4\\ (a+b)^5 &= a^5 + 5a^4b + 10a^3b^2 + 10a^2b^3 + 5ab^4 + b^5\end{aligned}$$

On constate que le développement de $(a+b)^n$ semble s'écrire comme une somme de termes de la forme $c(n,k)a^{n-k}b^k$ pour k variant entre 0 et n où les $c(n,k)$ sont des nombres entiers. Cette propriété se démontre facilement par récurrence. En effet, si on suppose qu'elle est vraie au rang n, on peut écrire [3] :

$$\begin{aligned}(a+b)^{n+1} &= (a+b)^n \cdot (a+b)\\ &= \left(\sum_{k=0}^{n} c(n,k)a^{n-k}b^k\right) \cdot (a+b)\\ &= \sum_{k=0}^{n} c(n,k)a^{n-k+1}b^k + \sum_{k=0}^{n} c(n,k)a^{n-k}b^{k+1}\\ &= \sum_{k=0}^{n} c(n,k)a^{n+1-k}b^k + \sum_{k=1}^{n+1} c(n,k-1)a^{n+1-k}b^k\end{aligned}$$

et on constate, en regroupant les deux termes en $a^{n+1-k}b^k$, que la dernière expression est bien de la forme voulue.

Définition 69. Les $c(n,k)$ s'appelent les *coefficients binomiaux*. On les note $\binom{n}{k}$.

Par ailleurs, il résulte du calcul que l'on vient de faire que les coefficients binomiaux vérifient les relations suivantes [4] qui les déterminent complètement :

$$\forall n \geq 0, \quad \binom{n}{0} = 1 \text{ et } \binom{n}{n} = 1 \tag{IV.15}$$

$$\forall n \geq 0,\ \forall k \in \{1,\dots,n\}, \quad \binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1} \tag{IV.16}$$

Il se trouve, en outre, qu'on dispose d'une formule explicite donnant la valeur des coefficients binomiaux :

3. On rappelle que la notation $\sum_{k=0}^{n} f(k)$ vaut par définition $f(0) + f(1) + \cdots + f(n)$.

4. Le signe $\forall$ se lit *pour tout*.

Proposition 70. Pour tout entier n et tout entier $k \in \{0, \dots, n\}$, on a :

$$\binom{n}{k} = \frac{n!}{k!\,(n-k)!}$$

où, par définition, $n!$ (lire *factorielle* n) est le produit $1 \times 2 \times \cdots \times n$.

Démonstration. Il s'agit de vérifier que les nombres $\frac{n!}{k!\,(n-k)!}$ satisfont aux relations (IV.15)–(IV.16), ce qui est un calcul simple laissé au lecteur. □

En résumé, nous venons de démontrer que :

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k \quad \text{avec} \quad \binom{n}{k} = \frac{n!}{k!\,(n-k)!}. \tag{IV.17}$$

C'est la formule du binôme de Newton.

Passons à présent aux autres identités remarquables. La seconde — à savoir $(a-b)^2 = a^2 - 2ab + b^2$ — se généralise immédiatement au vu de ce que l'on vient de faire : en remplaçant b par $-b$ dans la formule du binôme de Newton, on obtient

$$(a-b)^n = \sum_{k=0}^{n} (-1)^k \binom{n}{k} a^{n-k} b^k. \tag{IV.18}$$

Il reste à trouver une généralisation au degré n de la formule donnant la factorisation de $a^2 - b^2$. C'est :

$$\begin{aligned} a^n - b^n &= (a-b) \cdot (a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1}) \\ &= (a-b) \cdot \sum_{k=0}^{n-1} a^{n-k} b^k \end{aligned} \tag{IV.19}$$

comme on le vérifie facilement en développant le terme de droite et en constatant qu'il redonne celui de gauche.

Notion de polynôme. Un *polynôme* en la variable x est une expression de la forme :

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \tag{IV.20}$$

où les a_i sont des nombres réels [5] donnés (en particulier, il ne dépendent pas de x) appelés les *coefficients* de $P(x)$. Il est facile de vérifier que la somme et le produit de deux polynômes est encore un polynôme.

Si, dans l'expression (IV.20), on a $a_n \neq 0$ — c'est-à-dire si le terme en x^n apparaît bel et bien — on dit que le polynôme $P(x)$ est de *degré* n et on note $\deg P(x) = n$. On convient souvent que

5. En réalité, on peut travailler dans des espaces de nombres plus généraux comme l'ensemble des nombres complexes $\mathbb{C}$ ou celui des résidus modulo n noté généralement $\mathbb{Z}/n\mathbb{Z}$. Toutefois, on n'abordera pas ce sujet dans ce cours.

le degré du polynôme nul (celui pour lequel tous les a_i sont nuls) est $-\infty$. Le comportement du degré vis-à-vis de l'addition et de la multiplication est décrit par les formules suivantes :

$$\deg(P(x)+Q(x)) \leq \max(\deg P(x),\, \deg Q(x))$$
$$\deg(P(x)\cdot Q(x)) = \deg P(x) + \deg Q(x)$$

Le terme correspondant $a_n x^n$ (resp. le coefficient correspondant a_n) s'appelle le *terme dominant* (resp. le *coefficient dominant*). Lorsque le coefficient dominant que $P(x)$ est égal à 1, on dit que $P(x)$ est unitaire. Le coefficient a_0 s'appelle, quant à lui, le *coefficient constant*.

Exemple 71. L'expression $A(x) = x^2 - \sqrt{2}\,x^3 + 3\,x + \pi$ est un polynôme de degré 3 de terme dominant $-\sqrt{2}\,x^3$ et de coefficient constant π.

De la même manière, l'expression $B(x) = x^4 - x^3 + 2\,x^2 - 7\,x + 5$ est un polynôme unitaire de degre 4 de coefficient constant 5. On constate en outre que les coefficients de $B(x)$ sont des nombres entiers ; sans surprise, on dit que $B(x)$ est à *coefficients entiers*.

À l'instar des fonctions, les polynômes peuvent être évalués en n'importe quelle valeur réelle : si a est un nombre réel, le nombre réel $P(a)$ est celui que l'on obtient en remplaçant x par a dans l'expression de $P(x)$. En particulier, $P(0)$ est toujours égal au coefficient constant de P. Dans l'exemple ci-dessus, on a $A(0) = \pi$, $A(1) = 4 + \pi - \sqrt{2}$, $A(2) = 10 + \pi - 8\sqrt{2}$, $B(0) = 5$, $B(1) = 0$, $B(2) = 7$, *etc.* Un nombre a tel que $P(a) = 0$ est appelé une *racine* de P.

Polynômes et divisibilité. Il résulte de la factorisation (IV.19) qu'étant donné un polynôme $P(x)$, l'expression $P(x) - P(y)$ se factorise toujours par $x - y$. En effet, $P(x) - P(y)$ s'écrit comme une somme de termes $a_i(x^i - y^i)$ qui se factorisent tous par $x - y$.

Exemple 72. Si $B(x)$ désigne encore le polynôme de l'exemple IV.20, la différence $B(x) - B(y)$ se factorise comme suit :

$$\begin{aligned} B(x) - B(y) &= (x^4 - y^4) - (x^3 - y^3) + 2(x^2 - y^2) - 7(x - y) \\ &= (x - y)(x^3 + x^2y + xy^2 + y^3) \\ &\qquad - (x - y)(x^2 + xy + y^2) + 2(x - y)(x + y) - 7(x - y) \\ &= (x - y)(x^3 + x^2y + xy^2 + y^3 - x^2 - xy - y^3 + 2x + 2y - 7). \end{aligned}$$

Dans ce qui précède, x et y peuvent, au choix, être des variables formelles (*i.e.* auxquelles on n'a pas affecté de valeurs particulières) ou des nombres réels. Un cas intéressant est celui où x reste une variable mais y prend une valeur réelle déterminée, disons $y = a$:-). La différence $P(x) - P(a)$ — qui est alors un polynôme en x — est divisible par $x - a$ — qui est aussi un polynôme en x — et on s'aperçoit, en examinant les formules, que le quotient $\frac{P(x)-P(a)}{x-a}$ s'écrit encore comme un polynôme en x. Par exemple, en faisant $y = a = 2$ dans la factorisation de l'exemple 72, on trouve :

$$B(x) - 7 = B(x) - B(2) = (x - 2)(x^3 + x^2 + 4x + 1).$$

Un premier cas particulier notable est celui où le polynôme $P(x)$ est à coefficients entiers. Comme on le constate ci-dessus et comme on peut le démontrer en examinant la méthode de factorisation décrire précédemment, le quotient $\frac{P(x)-P(a)}{x-a}$ est, dans ce cas, un polynôme à coefficients entiers dès lors que a est un entier. La proposition suivante en résulte.

Proposition 73. Soit $P(x)$ un polynôme à coefficients entiers et soient a et b deux nombres entiers. Alors $a-b$ divise $P(a)-P(b)$.

En guise d'exemple, une application possible de la proposition 73 consiste à démontrer qu'il n'existe pas de polynôme $P(x)$ à coefficients entiers tel que $P(1)=7$ et $P(15)=8$. En effet, si un tel polynôme existait, on trouverait que $15-1=14$ divise $P(15)-P(1)=8-7=1$, ce qui n'est pas le cas.

Un autre cas important de la formule de factorisation est celui où a est une racine de $P(x)$. Il conduit à la proposition suivante.

Proposition 74. Soit $P(x)$ un polynôme de degré n et a un nombre réel tel que $P(a)=0$. Alors il existe un unique polynôme $Q(x)$ de degré $n-1$ tel que

$$P(x)=(x-a)\cdot Q(x). \tag{IV.21}$$

De plus si $P(x)$ est à coefficients entiers (resp. rationnels), alors $Q(x)$ l'est aussi.

Démonstration. L'existence de $Q(x)$ a déjà été démontrée. Pour l'unicité, on remarque que si $Q_1(x)$ et $Q_2(x)$ sont solutions de la factorisation (IV.21), alors

$$(x-a)\cdot(Q_1(x)-Q_2(x))=0.$$

En comparant les degrés, ceci implique que le polynôme $Q_1(x)-Q_2(x)$ est le polynôme nul et, par suite, que $Q_1(x)=Q_2(x)$. Enfin, la dernière propriété résulte du fait que la formule de factorisation (IV.19) ne fait intervenir que des coefficients entiers. □

Corollaire 75. Un polynôme de degré n a au plus n racines.

Démonstration. Soit $P(x)$ un polynôme de degré n et soient $a_1,\dots,a_k$ ses racines (sans répétition). On veut démontrer que $n\geq k$. Comme x_1 est une racine, il suit de la proposition précédente que :

$$P(x)=(x-a_1)P_1(x)$$

pour un certain polynôme $P_1(x)$ uniquement déterminé. En évaluant l'expression ci-dessus en a_2, on s'aperçoit que a_2 est une racine de $P_1(x)$. On peut ainsi continuer la factorisation comme suit :

$$P(x)=(x-a_1)(x-a_2)P_2(x)$$

où $P_2(x)$ est à nouveau un polynôme. Ainsi de suite, on aboutit à :

$$P(x)=(x-a_1)(x-a_2)\cdots(x-a_k)P_k(x)$$

où $P_k(x)$ est encore un polynôme, qui est clairement non nul. On en déduit que $P(x)$ est de degré au moins k, c'est-à-dire que $n\geq k$ comme voulu. □

Relations entre coefficients et racines. On a vu, dans la première partie de ce cours, que la somme et le produit des racines d'une équation de degré 2 s'exprimaient simplement en fonction des coefficients de l'équation. Il se trouve que ce phénomène se généralise au degré n comme nous allons l'expliquer ci-après. Soit donc :

$$P(x)=a_nx^n+a_{n-1}x^{n-1}+a_1x+a_0 \tag{IV.22}$$

un polynôme de degré n (*i.e.* $a_n \neq 0$) qui admet n racines notées $x_1, \dots, x_n$ supposées deux à deux distinctes[6]. D'après la démonstration du corollaire 75, le polynôme $P(x)$ se factorise ainsi :

$$P(x) = (x - x_1)(x - x_2) \cdots (x - x_n) \cdot Q(x)$$

où $Q(x)$ est un certain polynôme. En comparant les degrés, on trouve que $Q(x)$ est de degré 0, c'est-à-dire que $Q(x) = c \in \mathbb{R}$. En comparant à présent les coefficients dominants, on aboutit à $c = a_n$ et donc à la factorisation :

$$P(x) = a_n(x - x_1)(x - x_2) \cdots (x - x_n) \tag{IV.23}$$

En identifiant les coefficients entre les deux expressions (IV.22) et (IV.23) obtenues pour $P(x)$, on obtient des relations entre les coefficients a_i et les racines x_i. Avant d'écrire ces relations dans le cas général, examinons les petits degrés.

- Pour $n = 2$, on part de l'identité :

$$\begin{aligned} P(x) = a_2x^2 + a_1x + a_0 &= a_2(x - x_1)(x - x_2) \\ &= a_2x^2 - a_2(x_1 + x_2)x + a_2x_1x_2 \end{aligned}$$

  la dernière égalité étant obtenue en développant. En identifiant les coefficients, on aboutit à :

$$x_1 + x_2 = \frac{-a_1}{a_2} \quad \text{et} \quad x_1x_2 = \frac{a_0}{a_2}$$

  c'est-à-dire les relations que nous avions déjà obtenues dans la première partie de ce cours à partir des expressions explicites de x_1 et x_2 en fonction de (a_0, a_1, a_2). On se rend compte que connaître ces expressions — c'est-à-dire savoir résoudre l'équation $P(x) = 0$ — n'était en fait pas nécessaire pour pouvoir exprimer la somme et le produit des racines.

- Pour $n = 3$, on écrit :

$$a_3x^3 + a_2x^2 + a_1x + a_0 = a_3(x - x_1)(x - x_2)(x - x_3)$$

  et un calcul analogue au précédent conduit aux relations :

$$\begin{cases} x_1 + x_2 + x_3 = -a_2/a_3 \\ x_1x_2 + x_1x_3 + x_2x_3 = a_1/a_3 \\ x_1x_2x_3 = -a_0/a_3. \end{cases}$$

  À nouveau, la somme et le produit des x_i s'expriment aisément en fonction des a_i et, encore une fois, nous n'avons pas eu besoin de résoudre l'équation $P(x) = 0$ — ce que, d'ailleurs, nous ne savons *a priori* pas faire[7] — pour obtenir ces relations.

6. Cette hypothèse n'est, en réalité, pas nécessaire. Toutefois, si on souhaite l'ôter, il faut introduire la notion de multiplicité d'une racine, ce que nous avons choisi de ne pas aborder dans ce cours. Nous renvoyer au poly sur les polynômes pour des compléments à ce sujet.

7. En réalité, il existe des formules pour la résolution des équations de degré 3. Toutefois, elles sont compliquées et peu utiles en pratique. De telles formules existent également pour le degré 4 mais il n'y en a plus à partir du degré 5. Malgré tout, comme nous allons le voir dans la suite, les relations entre coefficients et racines, eux, existent en tout degré.

On en vient maintenant au cas général. Au vu des exemples précédents, il s'agit de comprendre comment le produit (IV.23) se développe. On introduit pour cela les *fonctions symétriques élémentaires* en n variables, qui sont les $\sigma_{n,k}$ ($1 \leq k \leq n$) définies par :

$$\sigma_{n,k}(x_1, x_2, \ldots, x_n) = \sum_{\substack{I \subset \{1,\ldots,n\} \\ \text{card } I = k}} \prod_{i \in I} x_i. \tag{IV.24}$$

La notation signifie que l'on fait la somme de tous les produits possibles de k nombres parmi les x_i. Par exemple, si $k = 1$, $\sigma_{n,1}(x_1, \ldots, x_n)$ n'est autre que la somme des x_i. Si $k = 2$, $\sigma_{n,2}(x_1, \ldots, x_n)$ est la somme des produits des x_i deux à deux :

$$\sigma_{n,2}(x_1, \ldots, x_n) = \sum_{1 \leq i < j \leq n} x_i x_j$$

l'ensemble I correspondant sur cette écriture à la paire $\{i, j\}$. Lorsque $k = n$, l'unique partie I qui contribue à la somme (IV.24) est $I = \{1, \ldots, n\}$, d'où on déduit que $\sigma_{n,n}(x_1, x_2, \ldots, x_n)$ s'identifie au produit des x_i. Par convention, on pose $\sigma_{n,0} = 1$ pour tout n.

Lemme 76. Pour tout entier n et tout $k \in \{1, \ldots, n\}$, on a la relation :

$$\sigma_{n+1,k}(x_1, \ldots, x_{n+1}) = \sigma_{n,k}(x_1, \ldots, x_n) + x_{n+1} \cdot \sigma_{n,k-1}(x_1, \ldots, x_n).$$

Démonstration. La relation annoncée s'obtient en séparant dans la somme définissant $\sigma_{n+1,k}(x_1, \ldots, x_{n+1}$ les termes correspondant aux parties I contenant $n + 1$ des autres. □

À partir du lemme 76, on démontre par une récurrence facile sur n (laissée au lecteur) l'identité suivante :

$$(x - x_1) \cdots (x - x_n) = \sum_{k=0}^{n} (-1)^k \sigma_{n,k}(x_1, \ldots, x_n) \cdot x^{n-k}.$$

En comparant les écritures (IV.22) et (IV.23), on obtient finalement les relations entre coefficients et racines que voici :

$$\forall k \in \{1, \ldots, n\}, \quad \sigma_{n,k}(x_1, \ldots, x_n) = (-1)^k \cdot \frac{a_{n-k}}{a_n}. \tag{IV.25}$$

En particulier, pour $k = 1$ et $k = n$, on trouve respectivement :

$$x_1 + \cdots + x_n = -\frac{a_{n-1}}{a_n} \quad \text{et} \quad x_1 \cdots x_n = (-1)^n \cdot \frac{a_0}{a_n}.$$

Par ailleurs, comme dans le cas du degré 2, ce calcul admet une réciproque qui s'énonce comme suit : si $x_1, \ldots, x_n$ sont des nombres réels pour lesquels $\sigma_{n,k}(x_1, \ldots, x_n) = \sigma_k$ pour tout k, alors les x_i sont, à permutation près, les solutions de l'équation :

$$x^n - \sigma_1 x^{n+1} + \sigma_2 x^{n-2} + \cdots + (-1)^{n-1} \sigma_{n-1} x + (-1)^n \sigma_n = 0. \tag{IV.26}$$

En effet, les x_i sont les solutions de l'équation $(x - x_1) \cdots (x - x_n) = 0$, qui redonne (IV.26) après développement. Dans le cas du degré 3, ceci signifie que résoudre le système :

$$\begin{cases} x_1 + x_2 + x_3 = \sigma_1 \\ x_1 x_2 + x_1 x_3 + x_2 x_3 = \sigma_2 \\ x_1 x_2 x_3 = \sigma_3 \end{cases}$$

(où les σ_i sont connus et les x_i sont les inconnues) revient à résoudre l'unique équation $x^3 - \sigma_1 x^2 + \sigma_2 x - \sigma_3 = 0$.

Les expressions des $\sigma_{n,k}(x_1, \ldots, x_n)$ peuvent sembler compliquées mais, hormis le fait que ce sont elles qui apparaissent lorsque l'on développe le produit $(x-x_1)\cdots(x-x_n)$, elles ont un intérêt majeur car elles permettent de reconstruire toutes les fonctions symétriques en les x_i. Ceci explique pourquoi on les appelle les *fonctions symétriques élémentaires*. Avant d'expliquer ceci plus en détails, il nous donner quelques définitions.

Définition 77. Un polynôme en n variables $P(x_1, \ldots, x_n)$ est une somme de termes de la forme $cx_1^{i_1} \cdots x_n^{i_n}$ où c est un nombre réel et les exposants i_k sont des entiers positifs ou nuls.

Le polynôme $P(x_1, \ldots, x_n)$ est dit symétrique si :

$$P(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) = P(x_1, \ldots, x_n)$$

pour toute permutation σ de $\{1, \ldots, n\}$.

Exemple 78. Le polynôme $S(x_1, x_2, x_3) = x_1^2 + x_2^2 + x_3^2$ est un polynôme symétrique en trois variables.

Il est facile de vérifier que les $\sigma_{n,k}(x_1, \ldots, x_n)$ sont des polynômes symétriques en n variables. Ils ont un intérêt particulier à cause du théorème suivant que nous admettrons [8].

Théoréme 79. Tout polynôme $P(x_1, \ldots, x_n)$ symétrique en n variable s'écrit de manière unique sous la forme :

$$P(x_1, \ldots, x_n) = Q(\sigma_{n,1}(x_1, \ldots, x_n), \ldots, \sigma_{n,n}(x_1, \ldots, x_n))$$

où $Q(\sigma_1, \ldots, \sigma_n)$ est un polynôme en n variables (par nécessairement symétrique).

Par exemple, le polynôme $S(x_1, x_2, x_3) = x_1^2 + x_2^2 + x_3^2$ de l'exemple 78 s'écrit :

$$S(x_1, x_2, x_3) = \sigma_{n,1}(x_1, x_2, x_3)^2 - 2\sigma_{n,2}(x_1, x_2, x_3).$$

Il n'est généralement pas difficile — quoique parfois un peu laborieux — de trouver à la main l'écriture d'un polynôme symétrique donné comme fonction des polynômes symétriques élémentaires. En combinant le théorème 79 avec la formule (IV.25), on trouve que toute expression polynômiale symétrique des n racines $x_1, \ldots, x_n$ de l'équation polynômiale

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0$$

s'exprime, de manière polynomiale, en fonction des $\frac{a_i}{a_n}$. En particulier, si les a_i sont des nombres rationnels, toute telle expression prend également une valeur rationnelle, alors que ce n'est évidemment pas le cas des x_i individuellement.

2 jeudi 20 après-midi : Arsène Pierrot

Inégalités

Sauf mention contraire, tous les nombres utilisés seront des réels strictement positifs.

Exercice 1

Pour $n = 2$, montrer que l'IAG équivaut à Cauchy-Schwarz (sans dire qu'elles sont toutes les deux vraies !).

8. La démonstration est un peu technique mais pas très compliquée. Le lecteur intéressé pourra la chercher par lui-même.

Exercice 2
Etant donnés $x_1, ..., x_n$, on pose
$H = \frac{n}{\frac{1}{x_1}+...+\frac{1}{x_n}}$
$G = \sqrt[n]{x_1 \times ... \times x_n}$
$A = \frac{x_1+...+x_n}{n}$
$Q = \sqrt{\frac{x_1^2+...x_n^2}{n}}$
(respectivement appelées moyennes harmonique, géométrique, arithmétique, et quadratique des (x_i)). Montrer que $H \leq G \leq A \leq Q$.

Exercice 3
$(x_1 + ... + x_n) \times (\frac{1}{x_1} + ... + \frac{1}{x_n}) \geq n^2$

Exercice 4
Soient $a_1, ..., a_n$ tels que $a_1 + ... + a_n = n$ et $b_1, ..., b_n$ tels que $b_1 \times .. \times b_n = 1$. Montrer que $(1 + a_1) \times ... \times (1 + a_n) \leq (1 + b_1) \times ... \times (1 + b_n)$.

Solution de l'exercice 1
CS $\Rightarrow$ IAG :
On prend $a = c = 1$ d'où $(1 + bd)^2 \leq (1 + b^2)(1 + d^2)$. En développant on a $bd \leq \frac{b^2+d^2}{2}$. D'où le résultat avec $b = \sqrt{x}$ et $d = \sqrt{y}$. IAG $\Rightarrow$ CS :
On veut $(ac + bd)^2 \leq (a^2 + b^2)(c^2 + d^2)$. En divisant par $a^2c^2 > 0$, cette inégalité équivaut à $(1 + \frac{b}{a}\frac{d}{c})^2 \leq (1 + (\frac{b}{a})^2)(1 + (\frac{d}{c})^2)$. En posant $x = \{\frac{b}{a}^2 > 0$ et $y = \frac{d}{c}^2 > 0$, puis en développant, on a
$1+2\sqrt{xy}+xy \leq 1+x+y+xy$, qui équivaut à l'IAG. Remarque : on remarque que la deuxième preuve donne en fait directement l'équivalence puisque l'on peut " remonter les calculs ". Mais pour être rigoureux, il faudrait parler de " bijections "....

Solution de l'exercice 2
On sait déjà que $G \leq A$.
$A \leq Q$ vient de CS avec $y_1 = ... = y_n = 1$.
$H \leq A$ vient de l'IAG appliquée aux $(\frac{1}{x_i})$ et de la décroissance de la fonction inverse.

Solution de l'exercice 3
Cette inégalité est équivalente à $H \leq A$ (notations de la solution précédente). Elle peut aussi venir de CS appliquée aux $(\sqrt{x_i})$ et $(\frac{1}{\sqrt{x_i}})$.

Solution de l'exercice 4
On va en fait montrer que $(1 + a_1) \times ... \times (1 + a_n) \leq 2^n \leq (1 + b_1) \times ... \times (1 + b_n)$.
Inégalité de gauche :
D'après l'IAG, on a $\sqrt[n]{(1 + a_1) \times ... \times (1 + a_n)} \leq \frac{(1+a_1)+...+(1+a_n)}{n} = 2$ d'après l'hypothèse sur la somme des (a_i). D'où le résultat en passant à la puissance n (tous les nombres étudiés sont strictement positifs).
Inégalité de droite :
On applique l'IAG à chaque terme : $1+b_i \geq 2\sqrt{1 \times b_i}$. Donc en passant au produit (les nombres sont encore positifs !) :
$(1 + b_1) \times ... \times (1 + b_n) \geq 2\sqrt{b_1} \times ... \times 2\sqrt{b_n} = 2^n\sqrt{b_1 \times ... \times b_n} = 2^n$ d'après l'hypothèse sur le produit des (b_i).

Polynomes

Exercice 5 Trouver tous les polynômes P tels que $P(0) = 0$ et $P(X^2 + 1) = P(X)^2 + 1$

Exercice 6 On pose $|x| = x$ si x est positif, $-x$ sinon. Montrer que $|X|$ n'est pas un polynôme.

Exercice 7 Soient a, b, c tels que $a + b + c = 4$, $a^2 + b^2 + c^2 = 12$, et $abc = 1$. Montrer que a, b, et c ne peuvent pas être tous trois positifs.

Solution de l'exercice 5 On appelle point fixe de P un nombre x tel que $P(x) = x$. Montrons par récurrence sur $n \geq 1$ que P a au moins n points fixes positifs.
Initialisation : 0 est point fixe de P.
Hérédité : Si P a au moins n points fixes positifs $0 \leq x_1 \leq ... \leq x_n$, on a : $P(x_n^2 + 1) = P(x_n)^2 + 1 = x_n^2 + 1$. Donc $x_{n+1} = x_n^2 + 1$ est aussi point fixe de P. Or $x_{n+1} \geq 2 \times x_n \geq x_n$ d'après l'IAG et $x_n \geq 0$, l'une des deux égalités étant stricte (sinon $x_n = 0 = 1$, absurde). Puisque $x_{n+1} > x_n$, x_{n+1} est différent de tous les x_i ($i \in [|1; n|]$). D'où l'hérédité.
Ainsi, P a une infinité de points fixes, et donc $Q(X) = P(X) - X$ a une infinité de racines. C'est donc le polynôme nul. Donc $P(X) = X$ est la seule solution (réciproquement, elle convient bien).

Solution de l'exercice 6 Si, par l'absurde, $|X|$ était un polynôme, alors $Q(X) = |X| - X$ en serait un aussi. Or $Q(X)$ a une infinité de racines (tous les réels positifs), mais n'est pas nul (car $Q(-1) = 2$), absurde.

Solution de l'exercice 7 On a $(a + b + c)^2 - (a^2 + b^2 + c^2) = 2ab + 2ac + 2bc = 4^2 - 12 = 4$. D'où $ab + ac + bc = 2$. Ainsi $abc \times (\frac{1}{a} + \frac{1}{b} + \frac{1}{c}) = 2$ et donc $\frac{1}{a} + \frac{1}{b} + \frac{1}{c} = 2$ car $abc = 1$.
La moyenne arithmétique de a, b, et c est donc $\frac{a+b+c}{3} = \frac{4}{3}$.
De même, leur moyenne harmonique est $\frac{3}{\frac{1}{a}+\frac{1}{b}+\frac{1}{c}} = \frac{3}{2}$.
Ainsi, l'inégalité entre moyenne arithmétique et moyenne harmonique n'est pas respectée, donc au moins un des nombres a, b, ou c n'est pas un réel positif (et donc un deuxième non plus, puisque leur produit vaut $1 > 0$).

3 Groupe C : polynômes

1 jeudi 20 matin : Igor Kortchemski

Il s'agissait d'un cours sur les polynômes à une variable. Les notions suivantes ont été abordées : opérations sur les polynômes, division euclidienne de polynômes, racines, factorisation, racines multiples et polynôme dérivé, interpolation, (polynômes de Lagrange), polynômes symétriques élémentaires, relations de Viète, formules de Newton.

Exercices donnés en cours

Exercice 1 Soit P un polynôme tel que le reste de la division euclidienne de P par $x - 1$ vaut 2 et le reste de la division euclidienne de P par $x - 2$ vaut 1. Quel est le reste de la division euclidienne de P par $(x - 1)(x - 2)$?

Exercice 2 Soit P un polynôme de degré 4 tel que $P(0) = P(1) = 1$, $P(2) = 4$, $P(3) = 9$ et $P(4) = 16$. Calculer $P(-2)$.

Exercice 3 Soient α, β, γ les trois racines de $x^3 - x - 1$. Que vaut $\frac{1-\alpha}{1+\alpha} + \frac{1-\beta}{1+\beta} + \frac{1-\gamma}{1+\gamma}$?

Exercice 4 Soit P et Q des polynômes unitaires de degré 2014, tels que pour tout réel x, $P(x) \neq Q(x)$. Montrer qu'il existe un réel x tel que $P(x-1) = Q(x+1)$.

Exercice 5 Trouver tous les polynômes $P \in \mathbb{R}[X]$ tels que pour tous réels a, b, c on ait :

$$P(a+b-2c) + P(b+c-2a) + P(c+a-2b) = 3P(a-b) + 3P(b-c) + 3P(c-a).$$

Exercice 6 Soit P un polynôme à coefficients réels. On suppose que toutes les racines de P sont réelles. Montrer que $(n-1)\left(P'(x)\right)^2 \geq nP(x)P''(x)$ et déterminer les cas d'égalité.

Solution des exercices

Solution de l'exercice 1 D'après les hypothèses, $P(1) = 2$ et $P(2) = 1$. Écrivons la division euclidienne de P par $(x-1)(x-2)$: $P(x) = Q(x)(x-1)(x-2) + ax + b$ avec $a, b \in \mathbb{R}$ qu'il s'agit de déterminer. En faisant $x = 1$ on obtien $2 = P(1) = a + b$ et $1 = P(2) = 2a + b$. On en déduit que $a = -1$ et $b = 3$. Ainsi, le reste de la division euclidienne de P par $(x-1)(x-2)$ est $-x+3$.

Solution de l'exercice 2 Dans ce genre d'exercice, on cherche un polynôme "proche" de P ayant (presque) autant de racines que son degré, pour l'avoir sous forme factorisée. Avec un soupçon d'observation, on se rend compte que $P(1) - 1^2 = P(2) - 2^2 = P(3) - 3^2 = P(4) - 4^2 = 0$. $P(X) - X^2$ est de degré au plus 4, donc il existe un réel c tel que $P(X) - X^2 = c(X-1)(X-2)(X-3)(X-4)$. Pour $X = 0$, on trouve $c = \frac{1}{24}$.

Solution de l'exercice 3 Une méthode sûre même si, en l'occurrence, on peut trouver plus rapide, est de chercher l'équation ayant pour racines $\frac{1-\alpha}{1+\alpha}, \frac{1-\beta}{1+\beta}, \frac{1-\gamma}{1+\gamma}$ et de calculer la somme des racines de cette dernière équation à partir de ses coefficients. Si x est racine de $x^3 - x - 1$, de quelle équation est racine $y = \frac{1-x}{1+x}$? On remarque que $x = \frac{1-y}{1+y}$ (la fonction est involutive), donc $\left(\frac{1-y}{1+y}\right)^3 - \left(\frac{1-y}{1+y}\right) - 1 = 0$, soit : $(1-y)^3 - (1-y)(1+y)^2 - (1+y)^3 = 0$. L'équation en y s'écrit donc : $-y^3 + y^2 - 7y - 1$, la somme de ses racines vaut 1.

Autre méthode : on aurait aussi pu tout mettre au même dénominateur, développer en haut et en bas, et tout exprimer en fonction des polynômes symétriques élémentaires.

Solution de l'exercice 4 Reformulons classiquement et légèrement l'énoncé : on veut une racine réelle au polynôme $R(X) = P(X-1) - Q(X+1)$. A quoi peut-il ressembler ? Il est clairement de degré au plus 2013 (le coefficient du terme de degré 2014 étant nul). S'il est de degré 2013, donc impair, alors il aura bien une racine impaire. Regardons de plus près, en posant $P(X) = X^{2014} + aX^{2013} + S(X)$ et $Q(X) = X^{2014} + bX^{2013} + T(X)$, où S et T sont de degré au plus 2012. Soit de plus c le coefficient de degré 2013 de R. On obtient $c = -2014 - 2014 + a - b = a - b - 4028$ (on regarde, dans $(X-1)^{2014}$, le terme de degré 2013, et de même pour $(X+1)^{2014}$). Se posent deux questions : comment gérer ce $a - b$? Et à quoi sert la condition $P(x) \neq Q(x)$ pour tout x réel ? Heureusement, elles sont liées !

$P - Q$ n'a pas de racine réelle, donc n'est pas de degré impair. Or $P - Q$ est de degré au plus 2013, et le coefficient du terme de degré 2013 est $a - b$. Donc $a - b = 0$.

Ainsi $c \neq 0$, et R est bien de degré 2013, ce que l'on voulait.

Solution de l'exercice 5 En injectant $a = b = c = 0$, on trouve $P(0) = 0$. En prenant $b = c = 0$, on obtient $P(2a) = 3P(a) + P(-a)$, et ce pour tout a. On suppose P de degré n. En examinant les coefficients dominants, on obtient $2^n = (-1)^n + 3$, donc n vaut 1 ou 2, et P est de la forme $aX^2 + bX$. On vérifie réciproquement que ces polynômes conviennent.

Solution de l'exercice 6 Notons $\alpha_1, \ldots, \alpha_n$ les n racines de P. On écrit :

$$\frac{P''(x)P(x) - P'(x)^2}{P(x)^2} = \left(\frac{P'(x)}{P(x)}\right)' = \sum_{i=1}^{n} \frac{-1}{(x-\alpha_i)^2}.$$

Ainsi,

$$\begin{aligned}(n-1)P'(x)^2 - nP(x)P''(x) &= P(x)^2 \cdot \frac{n(P'(x)^2 - P(x)P''(x)) - P'(x)^2}{P(x)^2} \\ &= P(x)^2 \left(\sum_{i=1}^{n} \frac{n}{(x-\alpha_i)^2} - \left(\sum_{i=1}^{n} \frac{1}{(x-\alpha_i)}\right)^2\right),\end{aligned}$$

qui est positif d'après l'inégalité de Cauchy–Scwharz. Le cas d'égalité s'obtient lorsque tous les α_i sont égaux, i.e. lorsque $P(x)$ est de la forme $P(x) = c(X-a)^n$.

2 jeudi 20 après-midi : Thomas Budzinski

Ce texte n'a pas encore été intégré.

4 Groupe D : géométrie

1 mercredi 19 après-midi : Thomas Budzinski

Les premiers exercices de la feuille sont des applications (pas forcément faciles !) du lemme suivant :

Lemme 80. Soient A, B, C et D quatre points du plan. Alors $(AC) \perp (BD)$ si et seulement si :

$$AB^2 + CD^2 = BC^2 + DA^2$$

Démonstration. Le sens direct est très facile : si $(AC) \perp (BD)$, on note X l'intersection des deux droites et le théorème de Pythagore donne $AB^2 + CD^2 = AX^2 + BX^2 + CX^2 + DX^2 = BC^2 + DA^2$.

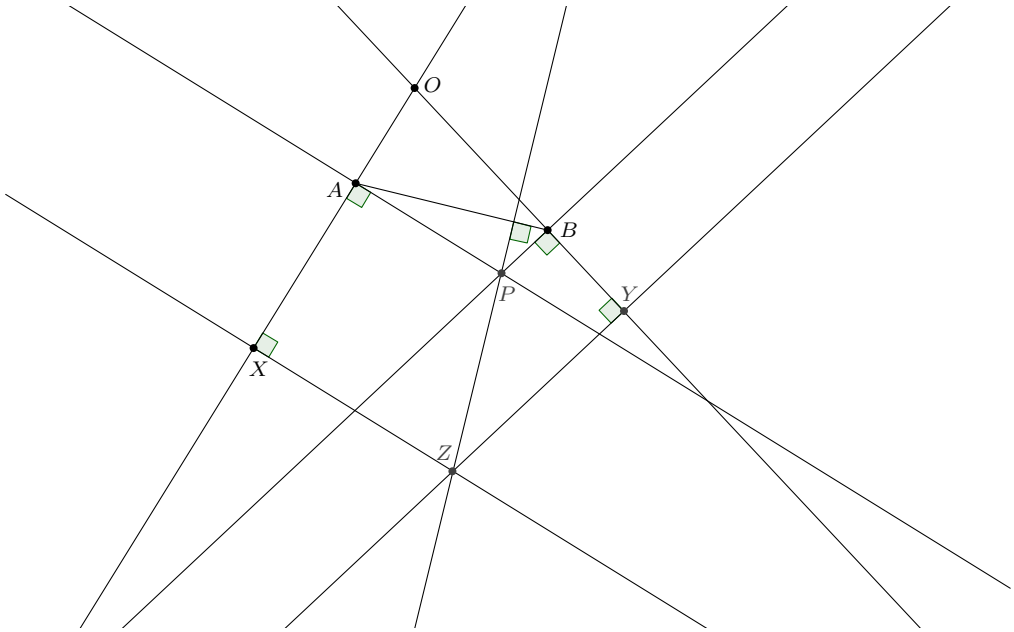
Pour le sens indirect, on peut utiliser le produit scalaire :

$$\begin{aligned}AB^2 + CD^2 - BC^2 + DA^2 &= (\vec{AB} + \vec{BC}) \cdot (\vec{AB} - \vec{BC}) + (\vec{CD} + \vec{DA}) \cdot (\vec{CD} - \vec{DA}) \\ &= \vec{AC} \cdot (\vec{AB} - \vec{BC} - \vec{CD} + \vec{DA}) \\ &= \vec{AC} \cdot (2\vec{DB})\end{aligned}$$

donc cette quantité s'annule ssi $\vec{AC}$ et $\vec{DB}$ sont orthogonaux. □

Exercice 1 Soient $[Ox)$ et $[Oy)$ deux demi-droites issues d'un point O et k un réel. On considère $A \in [Ox)$ et $B \in [Oy)$ variables tels que $OA + OB = k$. Soit P l'intersection des perpendiculaires à (Ox) passant par A et à (Oy) passant par B. Soit (d) la perpendiculaire à (AB) passant par B.

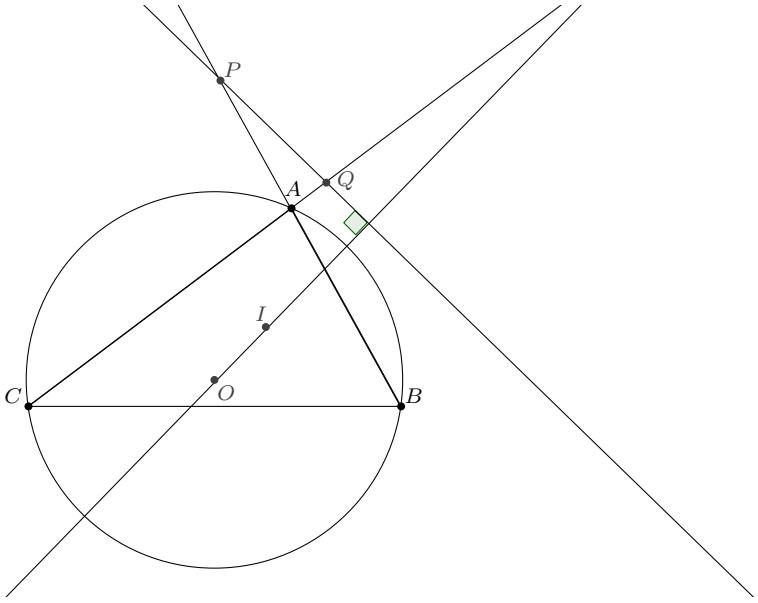
Montrer que (d) passe par un point fixe quand A et B varie.



<u>*Solution de l'exercice 1*</u> Soient $X \in [Ox)$ et $Y \in [Oy)$ tels que $OX = OY = k$. En testant les cas $A = O$ et $B = O$, il semble que le point fixe par lequel doit passer O soit l'intersection de la perpendiculaire à (OX) passant par X et de celle à (OY) par Y. On note Z cette intersection, et on veut montrer $(PZ) \perp (AB)$. Il suffit pour cela de montrer $AP^2 - BP^2 = AZ^2 - AZ^2$. Or, on a $AP^2 - BP^2 = OP^2 - OA^2 - OP^2 + OB^2 = OB^2 - OA^2$ et d'autre part $AZ^2 - BZ^2 = AX^2 + XZ^2 - BY^2 - YZ^2 = AX^2 - BY^2$. On en déduit le résultat car $OB = k - OA = OX - OA = AX$ et $BY = k - OB = OA$.

Exercice 2 Soit ABC un triangle, O le centre de son cercle circonscrit et I le centre de son cercle inscrit. Soient $P \in [BA)$ et $Q \in [CA)$ tels que $BP = CQ = AB$.

Montrer que $(PQ) \perp (OI)$.

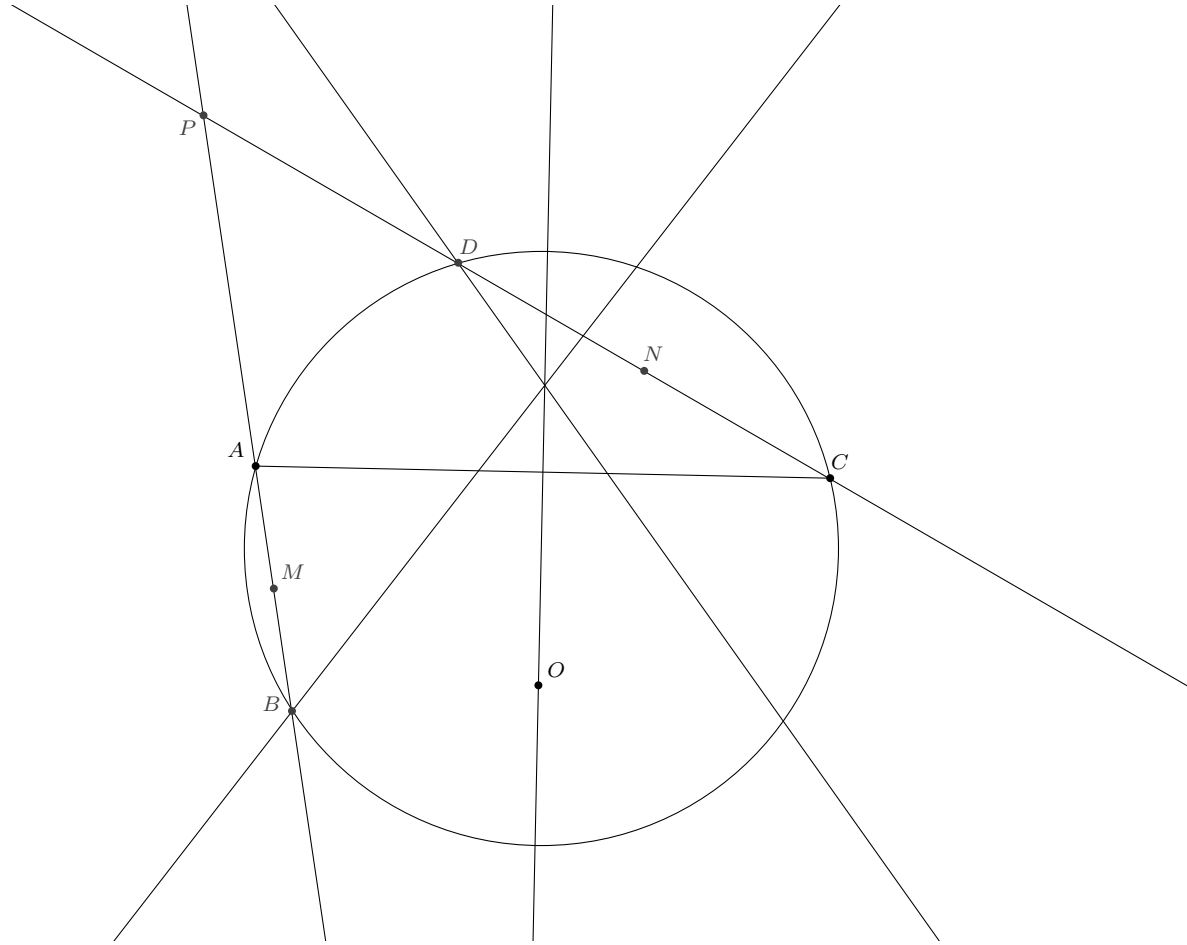


Solution de l'exercice 2 Il suffit de montrer $PI^2 - QI^2 = PO^2 - QO^2$. On introduit D et E, points de contacts du cercle inscrit avec $[AB]$ et $[AC]$. On note $x = AD = AE$, $y = BD$ et $z = CE$, r le rayon du cercle inscrit à ABC et R celui du cercle circonscrit. On a $PI^2 = PD^2 + ID^2 = (BC - BE)^2 + r^2 = z^2 + r^2$, et de même $QI^2 = y^2 + r^2$ donc $PI^2 - QI^2 = z^2 - y^2$.

Pour faire apparaître PO^2, on utilise la puissance de P par rapport au cercle circonscrit : $PO^2 - R^2 = PA \times PB = BC \times (BC - AB) = (y+z)(z-x)$ et de même $QO^2 - R^2 = (y+z)(y-x)$ donc $PO^2 - QO^2 = (y + z)(z - y) = z^2 - y^2$ d'où le résultat.

Exercice 3 Soient A et C sur un cercle Γ et O sur la médiatrice de $[AC]$. Les bissectrices de $[OA]$ et $[OC]$ recoupent Γ en B et D tels que A, B, C et D soient dans cet ordre sur Γ. (AB) et (CD) se recoupent en P, et on note M et N les milieux de $[AB]$ et $[CD]$.

Montrer que $(MN) \perp (OP)$.

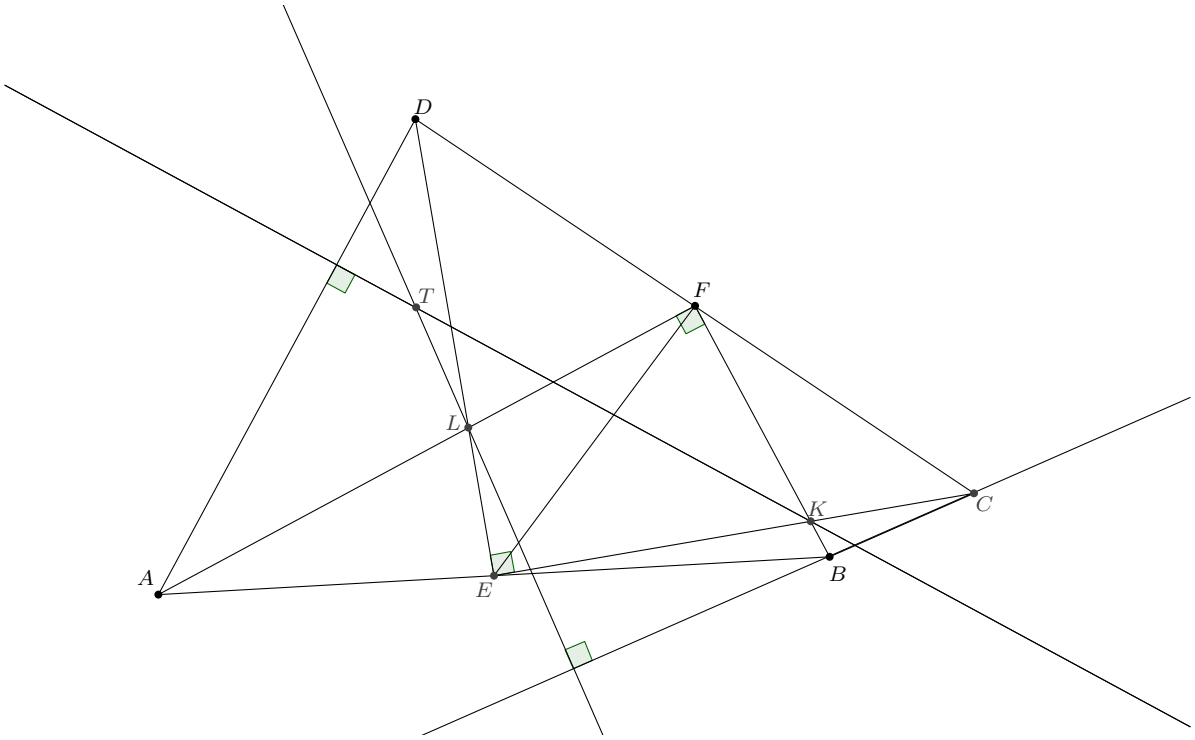


Solution de l'exercice 3 On veut montrer $OM^2 - ON^2 = PM^2 - PN^2$. La formule de la médiane donne $OM^2 = \frac{1}{2}OA^2 + \frac{1}{2}OB^2 - \frac{1}{4}AB^2$ donc $OM^2 - ON^2 = \frac{1}{2}(OB^2 - OD^2) + \frac{1}{4}(CD^2 - AB^2) = \frac{1}{4}(AB^2 - CD^2)$ en utilisant $OA = OC$, $OB = AB$ et $OD = CD$.

D'autre part, on a $PM^2 = (PA+AM)\times(PA-BM) = PA\times PB + AB\times AM - AM^2 = PA\times PB + \frac{1}{2}AB^2 - \frac{1}{4}AB^2$ donc $PM^2 - PN^2 = PA\times PB - PC\times PD + \frac{1}{4}(AB^2 - CD^2) = \frac{1}{4}(AB^2 - CD^2)$ d'où le résultat.

Exercice 4 Soit $ABCD$ un quadrilatère convexe, $E \in [AB]$ et $F \in [CD]$. On suppose $AE = BE = CF = DF = EF$. Les diagonales de $BCFE$ se coupent en K et celles de $ADFE$ en L. La perpendiculaire à $[AD]$ passant par K et celle à $[BC]$ passant par L se coupent en T.

Montrer que $TE = TF$.



Solution de l'exercice 4 D'après la formule de la médiane on a $4TE^2 = 2TA^2 + 2TB^2 - AB^2$, et de même pour TF. Comme $AB = CD$, il suffit de montrer $TA^2 + TB^2 = TC^2 + TD^2$. Comme $(TK) \perp (AD)$, on a $TA^2 - TD^2 = KA^2 - KD^2$ et de même $TC^2 - TB^2 = LC^2 - LB^2$ donc il suffit de montrer $KA^2 + LB^2 = KD^2 + LC^2$.

Comme $EA = EB = EF$, le triangle ABF est rectangle en F donc d'après Pythagore on peut écrire $KA^2 = KF^2 + FA^2$ et de même pour les autres longueurs. Le résultat est alors équivalent à :

$$KF^2 + AF^2 + LF^2 + BF^2 = KE^2 + DE^2 + LE^2 + CE^2$$

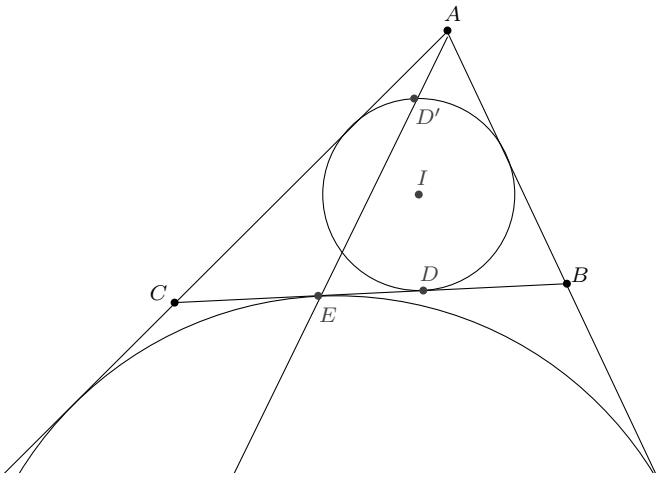
soit, toujours d'après Pythagore, $AB^2 + KL^2 = CD^2 + KL^2$, ce qui est immédiat.

Exercice 5 Soit $ABCD$ un quadrilatère circonscriptible et ω son cercle inscrit, de centre O. On note X l'intersection de (AB) et (CD). Le cercle ω_1 est tangent aux prolongements de $[AB]$ et $[CD]$ et au côté $[AD]$ en K. Le cercle ω_2 est tangent aux prolongements de $[AB]$ et $[CD]$ et au côté $[BC]$ en L. On suppose que X, K et L sont alignés.

Montrer que O, le milieu de $[AD]$ et le milieu de $[BC]$ sont alignés.

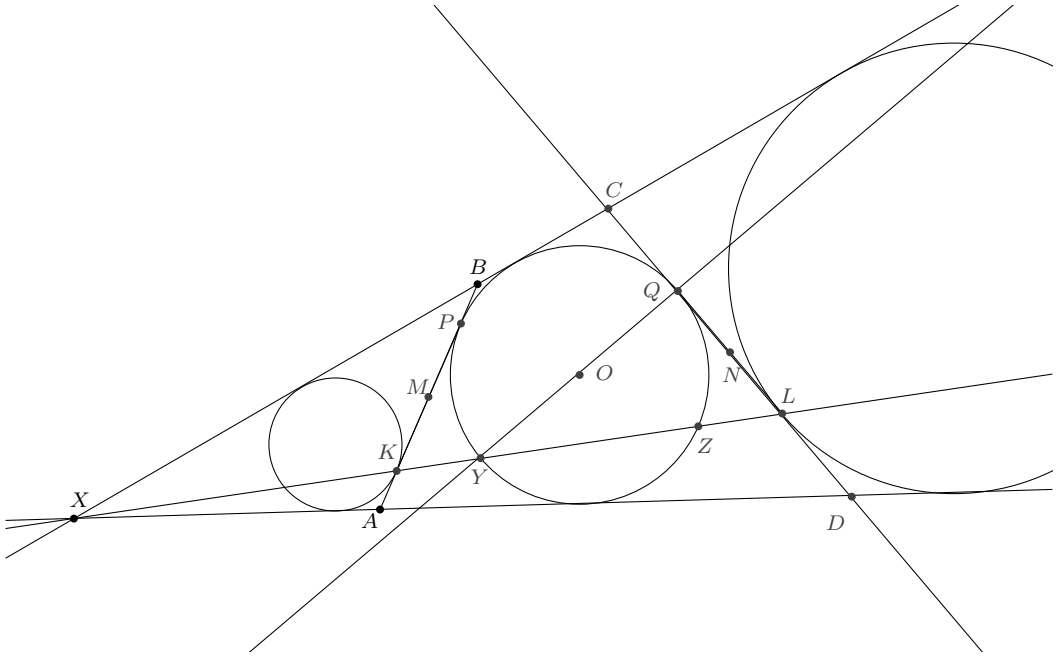
Commençons par rappeler un petit lemme :

Lemme 81. Soit ABC un triangle de cercle inscrit ω et D le point de contact de ω avec $[BC]$. On note D' le point diamétralement opposé à D sur ω. Soit E le point de contact du cercle A-exinscrit à ABC avec $[BC]$. Alors A, D' et E sont alignés.



Démonstration. Soit h l'homothétie de centre A qui envoie le cercle exinscrit sur ω et $E' = h(E)$: la tangente à ω en E' est parallèle à (BC) et n'est pas (BC). Mais la tangente à ω en D' est parallèle à celle en D, donc à (BC), et n'est pas (BC) donc c'est la même tangente et $D' = E'$ donc A, D' et E sont alignés. □

Revenons à notre exercice :



<u>*Solution de l'exercice 5*</u> Sans perte de généralité, on suppose que $A \in [BX]$ et $D \in [CX]$. On note P et Q les points de tangence de ω avec $[AD]$ et $[BC]$. D'après le lemme appliqué au triangle XBC, la droite (XL) passe par le point de ω diamétralement opposé à Q, qu'on note Y. Dans le lemme, on peut intervertir les rôles du cercle inscrit et du cercle exinscrit (la preuve est exactement la même). Appliqué au triangle XAD, cela montre que (XK) passe par le point de ω diamétralement opposé à P. On note ce point Z : les points X, K, Y, Z et L sont alignés dans cet ordre. De plus, $PQZY$ est un rectangle donc (PQ) est parallèle à (KL). Comme $\widehat{KPQ} = \widehat{LQP}$, $PQLK$ est donc un trapèze isocèle donc $PK = QL$.

De plus, notons M et N les milieux de $[AD]$ et de $[BC]$: une rapide chasse aux tangentes montre que $BP = AK = \frac{AB+AX-BX}{2}$ et $CQ = DL = \frac{CD=CX-DX}{2}$ donc M et N sont aussi les milieux de $[PK]$ et $[QL]$. Or, on sait que PYZ est rectangle en Y donc PYK est rectangle en Y donc M est le centre du cercle circonscrit à PYK. En particulier, M est sur la médiatrice de $[PY]$ donc (OM) est la médiatrice de $[PY]$. De même, (ON) est la médiatrice de $[QZ]$. Comme $PQZY$ est un rectangle, ces médiatrices sont confondues, d'où le résultat.

2 jeudi 20 matin : Joseph Najnudel

Exercice 1 (IMO 1986) Soit $A_0A_1A_2$ un triangle et P_0 un point du plan. On construit une suite de points $(P_n)_{n\geq 1}$ de la manière suivante : pour tout $n \geq 1$, P_n est l'image de P_{n-1} par la rotation de centre A_m et d'angle $2\pi/3$, m étant le reste de $n-1$ modulo 3. Montrer que si $P_{1986} = P_0$ alors le triange $A_0A_1A_2$ est équilatéral.

Exercice 2 Soit $A_0B_0C_0$ un triangle et P un point à l'intérieur du triangle. Pour $j = 0, 1, 2$, on note A_{j+1} (resp. B_{j+1}, C_{j+1}) le projeté de P sur le côté $[B_j, C_j]$ (resp. $[A_j, C_j]$, $[A_j, B_j]$). Montrer que les triangles $A_0B_0C_0$ et $A_3B_3C_3$ sont semblables.

Exercice 3 Soit $ABCD$ un parallélogramme dont l'angle en A est aigu. Le cercle de diamètre $[AC]$ rencontre les droites (BC) et (CD) en E et F respectivement. La tangente au cercle en A coupe la droite (BD) en P. Montrer que les points P, F, E sont alignés.

Exercice 4 Soient A, B, C trois points sur un cercle Γ avec $AB = BC$. Les tangentes à Γ en A et B se coupent en D. Soit E l'intersection de (DC) et Γ. Montrer que (AE) coupe $[BD]$ en son milieu.

Exercice 5 Soit ABC un triangle dont les trois angles sont aigus. La hauteur du triangle issue de B (resp. C) rencontre le cercle de diamètre $[AC]$ (resp. $[AB]$) en P et Q (resp. R et S). Montrer que P, Q, R, S sont cocycliques.

Exercice 6 (USAMO 1998) Soient $\mathcal{C}_1$ et $\mathcal{C}_2$ deux cercles concentriques, $\mathcal{C}_2$ à l'intérieur de $\mathcal{C}_1$. Soit A un point de $\mathcal{C}_1$ et B un point de $\mathcal{C}_2$ tels que (AB) est tangente à $\mathcal{C}_2$. Soit C le second point d'intersection de (AB) avec $\mathcal{C}_1$, et soit D le milieu de $[AB]$. Une droite passant par A coupe $\mathcal{C}_2$ en E et F de sorte que les médiatrices de $[DE]$ et $[CF]$ se coupent en un point M de (AB). Déterminer le ratio AM/MC.

Exercice 7 (IMO 1995) Soient A, B, C, D quatre points d'une droite, dans cet ordre. Les cercles de diamètres $[AC]$ et $[BD]$ se coupent en X et Y. La droite (XY) coupe (BC) en Z. Soit P un point de (XY) autre que Z. La droite (CP) coupe le cercle de diamètre $[AC]$ en C et M, et la droite (BP) coupe le cercle de diamètre $[BD]$ en B et N. Prouver que les droites (AM), (DN), (XY) sont concourantes.

Exercice 8 (théorème de Thébault) Sur chaque côté d'un parallélogramme, on construit un carré. Montrer que les centres ces quatre carrés ainsi construits en forment un cinquième.

Exercice 9 (IMO shortlist 1997) Soit $ABCD$ un tétraèdre régulier, M un point du plan ABC et $N \neq M$ un point du plan ADC. Montrer que les longueurs des segments $[MN]$, $[BN]$, $[MD]$ sont celles des côtés d'un triangle.

Exercice 10 Soit ABC un triangle, D et E sur $[AB]$ et $[AC]$, tels que (DE) est parallèle à (BC). Soit P un point intérieur au triangle ADE, F et G les intersections respectives de (DE) avec (BP) et (CP). Soit Q le second point d'intersection des cercles circonscrits aux triangles PDG et PFE. Montrer que A, P, Q sont alignés.

INDICATIONS

Solution de l'exercice 1 Montrer que le produit des trois premières rotations est égal à l'identité. Ensuite, appliquer ce produit à un point bien choisi.

Solution de l'exercice 2 Considérer les six angles PXY où X et Y sont deux points distincts parmi A_j, B_j, C_j. Voir comment ces angles évoluent quand on passe de j à $j+1$.

Solution de l'exercice 3 Montrer que $PB/PD = AB\cos\beta/AD\cos\alpha$, $EC/FC = \cos\alpha/\cos\beta$, $BE/DF = BA/DA$, α et β étant les angles $\widehat{BCA}$ et $\widehat{DCA}$. Utiliser le théorème de Ménélaüs.

Solution de l'exercice 4 Montrer que le cercle circonscrit à ADE est tangent à (DB). Utiliser ensuite la puissance d'un point par rapport à un cercle.

Solution de l'exercice 5 Montrer que l'orthocentre du triangle a même puissance par rapport aux deux cercles et en déduire la cocyclicité cherchée.

Solution de l'exercice 6 En utilisant la puissance d'un point par rapport à un cercle, montrer que D, E, F, C sont cocycliques. Montrer que M est le centre du cercle correspondant.

Solution de l'exercice 7 Montrer que B, C, M, N sont cocycliques. En faisant une chasse aux angles, montrer que A, D, M, N sont également cocycliques, puis conclure.

Solution de l'exercice 8 Exprimer les vecteurs allant du centre O du parallélogramme vers les centres de deux des carrés en fonction de deux vecteurs bien choisis et de la rotation de centre O et d'angle $\pi/2$.

Solution de l'exercice 9 La quatrième dimension !

Solution de l'exercice 10 Introduire les secondes intersections des cercles avec (AB) et (AC). Faire une chasse aux angles, utiliser la puissance d'un point par rapport à un cercle et la cocyclicité.

3 jeudi 20 après-midi : Jean-Louis Tu

Exercice 1 Une tangente variable à un cercle donné de centre A coupe un second cercle donné, centré en B, en C et D. Montrer que le cercle (BCD) reste tangent à un cercle fixe.

Exercice 2 Deux cordes perpendiculaires $[BC]$ et $[DE]$ d'un cercle se coupent en A. Montrer que la hauteur de ABD issue de A est une médiane de ACE.

Exercice 3 On donne deux diamètres orthogonaux $[MM']$ et $[NN']$ de deux cercles orthogonaux. Montrer que parmi $(MN), (MN'), (M'N)$ et $(M'N')$, deux passent par l'un des points d'intersection des deux cercles et les autres par l'autre point d'intersection.

Exercice 4 Soient Ω et Ω' les centres des inversions i et i' envoyant un cercle sur un cercle de rayon différent. Montrer que $i(\Omega')$ est le pied de l'axe radical des deux cercles.

Exercice 5 Deux cercles C_1 et C_2 de rayons différents sont extérieurement tangents. La droite d_1 est l'une des tangentes communes extérieures, et coupe C_1 et C_2 en A et D respectivement. La droite d_2 est parallèle à d_1, tangente à C_1 et coupe C_2 en E et F. La droite d_3 contient D et recoupe d_2 et C_2 en B et C. Montrer que le cercle circonscrit à ABC est tangent à d_1.

Exercice 6 On considère deux cercles tangents intérieurement en A. Soit C un point du cercle intérieur. La droite (AC) recoupe le grand cercle en P. La tangente en C au petit cercle coupe l'autre cercle en D et E. Montrer que (PE) est tangent au cercle (ACE).

Exercice 7 On donne deux cercles (C) et (C') de centres O et O' se coupant en A et B. Un cercle variable Γ passant par A les recoupe respectivement en M et M'. (AM) recoupe (C') en N', (AM') recoupe (C) en N. Le cercle (ANN') recoupe Γ en P. Montrer que le lieu de P est le cercle centré au milieu de $[OO']$ et passant par A.

Exercice 8 Soit ABC un triangle isocèle en A et D, E des points des petits arcs AB et AC. Les droites (AD) et (BC) se coupent en F et la droite (AE) recoupe le cercle FDE en G. Montrer que (AC) est tangent au cercle circonscrit à ECG.

Exercice 9 On donne deux cercles ω_1 et ω_2. Montrer que si $A, B, C \in \omega_1$ et $D, E, F \in \omega_2$ sont tels que $(BC), (CA), (AB)$ sont respectivement tangents en D, E, F à ω_2, alors le centre de gravité de DEF ne dépend pas de A, B, C, D, E, F.

Exercice 10 Deux cercles C et D sont extérieurement tangents en P. On mène deux tangentes (AM) et (AN) à D à partir d'un point A de C. Les droites (AM) et (AN) recoupent C en E et F respectivement. Montrer que $\dfrac{PE}{PF} = \dfrac{ME}{NF}$.

Exercice 11 Soit O un point à l'intérieur d'un triangle ABC tel que $OA = OB + OC$. On suppose que B' et C' sont les milieux des arcs AOC et AOB. Montrer que les cercles COC' et BOB' sont tangents entre eux.

Exercice 12 Un cercle ω de centre O est tangent intérieurement à un cercle Γ en S. Une corde $[AB]$ de Γ est tangente en T à ω. Le point P est situé sur (AO). Montrer que $(PB) \perp (AB)$ si et seulement si $(PS) \perp (TS)$.

Exercice 13 Soit ω le cercle circonscrit à ABC, et P un point intérieur au triangle. Les droites $(AP), (BP), (CP)$ recoupent ω en A_1, B_1, C_1. Soient A_2, B_2, C_2 les symétriques de A_1, B_1, C_1 par rapport aux milieux de $[BC], [CA], [AB]$ respectivement. Montrer que le cercle circonscrit à $A_2B_2C_2$ passe par l'orthocentre.

<u>*Solution de l'exercice 1*</u> L'inversion (B, BC^2) transforme (BCD) en (CD) qui reste tangent au cercle (A).

<u>*Solution de l'exercice 2*</u> L'inversion i de pôle A qui fixe le cercle envoie la hauteur de ABD sur une droite perpendiculaire au cercle ACE, qui passe donc par le milieu de $[CE]$.

Solution de l'exercice 3 On inverse par rapport à l'un des points d'intersections A des deux cercles. Alors $(i(M)A)$ et $(i(M')A)$ rencontrent l'inverse du second cercle C_2 en N_1 et N_1' tels que $(i(N_1)i(N_1'))$ est le diamètre de C_2 orthogonal à $[MM']$.

Solution de l'exercice 4 Notons K le rapport des rayons, I le pied de l'axe radical, $I' = i(I)$ et $[BD]$ le diamètre du premier cercle situé sur $[\Omega\Omega']$. On a $IB.ID = IB'.ID'$ donc $(I'B'.I'D')/(I'B.I'D) = (\Omega B'.\Omega D')/(\Omega B.\Omega D) = K^2$. Or, Ω' (centre d'homothétie envoyant le premier cercle sur le deuxième) vérifie la même relation que I'.

Solution de l'exercice 5 Inverser par rapport à A. La figure est symétrique par rapport à $(E'F')$, donc $(B'C')$ est parallèle à d_1. (On peut aussi inverser par rapport à D, la figure se conserve.)

Solution de l'exercice 6 L'inversion de centre P qui conserve le petit cercle envoie le grand cercle sur (DE) donc E sur lui-même. Il vient $PA.PC = PE^2$.

Solution de l'exercice 7 L'inversion (A, AB) envoie la figure sur deux droites sécantes en B. Alors $(Bi(N), Bi(M'), BA, Bi(P))$ est harmonique, donc P décrit un cercle passant par A et B, dont la tangente t en B est le conjugué harmonique de (BA) par rapport aux tangentes en B à (C) et (C'). Donc $t^\perp$ est le conjugué harmonique de $(BA)^\perp$ par rapport à (BO) et (BO'). En projetant sur (OO'), $t^\perp \cap (OO')$ est le milieu de $[OO']$.

Solution de l'exercice 8 L'inversion (A, AB) envoie B sur B, C sur C, (ABC) sur (BC), D sur F donc E sur G, d'où $AG.AE = AC^2$.

Solution de l'exercice 9 L'inversion de cercle ω_2 transforme A, B, C en les milieux des côtés de DEF, donc ω_1 en le cercle d'Euler de DEF. Le centre de celui-ci est fixe, ainsi que le centre du cercle circonscrit à DEF, donc le centre de gravité aussi.

Solution de l'exercice 10 Inverser par rapport à A. On a $E'M' = E'P'$ et $F'N' = F'P'$ donc $\dfrac{P'E'}{P'F'} = \dfrac{M'E'}{N'F'}$ donc $\dfrac{PE}{AP.AE} \times \dfrac{AP.AF}{PF} = \dfrac{ME}{AM.AE} \times \dfrac{AN.AF}{NF}$.

Solution de l'exercice 11 Inversion par rapport à O. Il faut montrer que si $\frac{1}{OA} = \frac{1}{OB} + \frac{1}{OC}$ et si la bissectrice extérieure de $\widehat{AOB}$ (resp. $\widehat{AOC}$) coupe (AB) (resp. (AC)) en C' (resp. B') alors $(BB') \parallel (CC')$. On a $\frac{OA}{OB} = \frac{C'A}{C'B}$, $\frac{OA}{OC} = \frac{B'A}{B'C} \Longrightarrow 1 = \frac{C'A}{C'B} + \frac{B'A}{B'C} \Longrightarrow \frac{C'A}{C'B} = \frac{CA}{CB'}$.

Solution de l'exercice 12 On définit P comme l'intersection de (AO) avec (TSB), il faut montrer que $\widehat{TBP}$ est droit. On inverse par rapport à T, alors il faut montrer que $(TP') \perp (B'S')$.

$(A'S')$ recoupe $(A'O'T)$ en K, symétrique de P' par rapport à ω'. Soit $R = (O'P') \cap \omega'$. Alors $\angle O'A'K = \angle P'A'T = \angle TO'P'$. $\angle S'P'O' = \angle S'RO' - \angle RS'B' = 90° - \angle TO'P' - \angle S'A'T = 90° - \angle O'A'T = \angle A'O'T = \angle A'P'T$. Comme $\widehat{A'T'O'} = \widehat{A'P'O'} = 90°$, on a $\widehat{TP'S'} = 90°$.

Solution de l'exercice 13 On inverse par rapport à H. Il faut montrer que A_2', B_2', C_2' sont alignés. Comme $A_2' \in (B'C')$, etc. il suffit d'après Ménélaüs de voir que $\prod \dfrac{B'A_2'}{C'A_2'} = 1$ (les longueurs étant orientées), donc que $\prod \dfrac{BA_2}{CA_2} = 1$, i.e. que $\prod \dfrac{CA_1}{BA_1} = 1$. Ceci découle de Céva trigonométrique.

V. Vendredi 21 matin : Test de mi parcours

Contenu de cette partie

1 Groupe A

1 Enoncé

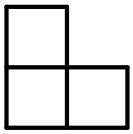
Exercice 1
Mathieu choisit un nombre entier n strictement supérieur à 7 et écrit les nombres de 1 à n au tableau. Le canard pouêt-pouët choisit deux entiers a et b écrits au tableau, puis remplace chacun des deux par $\frac{a+b}{2}$ et recommence cette opération. Est-il possible qu'il n'y ait plus que des 4 écrits au tableau ?

Exercice 2
Montrer que pour tous réels positifs a, b et c,

$$(a^2b + b^2c + c^2a)(ab^2 + bc^2 + ca^2) \geq 9a^2b^2c^2$$

Exercice 3

Soit n un entier naturel. On considère un damier de côté 2^n dont on a supprimé une case quelconque. Montrer qu'il est possible de le paver avec des pièces de la forme ci-dessous.



Exercice 4
Montrer que pour tout entier naturel n,

$$n! \leq \left(\frac{n+1}{2}\right)^n$$

2 Solution

Exercice 1

Attention à bien lire l'énoncé ! À chaque opération, a ET b sont remplacés par $\frac{a+b}{2}$ et le canard peut jouer autant de fois qu'il le souhaite. Si vous commencez une disjonction de cas, assurez-vous qu'elle est pertinente, rigoureuse et complète.

Montrons que la somme des nombres écrits au tableau est un invariant. À chaque étape, seuls deux nombres sont modifiés et leur somme reste constante puisque $\frac{a+b}{2} + \frac{a+b}{2} = a + b$, donc la somme totale est également conservée. Au départ la somme est $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$. S'il n'y avait que des nombres 4 écrits au tableau, leur somme serait $4n$. Or pour $n > 7$ on ne peut pas avoir $\frac{n(n+1)}{2} = 4n$, le canard pouêt-pouët ne peut donc pas atteindre son objectif maléfique.

Exercice 2

Première solution : On utilise l'inégalité arithmético-géométrique sur chaque parenthèse. On a

$$a^2b + b^2c + c^2a \geq 3\sqrt[3]{a^2b \times b^2c \times c^2a} = 3abc$$
$$ab^2 + bc^2 + ca^2 \geq 3\sqrt[3]{ab^2 \times bc^2 \times ca^2} = 3abc$$

et la multiplication de ces deux inégalités donne le résultat.

Deuxième solution : On peut également tout développer puis utiliser l'inégalité arithmético-géométrique de la façon suivante :

$$a^3b^3 + b^3c^3 + c^3a^3 + a^4bc + b^4ac + c^4ab \geq 6\sqrt[6]{a^3b^3 \times b^3c^3 \times c^3a^3 \times a^4bc \times b^4ac \times c^4ab} = 6a^2b^2c^2$$

Troisième solution : De façon équivalente, il est aussi possible de faire apparaître des carrés après développement. Ainsi, l'inégalité est équivalente à montrer que

$$(a^3b^3 - 2a^2b^2c^2 + c^4ab) + (b^3c^3 - 2a^2b^2c^2 + a^4bc) + (c^3a^3 - 2a^2b^2c^2 + b^4ac) \geq 0$$

ce qui se réécrit

$$(ab\sqrt{ab} - c^2\sqrt{ab})^2 + (bc\sqrt{bc} - a^2\sqrt{bc})^2 + (ca\sqrt{ca} - b^2\sqrt{ca})^2 \geq 0$$

Quatrième solution : Enfin, si on emploie l'inégalité de Cauchy-Schwartz, on obtient

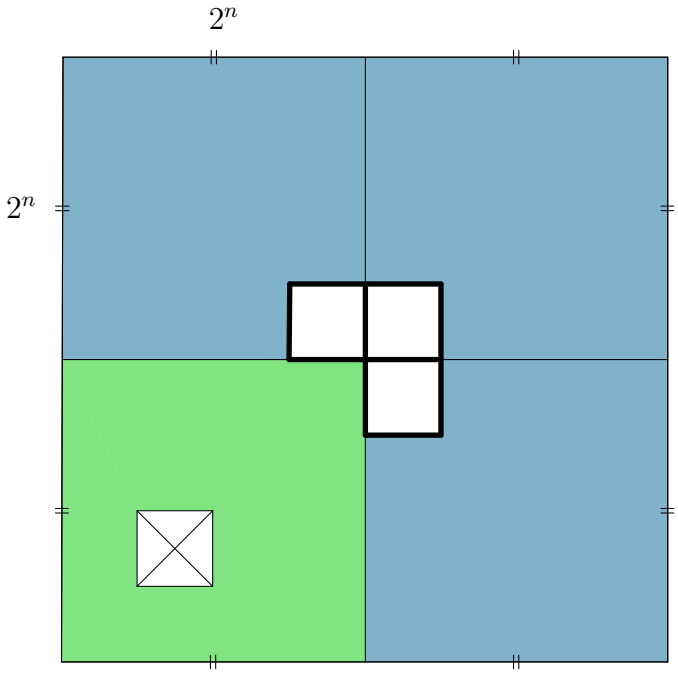
$$\begin{aligned}(a^2b+b^2c+c^2a)(ab^2+bc^2+ca^2) &= ((a\sqrt{b})^2+(b\sqrt{c})^2+(c\sqrt{a})^2)((\sqrt{b})^2+(a\sqrt{c})^2+(b\sqrt{a})^2) \\ &\geq (a\sqrt{b}c\sqrt{b}+b\sqrt{c}a\sqrt{c}+c\sqrt{a}b\sqrt{a})^2 = 9a^2b^2c^2\end{aligned}$$

Exercice 3

Faire des dessins c'est bien ! Cela permet de faire comprendre au correcteur que vous avez compris et de gagner considérablement en clarté dans votre raisonnement. Faites bien attention à la rédaction : n'écrivez pas "et ainsi de suite", ni "et on continue indéfiniment" ou "etc." mais faites une récurrence bien propre en deux parties. Souvenez-vous aussi qu'un coloriage permet de montrer qu'un pavage est impossible mais que ne pas avoir de contradiction avec le coloriage ne suffit pas à montrer que le pavage est possible. En effet, il faut encore prouver qu'on peut effectivement en construire un qui marche.

Montrons par récurrence que pour tout $n \in \mathbb{N}$ on peut paver avec des triminos un damier de côté 2^n auquel il manque une case.

- **Initialisation :** Pour $n = 1$ le pavage est évident car la case manquante est dans un coin du damier 2×2.
- **Hérédité :** Supposons qu'on puisse paver tout damier de côté 2^n auquel il manque une case. Considérons un damier de côté 2^{n+1} auquel il manque une case. On divise notre damier en quatre carrés de côté 2^n.



Le carré dans lequel il manque une case est pavable par hypothèse de récurrence (en vert). On place un trimino au centre du damier, de sorte qu'il recouvre un coin de chacun des trois autres carrés. Encore par hypothèse de récurrence, on peut paver ces trois carrés privés d'une case (en bleu). On a ainsi pavé l'intégralité de notre damier de taille 2^{n+1}.

Ainsi, un pavage est possible pour tout n et quelle que soit la case manquante.

Remarque : Cet exercice montre au passage que 3 divise $4^n - 1$ pour tout n lorsqu'on compte le nombre de cases du damier.

Exercice 4

Première solution : En utilisant l'inégalité arithmético-géométrique sur le membre de gauche, il s'ensuit directement que

$$n! = 1 \times 2 \times \cdots \times n \leq \left(\frac{1+2+\cdots+n}{n}\right)^n = \left(\frac{n+1}{2}\right)^n$$

Deuxième solution : On procède par récurrence sur l'entier n.

- **Initialisation :** Pour $n = 0$, on a bien $0! = \left(\frac{0+1}{2}\right)^0 = 1$.
- **Hérédité :** Supposons que

  $$n! \leq \left(\frac{n+1}{2}\right)^n$$

  pour un entier $n \geq 0$ et montrons que cette proposition est également vraie au rang $n+1$. En utilisant l'hypothèse de récurrence, il vient

  $$(n+1)! = n!(n+1) \leq 2\left(\frac{n+1}{2}\right)^{n+1}$$

  Il s'agit donc de montrer que

  $$2\left(\frac{n+1}{2}\right)^{n+1} \leq \left(\frac{n+2}{2}\right)^{n+1}$$

  soit

  $$\sqrt[n+1]{2}(n+1) \leq n+2$$

  ce qui est vrai d'après l'IAG en écrivant que $n+2 = \underbrace{1+\cdots+1}_{n}+2$.

Troisième solution : Si n est pair, l'inégalité arithmético-géométrique donne

$$\begin{aligned} 1 \times n &\leq \left(\frac{n+1}{2}\right)^2 \\ 2(n-1) &\leq \left(\frac{n+1}{2}\right)^2 \\ &\vdots \\ \frac{n}{2}\left(\frac{n}{2}+1\right) &\leq \left(\frac{n+1}{2}\right)^2 \end{aligned}$$

et en multipliant les $\frac{n}{2}$ inégalités précédentes, on obtient ce qu'il faut.

Si n est impair, on regroupe les termes comme suit :

$$\begin{aligned} 1 \times n &\leq \left(\frac{n+1}{2}\right)^2 \\ &\vdots \\ \frac{n-1}{2}\left(\frac{n+3}{2}\right) &\leq \left(\frac{n+1}{2}\right)^2 \end{aligned}$$

Le produit de ces $\frac{n-1}{2}$ inégalités fournit la conclusion attendue après multiplication par $\frac{n+1}{2}$.

2 Groupe B

1 Enoncé

Exercice 1
On considère l'ensemble des mots ne s'écrivant qu'avec les lettres x, y et t. De plus, on s'autorise à remplacer des groupes de lettres par d'autres selon les règles suivantes :

(i) $xy \longleftrightarrow yyx$

(ii) $xt \longleftrightarrow ttx$

(iii) $yt \longleftrightarrow ty$

En utilisant les opérations autorisées, peut-on passer :

a) du mot xy au mot xt ?

b) du mot $xytx$ au mot $txyt$?

c) du mot $xtxyy$ au mot $ttxyyyyx$?

Exercice 2
Soient x, y, z trois réels positifs tels que $x + y + z = 1$.

Montrer que

$$(1 - x)(1 - y)(1 - z) \geq 8xyz$$

.

Exercice 3
Soit n un entier naturel. Au stage de mathématiques de Valbonne, $2n + 1$ élèves se réunissent, chacun étant muni d'un pistolet à eau. On suppose que les distances entre les élèves sont deux à deux distinctes. A midi quarante-deux, chaque élève tire sur son plus proche voisin.

Montrer qu'il existe un élève qui ne sera pas mouillé.

Exercice 4
Soient a, b, c trois réels positifs tels que $a + b + c = 1$.

Montrer que

$$\frac{a^2}{\frac{b+c}{2} + \sqrt{bc}} + \frac{b^2}{\frac{c+a}{2} + \sqrt{ca}} + \frac{c^2}{\frac{a+b}{2} + \sqrt{ab}} \geq \frac{1}{2}$$

.

2 Solution

Solution de l'exercice 1

a) Le fait qu'il y ait un t dans un mot est un invariant pour les transformations possibles. Donc on ne peut pas passer de xy, qui ne contient pas de t, à xt, qui en contient un.

b) Le nombre de x dans un mot est un invariant, et $xytx$ en contient deux tandis que $txyt$ n'en contient qu'un. Donc on ne peut pas passer de $xytx$ à $txyt$.

c) On peut passer de $xtxyy$ à $ttxyyyyx$ de la façon suivante :

$$xtxyy \longleftrightarrow ttxyy \longleftrightarrow ttxyy \longleftrightarrow ttxyyyx \longleftrightarrow ttxyyxy \longleftrightarrow ttxyyyyx$$

Solution de l'exercice 2

On utilise la relation donnée pour réécrire $(1-x)(1-y)(1-z) = (y+z)(z+x)(x+y)$, puis on applique l'inégalité arithmético-géométrique : $x+y \geq 2\sqrt{xy}$, et de même $y+z \geq 2\sqrt{yz}$ et $z+x \geq 2\sqrt{zx}$.

En multipliant tous ces termes, il vient $(y+z)(z+x)(x+y) \geq 8\sqrt{x^2y^2z^2}$, d'où :

$$(1-x)(1-y)(1-z) \geq 8xyz$$

Une autre possibilité est de développer :

$$\begin{aligned}(1-x)(1-y)(1-z) \geq 8xyz &\iff 1-x-y-z+xy+yz+zx-xyz \geq 8xyz \\ &\iff xy+yz+zx \geq 9xyz \\ &\iff 1 \geq \frac{9}{\frac{1}{x}+\frac{1}{y}+\frac{1}{z}} \\ &\iff \frac{x+y+z}{3} \geq \frac{3}{\frac{1}{x}+\frac{1}{y}+\frac{1}{z}},\end{aligned}$$

ce qui est toujours vrai, puisqu'il s'agit de l'inégalité arithmético-harmonique.

Solution de l'exercice 3

On va procéder par récurrence sur n. L'initialisation, pour $n = 0$, ne pose pas de problème. Soit $n \in \mathbb{N}$ tel que, pour $2n+1$ élèves jouant entre-eux, on soit sûr qu'un élève n'est pas mouillé. On considère un groupe de $2n+3$ élèves.

On voudrait, pour se ramener à l'hypothèse de récurrence, pouvoir isoler deux élèves qui n'influent pas sur les autres, et appliquer ce qu'on sait aux $2n+1$ élèves restant. Pour cela, il faudrait que ces deux élèves se tirent mutuellement dessus : c'est par exemple le cas si on prend les deux élèves séparés par la distance minimale.

Or, si quelqu'un tire sur l'un de ces deux élèves, comme il y a autant de tirs que d'élèves et qu'on tire deux fois sur le même élève, il existe un élève qui restera sec.

Sinon, ces deux élèves agissent indépendamment du reste du groupe : on peut les oublier, et appliquer l'hypothèse de récurrence aux $2n+1$ élèves restant. Il existe donc, dans ce cas aussi, un élève qui restera sec.

Par principe de récurrence, la propriété est bien démontrée pour tout $n \in \mathbb{N}$.

Solution de l'exercice 4

Tout d'abord, on utilise l'inégalité arithmético-géométrique sur chaque terme pour simplifier le dénominateur excessivement douteux de nos fractions :

$$\frac{a^2}{\frac{b+c}{2}+\sqrt{bc}} + \frac{b^2}{\frac{c+a}{2}+\sqrt{ca}} + \frac{c^2}{\frac{a+b}{2}+\sqrt{ab}} \geq \frac{a^2}{b+c} + \frac{b^2}{c+a} + \frac{c^2}{a+b}$$

Reste à montrer que $2\left(\frac{a^2}{b+c}+\frac{b^2}{c+a}+\frac{c^2}{a+b}\right) \geq 1$.

Pour simplifier les carrés, on applique l'inégalité de Cauchy-Schwarz :

$$\begin{aligned} 2\left(\frac{a^2}{b+c}+\frac{b^2}{c+a}+\frac{c^2}{a+b}\right) &= (b+c+c+a+a+b)\left(\frac{a^2}{b+c}+\frac{b^2}{c+a}+\frac{c^2}{a+b}\right) \\ &\geq \sqrt{a^2}+\sqrt{b^2}+\sqrt{c^2} \\ &= 1, \end{aligned}$$

ce qui conclut.

3 Groupe C

1 Enoncé

Exercice 1
Soit $ABCDEF$ un hexagone convexe dont tous les sommets sont sur un cercle Γ. On suppose que les droites (AD), (BE) et (CF) sont concourantes. Montrer que :

$$AB \cdot CD \cdot EF = BC \cdot DE \cdot FA$$

Exercice 2
Soit P un polynôme à coefficients entiers. On suppose qu'il existe quatre entiers a, b, c et d deux à deux distincts tels que $P(a) = P(b) = P(c) = P(d) = 2015$.

Montrer qu'il n'existe pas d'entier x tel que $P(x) = 2018$.

Exercice 3
Trouver tous les polynômes à coefficients entiers P tels que pour tous entiers a et b on ait :

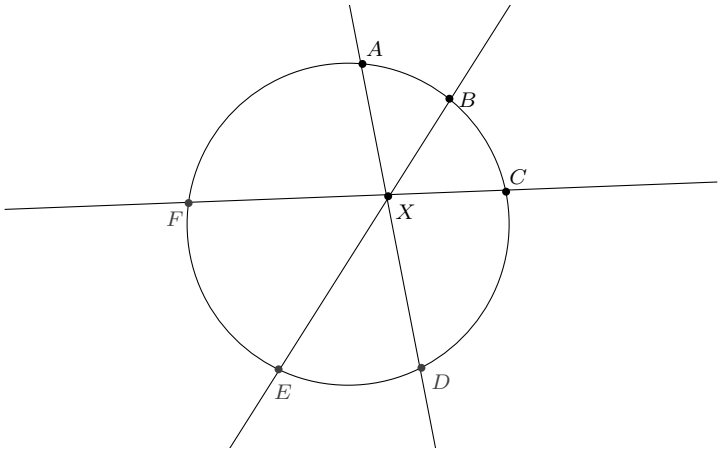
$$a + 2b \mid P(a) + 2P(b)$$

Exercice 4
Soit $ABCDE$ un pentagone convexe tel que $\widehat{BAC} = \widehat{CAD} = \widehat{DAE}$ et $\widehat{ABC} = \widehat{ACD} = \widehat{ADE}$. On note P l'intersection de (BD) et (CE).

Montrer que la droite (AP) recoupe le segment $[CD]$ en son milieu.

2 Solution

Solution de l'exercice 1



On applique le théorème de Ceva trigonométrique dans le triangle ACE aux droites (AD), (CF) et (EB) :

$$\frac{\sin \widehat{EAD}}{\sin \widehat{CAD}} \cdot \frac{\sin \widehat{ACF}}{\sin \widehat{ECF}} \cdot \frac{\sin \widehat{CEB}}{\sin \widehat{AEB}} = 1$$

De plus, si on note R le rayon de Γ : on sait que $\sin widehatEAD = \frac{DE}{2R}$ et de même pour les autres angles. Les $2R$ se simplifient et on obtient :

$$\frac{DE}{CD} \cdot \frac{FA}{EF} \cdot \frac{BC}{AB} = 1$$

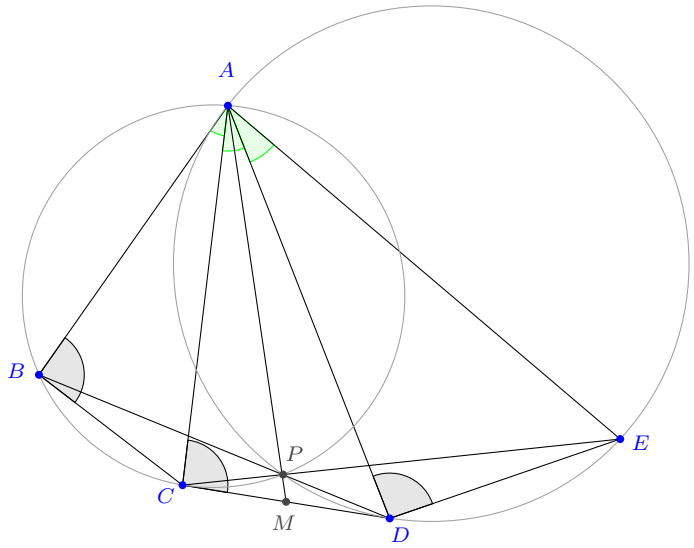
<u>*Solution de l'exercice 2*</u> Soit $Q = P - 2015$: a, b, c et d sont des racines de Q donc il existe un polynôme R tel que $Q(X) = (X-a)(X-b)(X-c)(X-d)R(x)$. Si il existe x tel que $P(x) = 2012$, alors $Q(x) = -3$, soit $(x-a)(x-b)(x-c)(x-d)R(x) = -3$. Cependant, $x-a$, $x-b$, $x-c$ et $x-d$ sont quatre entiers deux à deux distincts qui doivent être non nuls. Il y en a donc au plus deux qui valent 1 ou -1. On peut donc supposer $|x-a| > 1$ et $|x-b| > 1$, donc $|x-a| \geq 2$ et $|x-b| \geq 2$, donc $|(x-a)(x-b)| \geq 4$ donc $|Q(x)| \geq 4$ car il est non nul, ce qui est absurde.

<u>*Solution de l'exercice 3*</u> En prenant $a = b = 0$ on obtient $0|3P(0)$ donc $P(0) = 0$.

Pour tous a et b, on a d'une part $a + 2b|P(a) + 2P(b)$ et d'autre part $a + 2b|P(a) - P(-2b)$ car $a - (-2b) = a + 2b$. On a donc, en faisant la différence, $a + 2b|2P(b) + P(-2b)$ et ce pour tout a. Pour tout b, $2P(b) + P(-2b)$ a donc une infinité de diviseurs donc $2P(b) + P(-2b) = 0$.

Notons maintenant n le degré de P et a_n son coefficient dominant : l'équation précédente donne $2a_n + (-2)^n a_n = 0$ d'où, comme $a_n \neq 0$, $2 + (-2)^n = 0$ et $n = 1$. Comme $P(0) = 0$, P doit être linéaire.

Réciproquement, il est facile de vérifier que les fonctions linéaires conviennent.



Solution de l'exercice 4 On se rend immédiatement compte qu'il existe une similitude de centre A qui envoie B sur C, C sur D puis D sur E.

Donc, d'après le théorème 37 appliqué au couple de point $(B, D) \mapsto (C, E)$, A est sur le cercle circonscrit Γ_1 à PBC et Γ_2 à PDE. Ici, l'exercice commence à avoir bien la tête d'un exercice utilisant la puissance d'un point. On essaye donc de montrer que Γ_1 est tangent à (CD). Or c'est vrai d'après la récriproque du théorème de l'angle inscrit comme $\widehat{ABC} = \widehat{DCA}$. De même, comme $\widehat{DEA} = 180° - \widehat{EAD} - \widehat{EDA} = 180° - \widehat{CAD} - \widehat{ACD} = \widehat{CDA}$, Γ_2 est également tangent à (CD).

Finalement, en notant $M = (AP) \cap (CD)$, M est sur l'axe radical de Γ_1 et Γ_2 et on peut donc écrire $MC^2 = \mathcal{P}_{\Gamma_1}(M) = \mathcal{P}_{\Gamma_2}(M) = MD^2$ et la conclusion.

4 Groupe D

1 Enoncé

Exercice 1
Soit $ABCD$ un quadrilatère dont les angles en B et D sont droits, et tel que $AB = AD$. Soient F et E deux points de $[BC]$ et $[CD]$ respectivement tels que $(DF) \perp (AE)$. Prouver que $(AF) \perp (BE)$.

Exercice 2
Trouver tous les entiers $x, y, z \geq 0$ tels que $5^x 7^y + 4 = 3^z$.

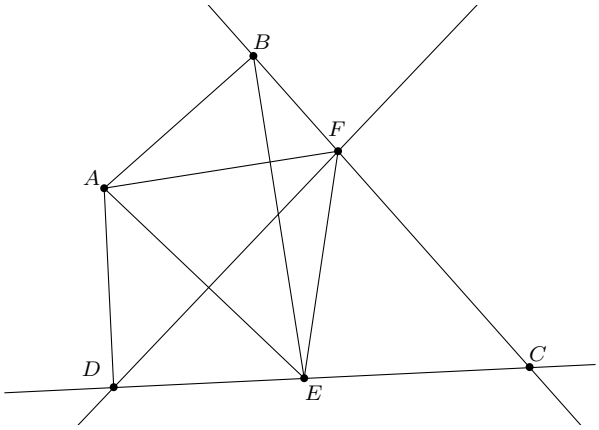
Exercice 3
Soit ABC un triangle, O le centre du cercle circonscrit, I le centre du cercle inscrit, I_a, I_b, I_c les centres des cercles exinscrits, S le symétrique de l'orthocentre par rapport à O. Soient D, E, F les points de contact des cercles exinscrits avec $(BC), (CA), (AB)$. On sait que $(AD), (BE), (CF)$ sont concourantes en un point appelé le point de Nagel N.

Montrer que $I_aI_bI_c$ et SIN ont les mêmes centres de gravité.

Exercice 4
Soit a_0, a_1, a_2, ... la suite définie par : $a_0 = 2, \quad a_{k+1} = 2a_k^2 - 1 \quad$ pour $k \geqslant 0$. Montrer que si un nombre premier impair p divise a_n, alors 2^{n+3} divise $p^2 - 1$.

2 Solution

Solution de l'exercice 1



Il suffit de prouver que $AE^2 + BF^2 = AB^2 + FE^2$.

Comme $(AE) \perp (DF)$, on a $AD^2 + EF^2 = AF^2 + DE^2$, donc $AB^2 + EF^2 = AF^2 + DE^2$. On est ainsi ramenés à montrer que $AF^2 + DE^2 = AE^2 + BF^2$, ou encore

$$(AB^2 + BF^2) + DE^2 = (AD^2 + DE^2) + BF^2,$$

ce qui est vrai puisque $AB = AD$.

Solution de l'exercice 2 Il est clair que $(x, y) \neq (0, 0)$ et que $z \geq 1$. Tout d'abord $(x, y, z) = (1, 0, 2)$ est bien solution.

Si $y = 0$ (et $x \geq 1$), en regardant l'équation modulo 5, on trouve $z \equiv 2 \mod 4$. Si $y \geq 1$, en regardant modulo 7, on trouve que $z \equiv 4 \mod 6$. Dans tous les cas, z est pair. On écrit donc $z = 2n$.

Alors $5^x 7^y = (3^n - 2)(3^n + 2)$. Comme $3^n - 2$ et $3^n + 2$ sont premiers entre eux, deux cas de figure se présentent :

Cas 1 : $3^n - 2 = 5^x$ *et* $3^n + 2 = 7^y$. En regardant modulo 3 la deuxième équation, on voit qu'il n'y a pas de solutions.

Cas 2 : $3^n - 2 = 7^y$ *et* $3^n + 2 = 5^x$. Alors $4 = 5^x - 7^y$. Supposons par l'absurde que $x, y \geq 1$. En regardant modulo 7, on voit $x \equiv 2 \mod 6$ et donc que x est pair. En regardant modulo 5, on voit que $y \equiv 0 \mod 4$ et donc que y est pair. En écrivant $x = 2x'$ et $y = 2y'$, on a donc $4 = (5^{x'} - 7^{y'})(5^{x'} + 7^{y'})$, ce qui ne donne pas des solutions. On a donc $x = 0$ ou $y = 0$, et on retrouve la seule solution $(x, y, z) = (1, 0, 2)$.

Solution de l'exercice 3 Rappels :

1) Dans un triangle, on a $\overrightarrow{OH} = 3\overrightarrow{OG} = 2\overrightarrow{O\omega}$ où ω est le centre du cercle d'Euler.

2) ABC est le triangle orthique de $I_aI_bI_c$, I est l'orthocentre de $I_aI_bI_c$, et O est le centre du cercle d'Euler de $I_aI_bI_c$.

3) On a $\overrightarrow{GN} = -2\overrightarrow{GI}$ (voir poly de Dehornoy, exercice 25).

De (1) appliqué à $I_aI_bI_c$ et (2), il vient $3G_I = 4O - I$.

De (3), il vient $2I + N = 3G$, donc d'après (1) on a $2I + N = 2O + H$. Il vient $S + I + N = 2O - H + I + N = 2O - H + I + 2O + H - 2I = 4O - I$. Finalement, $G_I = \dfrac{S + I + N}{3}$.

Solution de l'exercice 4

Notons $f(x) = (e^x + e^{-x})/2$ la fonction cosinus hyperbolique. On a $f(2x) = 2f(x)^2 - 1$. Prenons en particulier $x = \ln(2 + \sqrt{3})$, alors $f(x) = 2$, donc par récurrence on en déduit $a_n = f(2^n x)$ pour tout n. Ceci donne

$$a_n = \frac{(2 + \sqrt{3})^{2^n} + (2 - \sqrt{3})^{2^n}}{2}$$

(formule que l'on aurait pu démontrer par récurrence sans passer par les cosinus hyperboliques).

Cette formule a un sens dans le corps $K = \mathbb{F}_{p^2}$ (l'unique corps ayant p^2 éléments ; ce corps contient $\mathbb{Z}/p\mathbb{Z}$, et tout élément de $\mathbb{Z}/p\mathbb{Z}$ admet une racine carrée dans K).

Supposons $p \mid a_n$. On remarque déjà que 2 est un résidu quadratique modulo p car $2 = (2a_{n-1})^2$ modulo p. De plus, $(2 + \sqrt{3})^{2^n} + (2 - \sqrt{3})^{2^n} = 0$. Comme $\frac{2+\sqrt{3}}{2-\sqrt{3}} = (2 + \sqrt{3})^2$, on obtient $(2 + \sqrt{3})^{2^{n+1}} = -1$. Or, $2 + \sqrt{3} = \frac{(1+\sqrt{3})^2}{2}$; comme 2 est un résidu quadratique modulo p, il existe a tel que $a^2 = 2 + \sqrt{3}$. Par conséquent, $a^{2^{n+2}} = -1$. On en déduit que $a^{2^{n+3}} = 1$, donc que l'ordre de a est de la forme 2^k où $k \leqslant n + 3$. D'autre part, 2^k ne divise par 2^{n+2} car $a^{2^{n+2}} = -1$, donc $k = n + 3$.

D'autre part, tout élément b non nul de K vérifie $b^{p^2-1} = 1$, donc $2^{n+3} \mid p^2 - 1$.

VI. Troisième période

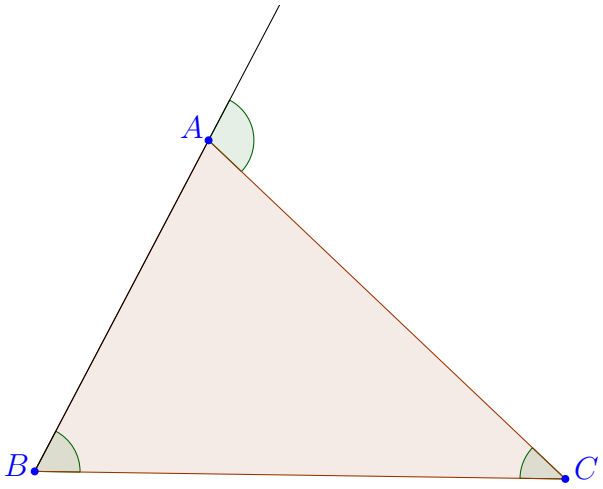
Contenu de cette partie

1 Groupe A : géométrie

1 samedi 22 matin : François Lo Jacomo

Les angles du triangle

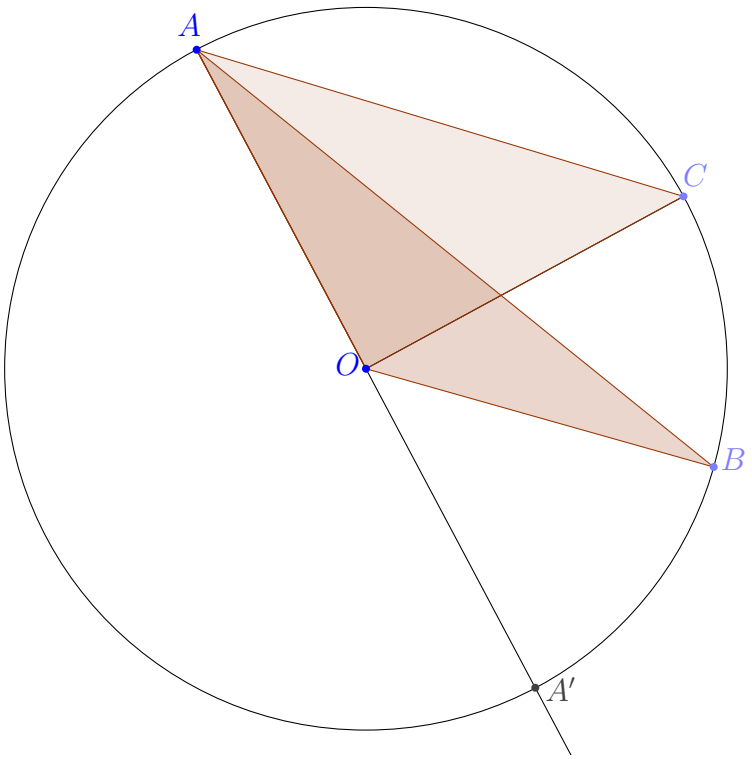
Les deux premiers résultats que l'on rappelle, c'est qu'un triangle ayant deux côtés égaux a deux angles égaux et réciproquement (triangle isocèle), et que la somme des trois angles du triangle est égale à $180°$. Ce dernier résultat s'utilise notamment sous la forme suivante (voir figure) : l'angle extérieur au triangle est la somme des angles à la base. En un sommet du triangle, j'appelle angle extérieur l'angle formé par un des côtés et le prolongement de l'autre.



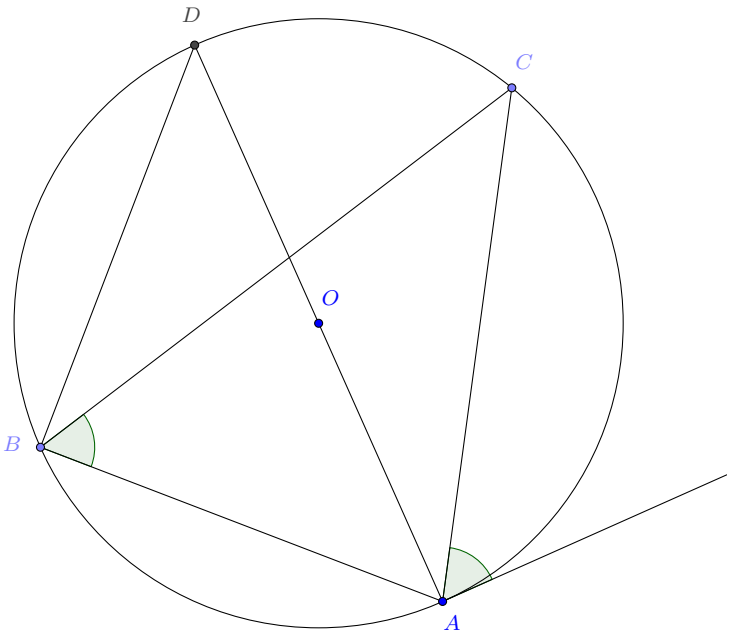
Angles inscrits

Si B et C sont deux points fixes d'un cercle, et qu'on fait varier un troisième point A sur ce même cercle, l'angle inscrit $\widehat{BAC}$ ne dépend pas de la position du point A.

Il existe plusieurs manières d'énoncer ce théorème : si quatre points A, B, C, D sont sur un même cercle, les angles $\widehat{BAC}$ et $\widehat{BDC}$ sont égaux si A et D sont du même côté de la droite (BC), supplémentaires s'ils sont de part et d'autre de (BC). Réciproquement, quatre points quelconques du plan, A, B, C, D vérifiant : $\widehat{BAC} = \widehat{BDC}$ si A et D du même côté de (BC) ou $\widehat{BAC} + \widehat{BDC} = 180°$ si A et D sont de part et d'autre de (BC) sont "cocycliques", c'est-à-dire sur un même cercle. La démonstration doit envisager tous les cas de figure, mais l'idée essentielle est que si A et B sont sur un cercle de centre O, le triangle AOB est isocèle. Si la droite (AO) recoupe le cercle en A', comme la somme des trois angles du triangle AOB est égale à $180°$, $\widehat{BOA'} = \widehat{BAO} + \widehat{ABO} = 2.\widehat{BAO}$, d'où l'on déduit que l'angle au centre $\widehat{BOC}$, qui ne dépend pas de A, est le double de l'angle inscrit $\widehat{BAC}$.



Une des manières d'énoncer ce théorème est de dire qu'un angle inscrit est égal à la moitié de l'arc qu'il intercepte. Ceci vaut par exemple pour un angle droit : $\widehat{ABC}$ est un angle droit si et seulement si AC est un diamètre du cercle circonscrit à ABC. Ceci vaut également pour l'angle formé par la tangente au cercle et une corde : l'angle entre la tangente en A et la corde AC, sur la figure ci-dessous, intercepte le même arc $\widehat{AC}$ que l'angle $\widehat{ABC}$, donc ces deux angles sont égaux. En effet, traçons le diamètre AD. Les angles inscrits $\widehat{DAC}$ et $\widehat{DBC}$ sont égaux, et comme AD est un diamètre, l'angle $\widehat{DBA}$ est droit, tout comme l'angle que fait le diamètre AD avec la tangente en A.



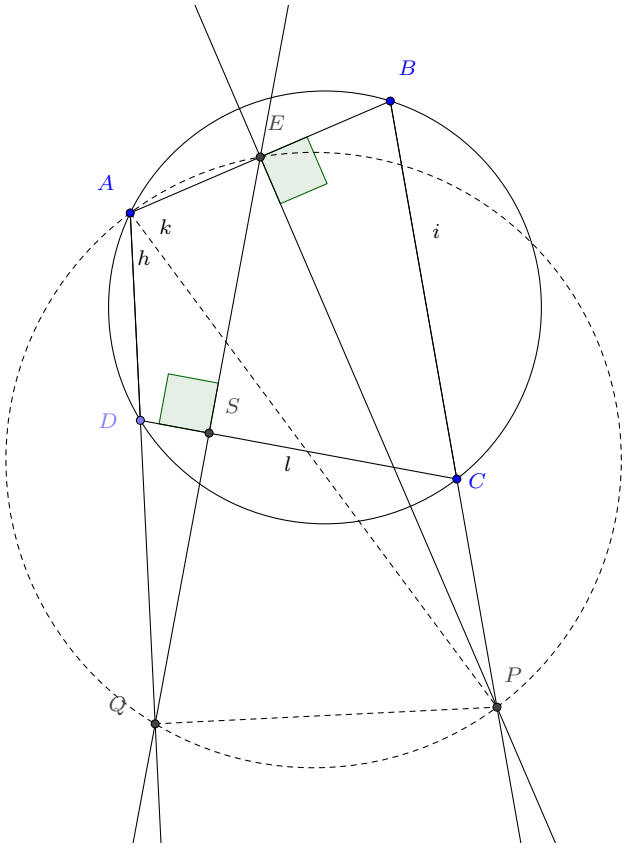
La technique de "chasse aux angles" consiste à utiliser ce théorème de l'angle inscrit dans les deux sens, prouver à l'aide d'égalités d'angles que des points sont sur un même cercle, et prouver à l'aide de cercles que des angles sont égaux. A partir d'un angle donné on cherche à exprimer le plus possible d'angles de la figure.

Exercice 1

Soit $ABCD$ un quadrilatère convexe inscriptible. On supposera que l'angle $\widehat{ABC}$ est aigu. Soit E le milieu de $[AB]$. La perpendiculaire à (AB) passant par E coupe (BC) en P. La perpendiculaire à (CD) passant par E coupe (AD) en Q. Montrer que (PQ) est perpendiculaire à (AD).

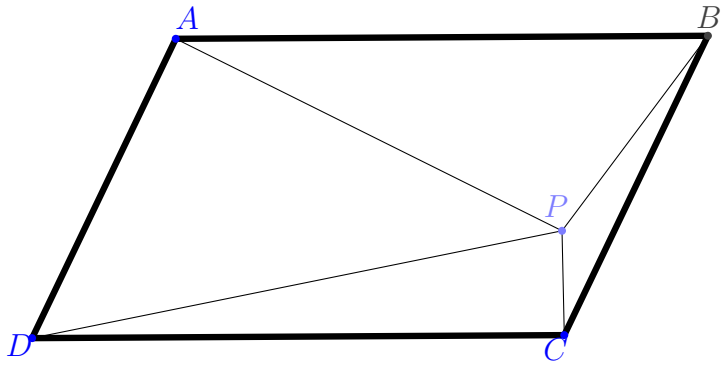
Solution de l'exercice 1

Posons $\alpha = \widehat{BPE}$. Comme $\widehat{PEB}$ est droit, $\widehat{EBP} = 90° - \alpha$. Or $\widehat{EBP} = \widehat{ABC}$ est supplémentaire de $\widehat{CDA}$ d'après le théorème de l'angle inscrit, donc $\widehat{CDA} = 90° + \alpha$, et si l'on nomme S l'intersection de (CD) et (AQ), $\widehat{SDQ} = 90° - \alpha$. Comme par hypothèse $\widehat{QSD} = 90°$, $\widehat{DQS} = \widehat{AQE} = \alpha$. Pour avoir des points cocycliques, il faudrait par exemple que $\widehat{APE} = \alpha$, mais c'est le cas, car P est sur la médiatrice de $[AB]$, donc le triangle APB est isocèle, et (AE) est la bissectrice de $\widehat{APB}$. Dès lors, $\widehat{APE} = \widehat{BPE} = \alpha$, les quatre points A, E, P, Q sont cocycliques, donc les deux angles $\widehat{AEP}$ et $\widehat{AQP}$ sont supplémentaires ; Comme $\widehat{AEP}$ est droit par hypothèse, $\widehat{AQP}$ est lui aussi droit, ce qui signifie que (PQ) est orthogonal à (AD).



Exercice 2

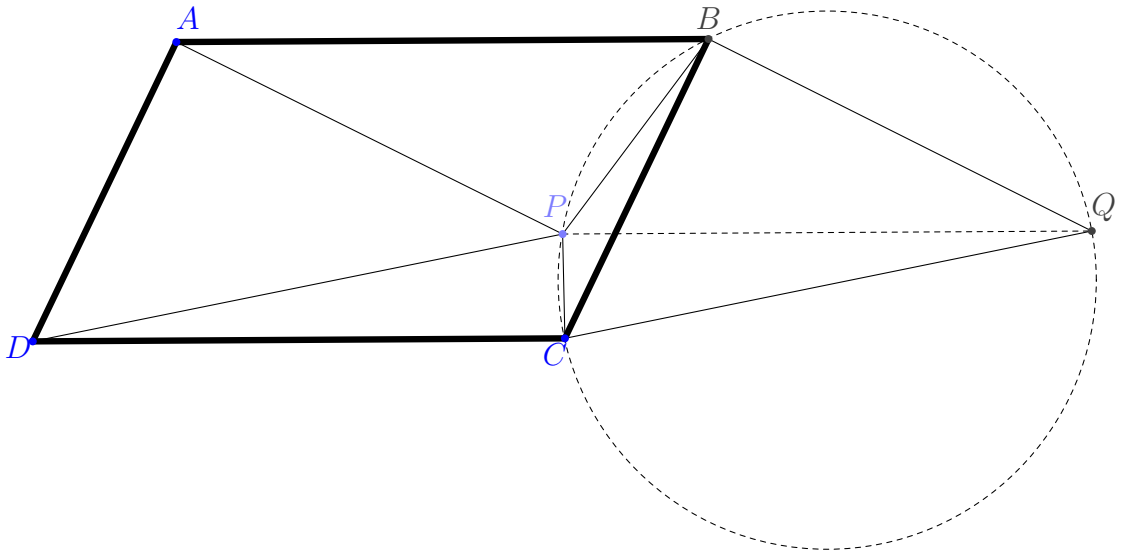
Soit $ABCD$ un parallélogramme, P un point intérieur au parallélogramme vérifiant : $\widehat{APD} + \widehat{CPB} = 180°$. Montrer que $\widehat{PBA} = \widehat{PDA}$.



Solution de l'exercice 2

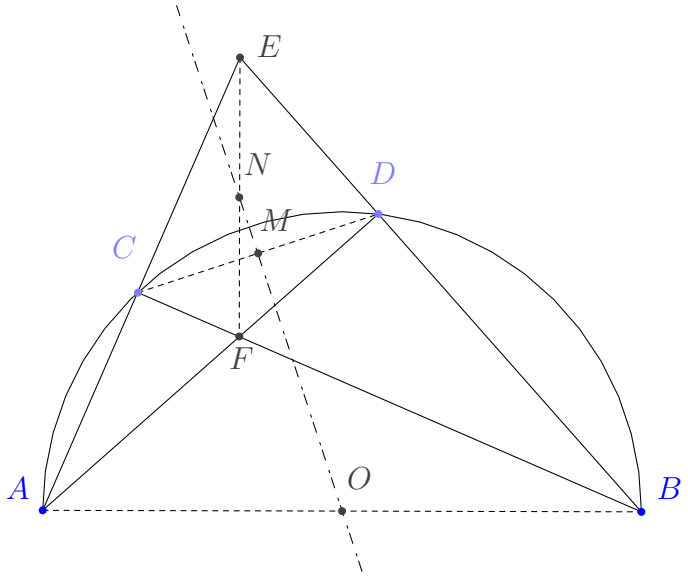
Nous avons deux angles supplémentaires, ce qui fait penser au théorème de l'angle inscrit si ce n'est qu'ils ne sont pas bien positionnés : il faudrait qu'ils soient tous deux de même base BC et de part et d'autre de (BC). Translatons le triangle APD vers la droite de la figure, c'est-à-dire introduisons un point Q tel que AB, PQ, DC soient tous trois parallèles et de même longueur. Les triangles APD et BQC sont isométriques, leurs côtés et leurs angles sont

égaux. En particulier, l'angle $\widehat{BQC}$ égal à $\widehat{APD}$ est supplémentaire de $\widehat{CPB}$. Là nous avons deux angles supplémentaires et positionnés de sorte que l'on peut affirmer : les quatre points B, Q, C, P sont cocycliques. Mais comme ces points sont cocycliques, d'autres angles inscrits apparaissent, notamment : $\widehat{QCB} = \widehat{QPB}$. Or $\widehat{QCB} = \widehat{PDA}$ car les triangles QCB et CDA sont isométriques, et $\widehat{QPB} = \widehat{PBA}$ car ils sont alternes - internes, ce qui achève la démonstration.



Exercice 3

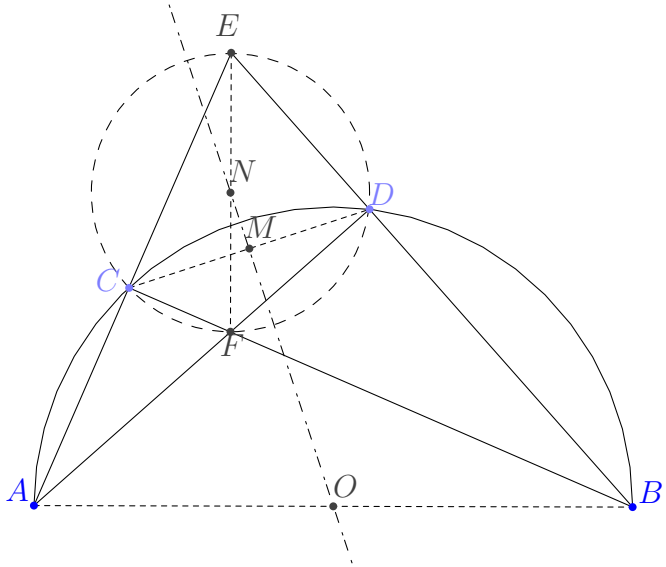
Soient C et D deux points distincts d'un demi-cercle de diamètre $[AB]$. Les droites (AC) et (BD) se coupent en F, les droites (AD) et (BC) se coupent en F. Montrer que les milieux des segments $[AB]$, $[CD]$ et $[EF]$ sont alignés.



Solution de l'exercice 3

L'hypothèse "C et D sur le cercle de diamètre $[AB]$" se traduit par : $\widehat{ACB} = 90°$ et $\widehat{ADB} = 90°$. Mais cela entraine manifestement : $\widehat{FCE} = 90°$ et $\widehat{FDE} = 90°$, donc (C) et (D) sont

également sur le cercle de diamètre $[EF]$. Le milieu N de $[EF]$ est le centre de ce cercle, donc $NC = ND$, ce qui entraine que N est sur la médiatrice de $[CD]$. Or, pour la même raison, le milieu O de $[AB]$ est lui aussi sur la médiatrice de $[CD]$. Et par définition, cette même médiatrice passe par le milieu M de $[CD]$.

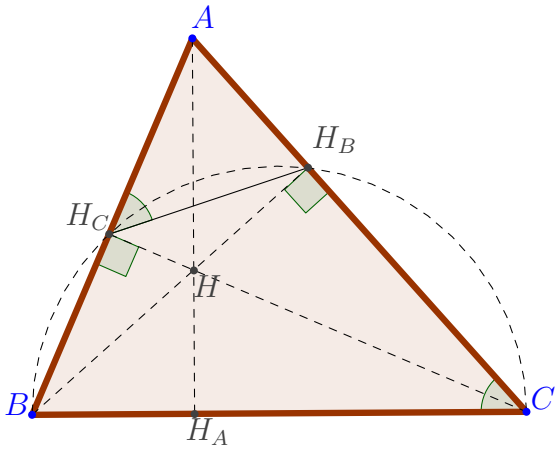


Points remarquables du triangle

Vous avez vu en classe que les médiatrices d'un triangle ABC se coupent en un point équidistant des trois sommets : c'est le centre du cercle circonscrit, traditionnellement appelé O. Les bissectrices se coupent en un point équidistant des trois côtés : c'est le centre I du cercle inscrit. Les médianes se coupent en un point G appelé centre de gravité du triangle ou isobarycentre. Les hauteurs se coupent en un point H, appelé orthocentre. Intéressons-nous pour commencer à ce point H.

Exercice 4

Soit H l'orthocentre d'un triangle ABC, et H_A, H_B, H_C les pieds des hauteurs issues de A, B, C. On supposera pour simplifier que H est à l'intérieur du triangle ABC, ce qui revient à dire que tous les angles du triangle sont aigus (un tel triangle est dit acutangle). Déterminer les angles des triangles AH_BH_C, H_ABH_C, H_AH_BC et $H_AH_BH_C$, en fonction des angles du triangle ABC, que l'on notera $\widehat{A}$, $\widehat{B}$ et $\widehat{C}$

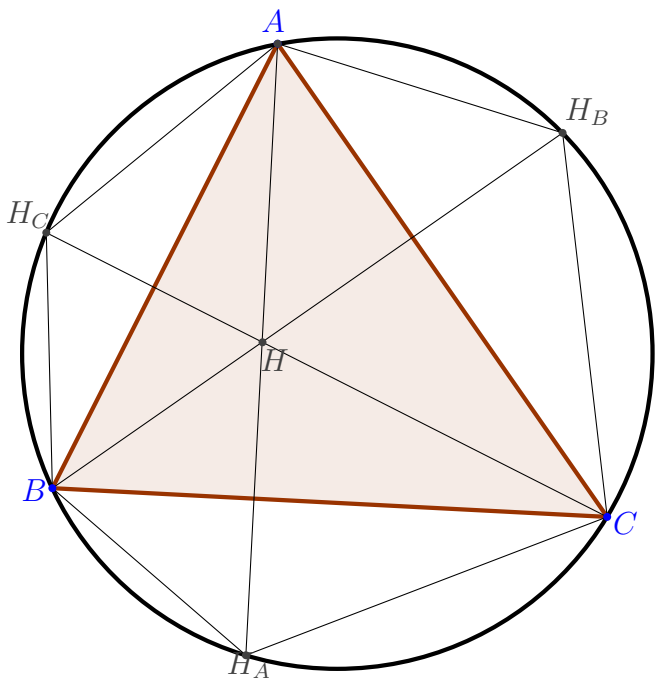


Solution de l'exercice 4

Etant donnés les angles droits $\widehat{BH_BC}$ et $\widehat{BH_CC}$, H_B et H_C sont sur le cercle de diamètre $[BC]$, d'où les angles inscrits $\widehat{BH_CH_B}$ et $\widehat{BCH_B}$ sont supplémentaires, puisque C et H_C sont de part et d'autre de (BH_B), d'où $\widehat{AH_CH_B} = \widehat{C}$. De même, $\widehat{AH_BH_C} = \widehat{B}$, puis $\widehat{BH_CH_A} = \widehat{C}$, $\widehat{BH_AH_C} = \widehat{A} = \widehat{CH_AH_B}$ et $\widehat{CH_BH_A} = \widehat{B}$. Donc d'une part $\widehat{H_AH_BH_C} = 180° - 2\widehat{B}$, $\widehat{H_BH_CH_A} = 180° - 2\widehat{C}$, $\widehat{H_CH_AH_B} = 180° - 2\widehat{A}$, d'autre part les hauteurs du triangle ABC sont les bissectrices du triangle $H_AH_BH_C$, et l'orthocentre de ABC est centre du cercle inscrit dans $H_AH_BH_C$.

Exercice 5

Soit ABC un triangle d'orthocentre H. On supposera pour simplifier que H est intérieur au triangle (triangle acutangle). Montrer que les symétriques de H par rapport aux côtés (AB), (BC) et (CA) du triangle sont sur le cercle circonscrit à ABC.



Solution de l'exercice 5

Il suffit d'étudier les angles de la figure : en appelant, cette fois, H_A, H_B et H_C les symétriques de H par rapport aux côtés du triangle, H'_A, H'_B et H'_C les pieds des hauteurs, milieux de HH_A, HH_B et HH_C : dans le triangle rectangle BH'_BC, $\widehat{H'_BBC} = 90° - \widehat{C}$. De même, $\widehat{H'_CCB} = 90° - \widehat{B}$. Donc le troisième angle du triangle BHC : $\widehat{BHC} = \widehat{B} + \widehat{C} = 180° - \widehat{A}$. $\widehat{BAC}$ et $\widehat{BHC}$ sont supplémentaires, mais H et A ne sont pas de part et d'autre de (BC), donc A, B, C et H ne sont pas cocycliques. En revanche, si H_A est le symétrique de H par rapport à (BC), les triangles BHC et BH_AC ont les mêmes angles, donc $\widehat{BH_AC}$ et $\widehat{BAC}$ sont encore supplémentaires, mais cette fois-ci A et H_A sont situés de part et d'autre de (BC), donc les quatre points A, H_A, B et C sont cocycliques. De même pour H_B et H_C.

2 samedi 22 après-midi : Mathieu Barré

- La chasse aux angles -

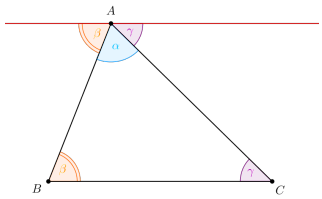
La chasse aux angles est un outil qui s'avère extrêmement utile dans la résolution de problèmes de géométrie. De nombreux problèmes apparemment complexes peuvent se reformuler de façon angulaire et ainsi être résolus grâce à cette technique. Elle consiste à donner un nom (en général avec des lettres grecques) aux angles qui apparaissent souvent dans la figure étudiée et à calculer tous les angles de cette figure à partir des angles de départ en utilisant les données de l'énoncé.

Avant de la mettre en application, il est nécessaire de connaître un certain nombre de résultats classiques que nous allons ici rappeler.

Théorème. Soit $n \geq 3$. La somme des angles dans un n-gone est $180(n-2)$ degrés.

Démonstration. Nous allons prouver ce résultat par récurrence.

- **Initialisation :** Le cas $n = 3$ est celui du triangle. Prenons donc un triangle quelconque ABC. On utilise la notation usuelle $\widehat{BAC} = \alpha$, $\widehat{CBA} = \beta$ et $\widehat{ACB} = \gamma$ (ces notations seront implicites par la suite). Menons donc la parallèle à (BC) passant par A. L'utilisation des angles alternes-internes donne alors que $\alpha + \beta + \gamma$ correspond à un angle plat, qui vaut par définition 180 degrés.

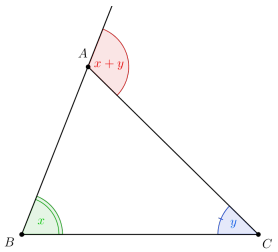


- **Hérédité :** Supposons notre propriété établie pour $n \geq 3$ et montrons qu'elle est également vraie pour $n+1$. Pour cela, on considère notre $(n+1)$-gone comme un n-gone auquel on a rajouté un triangle. La somme des angles du $(n+1)$-gone vaut alors $180(n-2)$ par hypothèse de récurrence, qu'on additionne aux 180 degrés du triangle rajouté, ce qui fait bien $180(n-1)$ degrés au total et achève la démonstration.

□

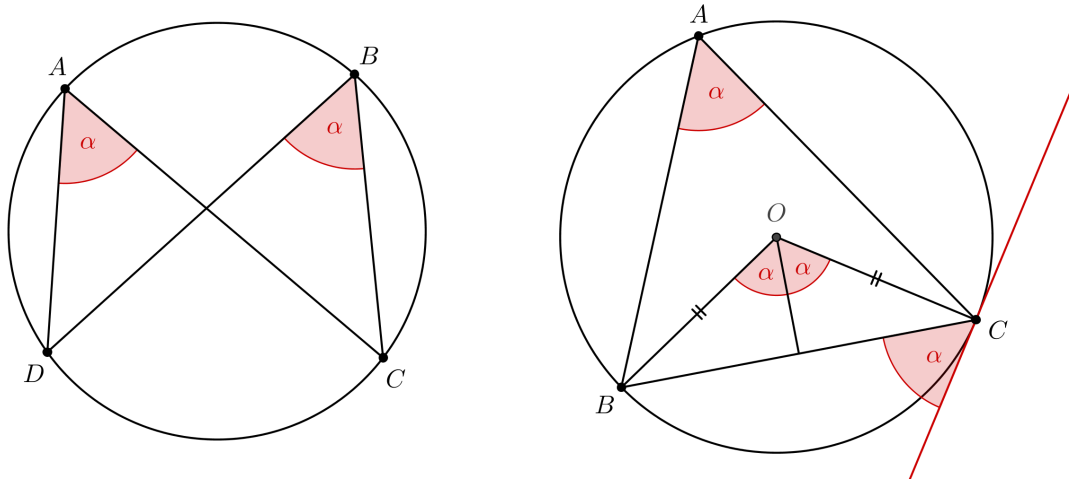
Corollaire. Dans un triangle, il suffit de connaître deux angles pour connaître le troisième.

En particulier, on retiendra la configuration ci-dessous :



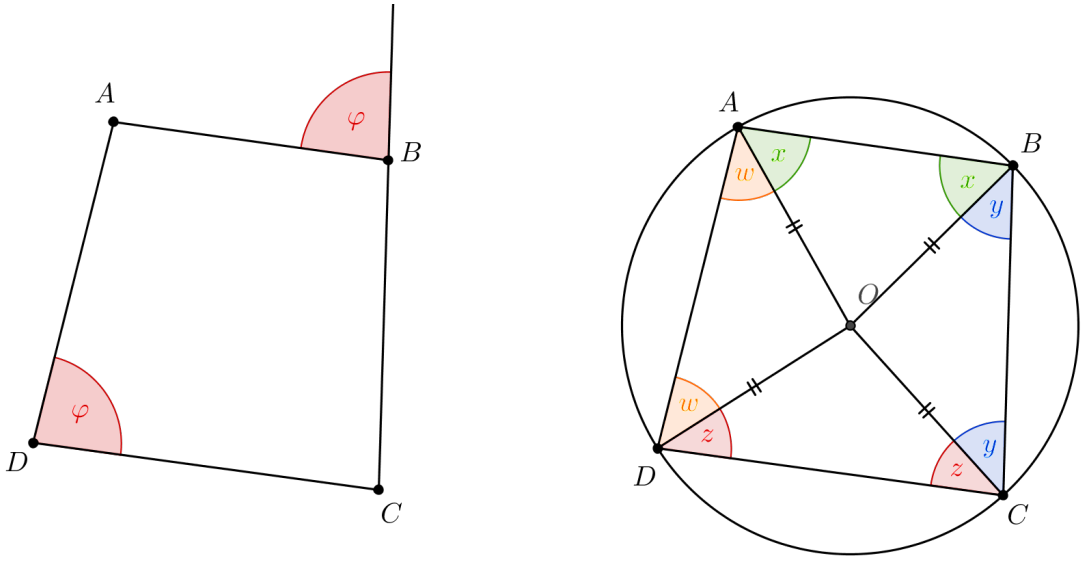
Le théorème suivant est sans doute un des plus importants à retenir.

Théorème (angle au centre, angle inscrit)**.** Sur la figure à gauche, les points A, B, C et D sont *cocycliques* (c'est-à-dire sur un même cercle) si et seulement si $\widehat{DAC} = \widehat{DBC}$. Autrement dit, deux angles intersectant le même arc ont même mesure. À droite est représenté le cas limite de ce théorème, lorsque deux points sont confondus et qu'une droite est alors tangente au cercle circonscrit à ABC.



Enfin, mentionnons un théorème tout aussi fondamental, qui fournit une condition angulaire nécessaire et suffisante à la cocyclicité de quatre points.

Théorème. Un quadrilatère est cyclique si et seulement si la somme de deux angles opposés est égale à 180 degrés.



Démonstration du sens direct. Le seul élément dont nous disposons pour démontrer notre théorème est que les quatre points sont sur un même cercle. Aussi, introduisons O, le centre de ce cercle. Il s'agit alors de repérer que l'on a énormément de triangles isocèles, à savoir les

triangles OAB, OBC, OCD et ODA, tous isocèles en O. Notre philosophie est donc de donner un nom à chacun des angles intervenant dans ces triangles : posons $\widehat{OAB} = x$, $\widehat{OBC} = y$, $\widehat{OCD} = z$ et $\widehat{ODA} = w$. On peut alors calculer tous les angles comme sur la figure ci-contre. En considérant le quadrilatère $ABCD$, nous savons alors d'après notre premier théorème que

$$2x + 2y + 2z + 2w = 360$$

d'où on conclut que

$$\widehat{ABC} + \widehat{CDA} = x + y + z + w = 180$$

□

Pour éviter des problèmes d'orientation et de position des points (par exemple, un point pourra être situé à droite ou à gauche d'une certaine droite, ce qui amène à distinguer des cas de façon fastidieuse et peu instructive), on préférera employer des angles orientés entre les droites pour formaliser les chasses aux angles qu'on peut faire "sur le dessin".

Plus précisément, si d et d' sont deux droites du plan, on désigne par (d, d') l'angle dont il faut tourner d vers la gauche (dans le sens trigonométrique, c'est-à-dire le sens inverse des aiguilles d'une montre) pour que d et d' se superposent.

On remarque que si l'on fait tourner une droite de 180 degrés sur elle-même, elle revient dans sa position de départ. Aussi, ajouter ou soustraire 180 degrés lorsqu'on calcule avec des angles orientés ne modifie pas le résultat. On dira que les angles orientés entre les droites sont définis *modulo* 180 degrés. En revanche, on convient que tourner vers la gauche est positif et vers la droite négatif, en particulier $(d, d') = -(d', d)$.

Enfin, l'intérêt de cette notion est qu'on peut toujours décomposer un angle orienté en plusieurs autres angles : lorsqu'on tourne une droite d pour arriver sur une droite d', on peut passer par une droite d'' puis aller de d'' à d' en conservant les propriétés angulaires de notre déplacement. Ainsi, on obtient le théorème suivant :

Théorème (relation de Chasles)**.**

$$(d, d') = (d, d'') + (d'', d')$$

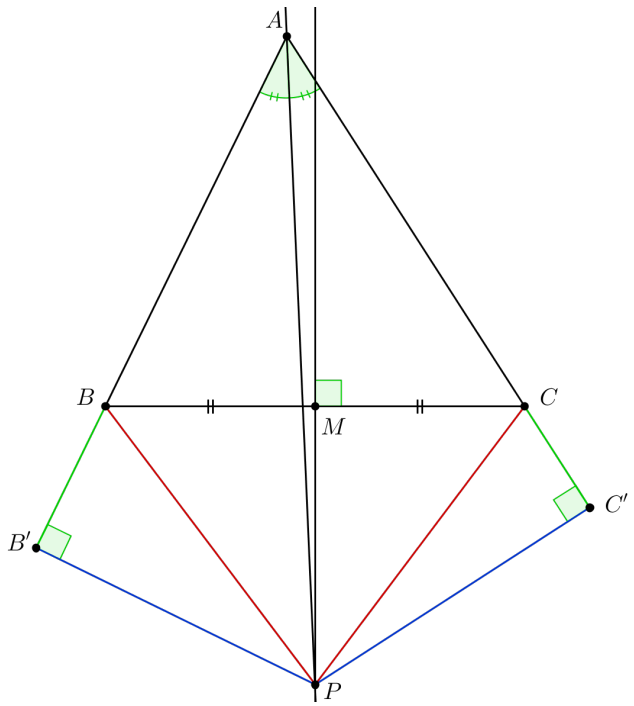
Pour se convaincre de l'utilité des angles orientés entre les droites, voyons que seulement raisonner avec des angles classiques permet de démontrer tout et n'importe quoi, par exemple :

Proposition (arnaque des angles classiques)**.** Tous les triangles sont équilatéraux.

Démonstration. Il nous suffit de montrer que tous les triangles sont isocèles et d'appliquer deux fois ce résultat pour prouver notre théorème.

Soit ABC un triangle. On note P l'intersection de la bissectrice issue de A avec la médiatrice de $[BC]$ ainsi que B' et C' les projetés orthogonaux de P sur (AB) et (AC) respectivement, comme sur la figure ci-dessous.

Puisque P appartient à la bissectrice de $\widehat{BAC}$, il s'ensuit que $AB' = AC'$ et que $PB' = PC'$. Par ailleurs, P est sur la médiatrice de $[BC]$, d'où $PB = PC$. Par le théorème de Pythagore, on obtient donc $BB' = CC'$. Combiné à $AB' = AC'$, cette dernière égalité donne $AB = AC$. □



On peut alors condenser nos résultats précédents en écrivant :

Théorème. Quatre points A, B, C et D sont cocycliques si et seulement si

$$(CB, CA) = (DB, DA)$$

Remarquons que ceci est tout à fait cohérent avec les angles des figures illustrant les propriétés déjà énoncées. De façon plus générale, tout raisonnement de chasse aux angles classique peut s'écrire avec des angles orientés, et réciproquement. Si les angles orientés éliminent les problèmes de configuration, il est souvent difficile de résoudre un exercice en utilisant directement cette notion. Une bonne méthode nous semble donc être de mener à bien la chasse aux angles habituelle sur la figure pour trouver les étapes du raisonnement puis de les rédiger soigneusement avec les angles orientés.

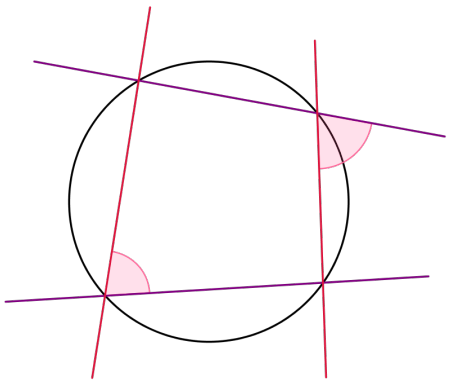
Cette propriété s'inscrit dans le cadre plus général des droites antiparallèles.

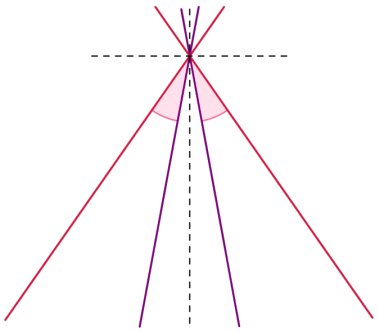
Définition. Deux couples de droites (d, d') et (D, D') sont *antiparallèles* s'ils ont les mêmes directions de bissectrices, autrement dit si

$$(d, D) = (D', d')$$

Si des couples (d, d') et (D, D') sont antiparallèles et concourants (voir la figure de droite), on dit qu'ils sont *isogonaux*.

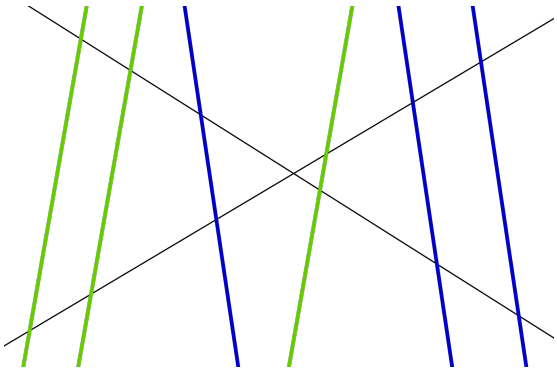
On écrit alors que d est antiparallèle à d', et on note $d \setminus\setminus d'$ par rapport à (D, D'). On omettra parfois de préciser par rapport à quel couple de droites on se place s'il n'y a pas de confusion possible, mais n'oublions pas que cette notion n'a de sens que par rapport à des sécantes données.





Les résultats suivants découlent directement de la définition précédente :

- $(AA') \backslash\backslash (BB')$ par rapport à $(AB, A'B') \Leftrightarrow (AB) \backslash\backslash (A'B')$ par rapport à (AA', BB').
- Quatre points A, B, C et D sont cocycliques si et seulement si les droites (AB) et (DC) sont antiparallèles par rapport aux droites (AD) et (BC).
- Dans un triangle, la tangente au cercle circonscrit en un sommet est antiparallèle au côté opposé (par rapport aux deux côtés contenant le sommet considéré).
- Si $d_1 \backslash\backslash d_3$ et $d_2 \backslash\backslash d_3$, alors $d_1 // d_2$. Autrement dit, si deux droites sont antiparallèles à une même droite (à chaque fois par rapport aux mêmes droites de référence), alors elles sont parallèles entre elles. Réciproquement, si $d_1 \backslash\backslash d_3$ et que $d_1 // d_2$ alors $d_2 \backslash\backslash d_3$.

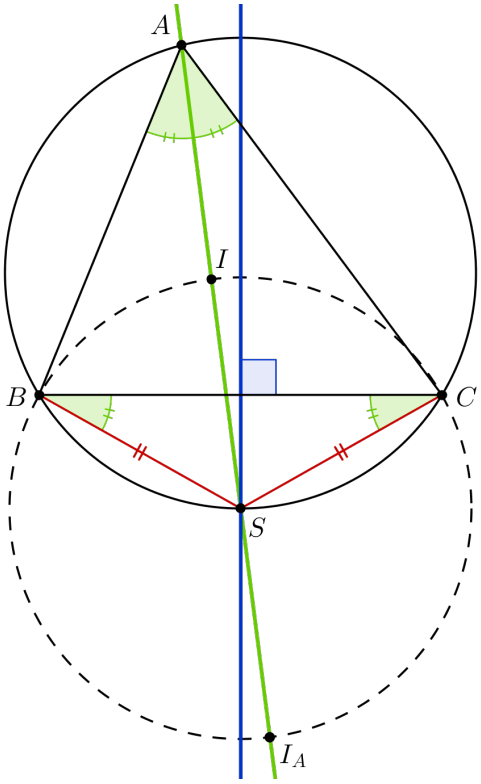


Sur la figure ci-contre, toutes les droites vertes sont parallèles entre elles, de même pour les droites bleues. Chacune des droites vertes est antiparallèle à chacune des droites bleues par rapport aux droites de référence noires. Lorsqu'on regarde les points d'intersection d'une droite verte et d'une droite bleue avec les droites de référence, on obtient quatre points cocycliques.

Enfin, citons un dernier théorème dont il est toujours utile de se souvenir lorsque l'exercice fait intervenir le centre du cercle inscrit, les bissectrices et les médiatrices d'un triangle ou encore le milieu d'un segment ou d'un arc.

Théorème (pôle Sud)**.** Soit ABC un triangle. La bissectrice intérieure issue de A et la médiatrice de $[BC]$ s'intersectent en un point S nommé *pôle Sud* qui appartient au cercle circonscrit d'ABC et qui est le milieu de l'arc $\overset{\frown}{BC}$.

De plus, S est le centre d'un cercle contenant B, C, I et I_A (centre du cercle exinscrit tangent à (BC)).



- Exercices -

Exercice 1

Trouver l'erreur dans l'arnaque des angles classiques.

Exercice 2

Soient Γ_1 et Γ_2 deux cercles s'intersectant en A et B. Une droite d passant par A coupe Γ_1 en P et Γ_2 en Q. De même, une droite d' passant par B recoupe Γ_1 en P' et Γ_2 en Q'.

Montrer que les droites (PP') et (QQ') sont parallèles.

Exercice 3

Soient A, B, C et D quatre points cocycliques. On note respectivement A' et C' les projetés orthogonaux de A et C sur (BD), et B' et D' les projetés orthogonaux de B et D sur (AC).

Montrer alors que A', B', C' et D' sont également cocycliques.

Exercice 4

Soit ABC un triangle et O le centre de son cercle circonscrit. Soient H_B et H_C les pieds des hauteurs issues de B et C.

Prouver que $(H_BH_C) \perp (AO)$.

Exercice 5

Tynawedd met sur une table une pièce de 1 euro, de 2 euros, de 2 centimes et de 50 centimes, comme sur la figure ci-dessous.

Montrer qu'A, B, C et D sont cocycliques.

Exercice 6

Soient A, B, C et D quatre points sur un cercle Γ de telle sorte que les cordes $[AB]$ et $[CD]$ s'intersectent en un point E à l'intérieur de Γ et soit P un point arbitraire sur $[BE]$. La tangente t au cercle circonscrit de DEP en E coupe (AC) en F.

Démontrer que $\widehat{EFC} = \widehat{BDP}$.

Exercice 7

Soient A, B, C et D quatre points dans cet ordre sur un cercle et soit S le milieu de l'arc $\overset{\frown}{AB}$ ne contenant pas C et D. Les droites (SD) et (SC) intersectent (AB) en E et F respectivement.

Montrer que C, D, E et F sont cocycliques.

Exercice 8

Soit $ABCD$ un quadrilatère inscriptible et tangentiel (c'est-à-dire dont tous les côtés sont tangents à un même cercle inscrit dans le quadrilatère). On note respectivement E, F, G et H les points de tangence de son cercle inscrit avec les côtés $[AB]$, $[BC]$, $[CA]$ et $[AD]$.

Prouver que $(EG) \perp (HF)$.

Exercice 9

Soient ABC un triangle et D l'intersection de la bissectrice intérieure issue de A avec $[BC]$. La médiatrice de $[AD]$ recoupe la bissectrice issue de B en M et celle issue de C en N.

Montrer que les points A, D, M et N sont sur un même cercle.

Exercice 10

Soit $ABCD$ un quadrilatère cyclique. On appelle respectivement I_A, I_B, I_C et I_D les centres des cercles inscrits des triangles BCD, DCA, ADB et BAC.

Quelle est la nature du quadrilatère $I_AI_BI_CI_D$?

Exercice 11

Soient A, B, C, D et E cinq points dans cet ordre sur un cercle, vérifiant $AB = BC$ et $CD = DE$. On appelle respectivement P, Q et T l'intersection des droites (AD) et (BE), (AC) et (BD), (BD) et (CE).

Montrer que le triangle PQT est isocèle.

- Solutions des exercices -

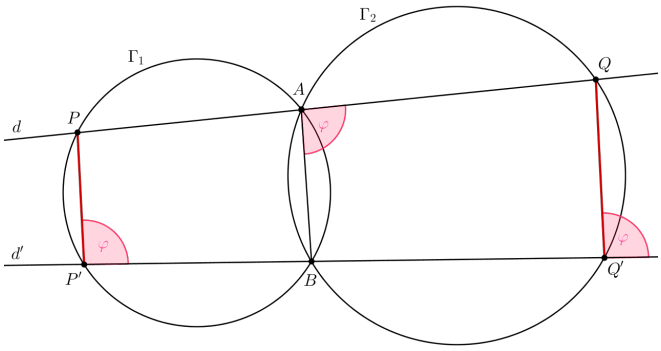
Comme nous l'avons dit, la chasse aux angles classique et l'utilisation des angles orientés sont deux rédactions différentes d'un même raisonnement. Ainsi, les solutions des exercices qui suivent sont pour la plupart rédigées avec des angles orientés pour éviter les problèmes de configuration évoqués précédemment, mais les chasses aux angles qu'on pourrait effectuer "à la main" apparaissent sur les figures pour une meilleure compréhension des preuves.

Solution de l'exercice 1

En fait, rien n'est faux en soi jusqu'à la dernière ligne de la preuve : pour obtenir $AB = AC$, on a implicitement utilisé que $AB = AB' - BB'$ et que $AC = AC' - CC'$. Or, cette soustraction n'est possible que si B' et C' sont tous deux situés à l'extérieur du triangle (ou tous deux à l'intérieur), ce qui n'est pas le cas. En effet, le théorème du pôle Sud montre que P est sur le cercle circonscrit de ABC, ce qui implique qu'un des points entre B' et C' sera à l'extérieur du triangle et l'autre à l'intérieur.

Solution de l'exercice 2

La chasse aux angles classiques figure sur le dessin ci-dessous.



En rédigeant avec les angles orientés, on écrit

$$\begin{aligned}(P'B, P'P) &= (AB, AP) \text{ car } A, B, P' \text{ et } P \text{ sont cocycliques}\\ &= (AB, AQ) \text{ car } P, A \text{ et } Q \text{ sont alignés}\\ &= (Q'B, Q'Q) \text{ car } A, B, Q' \text{ et } Q \text{ sont cocycliques}\\ &= (P'B, Q'Q) \text{ car } P', B \text{ et } Q' \text{ sont alignés}\end{aligned}$$

ce qui signifie bien que (PP') et (QQ') sont parallèles puisqu'on peut écrire

$$(P'P, Q'Q) = (P'P, P'B) + (P'B, Q'Q) = -(P'B, Q'Q) + (P'B, Q'Q) = 0$$

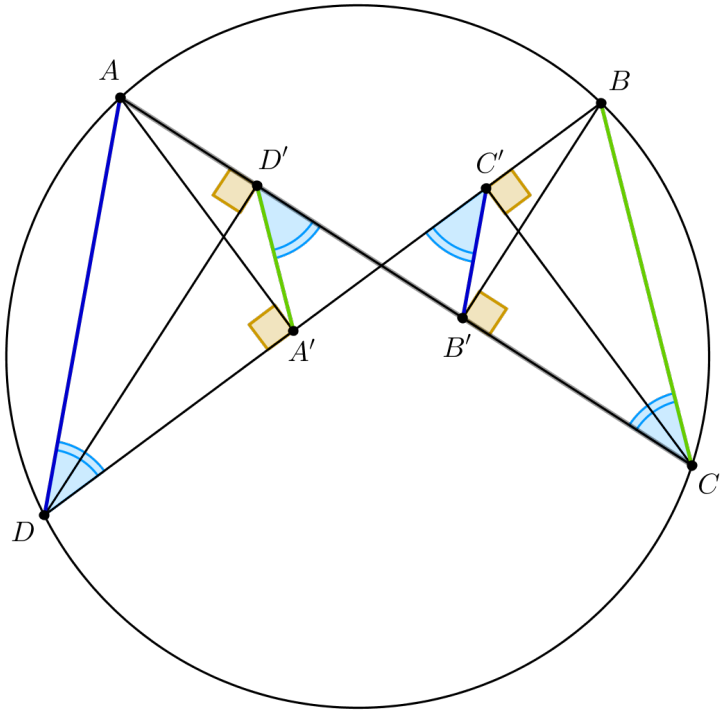
Remarque : Cet exercice constitue en fait une démonstration de la propriété "si deux droites sont antiparallèles à une même droite, alors elles sont parallèles entre elles". En effet, si on choisit comme droites de référence d et d', la cocyclicité sur Γ_1 donne $(PP') \backslash\backslash (AB)$

et celle sur Γ_2 implique $(QQ') \setminus\setminus (AB)$, d'où $(PP') \,//\, (QQ')$.

Solution de l'exercice 3

Première solution : Puisque $\widehat{AD'D} = \widehat{AA'D} = 90$, le théorème de l'angle inscrit permet d'affirmer que A, D, A' et D' sont cocycliques. On obtient de la même façon que B, C, B' et C' sont cocycliques.

On en déduit alors que $(DA', DA) = (D'A', D'A)$ car A, D, A' et D' sont cocycliques et que $(CB, CB') = (C'B, C'B')$ car B, C, B' et C' sont cocycliques. Or, A, B, C et D étant cocycliques, nous savons que $(DB, DA) = (CB, CA)$ et l'alignement des points D, A' et B d'une part et de C, B' et A d'autre part fait que cette dernière égalité se réécrit $(DA', DA) = (CB, CB')$. Finalement, on en conclut que $(D'A', D'A) = (C'B, C'B')$ soit $(D'A', D'B') = (C'A', C'B')$, ce qui démontre que A', B', C' et D' sont cocycliques.



Seconde solution : De façon équivalente, on peut raisonner avec des droites parallèles et antiparallèles, en prenant pour droites de référence (AC) et (BD). A, D, A' et D' étant cocycliques, $(AD) \setminus\setminus (A'D')$. De même, $(BC) \setminus\setminus (B'C')$. Par ailleurs, $(BC) \setminus\setminus (AD)$ par cocyclicité des point A, B, C et D. On a donc $(BC) \setminus\setminus (B'C')$ et $(BC) \setminus\setminus (AD)$ d'où $(B'C') \,//\, (AD)$. Combiné à $(AD) \setminus\setminus (A'D')$, ce dernier résultat donne $(B'C') \setminus\setminus (A'D')$, ce qui fournit la conclusion attendue.

Solution de l'exercice 4

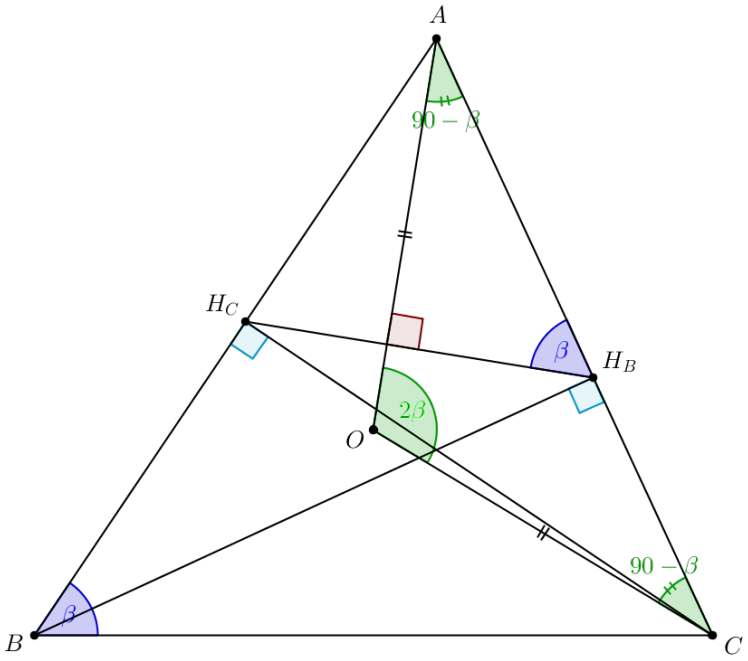
Les triangles BH_BC et BH_CC étant respectivement rectangles en H_B et H_C, le théorème de l'angle inscrit nous dit que B, C, H_B et H_C sont cocycliques, d'où on tire que $(BC, BH_C) = (H_BC, H_BH_C)$ soit

$$(BC, BA) = (H_BA, H_BH_C)$$

D'autre part, le théorème de l'angle au centre indique que $(OC, OA) = 2(BC, BA)$. Le

triangle AOC étant isocèle en O, on en déduit que

$$(AO, AH_B) = (AO, AC) = 90 - (BC, BA)$$



La relation de Chasles donne finalement

$$(AO, H_BH_C) = (AO, H_BA) + (H_BA, H_BH_C) = 90 - (BC, BA) + (BC, BA) = 90$$

Solution de l'exercice 5

Soient O_1, O_2, O_3 et O_4 les centres respectifs des pièces de 2 euros, 50 centimes, 1 euro et 2 centimes. La tangente commune aux pièces de 2 euros et de 50 centimes en A étant perpendiculaire à (O_1A) et à (O_2A), on en déduit que O_1, A et O_2 sont alignés. On prouve de même que $B \in (O_2O_3)$, $C \in (O_3O_4)$ et que $D \in (O_4O_1)$.

On remarque alors qu'on a alors énormément de triangles isocèles dans la figure, à savoir O_1AD, O_2AB, O_3BC et O_4CD, respectivement isocèles en O_1, O_2, O_3 et O_4. Il est donc naturel de poser $\widehat{O_1AD} = \widehat{O_1DA} = x$, $\widehat{O_2AB} = \widehat{O_2BA} = y$, $\widehat{O_3BC} = \widehat{O_3CB} = z$ et $\widehat{O_4CD} = \widehat{O_4DC} = w$, comme sur la figure ci-dessous.

La somme des angles du quadrilatère $O_1O_2O_3O_4$ donne

$$\widehat{O_4O_1O_2} + \widehat{O_1O_2O_3} + \widehat{O_2O_3O_4} + \widehat{O_3O_4O_1} = 360$$

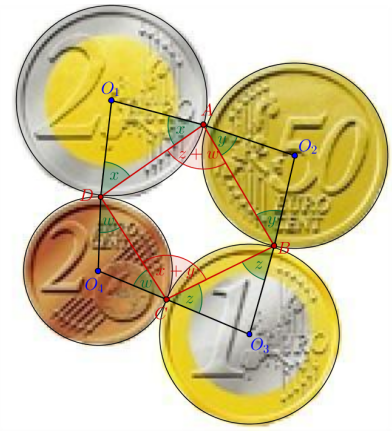
soit

$$(180 - 2x) + (180 - 2y) + (180 - 2z) + (180 - 2w) = 360$$

ce qui se réécrit plus simplement $x + y + z + w = 180$.

On en conclut alors que

$$\widehat{DAB} + \widehat{BCD} = (180 - x - y) + (180 - z - w) = (z + w) + (x + y) = 180$$

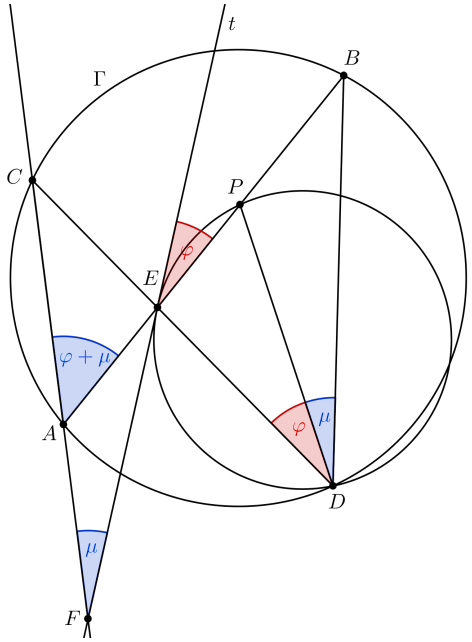


ce qui permet d'affirmer que les points A, B, C et D sont cocycliques.

Solution de l'exercice 6

A, B, C et D étant cocycliques, on a $(AB, AC) = (DB, DC)$. (EF) est tangente au cercle circonscrit de DEP, donc nous savons d'après le cas limite du théorème de l'angle inscrit que $(DP, DE) = (EP, EF)$. On écrit alors successivement

$$\begin{aligned}
\widehat{EFC} &= (FE, FC) \\
&= (AE, FC) + (FE, AE) \text{ d'après la relation de Chasles} \\
&= (AB, AC) - (EP, FE) \text{ car } E \in (AP) \text{ et } F \in (AC) \\
&= (DB, DC) - (DP, DE) \text{ d'après ce qui précède} \\
&= (DB, DE) + (DE, DP) \text{ car } D, E \text{ et } C \text{ sont alignés} \\
&= (DB, DP) \text{ d'après la relation de Chasles} \\
&= \widehat{BDP}
\end{aligned}$$

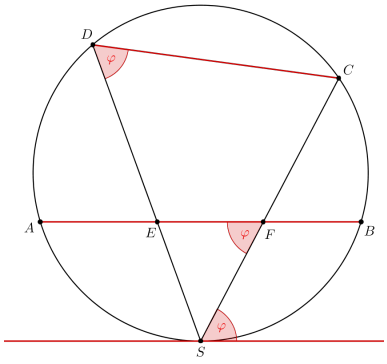


Solution de l'exercice 7

L'idée est de considérer la tangente au cercle en S, qu'on appelle t. Cette idée est motivée par le fait que, S étant le milieu de l'arc $\overset{\frown}{AB}$, $t \,//\, (AB)$. On a alors

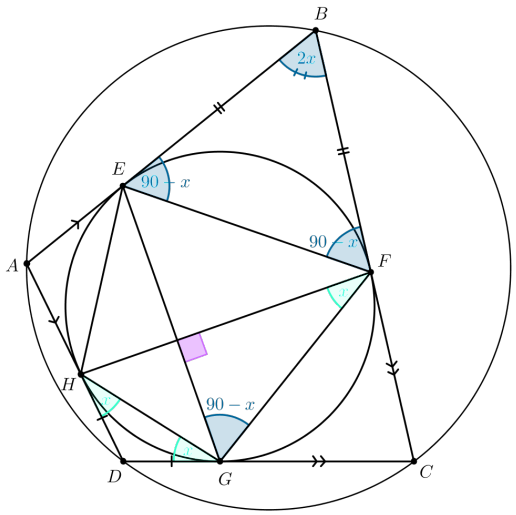
$$\begin{aligned}(DE, DC) &= (DS, DC) \text{ car } D, E \text{ et } S \text{ sont alignés}\\ &= (t, SC) \text{ d'après le cas limite du théorème de l'angle inscrit}\\ &= (AB, SC) \text{ puisque } t \,//\, (AB)\\ &= (FE, FS) \text{ (alignement des points)}\end{aligned}$$

ce qui prouve la cocyclicité des points C, D, E et F.



Solution de l'exercice 8

$$\begin{aligned}(GE, HF) &= (GE, GF) + (FG, FH) \text{ d'après la relation de Chasles}\\ &= (FE, FB) + (GD, GH) \text{ (cas limite du théorème de l'angle inscrit)}\\ &= \frac{(BE, BF)}{2} + \frac{(DA, DC)}{2} \text{ car } BE = BF \text{ et } DG = DH\\ &= 90 \text{ car } A, B, C \text{ et } D \text{ sont cocycliques, soit } (BA, BC) + (DA, DC) = 180\end{aligned}$$

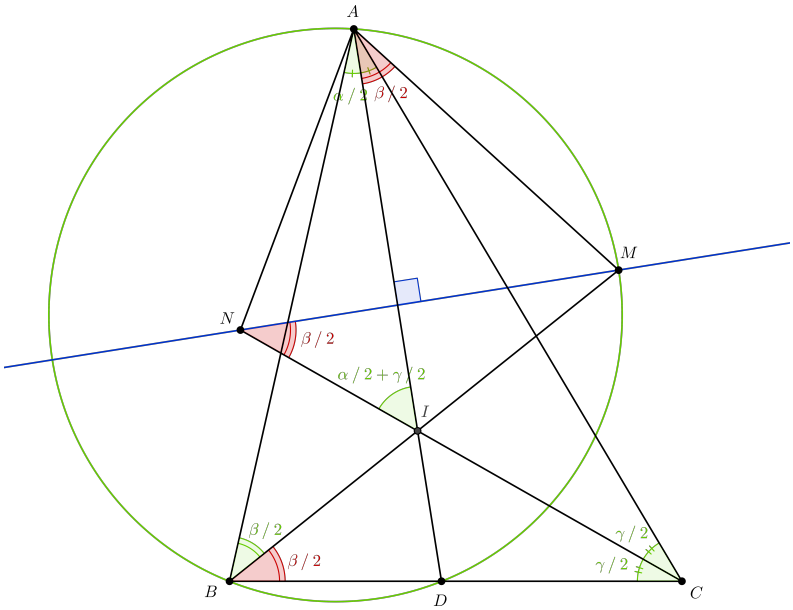


Solution de l'exercice 9

Le point M est défini comme l'intersection de la médiatrice de $[AD]$ avec la bissectrice de $\widehat{ABD}$. D'après le théorème du pôle Sud, M, A, B et D sont donc cocycliques. On en déduit que $(BD, BM) = (AD, AM) = \frac{(BC,BA)}{2}$. Par ailleurs,

$$\begin{aligned}(NM, NI) &= (NM, IA) + (AI, AC) + (CA, CI) \text{ (relation de Chasles)}\\ &= 90 + \frac{(AB, AC)}{2} + \frac{(CA, CB)}{2} \text{ par définition de } I\\ &= \frac{(AB, CB)}{2} \text{ d'après la relation de Chasles}\end{aligned}$$

Dès lors, $(NM, NI) = (AM, AI)$, ce qui prouve que A, M, I et N sont cocycliques.

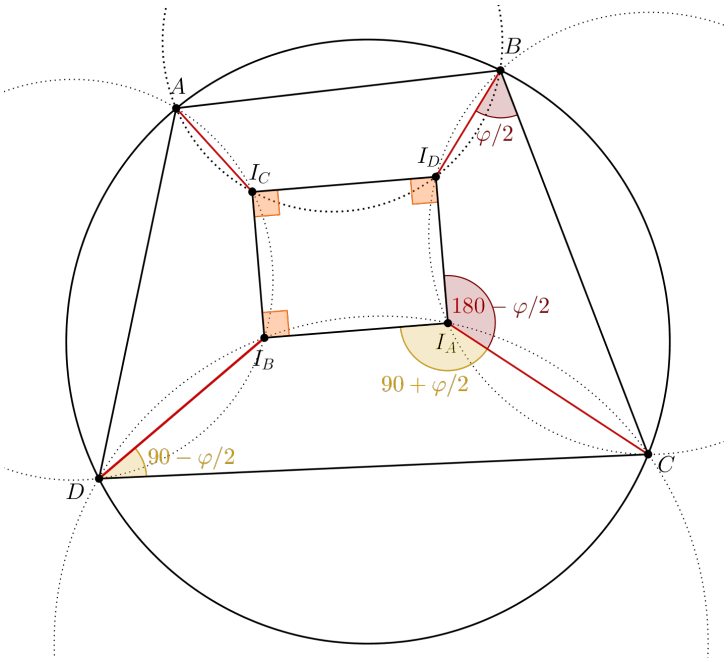


Solution de l'exercice 10

Là encore, il s'agit d'utiliser le théorème du pôle Sud pour faire apparaître des points cocycliques puis de conclure par chasse aux angles. Appelons S le milieu de l'arc $\widehat{AB}$. I_C étant le centre du cercle inscrit de DAB, le théorème du pôle Sud nous dit que $SA = SB = SI_C$. De même, $SA = SB = SI_D$. Finalement, c'est que A, B, I_C et I_D sont cocycliques, et on montre de même que les quadrilatères BCI_AI_D, CDI_BI_A et DAI_CI_B sont cycliques. On en tire :

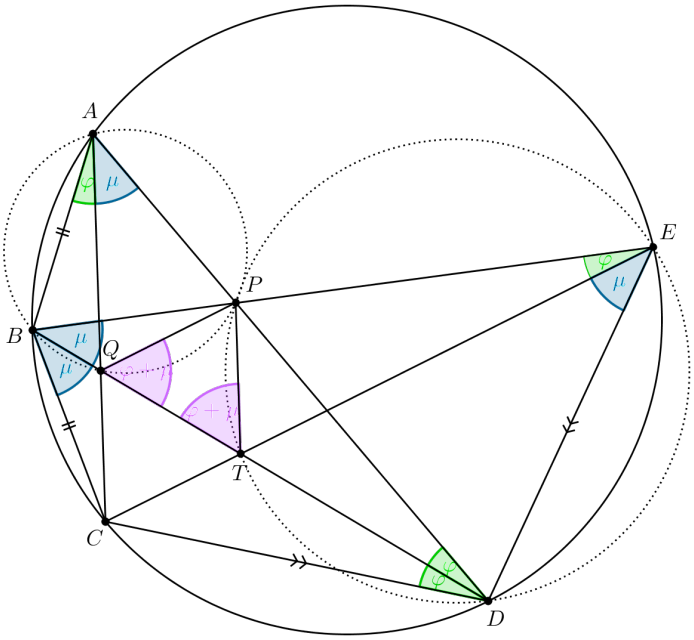
$$\begin{aligned}(I_AI_D, I_AI_B) &= (I_AC, I_AI_B) + (I_AI_D, I_AC) \text{ d'après la relation de Chasles}\\ &= (DI_B, DC) + (BI_D, BC) \text{ car les quadrilatères } CDI_BI_A \text{ et } BCI_AI_D \text{ sont cycliques}\\ &= \frac{(DA, DC)}{2} + \frac{(BA, BC)}{2} \text{ par définition des points } I_B \text{ et } I_D\\ &= 90 \text{ car } A, B, C \text{ et } D \text{ sont cocycliques, soit } (DA, DC) + (BA, BC) = 180\end{aligned}$$

En faisant de même autour des points I_B, I_C et I_D, on en conclut qu'$I_AI_BI_CI_D$ est un rectangle.



Solution de l'exercice 11 Les points A, B, C et D étant cocycliques, le théorème de l'angle inscrit nous permet d'écrire $(BC, BD) = (AC, AD)$. Puisque D est le milieu de l'arc $\widehat{CE}$, le théorème du pôle Sud affirme que $(BC, BD) = (BD, BE)$. Les deux résultats précédents, combinés à l'alignement des points B, P et E d'une part et B, Q, T et D d'autre part, donnent $(AQ, AP) = (BQ, BP)$, ce qui démontre que les points A, B, P et Q sont cocycliques. On prouve de la même façon que les points E, D, P et T sont cocycliques.

On a ainsi $(AB, AP) = (QT, QP)$ et $(EP, ED) = (TP, TQ)$. Mais $(AB, AP) = (EP, ED)$ car A, B, D et E sont cocycliques, d'où $(QT, QP) = (TP, TQ)$. Le triangle PQT est donc isocèle en P.



3 dimanche 23 matin : Clara Ding

Triangles semblables

Deux triangles semblables sont deux triangles qui ont la même "forme". Du coup, ils leurs trois angles égaux et la longueur de leurs côtés proportionnels. On a que les 4 propositions suivantes sont équivalentes :

- les triangles ABC et $A'B'C'$ sont semblables (ce qui est noté $ABC \sim A'B'C'$),
- $\widehat{A} = \widehat{A'}$, $\widehat{B} = \widehat{B'}$, et $\widehat{C} = \widehat{C'}$,
- $\frac{AB}{AC} = \frac{A'B'}{A'C'}$ et $\frac{BC}{BA} = \frac{B'C'}{B'A'}$,
- $\widehat{A} = \widehat{A'}$ et $\frac{AB}{AC} = \frac{A'B'}{A'C'}$.

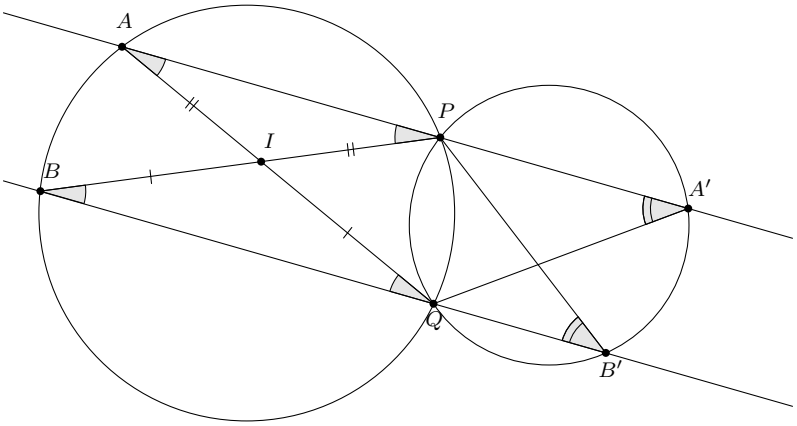
Remarque 82. Attention, les longueurs dont on prend les rapports dans la troisième condition doivent être celles des segments adjacents aux angles égaux choisis.

Exercice 1 Soit ABC un triangle et H_A et H_B les pieds des hauteurs issues de A et B. Montrer que CH_AH_B et CAB sont semblables.

Solution de l'exercice 1 On a $\widehat{AH_BB} = 90°$ et $\widehat{AH_AB} = 90°$, donc A, H_A, H_B et B sont cocycliques. Donc $\widehat{CH_BH_A} = \widehat{CBA}$ et $\widehat{CH_AH_B} = \widehat{CAB}$. Donc les triangles CH_AH_B et CAB ont leurs 3 angles égaux, ils sont donc semblables.

Exercice 2 Deux cercles se coupent en P et Q. Une droite passant par P coupe les deux cercles en A et A'. La droite parallèle passant par Q coupe les cercles en B et B'. Montrer que les triangles PBB' et QAA' sont isométriques.

Solution de l'exercice 2 Traçons la figure pour nous donner une idée.



Par les angles inscrits, $\widehat{PAQ} = \widehat{PBQ}$ et $\widehat{PA'Q} = \widehat{PB'Q}$. Les triangles PBB' et QAA' sont donc semblables. Si on trouve deux côtés égaux, on a gagné. On commence par introduire I le point d'intersection de $[PA]$ et $[QB]$. Comme on a des droites parallèles, les angles alternes-internes sont égaux, donc $\widehat{QBI} = \widehat{IPA}$ et $\widehat{IAP} = \widehat{IQB}$. Comme tous ces angles étaient déja égaux par les angles inscrits, on a des triangles isocèles à tire-larigot. Donc

$$AQ = AI + IQ = PI + IB = PB.$$

On a nos deux côtés égaux, les deux triangles sont isométriques.

Exercice 3 Soit un triangle ABC rectangle en C. Soit H le pied de la hauteur issue de C. Montrer que $CH^2 = AH.BH$

Solution de l'exercice 3 On va montrer que CHB et AHC sont semblables : on a $\widehat{AHC} = \widehat{BHC} = 90°$, et $\widehat{HAC} = 90° - \widehat{HBC} = \widehat{HCB}$, on a 2 paires d'angles identiques, donc CHB et AHC sont semblables. On a alors $\frac{CH}{HB} = \frac{AH}{HC}$ d'où $CH^2 = AH.BH$.

Exercice 4 Soit ABC un triangle rectangle en C. Sur la droite (AC) on place un point D tel que $CD = BC$, C étant situé entre A et D. La perpendiculaire à (AB) passant par D recoupe (BC) en E. Montrer que $AC = CE$.

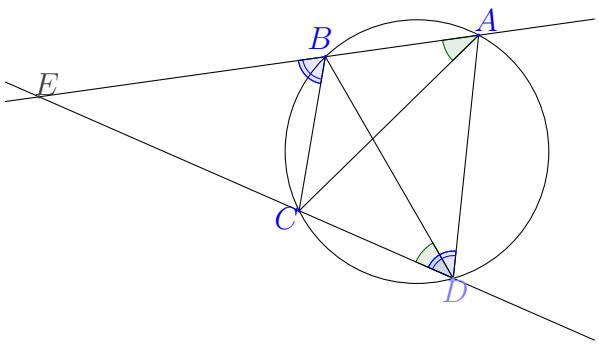
Solution de l'exercice 4 On a $\widehat{CBA} = \widehat{CDE}$, puisque (CB) est perpendiculaire à (CD) et (BA) à (DE). Il en résulte que les triangles CBA et CDE ont leurs angles égaux, ils sont semblables, et même égaux car $CB = CD$ par hypothèse. Cela entraîne $CA = CE$.

Exercice 5 Soient A, B, C et D quatre points cocycliques. (AB) et (CD) se coupent en E. Montrez que :

$$\frac{AC}{BC} \cdot \frac{AD}{BD} = \frac{AE}{BE}$$

.

Solution de l'exercice 5



Parce qu'ils ont les mêmes angles, les triangles ECA et EBD sont semblables ; d'où $\frac{AC}{BD}$=$\frac{EA}{ED}$. Les angles des triangles EBC et EDA sont aussi les mêmes, donc EBC et EDA sont aussi semblables, d'où : $\frac{BC}{AD} = \frac{EB}{ED}$. En faisant le produit, ED se simplifie, et il reste la relation recherchée.

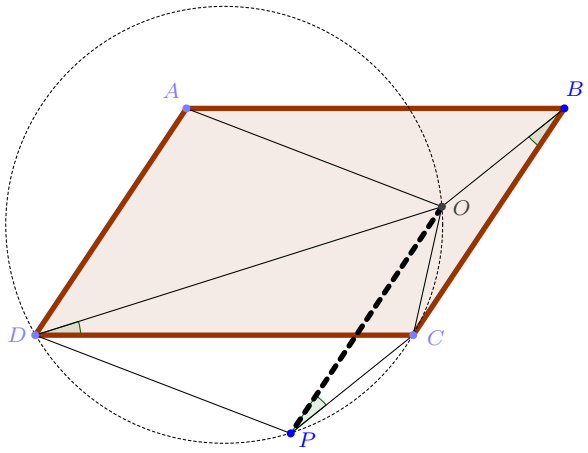
Exercice 6 Le quadrilatère $ABCD$ est inscriptible dans un cercle de centre O. Les diagonales AC et BD sont perpendiculaires. Montrer que la distance de O à la droite (AD) est égale à la moitié de la longueur du segment $[BC]$.

Solution de l'exercice 6 Par la propriété des angles inscrits, on a $\widehat{AOD} = 2\widehat{ABD}$ et donc $\widehat{IOA} = \widehat{ABD}$. De même $\widehat{COJ} = \widehat{CAB} = \frac{\pi}{2} - \widehat{ABD}$. On en déduit $\widehat{IOA} = \frac{\pi}{2} - \widehat{OJC} = \widehat{OCJ}$ puis que les triangles IOA et JCO sont semblables. Comme on a en outre $OA = OC$, ils sont isométriques et $CJ = IO$, ce qui permet de conclure.

Exercice 7 Soit $ABCD$ un parallélogramme, O un point intérieur tel que $\widehat{AOB} + \widehat{COD} = 180°$. Montrer que $\widehat{OBC} = \widehat{ODC}$.

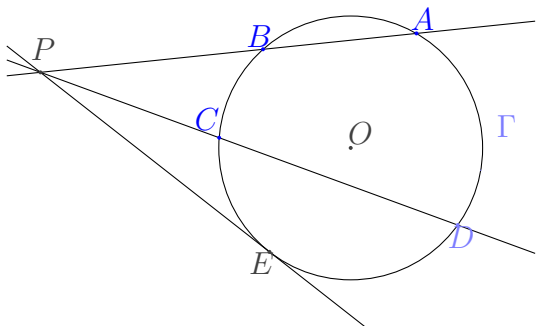
Solution de l'exercice 7

Translatons le point O d'un vecteur $\vec{BC}$: considérons donc le point P tel que $OPCB$ soit un parallélogramme. Le triangle PDC est translaté, donc isométrique, du triangle OAB. Les angles $\widehat{DPC}$ et $\widehat{COD}$ sont supplémentaires, de part et d'autre de (CD), donc les quatre points C, D, O, P sont cocycliques. On en déduit que les angles inscrits $\widehat{ODC}$ et $\widehat{OPC}$ sont égaux. Or dans le parallélogramme $OPCD$, $\widehat{OPC} = \widehat{OBC}$, d'où le résultat.



On notera qu'il est difficile de faire une figure juste en se basant sur la seule hypothèse, car peu de points O vérifient cette hypothèse. Mais on peut s'aider de la conclusion, donc tracer des angles $\widehat{ODC}$ et $\widehat{OBC}$ égaux pour construire une figure juste.

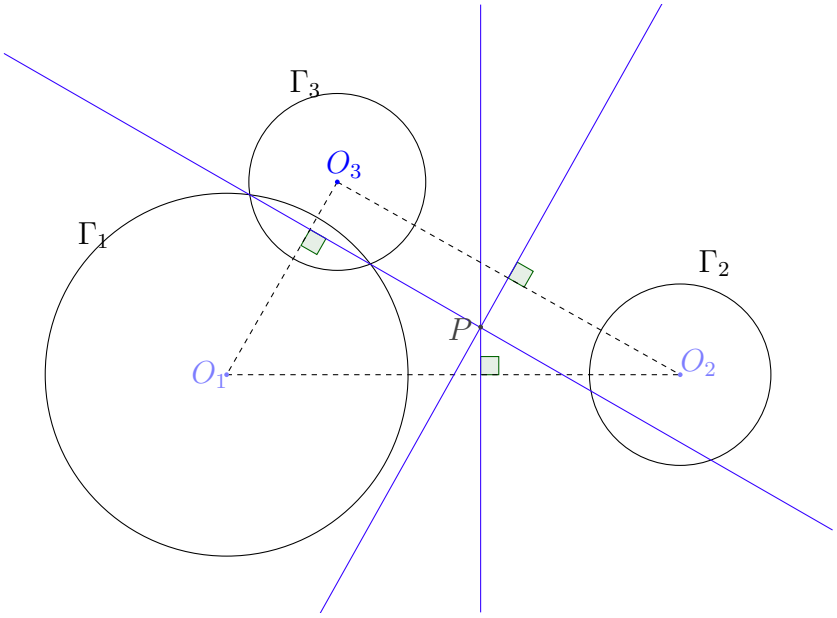
Puissance d'un point par rapport à un cercle / Axe radical



Proposition 83. $PA \cdot PB = PC \cdot PD = PE^2 = PO^2 - r^2$

Démonstration. Comme nous venons de voir dans le dernier exercice, les triangles PAC et PDB sont semblables (par égalité d'angles), d'où : $\frac{PA}{PD}=\frac{PC}{PB} \Leftrightarrow PA \cdot PB = PC \cdot PD$.
Cette quantité ne dépend pas de quelle droite passant par P on utilise, si on utilise la tangente on trouve PE^2, et si on utilise la droite passant par O, on trouve $(PO - r)(PO + r) = PO^2 - r^2$. □

Cette quantité, qui ne dépend pas de la droite passant par P avec laquelle on intersecte Γ, est appelée la puissance du point P par rapport au cercle Γ, et est notée $\mathcal{P}_\Gamma(P)$.
Lorsque qu'on a deux cercles Γ_1 et Γ_2, le lieu des points ayant la même puissance par rapport aux deux cercles est une droite. Elle est perpendiculaire à O_1O_2 (avec O_1 centre de Γ_1 et O_2 centre de Γ_2). Si les deux cercles Γ_1 et Γ_2 se coupent en deux points P et Q, alors leur axe radical est PQ.



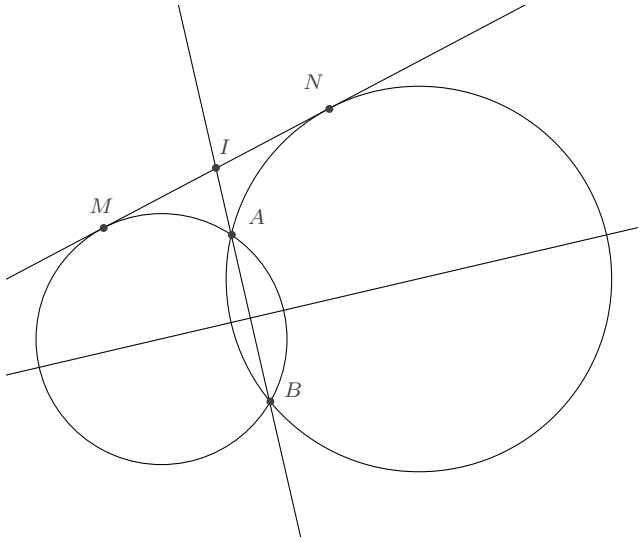
Proposition 84.

Soient Γ_1, Γ_2 et Γ_3 trois cercles. Les trois axes radicaux sont concourrants.

Démonstration. Soient Δ_{12} l'axe radical de Γ_1 et Γ_2, Δ_{23} l'axe radical de Γ_2 et Γ_3 et soit Δ_{13} l'axe radical de Γ_1 et Γ_3.
Soit P le point d'intersection de Δ_{12} et Δ_{23}. Comme P appartient à Δ_{12}, par définition : $\mathcal{P}_{\Gamma_1}(P) = \mathcal{P}_{\Gamma_2}(P)$. P appartient aussi à Δ_{23}, on a donc aussi $\mathcal{P}_{\Gamma_2}(P) = \mathcal{P}_{\Gamma_3}(P)$. Donc : $\mathcal{P}_{\Gamma_1}(P) = \mathcal{P}_{\Gamma_3}(P)$. Donc, P appartient aussi à Δ_{13}, et donc les trois axes radicaux sont concourants. □

Exercice 8 Soient Γ_1, Γ_2 deux cercles qui se coupent en A et en B. Soit Δ une droite tangente aux deux cercles en M et en N. Montrer que (AB) coupe le segment $[MN]$ en son milieu.

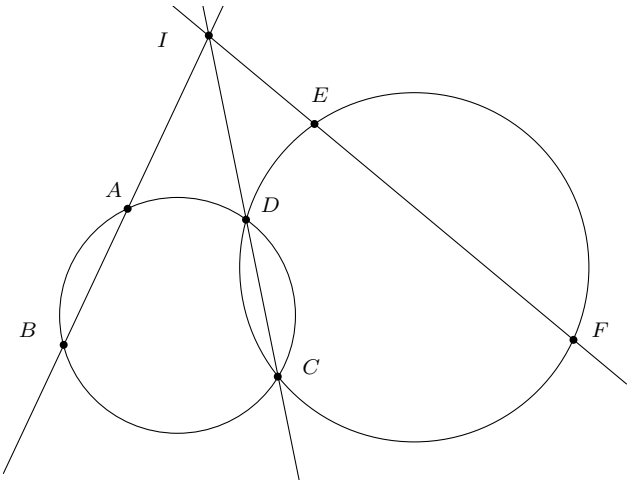
Solution de l'exercice 8



La puissance de I par rapport au premier cercle vaut $IM^2 = IA \cdot IB$. La puissance de I par rapport au deuxième cercle vaut $IA \cdot IB = IN^2$. On en déduit que $IM^2 = IN^2$, d'où $IM = IN$.

Exercice 9 Soient $ABCD$ et $CDEF$ deux quadrilatères inscrits dans deux cercles Γ_1, Γ_2. On suppose que parmi les droites (AB), (CD) et (EF) il n'y en a pas deux qui soient parallèles. Alors les droites (AB), (CD) et (EF) sont concourantes si, et seulement si, les points A, B, E et F sont cocycliques.

Solution de l'exercice 9



Supposons d'abord que les trois droites soient concourantes. Alors la puissance de I par rapport au cercle de gauche vaut $IA \cdot IB = ID \cdot IC$. La puissance de I par rapport au cercle de droite vaut $ID \cdot IC = IE \cdot IF$. On en déduit que $IA \cdot IB = IE \cdot IF$, et donc que A, B, F, E sont cocycliques.

Réciproquement, si A, B, F, E sont cocycliques, notons I le point d'intersection des droites (AB) et (EF). La puissance de I par rapport au cercle circonscrit à $ABFE$ vaut $IA \cdot IB = IE \cdot IF$. Donc I a même puissance par rapport aux deux cercles de la figure. I est donc sur leur axe radical, qui est (DC). Les trois droites (AB), (CD) et (EF) sont donc concourantes en I.

Exercice 10 Soit ABC un triangle. Soit H le pied de la hauteur issue de A. Soient M et N les milieux de $[AB]$ et de $[AC]$. Soit X la deuxième intersection des cercles circonscrits aux triangles BHM et CHN. Montrer que H, X et le milieu de $[MN]$ sont alignés.

Solution de l'exercice 10 D'après l'exercice précédent, il suffirait de montrer que (MN) est tangente aux cercles circonscrits aux triangles BHM et CHN en M et N. En effet, comme (HX) est l'axe radical de ces deux cercles, elle coupera bien $[MN]$ (une tangente commune aux deux cercles) en son milieu.
On a que (MN) est parallèle à (BC) car c'est la droite des milieux. Du coup, par angles alternes-internes, on a $\widehat{MNH} = \widehat{NHC}$. Comme ACH est rectangle en H et que N est le milieu de $[AC]$, on a que $\widehat{NHC} = \widehat{NCH}$. On a donc : $\widehat{MNH} = \widehat{NCH}$, et (MN) est donc bien tangente au cercle circonscrit à NCH en N.
Similairement, on montre que (MN) est aussi tangente au cercle circonscrit à MHB en M, ce qui finit la preuve.

Exercice 11 Dans un triangle ABC, P et Q sont respectivement sur les segments $[AB]$ et $[AC]$ tels que $AP = AQ$. On suppose qu'il existe 2 points S et R sur $[BC]$ avec B, S, R et C alignés dans cet ordre et $\widehat{BPS} = \widehat{PRS}$ et $\widehat{CQR} = \widehat{QSR}$. Montrer que P, S, R et Q sont cocycliques.

Solution de l'exercice 11 Les conditions d'angles signifient que (AP) est tangente au cercle circonscrit de PSR et que (AQ) est tangente au cercle circonscrit de QSR. Soit Γ_1 le cercle circonscrit de PSR et Γ_2 le cercle circonscrit de QSR, et supposons que Γ_1 et Γ_2 soient distincts. Alors $\mathcal{P}_{\Gamma_1}(A) = AP^2$ et $\mathcal{P}_{\Gamma_2}(A) = AQ^2$, donc $\mathcal{P}_{\Gamma 1}(A) = \mathcal{P}_{\Gamma 2}(A)$, donc A appartient à l'axe radical de Γ_1 et Γ_2, c'est-à-dire (BC) (car Γ_1 et Γ_2 s'intersectent en S et R qui appartiennent à (BC)), ce qui est une contradiction. Γ_1 et Γ_2 sont donc identiques, d'où la cocyclicité de P, Q, S et R.

2 Groupe B : géométrie

1 samedi 22 matin : Julien Portier

Dans ce cours, nous allons aborder les notions de base de la géométrie et montrer qu'avec ces notions simples, on peut résoudre une grande partie des exercices d'olympiades.

Chasse aux angles

Nous allons voir dans cette partie comment le calcul d'angles (=la chasse aux angles) peut nous aider à résoudre des problèmes où aucun angle n'apparaissait au départ.

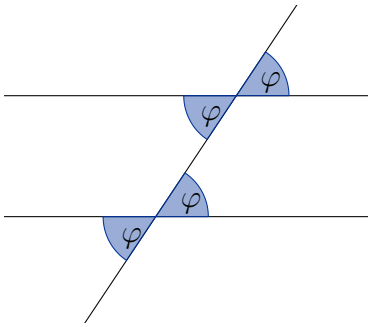
Exemple 85. Soient 2 cercles C1 et C2 se coupant en P et Q. A est le point diamétralement opposé de P sur C1 et B est le point diamétralement opposé de P sur C2. Montrons que A, Q et B sont alignés.

AP est un diamètre de C1, donc $\widehat{AQP} = 90°$. De même, BP est un diamètre de C2, donc $\widehat{BQP} = 90°$. On a alors $\widehat{AQB} = \widehat{AQP} + \widehat{PQB} = 90° + 90° = 180°$ donc A, Q et B sont alignés.

Ainsi, en général, pour prouver que X, Y et Z sont alignés dans cet ordre, il est parfois plus facile de montrer que $\widehat{XYZ} = 180°$.

Rappel du collège :

Proposition 86. Soient trois droites d_1, d_2 et Δ. Les droites d_1 et d_2 sont parallèles (éventuellement confondues) si et seulement si les égalités d'angle de cette figure sont vérifiées :



Proposition.

- si M et N sont du même côté de la droite AB, A, B, M, N sont cocycliques si et seulement si $\widehat{AMB} = \widehat{ANB}$.
- si M et N sont de part et d'autre de la droite AB, A, B, M, N sont cocycliques si et seulement si $\widehat{AMB} = 180° - \widehat{ANB}$.

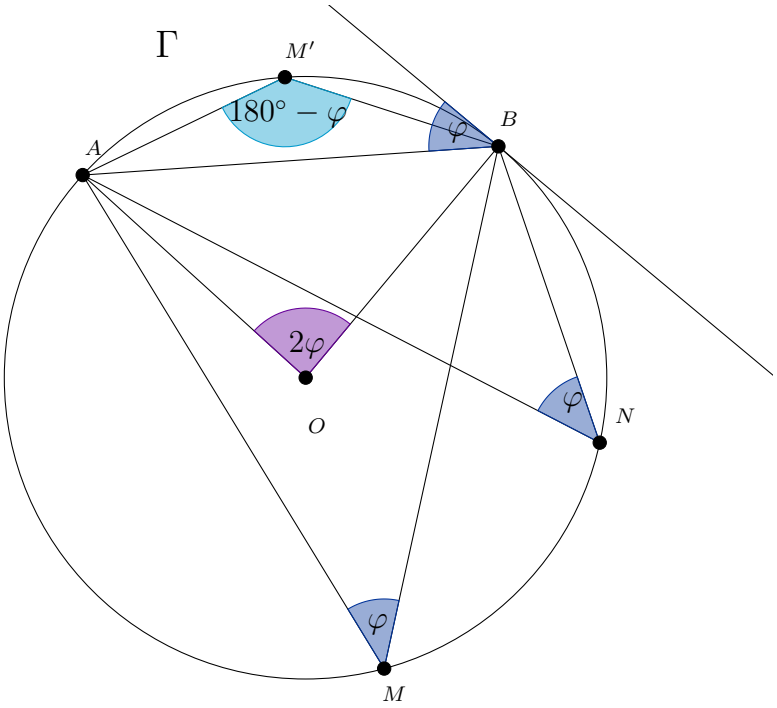
Remarque.

Cette proposition est toujours valable dans le cas limite : pour $N = B$ par exemple BB correspond à la tangente au cercle circonscrit à ABM en B.

Si A, B et M sont sur un cercle de centre O, on a :

- si M et O sont du même côté de la droite AB, $\widehat{AMB} = \frac{\widehat{AOB}}{2}$.
- si M et O sont de part et d'autre de la droite AB, $\widehat{AMB} = (180° - \frac{\widehat{AOB}}{2})$.

On a donc au total toutes ces égalités d'angles :



Exercice 1

Soient Γ_1, Γ_2 deux cercles ayant deux points d'intersection A et B. Soient d_A une droite passant par A et d_B une droite passant par B. On note C et E les points d'intersection de d_A avec Γ_1 et Γ_2 respectivement, et on définit de même D et F comme les points d'intersection de d_B avec Γ_1 et Γ_2 respectivement.

Montrer que les droites CD et EF sont parallèles.

Exercice 2

Théorème de Miquel. Soit ABC un triangle, P un point de BC, Q un point de CA, R un point de AB. Les cercles circonscrits à AQR et à BRP ont pour second oint d'intersection X. Montrer que X est aussi sur le cercle circonscrit à CPQ.

Exercice 3 Soient Γ_1 et Γ_2 deux cercles sécants en A et B. Soit C un point de Γ_1. On note D (respectivement E) l'intersection entre (BC) (respectivement (AC)) et Γ_2. Enfin, on note F l'intersection entre la tangente à Γ_1 en B et la droite (DE).

Montrer que le triangle BDF est isocèle.

Exercice 4 (Théorème du pôle Sud) Soit ABC un triangle et Γ son cercle circonscrit. On note I le centre de son cercle inscrit. La bissectrice issue de A coupe Γ en D.
Montrer que $DB = DC = DI$.

Triangles semblables.

Les quatre conditions suivantes sont deux à deux équivalentes :

- les triangles ABC et $A'B'C'$ sont semblables (ce qui est noté $ABC \sim A'B'C'$),
- $\widehat{A} = \widehat{A'}$, $\widehat{B} = \widehat{B'}$, et $\widehat{C} = \widehat{C'}$,

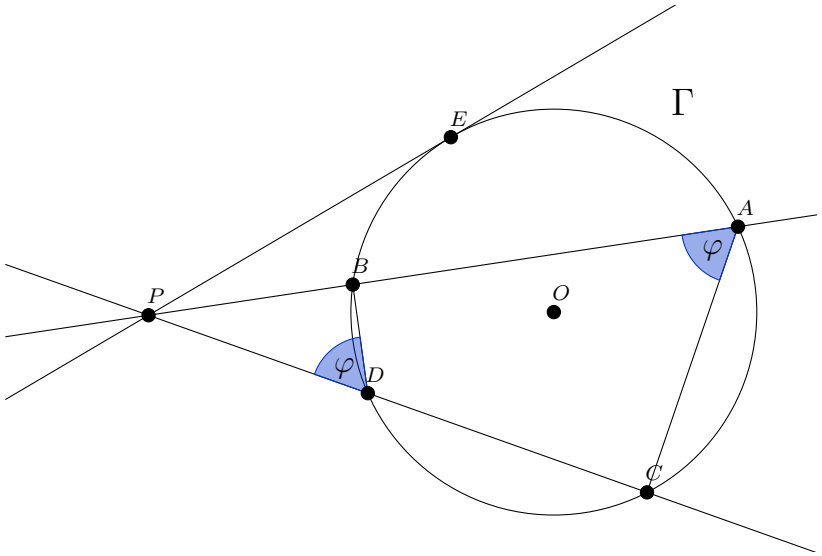
- $\frac{AB}{AC} = \frac{A'B'}{A'C'}$ et $\frac{BC}{BA} = \frac{B'C'}{B'A'}$,
- $\widehat{A} = \widehat{A'}$ et $\frac{AB}{AC} = \frac{A'B'}{A'C'}$.

Remarque 87. Attention, les longueurs dont on prend les rapports dans la troisième condition doivent être celles des segments adjacents aux angles égaux choisis.

Exercice 5 Soit un triangle ABC rectangle en C. Soit H le pied de la hauteur issue de C. Montrer que $CH^2 = AH.BH$

Puissance d'un point par rapport à un cercle.

Soient un cercle Γ de centre O et de rayon r et un point P. On considère trois droites passant par P et coupant le cercle Γ : la première le coupe en A et B, la deuxième en C et D, et la troisième est une tangente au cercle, qu'elle ne coupe donc qu'en un point, E.



On a alors : $PA \times PB = PC \times PD = PE^2 = PO^2 - r^2$.

Démonstration. Par chasse aux angles, on marque les angles φ et on constate que les triangles PAC et PDB sont semblables. Ainsi, $\frac{PA}{PC} = \frac{PD}{PB}$, d'où le résultat. Cet argument marche aussi pour le cas de la tangente. Enfin, lorsqu'on considère la droite PO, on a toujours la même égalité pour $(PO-r)(PO+r)$, ce qui conclut. □

Cette quantité ne dépend donc pas de la droite passant par P avec laquelle on intersecte Γ. Il s'agit de la puissance du point P par rapport au cercle Γ, notée $\mathcal{P}_\Gamma(P)$.

Lorsqu'on a deux cercles Γ_1, de centre O_1, et Γ_2, de centre O_2, le lieu des points ayant la même puissance par rapport au deux cercles est une droite, perpendiculaire à O_1O_2, appelé axe radical. Si les cercles Γ_1 et Γ_2 ont deux points d'intersection A et B, alors leur axe radical est la droite AB.

Exercice 6

Soient deux cercles Γ_1 et Γ_2 s'intersectant en deux points C et D. On considère une tangente commune à ces deux cercles, son point A de tangence à Γ_1 et son point B de tangence à Γ_2.

Montrer que CD coupe AB en son milieu.

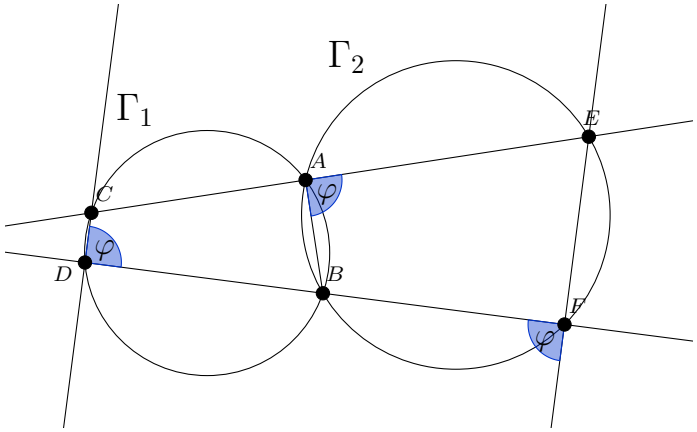
Exercice 7 Dans un triangle ABC, P et Q sont respectivement sur les segments AB et AC tels que $AP = AQ$. On suppose qu'il existe 2 points S et R sur BC avec B, S, R et C alignés dans cet ordre et $\widehat{BPS} = \widehat{PRS}$ et $\widehat{CQR} = \widehat{QSR}$. Montrer que P, S, R et Q sont cocycliques.

Solution de l'exercice 1

Soit $\varphi := \widehat{CDB}$. Comme les points A, B, C, D sont cocycliques, on obtient que $\widehat{BAC} = 180° - \varphi$. De plus, les points C, A, E sont alignés dans cet ordre. Donc $\widehat{BAE} = \varphi$.

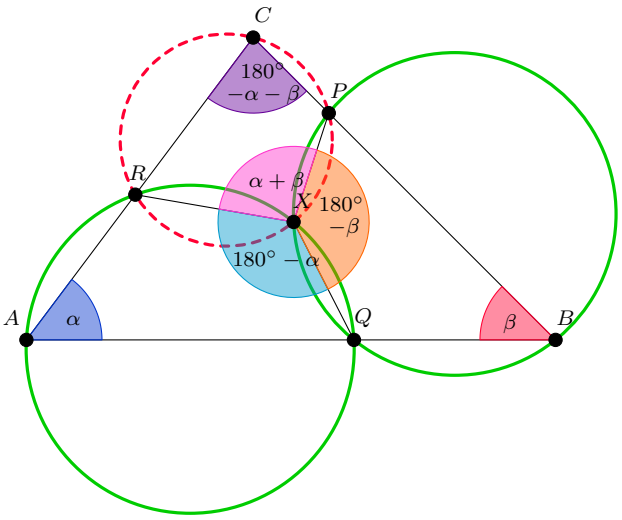
En outre, les points A, B, F, E sont cocycliques. Donc $\widehat{BFE} = 180° - \varphi$.

Donc les droites CD et EF sont parallèles.

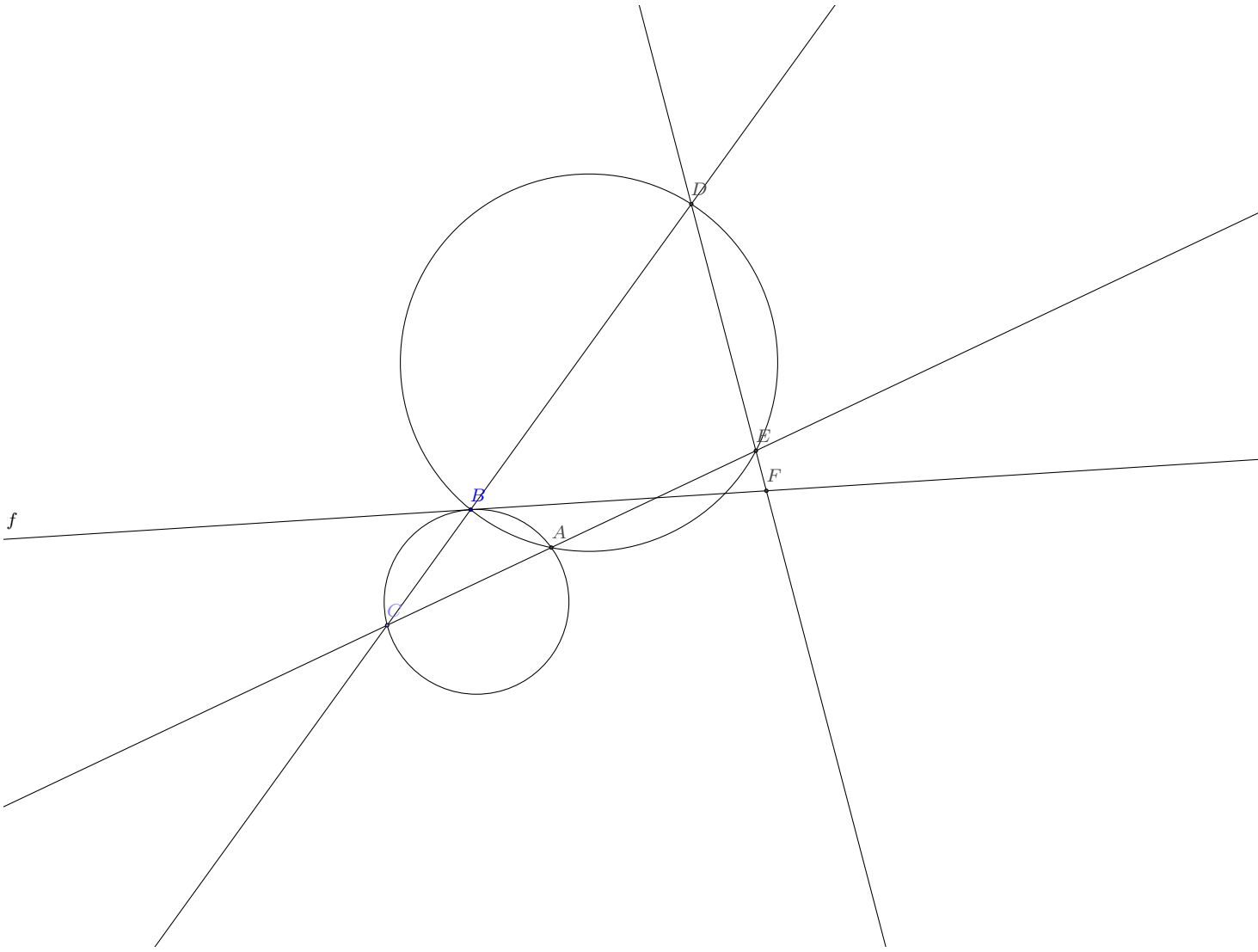


Solution de l'exercice 2

On pose $\alpha := \widehat{BAC}$ et $\beta := \widehat{CBA}$. Comme les points A, Q, R, X sont cocycliques, on a $\widehat{QXR} = 180° - \alpha$. De même, on a aussi $\widehat{PXQ} = 180° - \beta$. On en déduit que $\widehat{RXP} = \alpha + \beta = 180° - \widehat{PXC}$, car $\widehat{PXC} = 180° - \widehat{BAC} - \widehat{CBA} = 180° - \alpha - \beta$. Donc les points C, P, R, X sont également cocycliques.



Solution de l'exercice 3



En général, pour montrer qu'un triangle XYZ est isocèle en X, au lieu de montrer que $XY = XZ$, on peut montrer que $\widehat{XYZ} = \widehat{XZY}$. Dans notre exercice, on va donc montrer que $\widehat{FBD} = \widehat{FDB}$:

$\widehat{FBD} = 180° - \widehat{FBC} = 180° - \widehat{FBA} - \widehat{ABC} = 180° - \widehat{BCA} - \widehat{ABC} = \widehat{CAB} = \widehat{EAB} = \widehat{EDB} = \widehat{FDB}$

ce qui montre que le triangle FBD est isocèle en F.

Solution de l'exercice 4 Montrons que BDI est isocèle en I. On a $\widehat{IBC} = \beta/2$ et $\widehat{CBD} = \widehat{CAD} = \alpha/2$, donc $\widehat{IBD} = \alpha/2 + \beta/2$. De plus, $\widehat{BID} = 180° - \widehat{BIA} = \widehat{IBA} + \widehat{IAB} = \alpha/2 + \beta/2$. Donc $BD = ID$. De même, on montre que $CD = ID$, ce qui finit la preuve.

Solution de l'exercice 5 On va montrer que CHB et AHC sont semblables : on a $\widehat{AHC} = \widehat{BHC} = 90°$, et $\widehat{HAC} = 90° - \widehat{HBC} = \widehat{HCB}$, on a 2 paires d'angles identiques, donc CHB et AHC sont semblables. On a alors $\frac{CH}{HB} = \frac{AH}{HC}$ d'où $CH^2 = AH.BH$.

Solution de l'exercice 6

Soit M le point d'intersection de CD et de AB. Comme la droite CD est l'axe radical des cercles Γ_1 et Γ_2, le point M, qui lui appartient, vérifie $\mathcal{P}_{\Gamma_1}(M) = \mathcal{P}_{\Gamma_2}(M)$. Or $\mathcal{P}_{\Gamma_1}(M) = MA^2$ et $\mathcal{P}_{\Gamma_2}(M) = MB^2$. Donc $MA^2 = MB^2$ ce qui signifie que M est le milieu du segment AB.

Solution de l'exercice 7 Les conditions d'angles signifient que (AP) est tangente au cercle circonscrit de PSR et que (AQ) est tangente au cercle circonscrit de QSR. Soit Γ_1 le cercle circonscrit de PSR et Γ_2 le cercle circonscrit de QSR, et supposons que Γ_1 et Γ_2 soient distincts. Alors $\mathcal{P}_{\Gamma 1}(A) = AP^2$ et $\mathcal{P}_{\Gamma 2}(A) = AQ^2$, donc $\mathcal{P}_{\Gamma 1}(A) = \mathcal{P}_{\Gamma 2}(A)$, donc A appartient à l'axe radical de Γ_1 et Γ_2, c'est-à-dire (BC) (car Γ_1 et Γ_2 s'intersectent en S et R qui appartiennent à (BC)), ce qui est une contradiction. Γ_1 et Γ_2 sont donc identiques, d'où la cocyclicité de P, Q, S et R.

2 samedi 22 après-midi : Cécile Gachet

Introduction.

On montre ici diverses applications de la méthode de la chasse aux angles et de la puissance d'un point par rapport à un cercle.

Quelques théorèmes montrés ou utilisés dans ce cours.

Ces résultats sont recyclables, et servent souvent pour résoudre des exercices de géométrie : ils sont à retenir. Pour plus de détails, se référer au cours de géométrie de Pierre Dehornoy.

- **Théorème des axes radicaux :** les axes radicaux de trois cercles donnés (pris deux à deux) sont concourants, parallèles ou confondus (c'est le théorème 5 du polycopié de Dehornoy).
- **Théorème du cube :** soient $A, B, C, D, A', B', C', D'$ des points tels que A, B, C, D et A, B, A', B' et B, C, B', C' et C, D, C', D' et D, A, D', A' sont cocycliques. Alors A', B', C', D' sont aussi cocycliques (ce résultat est prouvé dans l'exercice 17 du polycopié de Dehornoy).
- **Triangle orthique :** il s'agit du triangle formé par les pieds des hauteurs dans un triangle donné. Il vérifie d'intéressantes propriétés (voir le théorème 8 du polycopié de Dehornoy).
- **Droite de Simpson :** soit ABC un triangle. Un point P appartient à son cercle circonscrit si et seulement si ses projetés orthogonaux sur les trois côtés du triangle sont alignés. Cette droite est alors appelée droite de Simpson (ce résultat est établi par l'exercice 13 du polycopié de Dehornoy).

Et quelques exercices...

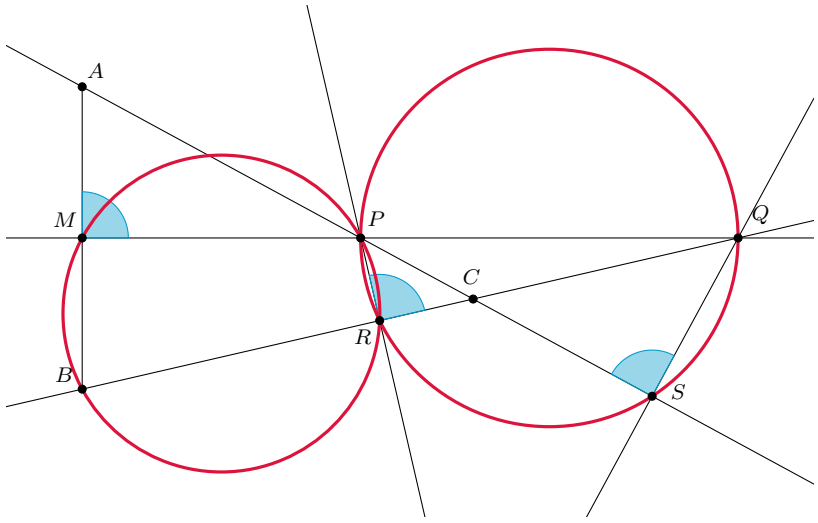
Ces exercices n'ont, certes, pas valeur de théorème, mais ils constituent des applications plus ou moins directes des principes déjà exposés : il est bon d'en chercher le plus possible pour se familiariser avec ces méthodes.

Exercice 1

Soient ABC un triangle, M le milieu de $[AB]$. La médiatrice de $[AB]$ coupe (AC) en P et (BC) en Q. Soient R et S les projetés orthogonaux de P sur (BC) et de Q sur (AC) respectivement.

Montrer que M, R, S sont alignés.

Solution de l'exercice 1



Les angles droits nous permettent tout d'abord d'établir que M, P, R, Q et Q, P, R, S sont cocycliques. On fait une chasse aux angles :

$$\begin{aligned}
\widehat{MRS} &= \widehat{MRP} + \widehat{PRQ} + \widehat{QRS} \\
&= \widehat{MBP} + 90° + \widehat{QRS} \text{ car } M, P, R, B \text{ sont cocycliques,} \\
&= \widehat{MBP} + 90° + \widehat{QPS} \text{ car } Q, P, R, S \text{ sont cocycliques,} \\
&= \widehat{MBP} + 90° + \widehat{APM} \\
&= 90° + \widehat{MAP} + \widehat{APM} \text{ car } APM \text{ isocèle en } P, \\
&= 180°
\end{aligned}$$

Donc M, R, S sont alignés.

Exercice 2

Soient ABC un triangle, M le milieu de $[AB]$. Soient x la demi-droite issue de A et du même côté de (AB) que C telle que $\widehat{xAB} = \widehat{ACM}$ et y la demi-droite issue de B et du même côté de (AB) que C telle que $\widehat{yBA} = \widehat{BCM}$.

Montrer que $x, y, (CM)$ sont concourantes.

Solution de l'exercice 2

La condition donnée sur les angles nous donne tout de suite envie de tracer les cercles circonscrits à ACX et BCY, où $X = (CM) \cap x$ et $Y = (CM) \cap y$.

En effet, ces cercles ont pour tangente commune (AB), donc, en regardant la puissance de M par rapport à ces cercles :

$$MX \cdot MC = MA^2 = MB^2 = MY \cdot MC$$

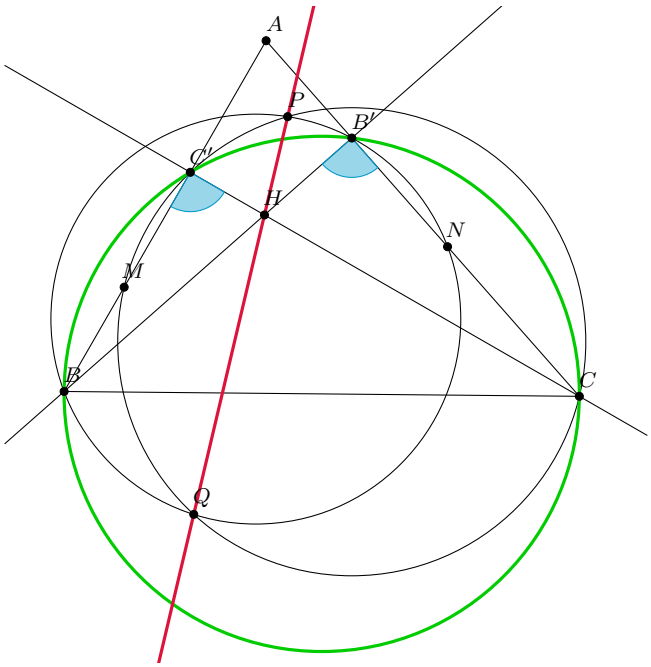
Donc $MX = MY$, et X, Y sont du même côté de M. Donc $X = Y$, d'où le concours de $x, y, (CM)$.

Exercice 3

Soient ABC un triangle, H son orthocentre. Soient M un point quelconque à l'intérieur du segment AB et N un point quelconque à l'intérieur du segment AC. On nomme P et Q les deux points d'intersection des cercles de diamètre BN et de diamètre CM.

Montrer que les points P, Q, H sont alignés.

Solution de l'exercice 3



Soit B' le pied de la hauteur issue de B et C' le pied de la hauteur issue de C.

Comme $\widehat{BB'N} = 90°$, B' appartient au cercle de diamètre BN. Donc les points B, B', N, P, Q sont cocycliques. De même, les points C, C', M, P, Q sont cocycliques.

De plus, l'axe radical de ces deux cercles est la droite PQ. Donc, pour montrer que le point H appartient à PQ, il suffit de montrer que la puissance de H par rapport aux cercles circonscrits à $BB'NPQ$ et à $CC'MPQ$ est la même. Il suffit donc de montrer que $HB \times HB' = HC \times HC'$: c'est exactement la puissance de H par rapport au cercle de diamètre $[BC]$, circonscrit à $BB'CC'$.

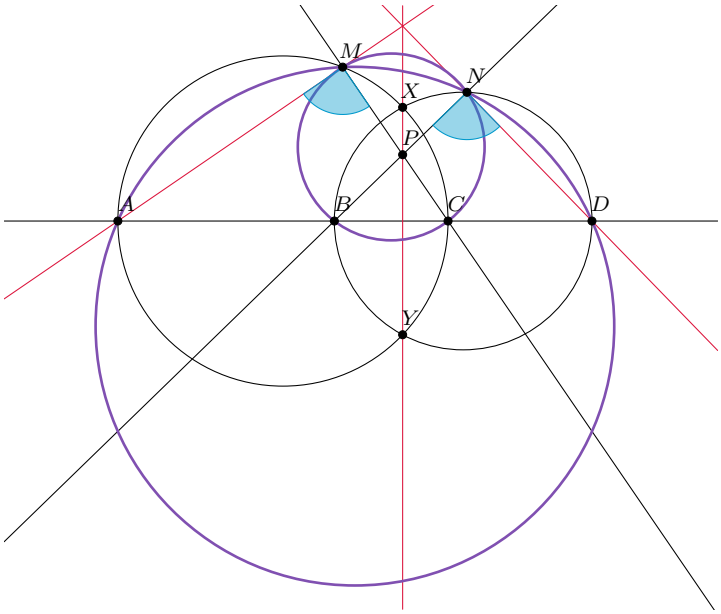
Donc P, Q, H sont alignés.

Exercice 4

Soient A, B, C, D quatre points alignés en cet ordre. On considère Γ_1 le cercle de diamètre $[AC]$ et Γ_2 le cercle de diamètre $[BD]$. Ils se coupent en X, Y. Soient P un point de (XY) quelconque, $M = (CP) \cap \Gamma_2$ et $N = (BP) \cap \Gamma_1$.

Montrer que les droites $(AM), (BN), (XY)$ sont concourantes.

Solution de l'exercice 4



D'après le théorème des axes radicaux, il suffit de montrer que A, M, D, N sont cocycliques pour conclure.

Or $\widehat{AMN} + \widehat{NDA} = 180°$ si et seulement si $\widehat{CMN} = \widehat{CBN}$, car $\widehat{AMC} = \widehat{BND} = 90°$ par construction.

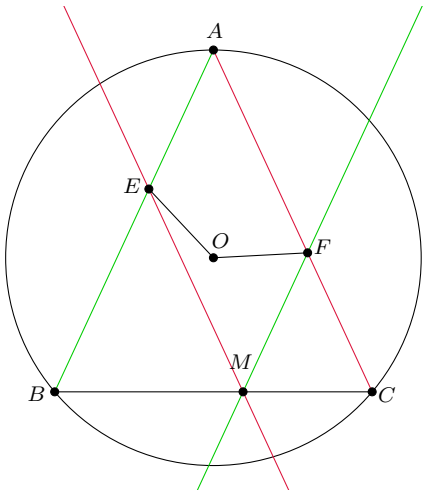
Il suffit donc de montrer que B, C, M, N sont cocycliques, i.e. $PB \cdot PN = PC \cdot PM$. On reconnaît ici la puissance de P par rapport à Γ_1 et par rapport à Γ_2, et ces deux puissances sont bien égales comme $P \in (XY)$. Ce qui conclut.

Exercice 5

Soient ABC un triangle isocèle en A et M un point quelconque de $[BC]$. Soient E l'intersection de la parallèle à (AC) passant par M et de (AB) et F l'intersection de la parallèle à (AB) passant par M et de (AC).

Montrer que E et F sont à la même distance du centre du cercle circonscrit à ABC.

Solution de l'exercice 5



Si on comprend bien E et F (ils sont sur des droites intéressantes), le point O sort un peu de nulle part : on peut donc simplifier l'énoncé en montrant que la puissance de E et de F

est la même par rapport au cercle circonscrit à ABC. Il suffit donc de montrer que $EA \cdot EB = FA \cdot FC$.

Calculons toutes les distances en jeu avec le théorème de Thalès :

$$FA = \frac{AC \cdot MB}{BC}$$
$$FC = \frac{AC \cdot MC}{BC}$$
$$EA = \frac{AB \cdot MC}{CB}$$
$$EB = \frac{AB \cdot MB}{CB}$$

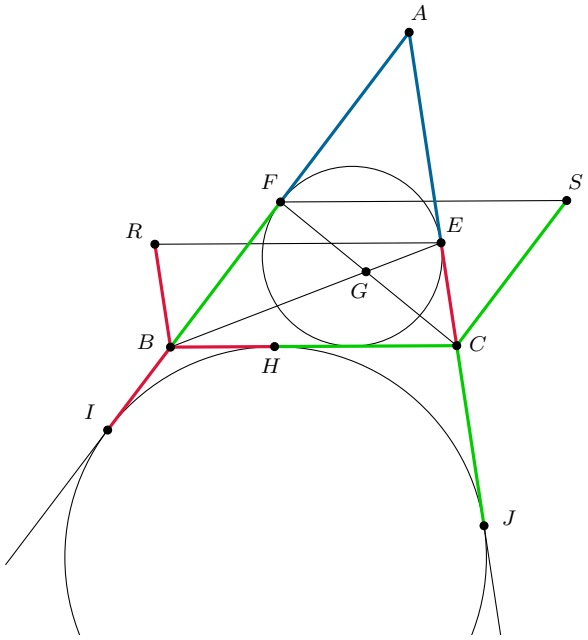
En multipliant, comme $AB = AC$, on obtient l'identité voulue.

Exercice 6

Soit ABC un triangle. On note E et F les points de tangence de son cercle inscrit sur les côtés $[AC]$ et $[BF]$ respectivement. Soit $G = CF \cap BE$. Soient enfin R et S tels que $BCER$ et $BCSF$ soient des parallélogrammes.

Montrer que $GR = GS$.

Solution de l'exercice 6



On prouve tout d'abord le lemme suivant : soient un cercle et un point P. Les points de tangence A et B des tangentes au cercle passant par P vérifient : $PA = PB$. Il suffit, pour montrer cela, d'écrire la puissance de P par rapport au cercle.

Sur la figure, deux longueurs de la même couleur sont donc égales : il s'agit d'ailleurs d'un résultat à part entière, à retenir ! (ce n'est pas complètement évident : on laisse au lecteur le soin d'écrire le système d'égalités au besoin).

On constate ainsi que la puissance de B par rapport au cercle exinscrit tracé est égale à BR^2 et que la puissance de E par rapport à ce cercle est égale à BC^2, donc à ER^2. Ainsi, l'axe radical du cercle exinscrit et du cercle de centre R et de rayon zéro est la droite (BE).

On montre de même que l'axe radical du cercle exinscrit et du cercle de centre S et de rayon zéro est la droite (CF).

Donc $G = (BE) \cap (CF)$ est sur l'axe radical du cercle de centre R et de rayon zéro et du cercle de centre S et de rayon zéro également, d'après le théorème des axes radicaux. Donc $GR = GS$.

3 dimanche 23 matin : Vincent Bouis

Exercice 1 Soit ABC un triangle isocèle en A. Soit I le centre du cercle inscrit de ABC. Soit ω le cercle tangent aux demi-droites $[AB)$ et $[AC)$ en B et C. Montrer que I est sur ω.

Exercice 2 Soit ABC un triangle. Soient A', B', C' les milieux des côtés [BC], [CA], [AB] respectivement. Soient H_A, H_B, H_C les pieds des hauteurs issues de A, B, C respectivement. Montrer que A', B', C', H_A, H_B, H_C sont sur un même cercle.

Exercice 3 Soit ABC un triangle. Soient A_1 et A_2 tels que A_1, B, C, A_2 soient alignés dans cet ordre, et vérifiant $A_1B = AC$ et $CA_2 = AB$. On définit de même B_1, B_2, C_1 et C_2. Montrer que A_1, A_2, B_1, B_2, C_1 et C_2 sont cocycliques.

Exercice 4 Soit ABC un triangle acutangle, H son orthocentre, O le centre de son cercle circonscrit. Montrer que les angles $\widehat{BAH} = \widehat{OAC}$.

Exercice 5 Soit S le pôle sud de A dans le triangle ABC. Montrer que la tangente au cercle circonscrit de ABC en S est parallèle à la droite (BC).

Exercice 6 Soit ABC un triangle. Soient B' et C' des points sur les côtés (AB) et (AC) respectivement tels que B, C, B', C' soient cocycliques. Soit O le centre du cercle circonscrit de AB'C'. Montrer que (AO) et (BC) sont perpendiculaires.

Exercice 7 Soit ABC un triangle et D le pied de la bissectrice issue de A. Soient ω, ω_1 et ω_2 les cercles circonscrits des triangles ABC, ABD et ACD respectivement. Soient enfin O, O_1 et O_2 les centres de ω, ω_1 et ω_2 respectivement. Montrer que $OO_1 = OO_2$.

Exercice 8 Soit ABC un triangle. Soit H le pied de la hauteur issue de A. Soient M et N les milieux de [AB] et de [AC]. Soit X la deuxième intersection des cercles circonscrits aux triangles BHM et CHN. Montrer que H, X et le milieu de [MN] sont alignés.

Exercice 9 Soit ABC un triangle acutangle (qui n'a que des angles aigus). On définit ω comme le cercle tangent aux droites (AB) en M et (AC) en N, et tangent intérieurement au cercle circonscrit de ABC. Soient X et Y les milieux de [AM] et de [AN]. Soient X' et Y' les intersections de la droite (XY) avec le cercle circonscrit de ABC. Montrer que X' et Y' sont les milieux des petits arcs AB et AC.

Exercice 10 Soit ABC un triangle et M un point sur la bissectrice intérieure de l'angle $\widehat{BAC}$. On suppose que le cercle tangent en M à la droite (CM) passant par A recoupe le cercle circonscrit de ABC en P et la droite AB en Q. Enfin soit R la seconde intersection de la droite CM avec le cercle ABC. Montrer que P, Q et R sont alignés.

Exercice 11 Soit ABC un triangle. Soit ω_A le cercle tangent aux droites (AB) et (AC) et tangent intérieurement au cercle circonscrit de ABC. On définit de même ω_B et ω_C. Soient T_A, T_B et T_C les points de tangence de ω_A, ω_B et ω_C avec le cercle circonscrit de ABC. Montrer que les droites (AT_A), (BT_B), (CT_C) sont concourantes.

Exercice 12 Soit ABC un triangle. On choisit trois points P, Q et R respectivement sur les côtés (BC), (CA) et (AB) du triangle. Soient ω_1, ω_2 et ω_3 les cercle circonscrits aux triangles AQR, BRP et CPQ.
a) Montrer qu'il existe un point M à la fois sur ω_1, ω_2 et ω_3.
On définit maintenant X, Y et Z sur les cercles ω_1, ω_2 et ω_3 respectivement tels qu'ils soient sur la droite (AP) (différents de A et de P).
b) Montrer que $\frac{YX}{XZ} = \frac{BP}{PC}$.

3 Groupe C : arithmétique

1 samedi 22 matin : Gabriel Pallier

Les rappels de cours sont ici succints, et comprennent seulement l'enchaînement des propriétés importantes. Pour un traitement plus complet, on pourra consulter les cours de l'OFM disponible sur le site.

Divisibilité

L'arithmétique de $\mathbb{Z}$ est l'étude de la relation de divisibilité dans $\mathbb{Z}$. On dit que a divise b, noté $a \mid b$ s'il existe $k \in \mathbb{Z}$ tel que $b = ak$. L'arithmétique de $\mathbb{Q}$ ou de $\mathbb{R}$ est sans intérêt ; mais celle de $\mathbb{Z}$ donne très vite lieu à des énoncés riches et difficile.

Division euclidienne Nous commencerons ici par rappeler une propriété forte de l'arithmétique de $\mathbb{Z}$: l'existence d'une division euclidienne.

Proposition 88. Soient a et b dans $\mathbb{Z}$, avec b non nul. Il existe un unique couple (q, r) avec $q \in \mathbb{Z}$ et $0 \leqslant r < |b|$ tel que $a = bq + r$.

P.G.C.D Rappelons sa définition

Définition 89. Soient a et b dans $\mathbb{Z}$. Un pgcd de a et b est un élément $c \in \mathbb{Z}$ tel que

$$d \mid a \quad \text{et} \quad d \mid b \iff d \mid c$$

Autrement dit, c'est un plus grand élément parmi les diviseurs communs, au sens de la relation de divisibilité. S'il existe, un pgcd est unique au signe près. En effet, si d_1 et d_2 sont deux pgcd alors $d_1 \mid d_2$ et $d_2 \mid d_1$, ce qui implique directement que $d_1 = \pm d_2$.

Notation 90. On écrira ici (a, b) pour désigner le pgcd positif de a et de b, s'il existe. Attention : on ne sait pas encore s'il existe.

Proposition 91. Pour tous a et b dans $\mathbb{Z}$ et $k \in \mathbb{Z}$, et sous réserve d'existence des pgcd en question, nous avons

$$\begin{aligned} (a, b) &= (b, a) \\ (a, b) &= (a, a + kb) \\ (0, a) &= a \end{aligned}$$

Les règles précédentes sont tout ce qu'il faut pour mettre en route l'algorithme d'Euclide.

Algorithme d'Euclide En voici une description rapide :

Algorithme 1. Entrée : a et b entiers naturels, $0 \leqslant a \leqslant b$, non tous deux nuls.
Sortie : un pgcd de a et b.
Si $a = 0$, renvoyer b
Sinon, recommencer avec (r, a) où r est le reste dans la division euclidienne de b par a.

L'algorithme d'Euclide termine et renvoie un entier : le plus grand des deux entiers auquel on l'applique est un monovariant strict. La quantité (a, b) est un invariant d'après les règles précédentes, et l'existence est finalement transférée à (a, b).

Remarque 92. L'algorithme d'Euclide constitue une preuve effective d'existence du pgcd dans $\mathbb{Z}$ (pour deux entiers non tous deux nuls).

Passons aux premiers exercices :

Exercice 1 (IMO 1959) Montrer que pour tout $n \in \mathbb{Z}$, la fraction $\frac{21n+4}{14n+3}$ est irréductible.

Solution de l'exercice 1 Voici une solution en une ligne :

$$(21n + 4, 14n + 3) = (7n + 1, 14n + 3) = (7n + 1, 7n + 2) = (1, 2) = 1$$

Exercice 2 On se donne $n, m \in \mathbb{N}$ et a un entier supérieur ou égal à 1. Calculer $(a^n - 1, a^m - 1)$.

Solution de l'exercice 2 On peut supposer $n \geqslant m$. Ecrivons $n = mq + r$ avec $0 \leqslant r < m$ la division euclidienne de n par m. Alors $a^m - 1$ divise $a^{mq} - 1$ puisque $a^{mq} - 1 = (a^m - 1)\left(1 + a^m + \cdots + a^{m(q-1)}\right)$ donc

$$\begin{aligned}(a^n - 1, a^m - 1) &= (a^r (a^{mq} - 1) + a^r - 1, a^m - 1) \\ &= (a^r - 1, a^m - 1)\end{aligned}$$

D'après l'algorithme d'Euclide,

$$(a^n - 1, a^m - 1) = \left(a^{(n,m)} - 1, a^0 - 1\right) = a^{(n,m)} - 1$$

Exercice 3 On note Fib_k le k-ième terme de la suite de Fibonacci, définie avec $\mathrm{Fib}_0 = 0$, $\mathrm{Fib}_1 = 1$. Montrer que si a et b sont deux entiers, $a \leqslant b$ et n est tel que $F_n \leqslant a < F_{n+1}$, alors la mise en oeuvre de l'algorithme d'Euclide pour a et b nécessite au plus n divisions euclidiennes.

Solution de l'exercice 3 Supposons que l'algorithme termine en N étapes. D'après l'algorithme d'Euclide on peut écrire $a = a_N$ et $b = b_N$, avec les relations de récurrence $a_0 = 0$, $b_0 = d$.

$$\begin{aligned}a_{n+1} &= b_n \\ b_{n+1} &= q_n b_n + a_n\end{aligned}$$

Avec $q_n \geqslant 1$, d'où : $b_{n+1} = q_n b_n + b_{n-1} \geqslant b_n + b_{n-1}$. En faisant remonter ces inégalités de proche en proche, on en déduit ce que l'on souhaitait.

Théorèmes de Bezout et de Gauss Allons un peu plus loin dans les conséquences de l'algorithme d'Euclide

Théoréme 93. Pour tous a et b dans $\mathbb{Z}$. Alors il existe u et v tels que

$$au + bv = (a, b)$$

De plus, u et v sont calculables, tout comme le pgcd, à l'aide de l'algorithme d'Euclide.

Démonstration.

Si $a = 0$ alors $u = 0$, $v = 1$ convient.

Sinon, écrivons $b = aq + r$, et soient u', v' tels que $ru' + v'a = (r, a) = (a, b)$.

Alors $(b - aq)\, u' + av' = (a, b)$ donc on peut prendre $u = v' - qu'$ et $v = u'$. On termine en réitérant cette étape, d'après l'algorithme d'Euclide.

□

On appelle parfois le calcul des coefficients de Bezout u et v "algorithme d'Euclide étendu". Les retombées théoriques importante sont l'inversibilité modulo n, et la simplification dans les congruences, traitées plus loin.

Théoréme 94. Si $a \mid bc$ et si a est premier à b alors $a \mid c$.

Démonstration. On écrit $bc = ka$. Le théorème de Bezout fournit l'existence de u et v tels que $auc + bvc = c$, donc $auc + kav = c$, ce qui donne finalement $a \mid c$.

□

Exercice 4 On se donne a et b premiers entre eux, $n \geqslant 1$ un entier. Montrer que

$$\left(b\frac{a^n - b^n}{a - b}, a - b\right) = (a - b, n)$$

Solution de l'exercice 4 Calculons :

$$\begin{aligned}
\left(b\frac{a^n - b^n}{a - b}, a - b\right) &= \left(\sum_{k=0}^{n-1} a^k b^{n-k}, a - b\right) \\
&= \left(\sum_{k=0}^{n-1} \left(a^k b^{n-k} - b^n\right) + nb^n, a - b\right) \\
&= \left(\sum_{k=0}^{n-1} \left(a^k - b^k\right) b^{n-k} + nb^n, a - b\right) \\
&= (nb^n, a - b)
\end{aligned}$$

La dernière ligne venant de ce que $a - b$ divise $a^k - b^k$ pour $k \geqslant 1$. b est premier à a, donc b^n est premier à $a - b$. Donc si d divise $a - b$, il est premier à b^n ; d'après le lemme de Gauss s'il divise nb^n alors il divise n. Finalement on retrouve $(nb^n, a - b) = (n, a - b)$.

Nombres premiers

Un nombre $p \in \mathbb{Z}$ est dit premier si ses uniques diviseurs sont ± 1 et $\pm p$.

Exercice 5 Montrer que $n^4 + 4^n$ n'est jamais premier si $n \geqslant 2$.

Solution de l'exercice 5 Si n est pair, n^4+4^n est pair et n'est pas égal à 2 ; en particulier il n'est pas premier. Sinon $n=2k+1$, et d'après la factorisation de Germain

$$\begin{aligned} n^4+4^n &= n^4+4\cdot\left(2^k\right)^4 \\ &= \left(n^2+2\cdot 2^{2k}\right)^2-4\cdot 2^{2k} \\ &= \left(n^2+2\cdot 2^{2k}-2\cdot 2^k\right)\left(n^2+2\cdot 2^{2k}+2\cdot 2^k\right) \end{aligned}$$

Il reste à voir que cette factorisation n'est pas triviale. Pour $n\geqslant 3$ on a l'encadrement

$$1<n^2+2\cdot 2^{2k}-2\cdot 2^k<n^4+4^n$$

ce qui permet de conclure.

lemme d'Euclide On peut voir ce lemme comme un cas particulier de celui de Gauss

Lemme 95. Soit p un nombre premier, $p\mid ab$. Alors $p\mid a$ ou $p\mid b$.

Exercice 6 Montrer que si n est un nombre premier, alors n divise $\binom{n}{k}$ pour tout k tel que $0<k<n$.

Solution de l'exercice 6 Si n est premier, alors pour tout k tel que $0<k<n$, n divise $n!=\binom{n}{k}k!\,(n-k)!$ donc l'un des trois termes de ce produit. Or n ne divise ni $k!$ ni $(n-k)!$, donc n divise $\binom{n}{k}$.

Théorème fondamental de l'arithmétique Utilisé couramment depuis les Eléments d'Euclide, c'est Gauss qui a été le premier à juger nécessaire de le démontrer en 1801.

Théoréme 96. Soit $n\in\mathbb{Z}$ non nul. Il existe une unique décomposition de n (à l'ordre des facteurs près) sous la forme

$$n=\pm p_1^{\alpha_1}\cdots p_r^{\alpha_r}$$

où les p_i sont premiers.

Nous ne ferons pas de preuve de ce théorème ici. Observons seulement que l'unicité découle du lemme de Gauss énoncé plus haut, tandis que l'existence peut se démontrer par récurrence.

Avec le théorème de décomposition vient le concept de valuation p-adique

Définition 97. Soit p un nombre premier et $n\in\mathbb{Z}$ non nul. La valuation p-adique de n, notée $\nu_p(n)$, est le plus grand entier k tel que p^k divise n.

Ainsi, par exemple $\nu_2(2014)=1$ tandis que $\nu_2(2016)=5$. D'après le théorème fondamental, un entier non nul est la donné de l'ensemble de ses valuations p-adiques. Le pgcd s'exprime à partir des valuations p-adiques sous la forme

$$\nu_p((n,m))=\min\left(\nu_p(m),\nu_p(n)\right)$$

Toutefois, il faut garder à l'esprit que cette expression n'est d'aucune utilité pratique pour calculer un pgcd, puisque décomposer n et m en facteurs premiers est un problème bien plus difficile que de leur appliquer l'algorithme d'Euclide. Pour illustrer l'intérêt de raisonner en valuation, revenons à la preuve de l'irrationalité de $\sqrt{2}$; on suppose par l'absurde $\sqrt{2}=p/q$;

ceci donne $p^2/q^2 = 2$ mais alors $\nu_2(p^2) = 2\nu_p(q) + 1$ ce qui est absurde (on peut aussi procéder par descente infinie).

Voici une preuve de l'infinitude de l'ensemble $\mathcal{P}$ des nombres premiers.

Exercice 7 On pose $F_n = 2^{2^n} + 1$; ce nombre est appelé n-ième nombre de Fermat.

(a) Montrer que deux nombres de Fermats distincts sont toujours premiers entre eux.

(b) En déduire une (nouvelle) preuve que l'ensemble $\mathcal{P}$ des nombres premiers est infini [Polya]

Solution de l'exercice 7

(a) Soient n et m distincts, supposons par exemple $n < m$ et d diviseur de F_n et F_m. d est impair, et $d \mid F_n - F_m$, soit

$$d \mid 2^{2^n}\left(2^{2^m - 2^n} + 1\right)$$

d étant premier avec 2^{2^n}, d'après le lemme de Gauss il divise $2^{2^m-2^n}+1$, donc aussi $2^{2^m}+2^{2^n} = F_n + F_m - 2$. Donc $d \mid 2$, mais d est impair donc $d = 1$.

Autre solution : on peut montrer par récurrence que

$$F_{n+1} = F_0 \cdots F_n + 2$$

(b) Supposons par l'absurde que $\mathcal{P}$ contient N éléments et considérons les nombres $F_1, \ldots F_{N+1}$. Ceux-ci sont $\geqslant 2$ donc admettent au moins un diviseur premier ; soit q_j le plus petit diviseur premier de F_j. D'après le principe des tiroirs il existe i et j différents tels que $q_i = q_j$; mais alors F_i et F_j ne sont pas premiers entre eux, ce qui entraîne une contradiction.

Exercice 8 Soit b un entier, $b \geqslant 2$ et z_n le nombre de zéros à la fin de l'écriture de $n!$ en base b. Montrer que si p est le plus grand diviseur premier de b alors pour tout n on a que

$$z_n < \frac{n}{p-1}$$

Solution de l'exercice 8 Si $n!$ s'écrit avec z_n zéros à la fin en base b, c'est que z_n est le plus grand entier k tel que b^k divise $n!$. En particulier, p^{z_n} divise $n!$, donc nous avons l'inégalité $z_n \leqslant \nu_p(n!)$. Or

$$\nu_p(n!) \quad = \quad \nu_p(1) + \cdots + \nu_p(n)$$

Parmi les entiers de 1 à n, il y en a $\lfloor n/p^k \rfloor$ dont la valuation p-adique est au moins k. Par conséquent nous avons (formule de Legendre)

$$\nu_p(n!) = \sum_{k \geqslant 0} \lfloor n/p^k \rfloor$$

Cette somme est bien finie car les termes sont nuls à partir d'un certain rang N. Dès que $k \geqslant N$, nous avons $0 < n/p^k < 1$, donc

$$\nu_p(n!) < \sum_{k=0}^{N} \frac{n}{p^k} = n\frac{1 - p^{-N-1}}{1-p} < \frac{n}{p-1}$$

Remarque : on pourrait montrer (ce n'est pas beaucoup plus difficile) que $\frac{z_n}{n}$ tend vers $\frac{1}{p-1}$ quand n tend vers $+\infty$.

Congruences

Définition 98. On dit que a et b sont congrus modulo n, ce que l'on note $a \equiv b \bmod n$ ou encore $a \equiv b\,[n]$, si $n \mid a - b$.

On peut vérifier que les opérations dans $\mathbb{Z}$ passent au quotient modulo n : si $a_1 \equiv a_2$ et $b_1 \equiv b_2 \bmod n$ alors modulo n

$$\begin{aligned} a_1 + b_1 &\equiv a_2 + b_2 \quad [n] \\ a_1 \times b_1 &\equiv a_2 \times b_2 \quad [n] \\ a_1^k &\equiv a_2^k \quad [n] \end{aligned}$$

Plus généralement si P est un polynôme à coefficients dans $\mathbb{Z}$ alors $P(a) \equiv P(b)$ dès que $a \equiv b$. On désigne par $\overline{k}$, la classe de k modulo n. Il s'agit de l'ensemble des entiers congrus à k modulo n ; d'après les observations précédentes, on peut effectuer des opérations sur les classes (les additionner, les multiplier, les mettre à une certaine puissance entère) aussi bien que sur les nombres entiers.

Attention Contrairement à ce qu'on pourrait croire un peu vite, $e_1 \equiv e_2\,[n]$ n'autorise pas à écrire $x^{e_1} \equiv x^{e_2}\,[n]$.

Afin d'avoir de bon réflexes dans les calculs de congruences, il faut avoir regardé les carrés, les cubes, modulo 3, modulo 4, modulo 8, modulo 9.

Exercice 9 (IMO 1961)
(a) Trouver tous les entiers n tels que $2^n - 1$ est divisible par 7.
(b) Montrer qu'aucun entier de la forme $2^n + 1$ n'est divisible par 7.

Solution de l'exercice 9 On regarde les puissances de 2 modulo 7 :

$$\begin{aligned} 2^2 &\equiv 4 \\ 2^3 &\equiv 1 \end{aligned}$$

Exercice 10 Montrer que 2015 n'est pas une somme de trois carrés.

Solution de l'exercice 10 Modulo 8, un carré est toujours congru à 0, 1 ou 4 :

$$0^2 \equiv 4^2 \equiv 0\,[8]$$

$$1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1\,[8]$$

$$2^2 \equiv 6^2 \equiv 4\,[8]$$

Par conséquent, une somme de trois carrés ne peut être congrue à 7 modulo 8, ce qui est le cas de 2015.

Exercice 11 Montrer que si $p > 5$ est premier alors $p^2 \equiv 1$ ou 19 modulo 30.

Solution de l'exercice 11 p étant premier, il est congru à $7, 11, 13, 17, 19$ ou 23 modulo 30. On vérifie alors que

$$7^2 \equiv 13^2 \equiv 17^2 \equiv 23^2 \equiv 19\,[30]$$

$$11^2 \equiv 19^2 \equiv 1\,[30]$$

Exercice 12 Soit p un nombre premier. Montrer que $\binom{2p}{p} \equiv 2\,[p]$.

Solution de l'exercice 12 D'après la formule de convolution de Vandermonde

$$\binom{2p}{p} = \sum_{0\leqslant n\leqslant p} \binom{p}{n}^2$$

Maintenant, $p \mid \binom{p}{n}$ pour $1 \leqslant n \leqslant p-1$, donc $\binom{2p}{p} \equiv \binom{p}{0} + \binom{p}{p} \equiv 2$ modulo p.

Exercice 13 Montrer que si 9 divise une somme de 3 carrés alors il divise la différence de deux d'entre eux.

Solution de l'exercice 13 Soient a, b et c tels que $9 \mid a^2+b^2+c^2$. Modulo 9 les carrés sont $\overline{0}, \overline{1}, \overline{4}, \overline{-2}$. Quitte à permuter a, b et c on a donc $(\overline{a}, \overline{b}, \overline{c})$ parmi $(0,0,0)$, $(1,1,-2)$ et $(-2,-2,4)$. Dans tous les cas deux sont congrus modulo 9.

Inverse modulo n

On dit que b est un inverse de a modulo n si $ab \equiv 1\,[n]$. D'après le théorème de Bezout, pour que a possède un inverse modulo n il faut et il suffit que $(a,n) = 1$. L'inverse est calculable par l'algorithme d'Euclide étendu. Il existe alors un unique inverse modulo n : si b et b' sont deux inverses de a alors $n \mid a\,(b'-b)$ donc d'après le lemme de Gauss $b' \equiv b\,[n]$. On peut donc parler de l'inverse d'une classe modulo n.

Exemple 99. Modulo 5, $\overline{2}^{-1} = \overline{3}$. Modulo 4, $\overline{-1}$ est inversible et c'est son propre inverse.

On note $(\mathbb{Z}/n\mathbb{Z})^\times$ l'ensemble des classes modulo n qui sont inversibles. L'inverse, le produit de deux classes inversibles est inversible. En particulier, si p est premier, tous les nombres qui ne sont pas multiple de p admettent un inverse modulo p. En d'autre termes, dans $\mathbb{Z}/p\mathbb{Z}$ toutes les classes non nulles sont inversibles.

Exercice 14 Montrer que pour tout p premier, l'équation

$$6n^2 + 5n + 1 \equiv 0\,[p]$$

a des solutions.

Solution de l'exercice 14 Déjà, si $p = 2$ alors l'équation se réduit à $n + 1 \equiv 0$, qui possède des solutions. Si $p = 5$ alors les solutions sont les entiers n tels que $n \equiv \pm 2$ modulo 5. Si ce n'est pas le cas, p est impair et 6 possède un inverse, disons v. Quitte à tout multiplier par v l'équation se réécrit

$$n^2 + 5vn + v \equiv 0\,[p]$$

On peut faire apparaître le début d'un carré, et mener la résolution comme dans $\mathbb{R}$; en fait la structure de $\mathbb{Z}/p\mathbb{Z}$ est très similaire. Le discriminant est $\overline{5}^2 - 4 \times \overline{6} = \overline{1}$, c'est un carré dans $\mathbb{Z}/p\mathbb{Z}$ et ses deux racines carrées sont $\overline{1}$ et $\overline{-1}$. Si u est l'inverse de 12, les solutions sont alors $-4u$ et $-6u$

Le lemme des restes chinois

Soit a, b, n trois entiers, d un diviseur de n, si $a \equiv b[n]$ alors $a \equiv b[d]$ car d divise n qui divise $a-b$. On a donc une fonction « naturelle »de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/d\mathbb{Z}$ qui à $\bar{k}$ associe $\bar{k}$. Elle est compatible avec l'addition et la multiplication.

Théorème 3.1. (Lemme chinois) Soit a et b deux entiers premiers entre eux, alors la fonction

$$\begin{cases} \mathbb{Z}/ab\mathbb{Z} & \longrightarrow & \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \\ \bar{k} & \longmapsto & (\bar{k}, \bar{k}) \end{cases}$$

est bijective. De plus, elle est compatible avec l'addition et la multiplication.

Démonstration. On démontre la bijectivité. Comme les ensembles en question sont de même cardinal, il suffit de montrer l'injectivité. Il faut montrer que si n et m sont deux entiers tels que $n \equiv m[a]$ et $n \equiv m[b]$, alors $n \equiv m[ab]$. C'est le cas car a et b divisent $n-m$ et comme a et b sont premiers entre eux, ab divise $n-m$. □

Cela signifie que pour calculer dans $\mathbb{Z}/ab\mathbb{Z}$, on peut se ramener à calculer dans $\mathbb{Z}/a\mathbb{Z}$ et $\mathbb{Z}/b\mathbb{Z}$, et réciproquement. On utilise le lemme chinois en particulier pour dire qu'un système de congruences modulo $\mathbb{Z}/a\mathbb{Z}$ et $\mathbb{Z}/b\mathbb{Z}$ est équivalent à une congruence modulo $\mathbb{Z}/ab\mathbb{Z}$, via la bijection.

Exercice 15 On considère le plan muni d'un repère orthonormé d'origine O. On dit qu'un point M est invisible s'il existe un point à coordonnées entières sur $]OM[$. Montrer que pour tout entier naturel L il existe un carré de côté L, parallèle aux axes, tel que tous les points à coordonnées entières dans le carré soient invisibles.

Solution de l'exercice 15 Un point $M = (a,b) \in \mathbb{Z}^2$ est invisible si $\gcd(a,b) > 1$ car si $d \neq 1$ divise a et b, $(\frac{a}{d}, \frac{b}{d})$ est sur $]OM[$. Si on se donne $(p_{i,j})_{0 \leq i,j \leq L}$ des nombres premiers deux à deux distincts, alors d'après le lemme chinois il existe des entiers a et b tels que pour tous $0 \leq i,j \leq L$, $a \equiv -i[p_{i,j}]$ $b \equiv -j[p_{i,j}]$. Alors $\gcd(a+i, b+j) \geq p_{i,j} > 1$ donc tous les points $(a+i, b+j)$ sont invisibles, et le carré de côté L dont le coin inférieur gauche est (a,b) répond au problème.

2 samedi 22 après-midi : Guillaume Conchon-Kerjan

L'Ordre Modulo n

Résumé du cours

Définition 100. Soient $a \in \mathbb{Z}$ et $n \in \mathbb{N}^*$ premiers entre eux. L'*ordre de a modulo n* est le plus petit entier $d > 0$ tel que $a^d \equiv 1 \pmod{n}$.

Proposition 101. L'ordre est bien défini, i.e il existe bien d tel que $a^d \equiv 1 \pmod{n}$. De plus, soit $k \in \mathbb{N}$: alors $a^k \equiv 1 \pmod{n}$ si et seulement si d divise k.

Remarque 102. ATTENTION ! ! ! Si $a^k \equiv 1 \pmod{n}$, cela ne veut pas forcément dire que k est l'ordre de a modulo n. La seule chose qu'on peut conclure est que l'ordre de a est un diviseur de k.

Théoréme 103. (Petit théorème de Fermat) Soient p premier et a non divisible par p. Alors $a^{p-1} \equiv 1 \pmod{p}$. Autrement dit, l'ordre de a modulo p est un diviseur de $p-1$.

Un corollaire immédiat parfois utilisé est que $a^p \equiv a \pmod{p}$ quel que soit a. Un autre est que si a est non nul, $a^{\frac{p-1}{2}}$ ne peut prendre que les valeurs ± 1.

Définition 104. Soit $n \geq 2$. On note φ de n le nombre d'entiers entre 0 et n qui sont premiers avec n. φ est appelée *fonction indicatrice d'Euler*.

Proposition 105. Si $n = p_1^{\alpha_1}...p_k^{\alpha_k}$ avec les p_i premiers, alors :

$$\varphi(n) = (p_1 - 1)p_1^{\alpha_1 - 1}...(p_k - 1)p_k^{\alpha_k - 1} = \Big(1 - \frac{1}{p_1}\Big)...\Big(1 - \frac{1}{p_k}\Big)n$$

Théoréme 106. (Théorème d'Euler) Soient n et a premier avec n. Alors $a^{\varphi(n)} \equiv 1 \pmod{n}$. Autrement dit, l'ordre de a est un diviseur de $\varphi(n)$.

Exercices :

Exercice 1 (Théorème de Wilson) Soit p un nombre premier. Montrer que :

$$(p-1)! \equiv -1 \pmod{p}$$

Exercice 2 Quels sont les couples d'entiers naturels (n, p), tels que $(p-1)! + 1 = p^n$?

Exercice 3 Soit $n \in \mathbb{N}^*$ premier avec 10. Montrer qu'il existe un multiple de n qui ne s'écrit qu'avec des 1.

Exercice 4 Montrer que pour tout entier naturel k, $19 | 2^{2^{6k+2}} + 3$.

Exercice 5 Soit $n \in \mathbb{N}^*$ impair. Montrer que $n | 2^{n!} - 1$.

Exercice 6 Trouver tous les $n \in \mathbb{N}^*$ tels que n divise $2^n - 1$.

Exercice 7 Soit E un ensemble de nombres premiers ayant deux éléments tel que si $p_1, \cdots, p_n \in E$ (les p_i étant distincts), alors tous les facteurs premiers de $p_1 \times \cdots \times p_n - 1$ sont dans E. Montrer que E est l'ensemble des nombres premiers.

Exercice 8 Montrer que pour tout nombre premier impair p, il existe une infinité d'entiers naturels n tels que

$$p | n2^n + 1.$$

Exercice 9 Trouver tous les $n \in \mathbb{N}^*$ impairs tels que n divise $3^n + 1$.

Exercice 10 Soit p un nombre premier. Montrer qu'il existe n tel que p divise :

$$2^n + 3^n + 6^n - 1$$

Exercice 11 Quels sont les nombres premiers p tels que -1 soit un carré modulo p (*ie* il existe un entier k tel que $k^2 \equiv -1 \pmod{p}$) ?

Solutions

Solution de l'exercice 1 En faisant le produit, on peut regrouper chaque élément de $(\mathbb{Z}/p\mathbb{Z})^*$ avec son inverse. Le produit vaut alors 1. Il ne reste alors que les termes qui sont leur propre inverse, c'est-à-dire tels que $x^2 = 1$, c'est-à-dire 1 et -1 (si $p = 2$ ce n'est pas tout à fait vrai car $1 = -1$ mais alors le résultat est trivial). Le produit modulo p vaut donc $1 \times 1 \times (-1) = -1$.

Solution de l'exercice 2 D'après l'exercice précédent, p doit être premier. Si $p = 2$ ou 3, seul $n = 1$ convient. Si $p = 5$, l'unique possibilité est $n = 2$.
Sinon, $\frac{p-1}{2} \neq 2$ est entier, et les facteurs $2, \frac{p-1}{2}, p-1$ apparaissent dans $(p-1)!$. Donc $(p-1)^2 | (p-1)!$. Or, $p^n - 1 = (1 + p + p^2 + \cdots + p^{n-1})$. Donc $p - 1 | 1 + p + \cdots + p^{n-1}$. Or pour tout $k \geq 0$, $p^k \equiv 1 \pmod{p-1}$, donc $1 + p + \cdots + p^{n-1} \equiv n \pmod{p-1}$. Ainsi, n doit être multiple de $p - 1$. Or $n > 0$ donc $p^n \geq p^{p-1} \geq p \times (p-1) \times \cdots \times 2 \geq p! > (p-1)! + 1$ car $p > 5$. L'égalité n'est donc pas possible.
Ainsi, les couples solution sont $(1, 2)$, $(1, 3)$ et $(2, 5)$.

Solution de l'exercice 3 Le nombre qui s'écrit avec k chiffres 1 est $11...1 = \frac{99...9}{9} = \frac{10^k - 1}{9}$. On cherche donc k tel que $n | \frac{10^k - 1}{9}$, i.e $9n | 10^k - 1$. D'après ce qu'on a vu en cours, il suffit de choisir pour k l'ordre de 10 modulo $9n$. Il existe bien car 10 est premier avec 9 et n, donc avec $9n$.

Solution de l'exercice 4 Il suffit de prouver que $2^{2^{6k+2}} \equiv 16 \equiv 2^4 \pmod{19}$. D'après le petit théorème de Fermat, $2^{18} \equiv 1 \pmod{19}$: si $2^{6k+2} = 18a + 4$, c'est gagné. Il suffit donc d'avoir $2^{6k+2} \equiv 4 \pmod{18}$. Or $2^{6k+2} \equiv 64^k \times 4 \equiv 4 \pmod{9}$ et $2^{6k+2} \equiv 0 \pmod{2}$, donc nécessairement $2^{6k+2} \equiv 4 \pmod{18}$ d'après le théorème des restes chinois.

Solution de l'exercice 5 On sait que l'ordre de 2 modulo n existe car n est impair, et divise $\varphi(n)$. Comme $\varphi(n) \leq n$, $\varphi(n) | n!$ donc $2^{n!} \equiv 1 \pmod{n}$.

Solution de l'exercice 6 Soient $n > 1$ tel que n divise $2^n - 1$, et p le plus petit diviseur premier de n. On note d l'ordre de 2 modulo p : on sait que d divise $p - 1$, et d'autre part d'après l'énoncé $p | 2^n - 1$ donc d divise n, donc d divise $PGCD(n, p-1)$.

Or, comme p est minimal, $p-1$ est plus petit que tous les diviseurs premiers de n, donc n et $p - 1$ n'ont aucun diviseur premier commun, donc leur $PGCD$ vaut 1, donc $d = 1$. Autrement dit, $2 \equiv 1 \pmod{p}$ donc $p = 1$, ce qui est absurde, donc seul $n = 1$ est solution.

Solution de l'exercice 7 Montrons que E est infini. Si E est fini, soient $p_1, \cdots, p_m$ ses éléments, les facteurs premiers de $p_1 \times \cdots \times p_m - 1$ sont dans E et différents des p_i, contradiction. Notons que $m \geq 2$ d'après l'énoncé, donc ce nombre est bien strictement plus grand que 1 et admet des facteurs premiers...
Maintenant, si p est premier quelconque, il existe au moins $p-1$ éléments de E ayant le même résidu modulo p par principe des tiroirs. Appelons les $e_1, \cdots, e_{p-1}$. Alors par petit théorème de Fermat, $e_1 \times \cdots \times e_{p-1} - 1$ est multiple de p, donc $p \in E$.

Solution de l'exercice 8 Si $n = k(p-1)$, alors $2^n \equiv 1 \pmod{p}$ par petit théorème de Fermat. Donc $n2^n + 1 \equiv n + 1 \pmod{p}$, donc il suffit que n soit congru à -1 modulo p, donc que k soit congru à 1 : prendre k de la forme $pk' + 1$, avec $k' \in \mathbb{N}$, suffit.

Solution de l'exercice 9 Tout d'abord, $n = 1$ est solution.

De plus, soit q le plus petit diviseur premier de n et d l'ordre de 3 modulo q : n est impair donc $q > 2$. D'une part $d | q-1$ et d'autre part $3^n \equiv -1 \pmod{q}$ donc $3^{2n} \equiv 1 \pmod{n}$ donc $d | 2n$

donc d divise le $PGCD$ de $2n$ et $q-1$, qui vaut 2 pour les mêmes raisons que dans l'exercice précédent, donc d vaut 1 ou 2, donc $q|3^2-1=8$ donc $q=2$, ce qui est absurde car n est impair.

$n=1$ est donc la seule solution.

Solution de l'exercice 10 On peut prendre $n=1$ pour $p=2$ et $n=2$ pour $p=3$.

Pour $p>3$, on prend $n=p-2$. Alors 2, 3 et 6 sont premiers avec p et par petit théorème de Fermat :

$$2^{p-2}+3^{p-2}+6^{p-2}-1 \equiv \frac{1}{2}+\frac{1}{3}+\frac{1}{6}-1 \equiv \frac{3+2+1-6}{6} \equiv 0 \pmod{p}$$

Solution de l'exercice 11 $p=2$ convient, et on suppose désormais p impair. Si un tel k existe, son ordre d divise 4 car $k^4 \equiv 1 \pmod{p}$. On vérifie aisément que $d=4$. D'après le petit théorème de Fermat, 4 divise $p-1$ donc $p \equiv 1 \pmod{4}$.
Réciproquement, si $p \equiv 1 \pmod{4}$, $(-1)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. On veut montrer que -1 est un carré modulo p. Si a est un carré non nul modulo p (aussi appelé "résidu quadratique"), l'équation $x^2=a$ a deux solutions (opposées) dans $\mathbb{Z}/p\mathbb{Z}$. Sinon, elle en a 0. Elle ne peut en avoir une seule, car on aurait $x \equiv -x \pmod{p}$ soit $x \equiv 0 \pmod{p}$ car $pgcd(2,p)=1$. Or, il y a $p-1$ éléments non nuls dans $\mathbb{Z}/p\mathbb{Z}$, il y a donc $\frac{p-1}{2}$ résidus quadratiques distincts.
Si a résidu quadratique, il existe b non nul tel que $b^2 \equiv a \pmod{p}$, donc par petit théorème de Fermat, $a^{\frac{p-1}{2}} \equiv b^{p-1} \equiv 1 \pmod{p}$. Ainsi, l'équation $X^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ a déjà $\frac{p-1}{2}$ solutions dans $\mathbb{Z}/p\mathbb{Z}$. Or une équation polynômiale de degré d ne peut avoir plus de d solutions dans $\mathbb{Z}/p\mathbb{Z}$ [c'est aussi vrai dans $\mathbb{R}$, et cela peut se prouver par récurrence sur d en factorisant par une racine du polynôme], donc les solutions de cette équation sont exactement les résidus quadratiques. D'après notre première remarque, -1 est solution, ce qui conclut.

3 dimanche 23 matin : François Lo Jacomo

Equations diophantiennes

Une équation diophantienne est une équation dont on cherche les solutions entières. Certaines sont parmi les problèmes les plus difficiles des mathématiques. Sur quelques exercices, nous étudierons quelques méthodes.

Exercice 1

Déterminer toutes les solutions $(m,n) \in \mathbf{N}^2$ de l'équation :

$$2^m - 3^n = 1$$

Exercice 2

Déterminer toutes les solutions $(m,n) \in$ fff$mathbf N^2$ de l'équation :

$$3^n - 2^m = 1$$

Exercice 3

Vérifier que 2 est solution de l'équation :

$$(x+1)^3+(x+2)^3+(x+3)^3=(x+4)^3$$

Cette équation admet-elle d'autres solutions entières ?

Exercice 4

Déterminer toutes les solutions entières de l'équation :

$$(x+1)^3 + (x+2)^3 + (x+3)^3 + (x+4)^3 = (x+5)^3$$

Exercice 5

Déterminer toutes les solutions $(x, y) \in \mathbf{N}^2$ de l'équation :

$$x(x+1) = 4y(y+1)$$

Exercice 6

Quelles valeurs peut prendre x^4 modulo 13 ?

Montrer que l'équation :

$$x^4 + 6 = y^3$$

n'admet pas de solution entière.

Exercice 7

Montrer que pour x entier, $x^2 + 1$ n'admet pas de diviseur congru à 3 modulo 4.

Déterminer toutes les solutions $(x, y) \in N^2$ de l'équation :

$$x^2 - y^3 = 7$$

Exercice 8

Montrer que l'équation : $x^2 + 2y^2 = z^2$ admet une infinité de solutions $(x, y, z) \in \mathbf{N}^3$. Existe-t-il des quadruplets d'entiers non nuls (x, y, z, t) tels que :

$$x^2 + 2y^2 = z^2$$

$$2x^2 + y^2 = t^2$$

Exercice 9

Montrer que pour tout n entier strictement positif, il existe $x_1, x_2, \cdots x_n$ entiers strictement positifs tels que :

$$x_1 + x_2 + \cdots + x_n = x_1 x_2 \cdots x_n$$

Exercice 10

Déterminer toutes les solutions $(m, n) \in \mathbf{N}^2$ de l'équation :

$$7^m - 3 \times 2^n = 1$$

SOLUTIONS

Solution de l'exercice 1

3^n est congru à 1 ou 3 modulo 8, selon que n est pair ou impair, donc $2^m = 3^n + 1$ doit être congru à 2 ou 4 modulo 8, ce qui n'est vérifié que pour $m = 1$ (donc $n = 0$) et $m = 2$ (donc $n = 1$).

Solution de l'exercice 2

Si n est impair, $3^n \equiv 3 \pmod 8$, donc on doit avoir $2^m \equiv 2 \pmod 8$, soit $m = 1$ et $n = 1$. Si $n = 2k$, $2^m = 3^{2k} - 1 = \left(3^k + 1\right)\left(3^k - 1\right)$, ce qui entraîne que $3^k + 1$ et $3^k - 1$ sont deux puissances de 2, dont la différence vaut 2 : ce ne peut être que 2 et 4, donc $k = 1$, $n = 2$, $m = 3$.

Solution de l'exercice 3

$3^3 + 4^3 + 5^3 = 27 + 64 + 125 = 216 = 6^3$. Plusieurs techniques peuvent être utilisées pour résoudre l'équation : poser $x = 2 + k$, ce qui, en développant, donne une équation du troisième degré en k dont une des racines est nulle (cette équation n'admet pas d'autre racine réelle). Mais on peut aussi développer directement : $(x+1)^3 + (x+2)^3 + (x+3)^3 - (x+4)^3 = 2x^3 + 6x^2 - 6x - 28$: pour que ceci soit nul, il faut que $2x$ divise le terme constant -28, ce qui limite le nombre de cas à étudier. On peut aussi voir que pour $x \geq 3$, $2x^3 > 28$ et $6x^2 > 6x$, donc $(x+1)^3 + (x+2)^3 + (x+3)^3 - (x+4)^3 > 0$ et pour $x \leq -2$, $(x+1)^3 + (x+2)^3 < 0$ et $(x+3)^3 - (x+4)^3 < 0$, donc $(x+1)^3 + (x+2)^3 + (x+3)^3 - (x+4)^3 < 0$: il reste quatre cas simples à étudier. Enfin, on peut remarquer que modulo 3, comme pour tout n entier, $n^3 \equiv n \pmod 3$, $(x+1)^3 + (x+2)^3 + (x+3)^3 - (x+4)^3 \equiv (x+1) + (x+2) + (x+3) - (x+4) = 2x + 2$, donc x doit être congru à 2 modulo 3.

Solution de l'exercice 4

Comme pour tout n entier, $n^3 \equiv n \pmod 3$, on doit avoir : $(x+1)+(x+2)+(x+3)+(x+4) \equiv x + 5 \pmod 3$, soit $4x + 10 \equiv x + 5 \pmod 3$, ce qui est impossible vu que $4x \equiv x$ et $10 \not\equiv 5$ modulo 3.

Solution de l'exercice 5

$(x, y) = (0, 0)$ est évidemment solution. Par ailleurs, l'équation peut s'écrire : $(2y+1)^2 = 4y(y+1) + 1 = x^2 + x + 1$, or pour $x > 0$, $x^2 + x + 1$, strictement compris entre x^2 et $(x+1)^2$, ne peut pas être un carré parfait.

Solution de l'exercice 6

Modulo 13, x^4 prend les valeurs $0, 1, 3$ et 9. Modulo 13, y^3 prend les valeurs $0, 1, 5, 8, 12$. Donc on ne peut pas avoir $x^4 + 6 \equiv y^3 \pmod{13}$, et a fortiori l'équation n'a pas de racine.

Pourquoi étudier cette équation modulo 13 ? C'est parce que $13 - 1$ est divisible par 3 que x^3 ne prend que 4 valeurs non nulles modulo 13. En effet, pour x non multiple de 13, $(x^3)^4 = x^{12} \equiv 1 \pmod{13}$ d'après Fermat, et dans l'ensemble des classes modulo un nombre premier p, une équation du quatrième degré ne peut avoir que quatre racines au maximum. Il faut donc choisir un nombre premier p tel que $p - 1$ soit divisible par 3 et par 4, donc par 12. On aurait pu également choisir 37 (mais il n'est pas certain que l'on aurait obtenu la même impossibilité avec 37).

Solution de l'exercice 7

La première question est un résultat très classique. Si $x^2 + 1$ admettait un diviseur congru à 3 modulo 4, il admettrait un diviseur premier congru à 3 modulo 4, car un nombre dont tous les facteurs premiers sont congrus à 1 modulo 4 est nécessairement lui-même congru à 1 modulo 4. Or si pour un nombre premier $p = 4k+3$, $x^2 \equiv -1 \pmod p$, alors $x^{p-1} = \left(x^2\right)^{2k+1} \equiv -1 \pmod p$, ce qui contredirait le théorème de Fermat.

A partir de là, pour l'équation : $x^2 - y^3 = 7$, distinguons deux cas : si y est pair, alors on a $x^2 \equiv 7 \pmod 8$, ce qui est impossible : un carré parfait est congru à $0, 1$ ou 4 modulo 8. Si maintenant $y = 2k + 1$, l'équation équivaut à : $x^2 + 1 = y^3 + 8 = (y+2)(y^2 - 2y + 4)$, or

$y^2-2y+4=4k^2+3\equiv 3 \pmod 4$: on a vu que x^2+1 ne peut pas admettre de diviseur congru à 3 modulo $'$.

Solution de l'exercice 8

L'équation étant homogène (tous les termes ont le même degré), si (x,y,z) est solution, pour tout k, (kx,ky,kz) est solution. Par exemple, $(1,2,3)$ est solution, donc pour tout entier k, $(k,2k,3k)$ est solution. Et ce ne sont pas les seules solutions ! il en existe une infinité d'autres.

En revanche, concernant le système des deux équations, deux méthodes (au moins) permettent de prouver qu'il n'admet pas de solution : supposons d'abord que x et y sont premiers entre eux (s'ils avaient un PGCD $d>1$, $\left(\frac{x}{d},\frac{y}{d},\frac{z}{d},\frac{t}{d}\right)$ serait également solution avec $\frac{x}{d}$ et $\frac{y}{d}$ premiers entre eux). Puis raisonnons

- soit modulo 8 : comme un carré est congru à $0,1$ ou 4 modulo 8, et que $x^2+2\equiv z^2$ est impossible modulo 8, la première équation entraîne que y est pair. Pour la même raison, la seconde équation entraîne que x est pair, ce qui contredit l'hypothèse que x et y sont premiers entre eux. On peut aussi formuler cette solution sous forme de "descente infinie" : si (x,y,z,t) est solution de l'équation, alors les quatre entiers sont pairs et $\left(\frac{x}{2},\frac{y}{2},\frac{z}{2},\frac{t}{2}\right)$ est également solution.

- soit modulo 3 : en additionnant les deux équations on obtient : $3(x^2+y^2)=z^2+t^2$. Or une somme de deux carrés n'est divisible par 3 que si chacun des nombres est divisible par 3 (du simple fait qu'un carré est congru à 0 ou 1 modulo 3). Si $z=3z'$ et $t=3t'$, $x^2+y^2=3\left(z'^2+t'^2\right)$, donc x et y sont tous deux multiples de 3, ce qui contredit le fait qu'ils sont premiers entre eux. Même remarque concernant la descente infinie.

Solution de l'exercice 9

Une solution simple : si $n=1$, n'importe quel x_1 est solution. Si $n=2$, $x_1=x_2=2$. Si $n>2$, $x_1=\cdots=x_{n-2}=1, x_{n-1}=2$ et $x_n=n$ est solution : somme et produit valent $2n$.

Solution de l'exercice 10

Ecrivons tout d'abord l'équation sous la forme : $7^x-1=3\times 2^y$. La solution fait appel à des factorisations, notamment : $7^x-1=(7-1)\left(7^{x-1}+7^{x-2}+\cdots+7+1\right)$. Comme $7-1=3\times 2$, l'équation devient : $7^{x-1}+7^{x-2}+\cdots+7+1=2^{y-1}$. Soit $y=1$, ce qui fournit une première solution ($x=y=1$), soit le second membre est pair et le premier contient un nombre pair de termes (tous impairs), donc x est pair. Dès lors, on peut encore factoriser par $(7+1)=2^3$, ce qui nous ramène à : $7^{x-2}+7^{x-4}+\cdots+7^2+1=2^{y-4}$. Une nouvelle fois, soit $y=4$ ce qui fournit une deuxième solution ($x=2$), soit les deux membres sont pairs, donc le premier contient un nombre pair de termes, x est multiple de 4. On peut à nouveau factoriser le premier membre en : $(7^2+1)\left(7^{x-4}+7^{x-8}+...+7^4+1\right)$. Mais cette fois-ci, $7^2+1=50$ ne peut pas diviser le deuxième membre qui est une puissance de 2, donc il n'y a pas de solution pour $y>4$. Les seules solutions sont $(1,1)$ et $(2,4)$.

4 Groupe D : combinatoire

1 samedi 22 matin : Guillaume Conchon-Kerjan

Pavages et découpages

Le bon wagon

Échauffons-nous :

Exercice 1 Peut-on découper un carré 6×6 en rectangles 1×4 ? Quelle est la condition nécessaire et suffisante pour découper un rectangle $m \times n$ en rectangles $1 \times k$?

On va chercher à généraliser cela.

Théoréme 107. Un rectangle $a \times b$ pavé par des rectangles semi-entiers (ie ils ont chacun un côté entier) est semi-entier.

Démonstration. S. Wagon (voir Sources) donne 14 preuves de ce résultat... explorons-en quelques-unes !
On fixe un repère orthonormé tel que les sommets du rectangle aient pour coordonnées $(0, 0)$, $(a, 0)$, (a, b) et $(0, b)$.

Première démonstration : On considère le réseau carré de côté $1/2$ induit par notre repère, et on le colorie comme une grille d'échecs. On voit facilement qu'un rectangle semi-entier contient autant de surface blanche que de surface noire. Maintenant, si on trace les droites horizontale d'ordonnée b et verticale d'abscisse a, notre rectangle est partagé en 4 rectangles. Trois sont clairement semi-entiers et contiennent autant de blanc que de noir. Le rectangle $(a - \lfloor a \rfloor) \times (b - \lfloor b \rfloor)$ l'est donc également. Or ses côtés sont < 1, donc l'un d'entre eux est nul, et a ou b est entier.

Deuxième démonstration : On bouge désormais les segments verticaux dont l'abscisse x n'est pas entière en $\lfloor x \rfloor + 1/2$. On fait de même avec les segments horizontaux. On obtient un nouveau rectangle R' dont les longueurs des côtés sont les moitiés d'entiers impairs dans le cas où R n'est pas semi-entier. R' contient donc un nombre impair de carrés de côtés $1/2$, or il est constitué de rectangles semi-entiers, qui contiennent chacun autant de carrés noirs que blancs, contradiction.

Troisième démonstration : Petite variante de la précédente, en décalant un segment vertical d'abscisse x non entière en $x + t$, pareil pour les horizontaux, avec t petit pour avoir toujours le même nombre de tuiles. L'aire du grand rectangle est une fonction affine de t. Si le grand rectangle n'est pas semi-entier, son aire devient $(a + t)(b + t)$ qui est un polynôme du second degré en t, absurde.

Quatrième démonstration : On dessine un graphe dont les arêtes sont les côtés entiers des petits rectangles. Attention, si un rectangle a 4 côtés entiers, on en choisit arbitrairement 2 opposés (mais pas les 4). Notons que tous les sommets ont un degré pair, sauf les sommets du grand rectangle. Regardons la composante connexe de l'origine : elle contient nécessairement un autre sommet du grand rectangle car la somme des degrés de ce graphe doit être paire. Le résultat en découle. □

On généralise le théorème précédent en dimension quelconque.

Théoréme 108. Une boîte de dimension d que l'on peut paver en boîtes ayant chacune au moins k de leurs dimensions entières a au moins k dimensions entières.

Démonstration. La troisième démonstration s'adapte sans souci. □

Exercice 2
Montrer que le théorème 1 reste vrai si on suppose seulement que les rectangles ayant au moins un sommet à coordonnées entières sont semi-entiers.

Le singe de Bruijn

Théoréme 109. (de Bruijn) Si un singe peut paver une boîte de dimension $B_1 \times \cdots \times B_d$ par des blocs de taille $b_1 \times \cdots \times b_d$, alors chaque b_i divise un B_j.

Démonstration. Si on divise toutes les dimensions par b_i, on se ramène à un cas particulier du théorème 2. □

Exercice 3 Soit $b_1, \leq \cdots \leq b_n$ des naturels strictement positifs. Montrer que $b_1 | \cdots | b_d$ si et seulement si toute boîte $B_1 \times \cdots \times B_d$ pavable par des boîtes $b_1 \times \cdots \times b_d$ est multiple de celles-ci.

D'autres pavages

Exercice 4 Russie 1996
Est-il possible de paver (en plusieurs couches) un rectangle 5×7 par des trominos en forme de L, de sorte que chaque carré soit recouvert par le même nombre de trominos ?

Exercice 5 Tournoi des villes 2004
Montrer que si un rectangle proportionnel à A peut être pavé avec des copies du rectangle B, alors un rectangle proportionnel à B peut être pavé avec des copies de A.

Exercice 6 Pacifique asiatique 2007
Lorsqu'on allume (ou éteint) une lampe d'une grille 5×5, ses voisines situées sur la même ligne ou même colonne qu'elle changent également d'état. Au départ, toutes les lampes sont éteintes. Un singe arrive et joue avec les interrupteurs. Finalement, une seule lampe est allumée. Déterminer sa (ses) position(s) possible(s).

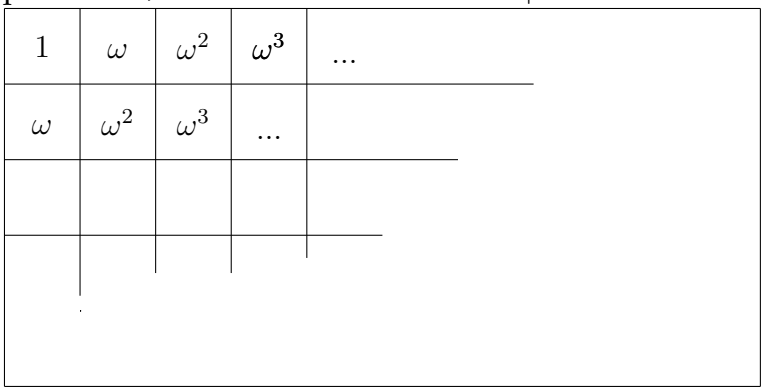
Exercice 7 États-Unis 1998
On colorie un damier de 98×98 carrés à la manière d'une grille d'échec. Un coup consiste à sélectionner un rectangle constitué de petits carrés et à inverser leurs couleurs. Combien de coups sont nécessaires au minimum pour rendre le damier monochrome ?

Exercice 8 Olympiades Balkaniques 2000
Combien peut-on placer de rectangles $1 \times 10\sqrt{2}$ dans un rectangle 50×90 sans recouvrement, les bords des petits étant parallèles à ceux des grands ?

Exercice 9 Olympiades de toutes les Russies 2006
Un carré de côté 3000 est découpé arbitrairement en dominos 1×2. Montrer qu'on peut les colorier en jaune, bleu et rouge de sorte que chaque couleur soit également représentée et que chaque domino ne touche (par un côté) pas plus de deux autres dominos de sa couleur.

Solutions

Solution de l'exercice 1 La réponse est non, il faut que k divise m ou n. Pour le voir, on peut colorier régulièrement le rectangle avec k couleurs, ou avec $1, \omega, \cdots, \omega^{k-1}$ où ω est une racine primitive k-ème de l'unité : c'est un nombre complexe tel que $w^k = 1$ et $\omega^i \neq 1$ si $1 \leq i \leq k-1$. En particulier, $\omega^i = 0$ si et seulement si $k|i$.



Un rectangle $1 \times k$ recouvre une et une seule fois chaque ω^i et $1 + \omega + \cdots + w^{k-1} = 0$. La somme totale doit valoir 0. Elle vaut

$$\frac{\omega^n - 1}{\omega - 1} \times \frac{\omega^m - 1}{\omega - 1}$$

d'où le résultat.
Enfin, cette condition est clairement suffisante.

Solution de l'exercice 2 On peut adapter la première démonstration.

Solution de l'exercice 3 Si on a la chaîne de divisibilité, par le théorème précédent, b_d divise un B_k, mettons B_d. Si on fait une coupe selon la d-ème dimension, on obtient une boîte $B_1 \times \cdots \times B_{d-1}$ pavée par des blocs (pas forcément $b_{i_1} \times \times b_{i_{d-1}}$, les i_j étant différents. Chacun de ces blocs est pavable par des blocs $b_1 \times \cdots \times b_{d-1}$ d'après la relation de divisibilité. Il suffit de répéter le raisonnement.
Si on ne l'a pas : si $d = 2$, on peut supposer $pgcd(d_1, d_2) = 1$, et on peut paver une boîte de dimension $b_1 b_2 \times (b_1 + b_2)$. Il est ensuite aisé de passer en dimension supérieure.

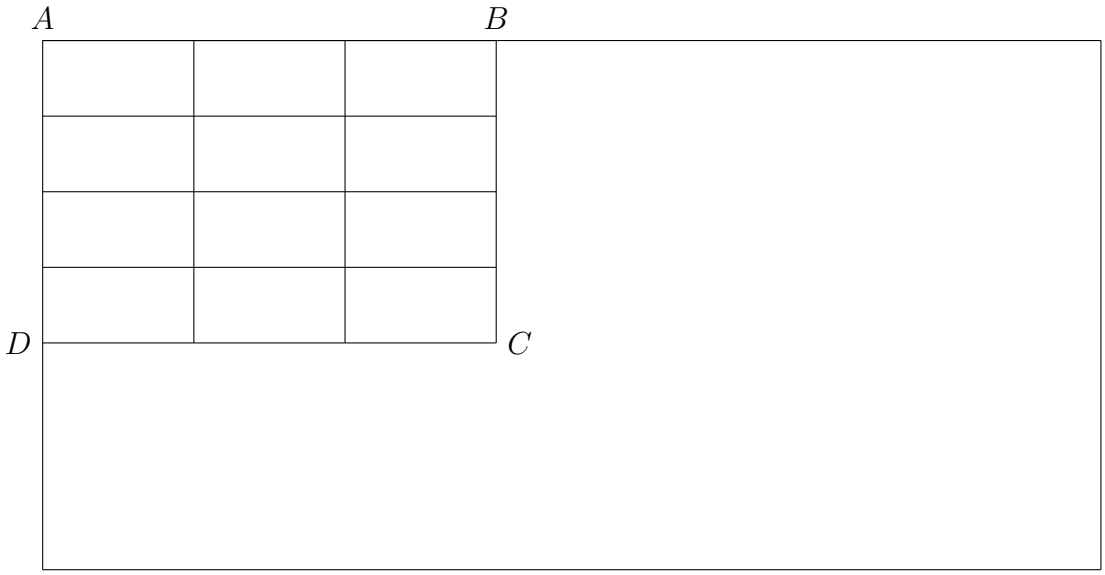
Solution de l'exercice 4 Non. Notons $n = 3k$ le nombre de couches, on utilise $35k$ trominos. On colorie la grille ainsi :
A B A B A B A
C D C D C D C
A B A B A B A
C D C D C D C
A B A B A B A
Il y a 12 A, et un tromino en recouvre au plus un. Il faut donc au moins $12 \times 3k = 36k$ trominos pour que chaque A soit recouvert 12 fois, or on n'en a que $35k$.

Solution de l'exercice 5 Notons $a_1 \times a_2$ et $b_1 \times b_2$ les tailles de ces rectangles.
Si $\frac{b_1}{b_2}$ est irrationnel, alors toutes les copies de A ont la même orientation. En effet, notons $ABCD$ le plus grand rectangle constitué de rectangles dans la position de celui en haut à gauche (voir figure), il y a un rectangle situé dans l'autre position le long de $[CD]$. L'irrationalité du rapport des côtés implique que le dernier rectangle longeant $[CD]$ va dépasser (sinon

un certain nombre entier de fois la largeur du rectangle serait égal à un certain nombre entier de fois la longueur). Le côté $[BC]$, toujours du fait de l'irrationalité, ne peut toucher que des rectangles dans la position de celui en haut à gauche. Donc $ABCD$ n'était pas le plus grand rectangle cherché, contradiction.
Si $\frac{b_1}{b_2}$ est rationnel on peut supposer b_1, b_2 entiers, et le rectangle similaire à A a pour dimensions $(ub_1 + vb_2) \times (xb_1 + yb_2)$ avec u, v, x, y naturels. De plus,

$$\frac{a_1}{a_2} = \frac{ub_1 + vb_2}{xb_1 + yb_2}.$$

Le rapport a_1/a_2 étant rationnel, on peut construire un carré avec des copies de A, et en assemblant ces carrés on peut faire un rectangle semblable à B.



Solution de l'exercice 6 P'tit invariant : la parité du nombre de lampes éteintes sur les 1ère, 3ème et 5ème colonnes qui ne sont pas sur la 3ème ligne. De même pour les lignes. Les seules candidates sont alors les lampes en position $(2, 2)$, $(2, 4)$, $(4, 2)$, $(4, 4)$ et $(3, 3)$. Par symétrie, il suffit de trouver une combinaison laissant seulement $(2, 2)$ allumée, et une avec $(3, 3)$. Amusez-vous pour les constructions...

Solution de l'exercice 7 Plus généralement, sur une grille $n \times m$, il suffit de $\lfloor \frac{n}{2} \rfloor + \lfloor \frac{m}{2} \rfloor$ coups en agissant sur les lignes et colonnes paires (l'ordre des opérations n'importe pas).
Penchons-nous d'abord sur un rectangle 1×98, qui a 97 frontières de cases problématiques. Sélectionner un sous-rectangle de celui-là en enlève au plus 2, donc il faut actionner au moins 49 tels sous rectangles. Considérons les 4 rectangles "limite" 1×98 sur le bord du rectangle. Chacun doit donc rencontrer au moins 49 des rectangles choisis. Si un de ces rectangles intersecte trois des quatre rectangles limite, c'est qu'il en croise deux opposés et contient le troisième. Un rectangle choisi agit donc utilement sur au plus deux rectangles limite. On aura donc besoin d'au moins $49 \times 4/2 = 98$ coups.

Solution de l'exercice 8 L'aire du grand rectangle fait entre 318 et 319 fois celle d'un petit. D'un autre côté, si on place 50 paquets de 6 petits rectangles allongés dans le grand, il reste un rectangle $50 \times 90 - 60\sqrt{2}$. Ce dernier peut accueillir 3×5 petits rectangles, ce qui nous en fait 315

au total, mais on voit difficilement comment faire mieux.
Retravaillons un peu la borne supérieure : dans un repère orthonormé classique, on place le grand rectangle de sorte que ses sommets soient en $(0,0)$, $(90,0)$, $(50,90)$ et $(0,50)$. On considère pour $k \in N^*$ les lignes dans le grand rectangle d'équation $x+y = 10k\sqrt{2}$. Chaque petit rectangle dont les côtés sont parallèles au grand intersecte certaines (une ou deux) de ces lignes sur une longueur totale de $\sqrt{2}$. La somme des longueurs des lignes fait $570\sqrt{2} - 360$, qui est strictement inférieur à $316\sqrt{2}$, ce qui permet de conclure.

Solution de l'exercice 9 On imagine la grille comme un damier. Le domino dont la case blanche est en (i,j) est de couleur $i - j \pmod 3$. Les dominos de même couleur s'échelonnent alors approximativement en diagonale. Une étude de cas rapide montre que la consigne de l'énoncé est toujours vérifiée.

Sources

-Yufei Zhao, *Tilings : Coloring and Weights*
-Stan Wagon, *Fourteen Proofs of a Result About Tiling a Rectangle*

2 samedi 22 après-midi : Joon Kwon

Le cours a porté sur les séries génératrices et on pourra consulter l'excellent chapitre rédigé par Margaret Bilu dans le polycopié du stage de Montpellier 2013.

3 dimanche 23 matin : Thomas Budzinski

Exercice 1 On donne 2016 points dans le plan, trois quelconques jamais alignés. Démontrer que l'on peut construire 504 quadrilatères deux à deux disjoints, non nécessairement convexes, et dont les sommets sont les points données.

Solution de l'exercice 1 Quitte à faire tourner la figure, on peut supposer que les points ont des abscisses deux à deux distinctes. On note P_i avec $1 \leq i \leq 2016$ les points ordonnés par abscisse croissante et, pour tout k entre 0 et 503, on considère un quadrilatère dont les sommets sont P_{4i+1}, P_{4i+2}, P_{4i+3} et P_{4i+4}.

Exercice 2 On considère 2015 droites du plan, deux à deux non parallèles et trois à trois non concourantes. On appelle E l'ensemble de leurs points d'intersection.

On veut attribuer une couleur à chacun des points de E de sorte que deux quelconques de ces points qui appartiennent à une même droite et dont le segment qui les relient ne contient aucun autre point de E, soient de couleurs différentes.

Combien faut-il au minimum de couleurs pour pouvoir réaliser une telle coloration ?

Solution de l'exercice 2 La configuration contient au moins un triangle. Cela peut par exemple se prouver par récurrence sur le nombre de droites : trois droites forment un triangle et si on ajoute une droite, soit elle laisse le triangle intact, soit elle le sépare en un triangle et une quadrilatère. Par conséquent, il est impossible d'effectuer un coloriage avec deux couleurs.

On va maintenant montrer qu'un coloriage à trois couleurs est possible : on ordonne les points par abscisse croissante comme tout à l'heure, et on les colorie dans cet ordre. Au moment où on doit colorier un point $P = (d_i) \cap (d_j)$, on a déjà colorié au plus un de ses voisins

sur (d_i) (celui qui est à gauche) et un sur (d_j) (aussi celui de gauche). On a donc au plus deux couleurs interdites et on peut toujours choisir la troisième. La réponse est donc 3 couleurs.

Exercice 3 On dit qu'un ensemble de points du plan est *obtus* lorsque trois points quelconques de cet ensemble sont toujours les sommets d'un triangle obtus.

Prouver que tout ensemble de n points du plan, trois quelconques jamais alignés, contient un sous-ensemble bon d'au moins $\sqrt{n}$ éléments.

Solution de l'exercice 3 Encore une fois, on range les points par abscisse croissante. Un résultat classique d'Erdös et Szekeres assure que la suite des ordonnées contient une sous-suite croissante ou décroissante de longueur $\sqrt{n}$. Or, il est facile de montrer (par exemple avec un produit scalaire) que si $x_1 < x_2 < x_3$ et $y_1 < y_2 < y_3$, alors les points de coordonnées (x_1, y_1), (x_2, y_2) et (x_3, y_3) forment un angle obtus. Voici l'énoncé et la preuve du théorème d'Erdös-Szekeres :

Théoréme 110. Toute suite réelle de longueur $n^2 + 1$ admet une sous-suite croissante ou décroissante de longueur $n + 1$.

Démonstration. Soit (x_i) une suite de longueur $n^2 + 1$. Pour tout i de 1 à $n^2 + 1$, on note a_i et b_i les longueurs de la plus longue sous-suite croissante et de la plus longue sous-suite décroissante qui se termine par x_i : si l'énoncé est faux, alors $1 \leq a_i \leq n$ et $1 \leq b_i \leq n$ pour tout i donc il existe $i < j$ tels que $a_i = a_j$ et $b_i = b_j$. Si $x_i \geq x_j$ alors on peut ajouter x_j à la plus grande sous-suite croissante qui termine par x_i donc $a_j \geq a_i + 1$ ce qui est absurde. Si $x_i \leq x_j$ alors on peut ajouter x_j à la plus grande sous-suite décroissante qui termine par x_i donc $b_j \geq b_i + 1$ ce qui est absurde. □

Exercice 4 (Théorème de Helly) On considère quatre parties convexes du plan telles que l'intersection de trois d'entre elles est toujours non vide.

a) Montrer que l'intersection des quatre convexes est non vide.
b) Le théorème reste-t-il vrai en remplaçant 4 par $n \geq 4$?

Solution de l'exercice 4

a) On note $\mathcal{C}_1$, $\mathcal{C}_2$, $\mathcal{C}_3$ et $\mathcal{C}_4$ les quatre convexes. Soit $A_1 \in \mathcal{C}_2 \cap \mathcal{C}_3 \cap \mathcal{C}_4$. On définit de même A_2, A_3 et A_4. Si A_1, A_2, A_3 et A_4 sont les sommets d'un quadrilatère convexe, peut supposer que $[A_1A_2]$ et $[A_3A_4]$ s'intersectent. On a $[A_1A_2] \subset \mathcal{C}_3 \cap \mathcal{C}_4$ et $[A_3A_4] \subset \mathcal{C}_1 \cap \mathcal{C}_2$. Sinon, on peut supposer que A_1 est à l'intérieur du triangle $A_2A_3A_4$ donc $A_1 \in \mathcal{C}_1$, donc A_1 est dans les quatre convexes.
b) Oui : on fait une récurrence sur n en utilisant le cas $n = 4$: si le théorème vrai pour n on prend $n+1$ convexes : n quelconques ont toujours une intersection non vide. On prend 4 points dans ces intersections et on applique la preuve précédente.

Exercice 5 Soit $A_1 \dots A_n$ un polygone convexe fixé. On considère X à l'intérieur du polygone. Pour tout i, on note B_i la deuxième intersection de (A_iX) avec le bord du polygone. Montrer qu'il est possible de choisir X de telle manière que pour tout i :

$$\frac{XA_i}{XB_i} \leq 2$$

Solution de l'exercice 5 La condition $\frac{XA_i}{XB_i} \leq 2$ équivaut à $\frac{A_iX}{A_iB_i} \geq \frac{2}{3}$, ce qui revient à dire que X est dans l'image du polygone par l'homothétie de centre A_i et de rapport $\frac{2}{3}$. On note P_i cette image : C'est un polygone convexe, et il suffit de vérifier :

$$\bigcap_{i=1}^{n} P_i \neq \emptyset$$

D'après le théorème de Helly, il suffit de vérifier que l'intersection de trois P_i n'est jamais vide. C'est vrai car pour tous i, j et k le centre de gravité de $A_iA_jA_k$ se trouve dans P_i, P_j et P_k.

Exercice 6 Soit $n \geq 1$: on place dans le plan $2n$ points, trois quelconques non alignés. On en colorie n en bleu et n en rouge. Montrer qu'il est possible de tracer n segments qui ne se croisent pas, chaque segment reliant un point bleu à un point rouge, de telle manière que chaque point soit utilisé une seule fois.

Solution de l'exercice 6 On raisonne par récurrence forte sur n : le résultat est trivial pour $n = 1$. Il suffit donc de séparer les $2n$ points par une droite de manière à avoir de chaque côté de la droite autant de points bleus que rouges, et de traiter séparément chaque côté de la droite.

On considère le bord de l'enveloppe convexe des $2n$ points : si elle contient deux points de couleurs différentes, alors elle contient deux points consécutifs de couleur différente. On peut isoler ces deux points par une droite et on a gagné.

Sinon, on suppose que le bord de l'enveloppe convexe est bleu. Quitte à faire une rotation, les ordonnées des points sont deux à deux distinctes. On fait descendre une droite horizontale : le point le plus haut A_1 et le plus bas A_{2n} sont sur le bord donc sont bleus. On a donc un point bleu "en trop" au-dessus de la droite juste après avoir passé A_0 et un point rouge en trop juste avant A_{2n}. Comme on passe les points un par un on aura à un moment autant de points bleus que de rouges au-dessus de la droite, donc on a gagné !

Exercice 7 (IMO 2013) On considère un ensemble S de 4031 points dans le plan, trois quelconques non alignés, dont 2015 coloriés en bleu et 2016 en rouge. Montrer qu'il est possible de tracer 2015 droites dans le plan de telle manière que :

(i) Aucune droite ne passe par un point de S.

(ii) Aucune des régions délimitées par les 2015 droites ne contient deux points de S de couleurs différentes.

Solution de l'exercice 7 On raisonne par récurrence sur 4031. Plus précisément, on montre par récurrence sur n qu'avec $2n+1$ points on peut tracer n droites vérifiant la condition voulue, le nombre de points rouges et de points bleus n'ayant en fait aucune importance : avec 3 points, si il y en a 2 bleus et 1 rouge, il est facile de tracer une droite qui isole le point rouge. Si le problème est résolu pour n, considérons $2n+3$ points. Soient A et B deux sommets consécutifs de l'enveloppe convexe. Par hypothèse de récurrence, il existe n droites qui marchent pour $S\backslash\{A, B\}$.

Si A et B sont de la même couleur, on ajoute une droite qui isole A et B du reste et on a gagné. Sinon, on suppose A bleu et B rouge : si A et B sont dans la même région, tous les points de S dans cette région autres que A et B sont de la même couleur, par exemple rouge. On ajoute un droite qui isole A et on a gagné. Si A et B sont dans des régions différentes :

— Si la région de A ne contient que des bleus et celle de B que des rouges, on a gagné.

— Si la région de A ne contient que des rouges et celle de B que des rouges, on ajoute une droite qui isole A.

— Si la région de A ne contient que des bleus et celle de B que des bleus, on ajoute une droite qui isole B.
— Si la région de A ne contient que des rouges et celle de B que des bleus, on ajoute une droite qui isole A et B.

Exercice 8 (TFJM 2015) Soit $n \geq 1$ et S un ensemble de n points du plan. Sur chaque point de S se trouve une caméra, capable de surveiller un faisceau d'angle $\theta = \frac{2\pi}{n}$. Montrer qu'il est possible d'orienter les caméras de manière à ce que tout le plan soit surveillé.

Solution de l'exercice 8 Le principal outil de la solution est le lemme suivant :

Lemme 111. Soient $k \geq 1$ et θ tels que $k\theta \leq \pi$. On considère k caméras dans un secteur angulaire d'angle $k\theta$. Alors il est possible d'orienter les caméras de manière à surveiller le secteur opposé.

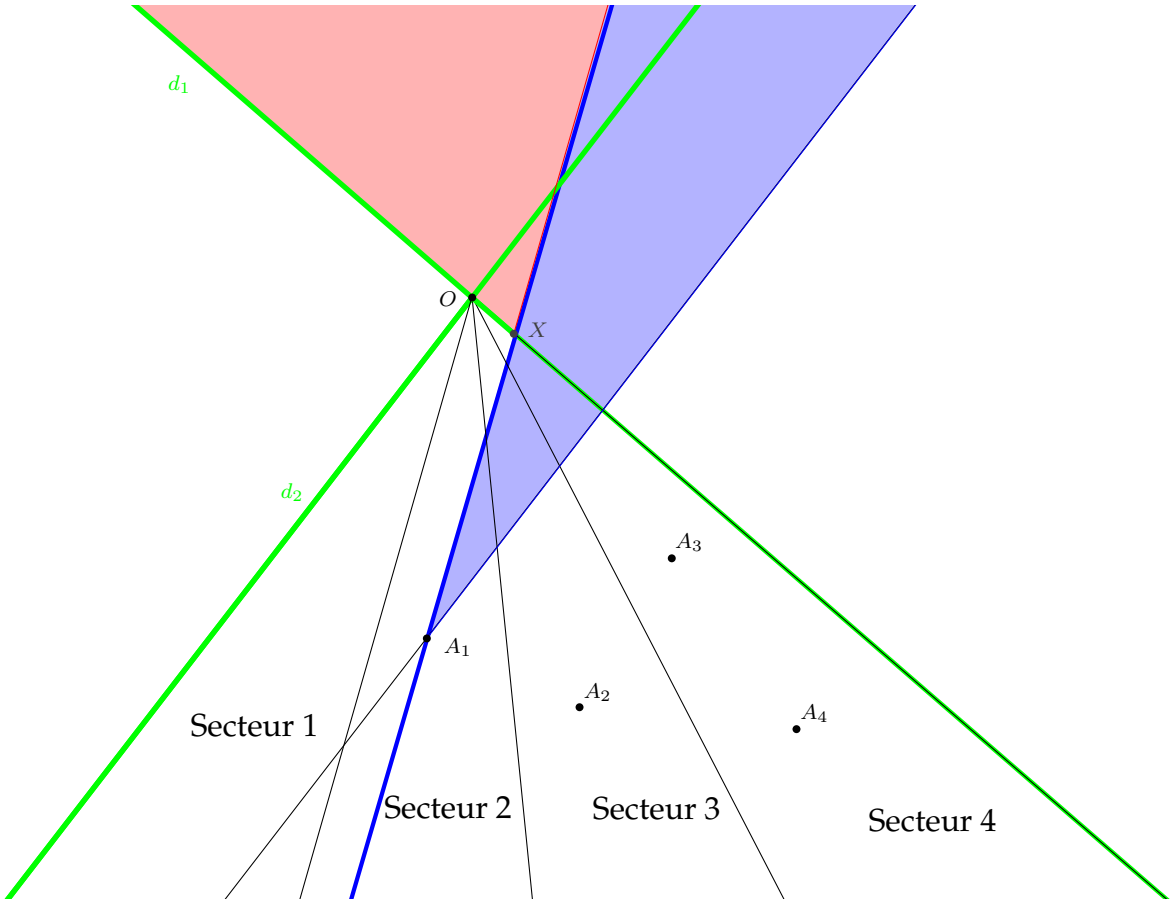
Supposons le lemme démontré : si n est pair, soit (d) une droite avec $\frac{n}{2}$ caméras de chaque côté de la droite : d'après le lemme pour $k = \frac{n}{2}$, les caméras en-dessous de la droite peuvent surveiller la zone au-dessus, et réciproquement.

Si $n = 2k + 1$ est impair, il faut diviser le plan en 3 secteurs d'angles θ, $k\theta$ et $k\theta$ tels que le premier secteur contient une caméra et les deux autres k chacun. Pour cela, il existe un point A de S sur le bord de l'enveloppe convexe tel que l'angle que fait l'enveloppe convexe en A soit au plus $\frac{n-2}{n}\pi$ (il existe car la somme des angles vaut $(k-2)\pi$ où $k \leq n$ est le nombre de sommets de l'enveloppe convexe). On choisit une demi-droite $[d)$ issue de A qui sépare les $2k$ caméras restantes en 2 groupes de k. L'hypothèse $\widehat{A} \leq \frac{n-2}{n}\pi$ assure que le secteur d'angle θ opposé à la droite ne contient pas d'autre point de S que A donc on a gagné.

Preuve du lemme. On raisonne par récurrence forte sur k : le lemme est trivial pour $k = 1$. Supposons le lemme vrai pour tout $\ell < k$: on divise notre secteur en k secteurs d'angle θ, numérotés de 1 à k dans le sens trigonométrique.

Pour tout ℓ de 1 à k, on note a_ℓ le nombre total de caméras dans les petits secteurs de 1 à, ℓ. Supposons que les secteurs 1 et k contiennent chacun au moins une caméra : cela signifie que $a_1 \geq 1$ et $a_{k-1} \leq k-1$. En posant $b_\ell = a_\ell - \ell$, on a donc $b_1 \geq 0$ et $b_{n-1} \leq 0$. Or, en passant de b_i à b_{i+1}, on ajoute le nombre de caméras du secteur i et on retire 1, donc on ne retire jamais plus de 1. Par conséquent, il existe forcément ℓ avec $1 \leq \ell \leq k-1$ tel que $b_\ell = 0$. Il y a donc ℓ caméras dans les secteurs 1 à ℓ, et $k - \ell$ dans les $k - \ell$ secteurs restants. L'hypothèse de récurrence permet de conclure.

Sinon, on peut supposer par symétrie que le secteur 1 est vide. On prend la demi-droite qui sépare le secteur 1 du secteur 2 et on l'"éloigne" du secteur 1 en conservant la direction. Soit A_1 la première caméra qu'on rencontre :



On note (d_1) et (d_2) les droites qui délimitent le grand secteur, et (d) la parallèle passant par A_1 à la droite qui sépare les secteurs 1 et 2. Cette droite recoupe (d_1) en X. On oriente A_1 pour qu'elle surveille le secteur bleu (dont le bord droit est parallèle à (d_2)). De plus, les droites (d) et (d_2) forment un angle $(k-1)\theta$ et on a $k-1$ caméras dans le secteur correspondant. Par hypothèse de récurrence, ces $k-1$ caméras peuvent surveiller le secteur rouge. L'union des secteurs bleu et rouge recouvre bien le secteur supérieur entre (d_1) et (d_2), d'où le lemme par récurrence. Ouf ! □

VII. Quatrième période

Contenu de cette partie

1 Groupe A : arithmétique

1 dimanche 23 après-midi : Eva Philippe

Arithmétique, premières notions

L'arithmétique est l'étude des nombres entiers $0, 1, 2, -3, -27\ldots$ On note $\mathbb{Z}$ l'ensemble des nombres entiers relatifs ($\mathbb{N}$ l'ensemble des entiers naturels, c'est-à-dire positifs) et on utilisera aussi la notation $n \in \mathbb{Z}$, qui se lit « n appartient à $\mathbb{Z}$ » pour dire que n est un nombre entier.

- Divisibilité -

Définition 112. Si a et b sont deux entiers, on dit que a *divise* b s'il existe un entier k tel que

$$b = ka$$

On note $a \mid b$.
On dit aussi :

- a est un diviseur de b
- b est un multiple de a
- b est divisible par a

Exemples :

- Quels sont les diviseurs de 12 ?
  $1, -1, 2, -2, 3, -3, 4, -4, 6, -6, 12, -12$
- Montrer que 421421 est divisible par 7, 11 et 13.
  $421421 = 421 \times 1001$ or $1001 = 7 \times 11 \times 13$

Proposition 113. Soient $a, b, c \in \mathbb{Z}$.

1. $a \mid b \Leftrightarrow \frac{b}{a} \in \mathbb{Z}$
2. $a \mid 0$
3. $1 \mid a$
4. $a \mid a$
5. Si $c \neq 0$, $a \mid b \Leftrightarrow ac \mid bc$
6. Si $a \mid b$ et $b \mid a$, alors $a = b$ ou $a = -b$
7. Si $a \mid b$ et $b \neq 0$, alors $|a| \leq |b|$
8. Si $a \mid b$ et $b \mid c$, alors $a \mid c$
9. Si $a \mid b$ et $a \mid c$, alors pour tous entiers u et v on a $a \mid bu + cv$

Démonstration. Montrons ces propositions point par point :

1. Par définition, $a \mid b \Leftrightarrow$ il existe $k \in \mathbb{Z}$ tel que $b = ka$. D'où $\frac{b}{a} = k \in \mathbb{Z}$.
   Dans l'autre sens, si $\frac{b}{a} \in \mathbb{Z}$, on a bien $b = \frac{b}{a} \times a$
2. $0 = 0 \times a$
3. $a = a \times 1$
4. $a = 1 \times a$
5. $a \mid b \Leftrightarrow$ il existe $k \in \mathbb{Z}$ tel que $b = ka$. Or $b = ka \Leftrightarrow bc = kac$, d'où $a \mid b \Leftrightarrow ac \mid bc$
6. Soient k_1 et k_2 des entiers tels que $b = k_1 a$ et $a = k_2 b$. Alors $b = k_1 k_2 b$ et $a = k_1 k_2 a$, d'où $a = b = 0$ ou $k_1 k_2 = 1$, c'est-à-dire $k_1 = k_2 = 1$ ou $k_1 = k_2 = -1$ car k_1 et k_2 sont entiers.
7. Soit $k \in \mathbb{Z}$ tel que $b = ka$. On a $|k| \geq 1$ car k est un entier non nul comme $b \neq 0$. D'où $|b| \geq |a|$
8. Soient k_1 et k_2 des entiers tels que $b = k_1 a$ et $c = k_2 b$. Alors $c = k_1 k_2 a$ d'où $a \mid c$.
9. Soient k_1 et k_2 des entiers tels que $b = k_1 a$ et $c = k_2 a$. Soient u et v deux entiers. On a $bu + cv = (uk_1 + vk_2)a$, d'où $a \mid bu + cv$.

□

Exercice 1 Montrer que 11 divise $4x + 9y$ si et seulement si 11 divise $7x + 2y$.

Solution de l'exercice 1 $4x + 9y = (11 - 7)x + (11 - 2)y = 11(x + y) - (7x + 2y)$ donc d'après la propriété 9, on a le résultat.

Exercice 2 Trouver les entiers positifs n tels que $n^2 + 1 \mid n + 1$.

Solution de l'exercice 2 Si $n^2 + 1 \mid n + 1$, on a $n + 1 \geq n^2 + 1$ (d'après la proposition 8) , d'où $n = 0$ ou $n = 1$. On vérifie que ces solutions fonctionnent.

Définition 114. Un nombre entier $p > 1$ est dit *premier* si ses seuls diviseurs positifs sont 1 et lui-même.

Exemples
7 est premier
1 n'est pas premier
Le seul nombre premier pair est 2.

- Division euclidienne -

Théoréme 115. Soit $a \in \mathbb{Z}$ et $b \in \mathbb{N}$, $b > 0$.
Il existe un unique couple (q, r) tel que

$$\begin{cases} a = bq + r \\ 0 \leq r < b \end{cases}$$

Il s'agit de la division euclidienne que vous connaissez bien, on appelle q le *quotient* et r le *reste* de la division.

Rappel
Pour tout $x \in \mathbb{R}$, on appelle *partie entière*, notée $\lfloor x \rfloor$, l'unique entier n tel que $n \leq x < n+1$. Si on écrit $q = \left\lfloor \frac{a}{b} \right\rfloor$ et $r = a - bq$, on a bien $a = bq + r$ et $0 \leq r < b$. L'unicité du quotient et du reste se montre par l'absurde.

Exemple
Division euclidienne de 135 par 17 : $135 = 17 \times 7 + 16$
Division euclidienne de $2x^2 + 3x - 5$ par $x + 7$: $2x^2 + 3x - 5 = (x + 7)(2x - 1) - 30$

- PGCD et algorithme d'Euclide -

Définition 116. Soient $a, b \in \mathbb{Z}$.
Le PGCD de a et b, noté $a \wedge b$ est le *plus grand commun diviseur* de a et b, c'est-à-dire le plus grand entier d tel que $d \mid a$ et $d \mid b$.
Le PPCM de deux entiers a et b, noté $a \vee b$, est le *plus petit commun multiple* de a et de b, c'est-à-dire le plus petit entier m tel que $a \mid m$ et $b \mid m$.

Remarque 117. Deux entiers a et b sont premiers entre eux si $a \wedge b = 1$. Dans le cas général, si a et b sont deux entiers quelconques, et si l'on pose $d = a \wedge b$, alors on peut écrire $a = d \times a'$ et $b = d \times b'$ où a' et b' sont deux entiers premiers entre eux.

Exemples
$9 \wedge 12 = 3$
$9 \vee 12 = 36$

Proposition 118. $a \wedge b = a \wedge (a + b)$
Plus généralement, pour tout entier $k \in \mathbb{Z}$, on a $a \wedge b = b \wedge (a + kb)$.
Démonstration. Soit $k \in \mathbb{Z}$. On note $d = a \wedge b$ et $d' = b \wedge (a + kb)$.
D'une part, $d \mid a$ et $d \mid b$ donc $d \mid a + kb$ et $d \leq d'$ (car d' est le *plus grand* diviseur commun de b et $a + kb$.
D'autre part, $d' \mid a + kb$ et $d' \mid b$ d'où $d' \mid a$ et $d' \leq d$.
Ainsi, $d = d'$. □

Définition 119. Étant donnés des entiers $a = r_0$ et $b = r_1$, l'*algorithme d'Euclide* consiste à l'étape k à effectuer la division euclidienne de r_{k-1} par r_k : $r_{k-1} = r_k \times q_k + r_{k+1}$ etc.

$$\begin{aligned} r_0 &= r_1 q_1 + r_2, \\ r_1 &= r_2 q_2 + r_3, \\ &\vdots \qquad \vdots \\ r_{l-2} &= r_{l-1} q_{l-1} + r_l, \\ r_{l-1} &= r_l q_l + 0. \end{aligned}$$

D'après la proposition précédente on a à chaque étape k, $r_k \wedge r_{k+1} = r_{k+1} \wedge r_{k+2}$.

La suite des r_k est une suite strictement décroissante d'entiers, donc elle doit finir par s'annuler. Le dernier reste non nul (ici r_l) est alors le pgcd de a et de b.

Théoréme 120. *Théorème de Bézout*

Soient $a, b \in \mathbb{Z}$ et $d = a \wedge b$. Alors il existe $u, v \in \mathbb{Z}$ tels que $au + bv = d$.

En particulier, si a et b sont premiers entre eux, il existe $u, v \in \mathbb{Z}$ tels que $au + bv = 1$.

Pour trouver la relation de Bézout entre deux entiers a et b (c'est-à-dire les u et v), on peut remonter l'algorithme d'Euclide : on part du dernier reste non nul r_l, égal à d, et on l'exprime en fonction de r_{l-1} et r_{l-2}. On exprime ainsi successivement les r_k en fonction des termes précédents jusqu'à obtenir une expression de r_l uniquement en fonction de r_0 et r_1.

Exemple

Utilisons l'algorithme d'Euclide pour trouver le pgcd de 153 et 71 et la relation de Bézout associée :

$$\begin{aligned} 153 &= 71 \times 2 + 11 \\ 71 &= 11 \times 6 + 5 \\ 11 &= 5 \times 2 + 1 \\ 5 &= 1 \times 5 + 0 \end{aligned}$$

On obtient donc $153 \wedge 71 = 1$. De plus on a en remontant :

$$\begin{aligned} 1 &= 11 - 5 \times 2 \\ 1 &= 11 - (71 - 11 \times 6) \times 2 \\ 1 &= (153 - 71 \times 2) - (71 - (153 - 71 \times 2) \times 6) \times 2 \\ 1 &= 153 \times (1 + 6 \times 2) + 71 \times (-2 - (1 + 2 \times 6) \times 2) \end{aligned}$$

On obtient finalement $1 = 153 \times 13 + 71 \times (-28)$.

Corollaire 121. *Lemme de Gauss*

Si $a \mid bc$ et $a \wedge b = 1$, alors $a \mid c$.

Démonstration. $a \wedge b = 1$ donc d'après le théorème de Bézout il existe $u, v \in \mathbb{Z}$ tel que $au + bv = 1$, d'où $cau + cbv = c$. Or $a \mid cau$ et $a \mid bc$, d'où $a \mid c$. □ Ce texte n'a pas encore été intégré.

2 lundi 24 matin : Julien Portier

- Congruences -

Définition 122 (Congruences)**.** On dit que a et b sont congrus modulo n et on note $a \equiv b \mod n$ si a et b ont le même reste dans la division euclidienne par n, c'est-à-dire si n divise $a - b$.

La relation de congruence vérifie les propriétés suivantes :
— si $a \equiv b \mod n$ et $c \equiv d \mod n$, alors $a + c \equiv b + d \mod n$,
— si $a \equiv b \mod n$ et $c \equiv d \mod n$, alors $ac \equiv bd \mod n$.
— si $a \equiv b \mod n$ et q est un entier naturel, alors $a^q \equiv b^q \mod n$

Démonstrations : 1er point : $a \equiv b \mod n$ veut dire qu'il existe des entiers k, k' et r tels que $a = nk + r$ et $b = nk' + r$. De même, comme $c \equiv d \mod n$, il existe des entiers q, q' et r' tels que $c = qn + r'$ et $d = q'n + r'$, donc $a + c = n(k + q) + (r + r')$ et $b + d = n(k' + q') + (r + r')$ donc $a + c$ et $b + d$ ont le même reste modulo n, d'où $a + c \equiv b + d \mod n$.

2ème point : se prouve de manière similaire à la première preuve.

3ème point : preuve par récurrence sur q :
— initialisation : pour $q = 1$, c'est évidemment vrai
— hérédité : supposons la propriété vraie au rang k, c'est-à-dire $a^k \equiv b^k \mod n$, alors :

$a^{k+1} \equiv a \times a^k \equiv a \times b^k \equiv b \times b^k \equiv b^{k+1} \mod n$, donc la propriété est vraie au rang $k + 1$, ce qui finit la preuve.

Attention : si $a \equiv b \mod n$, il n'est pas toujours vrai que $c^a \equiv c^b \mod n$. Par exemple $0 \equiv 3 \mod 3$, mais $2^0 \equiv 2^3 \mod 3$ est faux !

Exemple 123. Montrons qu'il n'existe pas d'entiers n et k tels que $n^2 = 4k + 3$. D'après l'équation, on a $n^2 \equiv 3 \mod 4$, or (on pourra faire un tableau pour une meilleure présentation)
— si $n \equiv 0 \mod 4$ alors $n^2 \equiv 0 \mod 4$
— si $n \equiv 1 \mod 4$ alors $n^2 \equiv 1 \mod 4$
— si $n \equiv 2 \mod 4$ alors $n^2 \equiv 0 \mod 4$
— si $n \equiv 3 \mod 4$ alors $n^2 \equiv 1 \mod 4$

il est donc impossible que $n^2 \equiv 3 \mod 4$, l'équation proposée n'a donc aucune solution.

Exercice 1 Quel est le chiffre des unités de 21^{2015} ?

Exercice 2 Trouver tous les entiers positifs a et b tels que $3a^2 = b^2 + 1$

Exercice 3 Trouver tous les entiers positifs n tels que $2^n + 3$ est un carré parfait.

Exercice 4 Trouver tous les entiers n strictement positifs tels que $n - 1 | 3n + 4$

Exercice 5 Trouver tous les entiers n strcitement positifs tels que $n + 2 | n^2 + 3n$

Exercice 6 Soit y un entier naturel non nul. Montrer que $y - 1$ divise $y^{(y^2)} - 2y^{y+1} + 1$.

Exercice 7 Trouver tous les a entiers positifs tels que $a^2 + 2a$ soit un carré parfait.

Exercice 8 Trouver tous les entiers relatifs x tels que $x^3 + (x + 1)^3 + (x + 2)^3 = (x + 3)^3$.

Exercice 9 Trouver tous les entiers positifs x, y et z tels que :

$$x^2 + y^2 - z^2 = 9 - 2xy$$

Exercice 10 Trouver tous les entiers relatifs x, y tels que $2x^3 + xy - 7 = 0$. **Exercice 11** Trouver tous les triplets d'entiers positifs (x, y, z) tels que :

$$x^2 + y^2 + 1 = 2^z$$

Solution de l'exercice 1 $21 \equiv 1 \mod 10$, donc $21^{2015} \equiv 1^{2015} \equiv 1 \mod 10$, donc le chiffre des unités de 21^{2015} est 1.

Solution de l'exercice 2 On regarde modulo 3 :
- si $b \equiv 0 \mod 3$ alors $b^2 \equiv 0 \mod 3$
- si $b \equiv 1 \mod 3$ alors $b^2 \equiv 1 \mod 3$
- si $b \equiv 2 \mod 3$ alors $b^2 \equiv 1 \mod 3$

Or, on veut, d'après l'équation $b^2 + 1 \equiv 0 \mod 3$, c'est-à-dire $b^2 \equiv 2 \mod 3$, ce qui est impossible. L'équation proposée n'a donc aucune solution.

Solution de l'exercice 3 Il s'agit de résoudre $2^n + 3 = a^2$ avec a un entier naturel. Si $2 \leq n$, alors on a $a^2 \equiv 3 \mod 4$, ce qui n'est pas possible d'après ce que nous avons vu tout à l'heure. Donc les seules possibilités sont $n = 0$ et $n = 1$, qui, après vérification, donne $n = 0$ comme seule solution.

Solution de l'exercice 4 $n-1|3n+4$ donc $n-1|(3n+4)-3(n-1) = 7$. Or, $n-1$ est positif et les seuls diviseurs positifs de 7 sont 1 et 7, donc $n-1 = 1$ ou $n-1 = 7$ c'est-à-dire $n = 2$ ou $n = 8$. Réciproquement, pour $n = 2$, on a bien $1|7 = 3x1+4$, et pour $n = 8$, on a bien $7|28 = 3 \times 8 + 4$.

Solution de l'exercice 5 $n + 2|n^2 + 3n$ donc $n + 2|(n^2 + 3n) - n(n + 2) = n$, donc $n + 2 \leq n$ c'est-à-dire $2 \leq 0$ ce qui est impossible, il n'y a donc pas de solution à l'équation proposée.

Solution de l'exercice 6 Plaçons nous modulo $y - 1$: $y \equiv 1$ (mod. $y - 1$), donc $y^{(y^2)} - 2y^{y+1} + 1 \equiv 1^{(y^2)} - 2 \times 1^{y+1} + 1 \equiv 1 - 2 + 1 \equiv 0$ (mod. $y - 1$).

Solution de l'exercice 7 On distingue deux cas. Si $a > 0$, on remarque que $a^2 < a^2 + 2a < a^2 + 2a + 1 = (a+1)^2$. Donc $a^2 + 2a$ ne peut être un carré parfait. Si $a = 0$, on trouve $a^2 + 2a = 0$ qui est un carré parfait. C'est donc le seul.

Solution de l'exercice 8 Développons les deux membres de l'égalité :

$$x^3 + x^3 + 3x^2 + 3x + 1 + x^3 + 6x^2 + 12x + 8 = x^3 + 9x^2 + 27x + 27$$

, donc

$x^3 - 6x - 9 = 0$. On en déduit que x divise 9, donc x vaut -9, -3, -1, 1, 3 ou 9. De toutes ces possibilités, seule 3 est correcte. La solution à cette équation est donc 3.

Solution de l'exercice 9 On a $(x + y)^2 - z^2 = 9, donc$(x+y-z)(x+y+z)=9, d'où en regardant les diviseurs positifs de 9 :
- $x + y - z = 3$ et $x + y + z = 3$, ce qui donne $x + y = 3$ et $z = 0$, donc en solutions $(3, 0, 0)$, $(2, 1, 0)$, $(1, 2, 0) et$(0,3,0).
- $x + y - z = 1$ et $x + y + z = 9$, ce qui donne $x + y = 5$ et $z = 4$, donc en solutions $(5, 0, 4)$, $(4, 1, 4)$, $(3, 2, 4)$, $(2, 3, 4)$, $(1, 4, 4)$ et $(0, 5, 5)$.

Solution de l'exercice 10 Tout d'abord, il est clair que $x \neq 0$. L'entier x divise 7, on a donc $x = -7, -1, 1$ ou 7. On obtient :

- si $x = -7$, $-2 \cdot 7^3 - 7y - 7 = 0$, donc $y = -2 \cdot 7^2 - 1 = -99$,
- si $x = -1$, $y = -9$,
- si $x = 1$, $y = 5$,
- si $x = 7$, $y = -97$.

Les solutions sont donc $(-7, -99)$, $(-1, -9)$, $(1, 5)$ et $(7, -97)$.

3 lundi 24 après-midi : Vincent Bouis

Définition 124. Soit p un nombre premier et n un entier non nul. On appelle *valuation p-adique* et on note $v_p(n)$ le plus grand entier positif tel que $\frac{n}{p^{v_p(n)}}$ soit entier.

Théoréme 125. Tout nombre $n \in \mathbb{N}$ supérieur ou égal à 2 s'écrit de manière unique (à ordre près des p_i) comme :

$$n = \prod_{i=1}^{k} p_i^{\alpha_i}$$

pour un certain $k \in \mathbb{N}_{>0}$, α_1, α_2, ..., α_k des entiers strictement positifs et p_1, p_2, ..., p_k des entiers premiers distincts.

Remarque 126. Avec les notations précédentes, α_i est la valuation $p_i - adique$ de n.

- Exercices -

Exercice 1 Reformuler la définition du pgcd et du ppcm avec la décomposition en facteurs premiers.

Exercice 2 Montrer qu'il existe une infinité de nombres premiers.

Exercice 3 Montrer qu'il existe une infinité de nombres premiers congrus à 3 modulo 4.

Exercice 4 Montrer que si pour p premier, a et n entiers strictement positifs tels que $p|a^n$, on a aussi $p^n|a^n$.

Exercice 5 Trouver le nombre de diviseurs (positifs) de n (un entier naturel) en fonction de sa décomposition en facteurs premiers.

Exercice 6 Montrer que $6|n^3 + 5n$.

Exercice 7 Montrer que $24|p^2 - 1$ pour tout p premier supérieur ou égal à 5.

Exercice 8 Montrer que la somme de trois cubes consécutifs est divisible par 9.

Exercice 9

(i) Trouver tous les entiers $m \geq 1$ tels que $m(m+1)$ est une puissance d'un nombre premier.

(ii) Trouver tous les entiers $m \geq 1$ tels qu'il existe deux entiers $a \geq 1$ et $k \geq 2$ tels que $m(m+1) = a^k$.

Exercice 10 Soit p un nombre premier. Montrer que l'équation $\frac{1}{x}+\frac{1}{y}=\frac{1}{p}$ avec x et y des entiers strictement positifs admet exactement 3 solutions.

Exercice 11 Soit A le nombre constitué de 600 fois le chiffre 6 suivis d'un certain nombre de fois le chiffre 0. Est-ce que A est un carré parfait ?

- Solutions -

Solution de l'exercice 1 Le pgcd (plus grand commun diviseur) de $n == \prod_{i=1}^{k} p_i^{\alpha_i}$ et $m = \prod_{i=1}^{k} p_i^{\beta_i}$ avec les α_i et les β_i positifs ou nuls, est $n \wedge m = \prod_{i=1}^{k} p_i^{min\alpha_i,\beta_i}$. De même le ppcm (plus petit commun multiple de n et m est $n \vee m = \prod_{i=1}^{k} p_i^{max\alpha_i,\beta_i}$.

Solution de l'exercice 2 Supposons par l'absurde qu'il n'en existe qu'un nombre fini, disons k (k est strictement positif car 2 est premier). On nomme ces nombres p_1, p_2, ..., p_k. Soit $A = \prod_{i=1}^{k} p_i + 1$. Comme $A > 1$, il existe un nombre premier qui le divise, disons p. Mais p fait partie des p_i donc p divise 1 : contradiction.

Solution de l'exercice 3 Supposons par l'absurde qu'il n'en existe qu'un nombre fini, disons k (k est strictement positif car 3 est premier congru à 3 modulo 4). On nomme ces nombres p_1, p_2, ..., p_k. Soit $A = 4\prod_{i=1}^{k} p_i - 1$. Comme $A > 1$, il existe au moins un nombre premier qui le divise (et 2 ne divise pas A). Si tous ces nombres premiers sont congrus à 1 modulo 4 alors leur produit (éventuellement avec multiplicité) aussi : c'est impossible donc il existe p premier qui divise A avec p congru à 3 modulo 4. On a donc p qui fait partie des p_i, d'où p divise -1 : contradiction. On a donc ce que l'on voulait.

Solution de l'exercice 4 On a $a = \prod_{i=1}^{k} p_i^{\alpha_i}$ donc $a^n = \prod_{i=1}^{k} p_i^{n\alpha_i}$. Si $p|a^n$ alors p fait partie des p_i et comme $\alpha_i > 0$ par définition. D'où $\alpha_i \geq 1$. Le fait que $p^n|a^n$ est équivalent à $n \leq n\alpha_i$, ce qui est équivalent à $\alpha_i \geq 1$, ce qui est vrai.

Solution de l'exercice 5 Si $n = \prod_{i=1}^{k} p_i^{\alpha_i}$, chaque diviseur positif de n correspond à exactement un $d = \prod_{i=1}^{k} p_i^{\beta_i}$ avec $0 \leq \beta_i \leq \alpha_i$. Chaque β_i peut donc être choisi de manière indépendante parmi $\alpha_i + 1$ valeurs. n a donc $\prod_{i=1}^{k} (\alpha_i + 1)$ diviseurs positifs.

Solution de l'exercice 6 On regarde les valeurs modulo 6 de $n^3 + 5n$ en fonction des valeurs de n modulo 6.

Solution de l'exercice 7 On a $p^2 \equiv 1[8]$ puisque p impair et $p^2 \equiv 1[3]$ car p n'est pas divisible par 3. On en déduit le résultat.

Solution de l'exercice 8 Il faut et il suffit de montrer que $a^3 + (a+1)^3 + (a+2)^3 \equiv 0[9]$, soit en développant avec le binôme de Newton $3a^3 + 9a^2 + 15a + 9 \equiv 0[9]$, soit $3a(a^2+5) \equiv 0[9]$. Or soit a est divisible par 3 et on a fini, soit a ne l'est pas et $a^2 + 5$ est divisible par 3 et on a aussi fini.

Solution de l'exercice 9

(i) Écrivons $m(m+1) = p^k$ avec p un nombre premier et $k \geq 1$. Alors m et $m+1$ sont tous les deux des puissances de p. Écrivons donc $m = p^a$ et $m+1 = p^b$ avec $a, b \geq 0$ et $a + b = k$. Comme $p^b = m + 1 \geq m = p^a$, on a $b \geq a$. Mais on a $p^b - p^a = 1$. Ainsi, si $a \geq 1$, p divise $p^b - p^a$ et donc p divise 1, absurde. Donc $a = 0$. Ainsi, $p^b = 2$, et donc $p = 2$ et $b = 1$, ce qui entraine forcément $m = 1$.

(ii) Par l'absurde, supposons qu'il existe des entiers $m \geq 1$, $a \geq 1$ et $k \geq 2$ tels que $m(m+1) = a^k$. Comme m et $m+1$ sont premiers entre eux, il existe deux entiers positifs b, c premiers entre eux tels que $m = b^k$, $m+1 = c^k$ et $bc = a$. Alors $c^k - b^k = 1$. Or $c - b$ divise $c^k - b^k$. Donc $c - b$ divise 1. Donc, comme $c \geq b$, on a $c = b + 1$. Donc $1 + b^k = (b+1)^k$. En développant $(b+1)^k$, on obtient :

$$1 + b^k = 1 + \binom{k}{1} b + \binom{k}{2} b^2 + \cdots + \binom{k}{k-1} b^{k-1} + b^k.$$

En simplifiant :

$$0 = \binom{k}{1} b + \binom{k}{2} b^2 + \cdots + \binom{k}{k-1} b^{k-1}.$$

Comme $b > 0$ et $k > 2$, le terme de droite est strictement positif, contradiction.

Solution de l'exercice 10 On voit que x et y sont strictement supérieurs à p. On pose alors $x = a + p$ et $y = b + p$. L'équation est alors équivalente à $p(a+p) + p(b+p) = (a+p)(b+p)$, soit $p^2 = ab$. Les seules solutions pour (a, b) (a et b étant positifs) sont donc $(1, p^2)$, (p, p), $(p^2, 1)$, ce qui fait bien trois solutions.

Solution de l'exercice 11 On regarde la valuation 5-adique de A pour savoir que le nombre de 0, disons n, est pair. A est donc un carré si et seulement si $B = \frac{A}{10^n}$ en est un. Or la valuation 2-adique de B est 1 et donc B ne peut pas être un carré.

2 Groupe B : arithmétique

1 dimanche 23 après-midi : Julien Portier

Ce cours a pour but de donner les bases de l'arithmétique, qui est l'étude des nombres entiers.

- Divisibilité -

Définition 127. Si a et b sont deux entiers, on dit que a divise b, ou que b est divisible par a, s'il existe un entier q tel que $b = aq$. On dit que a est un diviseur de b, ou que b est un multiple de a. On le note $a|b$.

Exemple 128. 4 divise 12 puisque $12 = 4 \times 3$ et 3 est entier, mais 4 ne divise pas 18 car $18 = 4 \times 4,5$ et 4,5 n'est pas entier.

Quelques remarques :
— tout entier a divise 0 et est divisible par -1, 1, $-a$ et a,
— si $a|b$ et $b|c$ alors $a|c$,
— soit m un entier non nul, $a|b$ est équivalent à $ma|mb$,
— si $a|b$ et $a|c$, alors $a|bx + cy$ pour tous entiers x, y. En particulier, $a|b - c$ et $a|b + c$.
— si a et b sont des entiers strictement positifs tels que $a|b$, alors $a \leqslant b$
— si $a|b$ et $b|a$, alors $a = b$ ou $a = -b$

Démonstration du 2ème point : si $a|b$, alors il existe un entier q avec $b = aq$. Si $b|c$, alors il existe un entier k avec $c = bk$, donc $c = kqa$, kq est bien un entier, donc $a|c$. Les autres points sont soit évidents, soit s'obtiennent de la même manière.

Exemple 129. Trouver tous les entiers n positifs tels que $n+1|n+3$.

$n+1|(n+3)-(n+1)=2$. $n+1$ est positif et les seuls diviseurs positifs de 2 sont 1 et 2, donc $n+1=1$ ou $n+1=2$, donc $n=0$ ou $n=1$. Réciproquement, ces nombres sont bien solutions.

Exercice 1 Trouver tous les entiers n strictement positifs tels que $n-1|3n+4$

Exercice 2 Trouver tous les entiers n strcitement positifs tels que $n+2|n^2+3n$

Exercice 3 Pour quels entiers n strictement positifs, le nombre n^2+1 divise-t-il $n+1$?

Exercice 4 Trouver tous les entiers relatifs x, y tels que $2x^3+xy-7=0$.

<u>Solution de l'exercice 1</u> $n-1|3n+4$ donc $n-1|(3n+4)-3(n-1)=7$. Or, $n-1$ est positif et les seuls diviseurs positifs de 7 sont 1 et 7, donc $n-1=1$ ou $n-1=7$ c'est-à-dire $n=2$ ou $n=8$. Réciproquement, pour $n=2$, on a bien $1|7=3\times1+4$, et pour $n=8$, on a bien $7|28=3\times8+4$.

<u>Solution de l'exercice 2</u> $n+2|n^2+3n$ donc $n+2|(n^2+3n)-n(n+2)=n$, donc $n+2\leq n$ c'est-à-dire $2\leq 0$ ce qui est impossible, il n'y a donc pas de solution à l'équation proposée.

<u>Solution de l'exercice 3</u> Si n^2+1 divise $n+1$, on doit avoir $n^2+1\leq n+1$, ou encore $n^2\leq n$, c'est-à-dire $n\leq 1$. La seule possibilité est donc $n=1$. Réciproquement, $n=1$ convient bien.

<u>Solution de l'exercice 4</u> Tout d'abord, il est clair que $x\neq 0$. L'entier x divise 7, on a donc $x=-7,-1,1$ ou 7. On obtient :

- si $x=-7$, $-2\cdot 7^3-7y-7=0$, donc $y=-2\cdot 7^2-1=-99$,
- si $x=-1$, $y=-9$,
- si $x=1$, $y=5$,
- si $x=7$, $y=-97$.

Les solutions sont donc $(-7,-99)$, $(-1,-9)$, $(1,5)$ et $(7,-97)$.

- Pgcd -

Définition 130 (Plus grand commun diviseur)**.** Un entier divisant à la fois l'entier a et l'entier b (non tous les deux nuls), est appelé diviseur commun de a et b. Le plus grand nombre strictement positif parmi ces diviseurs communs est appelé plus grand commun diviseur de a et b, on le note $\mathrm{pgcd}(a,b)$. On dit que a et b sont premiers entre eux si $pgcd(a,b)=1$. On peut alors écrire $a=da'$ et $b=db'$ avec a' et b' premiers entre eux.

Exemple 131. On choisit $n+1$ entiers compris entre 1 et $2n$. Montrer que parmi eux il y en a deux qui sont premiers entre eux.

Si on choisit $n+1$ entiers dans $\{1,\ldots,2n\}$, il y en aura forcément deux qui seront consécutifs : ces deux-là seront premiers entre eux.

Exercice 5 Trouver toutes les solutions $(x,y)\in\mathbb{N}^2$ de l'équation : $d+\frac{xy}{d}=x+y$ avec d le pgcd de x et y.

Solution de l'exercice 5 Il existe $x', y' \in \mathbb{N}$ tels que :

$$\begin{cases} x = dx' \\ y = dy' \\ x' et\ y'\ sont\ premiers\ entre\ eux \end{cases}$$

L'équation devient :

$$\begin{aligned} 1 + x'y' = x' + y' &\iff (x'-1)(y'-1) = 0 \\ &\iff x' = 1 \text{ ou } y' = 1. \end{aligned}$$

Ainsi (x, y) est de la forme (d, dk) ou (dk, d) avec $d, k \in \mathbb{N}$.

Réciproquement, ces couples sont bien solution.

- Nombres premiers -

Définition 132 (Nombres premiers)**.** Un entier naturel $p > 1$ est dit premier s'il possède exactement deux diviseurs naturels : c'est-à-dire 1 et p. Un nombre qui n'est pas premier est un nombre composé.

Exemple 133. $2, 3, 5, 7, 11, 13, 17, \ldots$ sont des nombres premiers mais 21 est composé car $3|21$.

Théoréme 134 (Théorème fondamental de l'arithmétique)**.** Tout entier naturel $n > 1$ se décompose de manière unique en produit de nombres premiers. On a donc

$$n = p_1^{\alpha_1} \times \cdots \times p_k^{\alpha_k} = \prod_{i=1}^{k} p_i^{\alpha_i},$$

où les p_i sont des nombres premiers distincts $p_1 < \cdots < p_k$ et les α_i strictement positifs.

Exemple 135. La décomposition en facteurs premiers de 60 est $60 = 2^2 \times 3 \times 5$

Théoréme 136. L'ensemble des nombres premiers est infini.

Démonstration. Supposons par l'absurde qu'il n'y a qu'un nombre fini n de nombres premiers. Notons ces nombres premiers $p_1, \ldots, p_n$, et posons $N = p_1 p_2 \ldots p_n + 1$. L'entier N n'est divisible par aucun des p_i. Donc soit il est premier, soit il admet un diviseur premier différent de $p_1, \ldots, p_n$. Dans tous les cas, on obtient une contradiction.

Lemme de Gauss : soit trois entiers a, b et c tels que $a \mid b \times c$. Si a et b sont premiers entre eux, alors $a \mid c$.

Avec ce que l'on a vu précédemment, ce résultat est assez intuitif. L'hypothèse $a \mid b \times c$ peut se traduire par le fait que l'on retrouve tous les éléments de la décomposition en facteurs premiers de a dans le produit $b \times c$. Mais comme $a \wedge b = 1$, aucun de ces éléments ne figure dans la décomposition de b. Ils doivent donc tous venir de c, d'où la conclusion.

Exemple 137. Montrer que si deux entiers premiers entre eux a et b divisent n, alors le produit ab divise également n.

Comme a divise n, on peut écrire $n = ak$ pour un certain entier k. Mais alors b divise ak et comme il est premier avec a, il divise k. Ainsi $k = bk'$ pour un entier k' et puis $n = abk'$, ce qui prouve bien que ab divise n.

On peut aussi voir cela différemment : a divise n veut dire que l'on retrouve tous les éléments de la décomposition en facteurs premiers de a dans n. De même, b divise n veut dire que l'on retrouve tous les éléments de la décomposition en facteurs premiers de b dans n. Or, comme les facteurs premiers de a et b sont distincts (car a et b sont premiers entre eux), on en conclut que ab divise n.

- Congruences -

Théoréme 138 (Division euclidienne)**.** Soit b un entier strictement positif. Tout entier a s'écrit, de manière unique, sous la forme $a = bq + r$, où q et r sont des entiers, avec $0 \leq r < b$. On appelle q le quotient et r le reste de la division euclidienne de a par b.

Définition 139 (Congruences)**.** On dit que a et b sont congrus modulo n et on note $a \equiv b \mod n$ si a et b ont le même reste dans la division euclidienne par n, c'est-à-dire si n divise $a - b$.

La relation de congruence vérifie les propriétés suivantes :
— si $a \equiv b \mod n$ et $c \equiv d \mod n$, alors $a + c \equiv b + d \mod n$,
— si $a \equiv b \mod n$ et $c \equiv d \mod n$, alors $ac \equiv bd \mod n$.
— si $a \equiv b \mod n$ et q est un entier naturel, alors $a^q \equiv b^q \mod n$

Démonstrations : $a \equiv b \mod n$ veut dire qu'il existe des entiers k, k' et r tels que $a = nk + r$ et $b = nk' + r$. De même, comme $c \equiv d \mod n$, il existe des entiers q, q' et r' tels que $c = qn + r'$ et $d = q'n + r'$, donc $a + c = n(k + q) + (r + r')$ et $b + d = n(k' + q') + (r + r')$ donc $a + c$ et $b + d$ ont le même reste modulo n, d'où $a + c \equiv b + d \mod n$. Le 2ème point se prouve de manière similaire, et le 3ème se prouve facilement par récurrence.

Attention : si $a \equiv b \mod n$, il n'est pas toujours vrai que $c^a \equiv c^b \mod n$. Par exemple $0 \equiv 3 \mod 3$, mais $2^0 \equiv 2^3 \mod 3$ est faux !

Exemple 140. Montrons qu'il n'existe pas d'entiers n et k tels que $n^2 = 4k + 3$. D'après l'équation, on a $n^2 \equiv 3 \mod 4$, or (on pourra faire un tableau pour une meilleure présentation)
— si $n \equiv 0 \mod 4$ alors $n^2 \equiv 0 \mod 4$
— si $n \equiv 1 \mod 4$ alors $n^2 \equiv 1 \mod 4$
— si $n \equiv 2 \mod 4$ alors $n^2 \equiv 0 \mod 4$
— si $n \equiv 3 \mod 4$ alors $n^2 \equiv 1 \mod 4$
il est donc impossible que $n^2 \equiv 3 \mod 4$, l'équation proposée n'a donc aucune solution.

Exercice 6 Trouver tous les entiers positifs a et b tels que $3a^2 = b^2 + 1$

Exercice 7 Trouver tous les triplets d'entiers positifs (x, y, z) tels que :

$$x^2 + y^2 + 1 = 2^z$$

Exercice 8 Trouver tous les entiers strictement positifs a et b tels que $a + 1$ divise $a^3b - 1$ et $b - 1$ divise $b^3a + 1$

Solution de l'exercice 6 On regarde modulo 3 :
— si $b \equiv 0 \mod 3$ alors $b^2 \equiv 0 \mod 3$
— si $b \equiv 1 \mod 3$ alors $b^2 \equiv 1 \mod 3$
— si $b \equiv 2 \mod 3$ alors $b^2 \equiv 1 \mod 3$

Or, on veut, d'après l'équation $b^2+1 \equiv 0 \mod 3$, c'est-à-dire $b^2 \equiv 2 \mod 3$, ce qui est impossible. L'équation proposée n'a donc aucune solution.

Solution de l'exercice 7 On regarde modulo 4 : si $2 \leq z$, alors le membre de gauche est divisible par 4, or modulo 4 :

— si $n \equiv 0 \mod 4$ alors $n^2 \equiv 0 \mod 4$
— si $n \equiv 1 \mod 4$ alors $n^2 \equiv 1 \mod 4$
— si $n \equiv 2 \mod 4$ alors $n^2 \equiv 0 \mod 4$
— si $n \equiv 3 \mod 4$ alors $n^2 \equiv 1 \mod 4$

donc $n^2 \equiv 0 \mod 4$ ou $n^2 \equiv 1 \mod 4$, donc x^2+y^2+1 est congru à 0, 1, 2, 3 modulo 4, donc le membre de gauche n'est jamais divisible par 4, ce qui impose $z \leq 1$.

— $z=1$ donne $x^2+y^2=1$, donc $x=0$ et $y=1$ ou $x=1$ et $y=0$
— $z=0$ donne $x^2+y^2=0$, donc $x=0$ et $y=0$

Solution de l'exercice 8 On veut $a^3b-1 \equiv 0 \mod a+1$. Or $a+1 \equiv 0 \mod a+1$ donc $a \equiv -1 \mod a+1$, donc $a^3 \equiv (-1)^3 \mod a+1$, d'où $a^3 \equiv -1 \mod a+1$. En reportant dans $a^3b-1 \equiv 0 \mod a+1$, on obtient $-b-1 \equiv 0 \mod a+1$, c'est-à-dire $b+1 \equiv 0 \mod a+1$ donc $a+1$ divise $b+1$.

D'autre part, on veut $b^3a+1 \equiv 0 \mod b-1$. Or, $b \equiv 1 \mod b-1$, donc $b^3 \equiv 1 \mod b-1$, donc en reportant dans $b^3a+1 \equiv 0 \mod b-1$, on obtient que $a+1 \equiv 0 \mod b-1$, c'est-à-dire $b-1$ divise $a+1$.

On a $b-1$ divise $a+1$ et $a+1$ divise $b+1$, donc $b-1$ divise $b+1$, donc $b-1$ divise 2, ce qui donne :

— 1er cas : $b-1=2$, donc $b=3$, ce qui donne $a=3$ ou $a=1$.
— 2ème cas : $b-1=1$, donc $b=2$, ce qui donne $a=2$.

Finalement, les solutions sont donc $b=3$ et $a=1$, $a=b=2$ et $a=b=3$.

2 lundi 24 matin : Louise Gassot

- Algorithme d'Euclide et théorème de Bézout -

Proposition 141 (Algorithme d'Euclide)**.** Soient $a \geq b > 0$ deux entiers. On définit une suite (u_n) par : $u_1 = a$, $u_2 = b$ et tant que u_n n'est pas nul, u_{n+1} est le reste de la division euclidienne de u_{n-1} par u_n. Alors la suite (u_n) s'arrête nécessairement et le dernier terme non nul de cette suite vaut $\mathrm{pgcd}(a,b)$.

Exercice 1 Montrer que pour tout n entier, la fraction $\frac{39n+4}{26n+3}$ est irréductible.

Solution de l'exercice 1 Les exercices de ce types amènent à faire la divisions euclidienne du numérateur par le dénominateur et à réitérer conformément à l'algorithme d'Euclide. Cela s'écrit :

$$39n+4 = (26n+3)+(13n+1)$$

$$26n+3 = 2(13n+1)+1$$

Le pgcd de $39n+4$ et $26n+3$ vaut donc 1, ce qui montre que la fraction est irréductible.

Théorème 2.1 (Bézout)**.** Soient a et b deux entiers relatifs non tous les deux nuls, et d leur pgcd. Alors il existe des entiers relatifs u et v tels que $au + bv = d$.
En particulier, a et b sont premiers entre eux si, et seulement s'il existe des entiers u et v tels que $au + bv = 1$.

Exercice 2 Existe-t-il un entier n tel que $21n \equiv 1[74]$?

Solution de l'exercice 2 On applique l'algorithme d'Euclide étendu :

$$74 = 21 \times 3 + 11$$
$$21 = 11 \times 1 + 10$$
$$11 = 10 \times 1 + 1$$

21 et 74 sont premiers entre eux, donc on peut trouver u et v tels que $21u + 74v = 1$. L'entier u conviendra alors.

$$1 = 11 - 10$$
$$1 = 11 - (21 - 11) = -21 + 2 \times 11$$
$$1 = -21 + 2 \times (74 - 21 \times 3) = 2 \times 74 - 7 \times 21$$

On a donc : $21 \times (-7) \equiv 1[74]$. On dira que -7 est un inverse de 21 modulo 74 (n'oubions pas que la classe de -7 modulo 74 est la même que la classe de 67 !).

Proposition 142. Si a et b sont premiers entre eux, alors a possède un inverse modulo b.

- Valuation p-adique -

Définition 143 (Valuation p-adique)**.** Si p est un nombre premier, et n un entier non nul, la valuation p-adique de n, notée $v_p(n)$, est le plus grand entier k tel que p^k divise n (on convient que $v_p(0) = +\infty$).

Si n non nul se décompose sous la forme $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, alors $v_{p_i}(n) = \alpha_i$ pour tout $1 \leq i \leq k$, et $v_p(n) = 0$ si p est distinct des p_i. Ainsi, $v_p(n) = 0$ sauf pour un nombre fini de p premiers. Si a et b sont deux entiers, on a, pour tout nombre premier p :

$$v_p(ab) = v_p(a) + v_p(b)$$

$$v_p(a + b) \geq \min(v_p(a), v_p(b))$$

et la dernière inégalité est une égalité dès que $v_p(a) \neq v_p(b)$.

Exemple 144. $v_3(54) = v_3(3^3 \times 2) = 3$

Théoréme 145 (Formule de Legendre)**.** On note $[x]$ la partie entière du réel x. Montrer que si p est un nombre premier et n est un entier positif, on a

$$v_p(n!) = \sum_{i=1}^{\infty} \left[\frac{n}{p^i}\right] = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \dots.$$

Lorsque $p^i > n$, on a $[\frac{n}{p^i}] = 0$. Ceci assure qu'il n'y a bien qu'un nombre fini de termes non nuls dans la somme précédente.

Démonstration. Pour un entier positif ou nul i, soit n_i le nombre d'entiers compris entre 1 et n dont la valuation p-adique est exactement i. On a alors :

$$v_p(n!) = n_1 + 2n_2 + 3n_3 \dots$$

Or les entiers donc la valuation p-adiques vaut au moins i sont les multiples de p^i, il y en a $\left[\frac{n!}{p^i}\right]$ entre 1 et $n!$, c'est-à-dire :

$$\left[\frac{n!}{p^i}\right] = n_i + n_{i+1} + \dots$$

Ce qui conduit au résultat.

Exercice 3 Calculer le nombre de zéros à la fin de $2015!$.

<u>*Solution de l'exercice 3*</u> Comme $10 = 2\times5$, le nombre de zéros à la fin de $2015!$ vaut $\min(v_2(2015!), v_5(2015!))$ Or il y a plus de facteurs 2 que de facteurs 5. Donc on calcule $v_5(2015!)$ à l'aide de la formule de Legendre :

$$v_5(2015!) = \sum_{k=1}^{+\infty} \left[\frac{2015}{5^k}\right] = 502$$

- Théorème chinois -

Théoréme 146 (Théorème chinois)**.** Soient $a_1, \dots, a_d$ des entiers relatifs et $N_1, \dots, N_d$ des entiers strictement positifs deux à deux premiers entre eux. Alors il existe un entier a tel que le système de congruences :

$$\begin{cases} x & \equiv a_1[N_1] \\ & \vdots \\ x & \equiv a_d[N_d] \end{cases}$$

soit équivalent à la seule congruence $x \equiv a[N_1 \dots N_d]$

Démonstration. On remarque dans un premier temps qu'il suffit de prouver le théorème lorsque $k = 2$. Une récurrence directe permettra ensuite de l'avoir dans toute sa généralité. On cherche à résoudre l'équation

$$\begin{cases} x & \equiv a_1[N_1] \\ x & \equiv a_2[N_2]. \end{cases}$$

La première condition assure l'existence d'un entier q tel que $x = a_1 + qN_1$ et la seconde congruence s'écrit alors :

$$a_1 + qN_1 \equiv a_2[N_2],$$

ce qui fournit :

$$q \equiv (a_2 - a_1)N_1'[N_2],$$

où N_1' désigne un inverse de N_1 modulo N_2, qui existe bien car N_1 et N_2 sont supposés premiers entre eux. Ainsi, en posant $a = a_1 + (a_2 - a_1)N_1'N_1$, on obtient $x \equiv a[N_1N_2]$.

La réciproque est immédiate.

Exercice 4 Trouver tous les entiers n congrus à 10 modulo 11 et à 7 modulo 18.

Solution de l'exercice 4 11 et 18 sont premiers entre eux donc on peut utiliser la démonstration du théorème chinois. On a : $a_1 = 10, a_2 = 7, N_1 = 11, N_2 = 18$. Pour trouver un inverse de 11 modulo 18, on applique l'algorithme d'Euclide étendu :

$$18 = 11 + 711 = 7 + 47 = 4 + 34 = 3 + 1$$

En remontant, on a donc

$$1 = 4 - 3 = -7 + 2 \times 4 = -3 \times 7 + 2 \times 11 = -3 \times 18 + 5 \times 11.$$

Donc 5 est un inverse de 11 modulo 18. Par conséquent, les entiers n congrus à 10 modulo 11 et à 7 modulo 18 sont ceux qui vérifient :

$$n \equiv a[198],$$

avec $a = 10-3\times5\times11 = -155$. Or $a \equiv 43[198]$ donc les solutions sont les n tels que $n \equiv 43[198]$.

- Petit théorème de Fermat -

Théoréme 147 (Petit théorème de Fermat)**.** Soit p un nombre premier. Alors pour tout entier a premier avec p, on a

$$a^{p-1} \equiv 1[p].$$

Ce théorème se réécrit aussi : pour tout entier a,

$$a^p \equiv a[p].$$

Démonstration. La multiplication par a définit une bijection de $(\mathbb{Z}/p\mathbb{Z})^*$ sur $(\mathbb{Z}/p\mathbb{Z})^*$. En effet, l'ensemble des résidus est fini et si $ax \equiv ay[p]$, alors $x \equiv y[p]$. Par conséquent,

$$(1a)(2a)(3a)\dots((p-1)a) \equiv (1)(2)(3)\dots(p-1)[p].$$

Ceci se réécrit $(p-1)!a^{p-1} \equiv (p-1)![p]$. Le facteur $(p-1)!$ est premier avec p, donc inversible modulo p, ce qui conclut.

Exercice 5 Soit p un nombre premier. Démontrer que, pour tout entier naturel n, p divise $3^{n+p} - 3^{n+1}$.

Solution de l'exercice 5 D'après le petit théorème de Fermat, $3^p \equiv 3[p]$.
Donc pour tout entier naturel n,

$$3^{n+p} \equiv 3^n \times 3[p]$$

donc

$$3^{n+p} \equiv 3^{n+1}[p].$$

Exercice 6 Démontrer que pour tout entier naturel n, 42 divise $n(n^6 - 1)$.

Solution de l'exercice 6 $42 = 2 \times 3 \times 7$ donc il suffit de montrer que $2, 3$ et 7 divisent $n(n^6 - 1)$.
D'après le petit théorème de Fermat, $n^7 \equiv n[7]$ donc 7 divise $n(n^6 - 1)$.
De plus, $n(n^6 - 1) = n(n^2 - 1)(n^4 + n^2 + 1)$ et d'après le petit théorème de Fermat, $n^3 \equiv n[3]$ donc 3 divise $n(n^6 - 1)$. De plus, n et $n^2 - 1$ sont de parités différentes donc 2 divise $n(n^6 - 1)$.

- Théorème de Wilson -

Théoréme 148. Soit $n > 1$ un entier. Alors n est premier si, et seulement si on a la congruence $(n-1)! \equiv -1[n]$

Démonstration. Si $n = p$ est premier, on élimine, dans le produit des $p-1$ éléments de $\mathbb{Z}/p\mathbb{Z}$, chaque produit d'un élément par son inverse, à l'exception des éléments qui sont leur propre inverse. Or $a^2 \equiv 1[p]$ équivaut à $a \equiv 1[p]$ ou $a \equiv -1[p]$. Donc en éliminant, dans le produit, les paires d'inverses mutuels dont le produit vaut 1, il reste uniquement les classes $\overline{-1}$ et $\overline{1}$, d'où

$$(p-1)! \equiv -1[p].$$

Si n est le carré d'un nombre premier, on pose $n = p^2$ et alors

$$v_p((p^2-1)!) \geq \left[\frac{p^2-1}{p}\right] \geq p-1$$

Si $p > 2$, le nombre $(p^2-1)!$ est multiple de p^2 est donc non congru à -1 modulo p^2. On vérifie que c'est également le cas pour $p = 2$.

Sinon, on peut écrire $n = ab$ pour deux entiers $a, b \leq n-1$ et distincts. On voit alors que n divise $(n-1)!$.

- Autour des congruences -

Proposition 149. Si n est un entier, alors $n^2 \equiv 0$ ou $1[4]$.

Exercice 7 Trouver tous les entiers naturels n tels que $2^n + 3$ soit un carré parfait.

Solution de l'exercice 7 Pour $n = 0$, $2^n + 3 = 2^2$ est un carré parfait. On vérifie que $n = 1$ n'est pas solution. Donc on peut supposer $n \geq 2$ et alors $2^n + 3 \equiv 3[4]$. Or un carré est congru à 0 ou 1 modulo 4 donc pour $n \geq 2$, $2^n + 3$ n'est pas un carré parfait.

Proposition 150. Si n est un entier, alors $n^3 \equiv -1, 0$ ou $1[7]$.

Exercice 8 Montrer que si 7 divise $x^3 + y^3 + z^3$, avec $(x, y, z) \in \mathbb{Z}^3$, alors 7 divise xyz.

Solution de l'exercice 8 D'après la propriété qui précède, si $7|x^3 + y^3 + z^3$, alors soit x, y et z sont tous divisibles par 7, soit $x^3, y^3, z^3 = 0, -1, 1[7]$. Donc 7 divise x^3, y^3 ou z^3, donc 7 divise xyz.

Remarque 151. Si p est un nombre premier et n un entier, alors $n^{\frac{p-1}{2}} \equiv -1, 0$ ou $1[p]$.

3 lundi 24 après-midi : Félix Lequen

Tout d'abord, quelques remarques générales :

1. En arithmétique, il est important de tester numériquement, de calculer, de noircir des feuilles (mais pas trop), d'essayer de formuler des conjectures, etc. De même, ne pas hésiter à traiter tous les cas à la main, lorsqu'il n'y en a pas trop.
2. Vous avez à votre disposition plusieurs outils : parité et congruences, PGCD, divisibilité et valuations p-adiques, inégalités, etc. De nombreux problèmes, notamment des équations diophantiennes, sont des exercices finalement assez simples où il s'agit d'utiliser tout cet arsenal judicieusement, sans forcément nécessiter d'astuces ou d'idée particulières.

3. Les PGCD sont souvent des objets très pertinents à introduire. Lorsque l'on comprend bien les PGCD des différents entiers en jeu, on est très souvent proche du but.
4. Si possible, essayez dès lors qu'un problème semble un peu compliqué de vous ramener à un cas plus simple : par exemple, en artihmétique, il est souvent très pratique de travailler avec des nombres premiers. Par exemple, si vous voulez montrer qu'un entier n vaut 1 ou -1, il est souvent utile de considérer un facteur premier p de n, et d'aboutir à une contradiction.
5. Bien comprendre ce que signifie la factorisation en nombres premiers. En particulier, elle implique (essentiellement) que tout problème d'arithmétique où n'interviennent pas d'additions est assez facile.
6. Ne pas hésiter à séparer différents cas (par exemple quand une variable est nulle ou vaut 1, etc.).

Exercices pas trop durs

Exercice 1 Soit n un entier naturel. Montrer que $n-1$ divise n^2+n-2.

Exercice 2 Soit a, b et n trois entiers naturels, tels que $a \neq 0$. On note d le PGCD de a et b. Montrer que n divise a et b si et seulement si n divise d. En déduire, pour tout entier $c > 0$, la relation $\mathrm{PGCD}(ac, bc) = c\mathrm{PGCD}(a, b)$.

Exercice 3 Soit a un entier. Montrer que 2 divise $a^2 - a$ et que 3 divise $a^3 - a$.

Exercice 4 Soit $P(X) = aX^3 + bX^2 + cX + d$ un polynôme à coefficients entiers, et x, y deux entiers distincts. Montrer que $x - y$ divise $P(x) - P(y)$.

Exercice 5 Soit y un entier naturel non nul. Montrer que $y-1$ divise $y^{(y^2)} - 2y^{y+1} + 1$.

Exercice 6 Trouver les entiers n tels que 5 divise $3n-2$ et 7 divise $2n+1$.

Exercice 7 Trouver les entiers n tels que 6 divise $n-4$ et 10 divise $n-8$.

Exercice 8 Trouver l'ensemble des entiers a tels que l'équation $2a^2 = 7k+2$ admet une solution k entière.

Exercice 9 (JBMO 2013) Trouver les entiers naturels non nuls a et b tels que $\frac{a^3b-1}{a+1}$ et $\frac{b^3a+1}{b-1}$ sont entiers.

Exercice 10 Trouver l'ensemble des entiers a tels que 35 divise $a^3 - 1$.

Exercice 11 Trouver tous les entiers n tels que $n(n+1)$ soit un carré parfait.

Exercice 12 Trouver les entiers $a, b, c \geq 1$ tels que $\frac{1}{a} + \frac{1}{b} + \frac{1}{c} = 1$.

Exercice 13 Quels sont les deux derniers chiffres de $7^{9^{9^9}}$?

Exercice 14 Donner une condition nécessaire et suffisante sur p et q pour que pour tout réel x, $x \in \mathbb{Q}$ si et seulement si $x^p \in \mathbb{Q}$ et $x^q \in \mathbb{Q}$.

Exercice 15 Montrer que l'équation $a^2 + b^2 + c^2 = 2007$ n'admet pas de solutions entières.

Exercice 16 Calculer le nombre de 0 à la fin de 2014 !.

Exercice 17 Montrer que la somme de cinq carrés d'entiers consécutifs n'est jamais un carré parfait.

Exercice 18 (À retenir) Soit $n = \prod p_i^{\alpha_i}$. Montrer que le nombre de diviseurs de n est $\prod(\alpha_i + 1)$.

Exercice 19 (À retenir) On note $P(n)$ le produit des diviseurs de n et $d(n)$ le nombre de diviseurs de n. Montrer que $P(n) = n^{d(n)/2}$.

Exercice 20 (À retenir) Soit $a \geq 1$ et $b \geq 2$ tels que $a^b - 1$ est premier. Montrer que $a = 2$ et b est premier.

Exercices un peu plus délicats

Exercice 21 Déterminer tous les couples d'entiers naturels a, b tels que $a^b = b^a$.

Exercice 22 Soit $a \geq 2$, $m \geq n \geq 1$.
a) Montrer que PGCD$(a^m - 1, a^n - 1)$ = PGCD$(a^{m-n} - 1, a^n - 1)$.
b) Montrer que PGCD$(a^{m-1}, a^n - 1)$ = $a^{\text{PGCD}(m,n)} - 1$.
c) Montrer que $a^m - 1 \mid a^n - 1 \Leftrightarrow m \mid n$.

Exercice 23 (Ordre d'un élément) Soit a et n deux entiers naturels non nuls, premiers entre eux. Montrer qu'il existe un entier d tel que, pour tout entier $b \in \mathbb{N}$, n divise $a^b - 1$ si et seulement si d divise b.

Exercice 24 (Sophie Germain, parfois assez utile) Montrer qu'il existe une infinité d'entiers $a \geq 0$ tels que $n^4 + a$ n'est premier pour aucun n.

Exercice 25 Montrer que $\prod_{k=0}^{n-1}(2^n - 2^k)$ est divisible par $n!$.

Exercice 26 (Théorème de Wilson, à retenir) Soit p un entier > 1. Montrer que p est premier si et seulement si $(p-1)! \equiv -1 \pmod{p}$.

Exercices plus difficiles

Exercice 27 (OIM 99-4) Déterminer les couples d'entiers strictement positifs (n, p) tels que
— p est un nombre premier,
— $n \leqslant 2p$,
— $(p-1)^n + 1$ est divisible par n^{p-1}.

Exercice 28 (OIM 2002-4) Soit n un entier strictement plus grand que 1. On note $d_1, d_2, \cdots, d_k$ les diviseurs positifs de n avec

$$1 = d_1 < d_2 < \cdots < d_k = n.$$

On pose $D = d_1d_2 + d_2d_3 + \cdots + d_{k-1}d_k$.
Montrer que $D < n^2$.
Trouver les n tels que D est un diviseur de n^2.

Exercice 29 Calculer le chiffre des unités du nombre suivant :

$$\left[\frac{10^{1992}}{10^{83} + 7}\right]$$

Exercice 30 Trouver tous les entiers a et b tels que $7^a - 3 \times 2^b = 1$.

Exercice 31 (OIM 2005) Trouver tous les entiers premiers avec tous les termes de la suite définie par $u_n = 2^n + 3^n + 6^n - 1$ pour $n \in \mathbb{N}^*$.

Solution de l'exercice 1 Il y a plusieurs manières de faire. Par exemple, on peut remarquer que $(n-1)(n+2) = n^2 + n - 2$. Une façon élégante et qui est bien utile dans de nombreux cas est de raisonner modulo $n-1$: on a en effet $n \equiv 1 \pmod{n-1}$, donc $n^2 + n - 2 \equiv 1^2 + 1 - 2 \equiv 0 \pmod{n-1}$, ce qui est exactement ce que l'on veut démontrer.

Solution de l'exercice 2 Rappelons-nous la caractérisation du PGCD en utilisant $a\mathbb{Z}$ et $b\mathbb{Z}$: si a et b sont deux entiers naturels non nuls, $\mathrm{PGCD}(a,b)$ est l'entier $d \geq 1$ tel que $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$. En particulier, d est l'élément minimal de l'ensemble $(a\mathbb{Z} + b\mathbb{Z}) \cap \mathbb{N}^*$.

Maintenant, soit $d = \mathrm{PGCD}(a,b)$ et $D = \mathrm{PGCD}(ac, bc)$. Puisque $D \in (ac)\mathbb{Z} + (bc)\mathbb{Z}$, il existe des entiers u, v, U et C que $au + bv = d$ et $acu + bcv = D$. En particulier, $D = (au + bv)c$ est divisible par c, et $\frac{D}{c} = au + bv$ est un élément de $(a\mathbb{Z} + b\mathbb{Z}) \cap \mathbb{N}^*$. De même, $(ac)u + (bc)v = cd$ est un élément de $(ac\mathbb{Z} + bc\mathbb{Z}) \cap \mathbb{N}^*$. Par minimalité de d et de D, on en déduit que $cd \geq D$ et que $\frac{D}{c} \geq d$, c'est-à-dire que $cd = D$.

Solution de l'exercice 3 On pourrait invoquer directement le petit théorème de Fermat ci-dessous, mais on va simplement considérer les deux cas séparément :

— Si $p = 2$, alors $a^2 - a = a(a-1)$: si a est pair, alors $a(a-1)$ aussi ; si a est impair, alors $a-1$ est pair, donc $a(a-1)$ aussi.

— Si $p = 3$, alors $a^3 - a = a(a-1)(a-2) + 3(a^2 - a)$: que 3 divise a, $a-1$ ou $a-2$, il divisera toujours $a^3 - a$.

Notons que l'on aurait également pu utiliser des congruences modulo 2 ou 3.

Solution de l'exercice 4 Regardons $P(x)$ et $P(y)$ modulo $x-y$: puisque $x \equiv y$ (mod. $x-y$), alors

$$P(x) \equiv ax^3 + bx^2 + cx + d \equiv ay^3 + by^2 + cy + d \equiv P(y) \pmod{x-y}.$$

Cela signifie exactement que $x - y$ divise $P(x) - P(y)$.

Solution de l'exercice 5 Plaçons nous modulo $y-1$: $y \equiv 1$ (mod. $y-1$), donc $y^{(y^2)} - 2y^{y+1} + 1 \equiv 1^{(y^2)} - 2 \times 1^{y+1} + 1 \equiv 1 - 2 + 1 \equiv 0$ (mod. $y-1$).

Solution de l'exercice 6 On va utiliser le théorème Chinois. Tout d'abord, en se plaçant modulo 5, on observe que $3n - 2 \equiv 0$ (mod. 5) si et seulement si $n \equiv 4$ (mod. 5). De même, en se plaçant modulo 7, on observe que $2n + 1 \equiv 0$ (mod. 7) si et seulement si $n \equiv 3$ (mod. 7).

Notons que 5 et 7 sont premiers entre eux : d'après le théorème de Bézout, il existe des entiers u et v tels que $5u + 7v = 1$. Par exemple, $(u,v) = (3,-1)$ convient. D'après le théorème Chinois, les entiers n tels que $n \equiv 4$ (mod. 5) et $n \equiv 3$ (mod. 7) sont donc les entiers $n \equiv 4(7v) + 3(5u) \equiv -11$ (mod. 35).

Les entiers recherchés sont donc les entiers de la forme $35k - 11$, où k est entier.

Solution de l'exercice 7 On va, une fois de plus, utiliser le théorème Chinois. Notons que $6 = 2 \times 3$ et que $10 = 2 \times 5$. Dire que $n \equiv 4$ (mod. 6) revient à dire que $n \equiv 4$ (mod. 2) et $n \equiv 1$ (mod. 3). Dire que $n \equiv 8$ (mod. 10) revient à dire que $n \equiv 8$ (mod. 2) et $n \equiv 8$ (mod. 5).

On cherche donc les entiers n tels que $n \equiv 0$ (mod. 2), $n \equiv 1$ (mod. 3) et $n \equiv 3$ (mod. 5). Or $n = -2$ est un tel entier. D'après le théorème Chinois, les entiers recherchés sont donc les entiers $n \equiv -2$ (mod. 30), c'est à dire les entiers de la forme $30k - 2$, où k est entier.

Solution de l'exercice 8 Le problème peut se reformuler comme suit : trouver les entiers a tels que $2a^2 \equiv 2$ (mod. 7). Une telle relation ne dépend que de la congruence de a modulo 7. On

vérifie alors à la main que $2\times 0^2\equiv 0$ (mod. 7), $2\times 1^2\equiv 2\times 6^2\equiv 2$ (mod. 7), $2\times 2^2\equiv 2\times 5^2\equiv 1$ (mod. 7) et $2\times 3^2\equiv 2\times 4^2\equiv 4$ (mod. 7). Il s'ensuit que $\frac{2a^2-2}{7}$ est un entier si et seulement si a est de la forme $7\ell+1$ ou $7\ell-1$.

Solution de l'exercice 9 On veut trouver $a>0$ et $b>0$ entiers tels que $a^3b-1\equiv 0$ (mod. $a+1$) et $b^3a+1\equiv 0$ (mod. $b+1$). Or, $a\equiv -1$ (mod. $a+1$), donc $a^3b-1\equiv(-1)^3b-1\equiv -(b+1)$ (mod.$a+1$). De même, $b\equiv 1$ (mod. $b-1$), donc $b^3a+1\equiv 1a+1\equiv a+1$ (mod.$b-1$). En particulier, $b-1$ divise alors $a+1$, qui lui-même divise $b+1$. Donc $b-1$ divise $b+1$ et divise même $(b+1)-(b-1)=2$. Puisque $b-1\geq 0$, on en déduit que $b-1\in\{1,2\}$:

1. si $b-1=1$, $a+1$ divise $b+1=3$ et, puisque $a+1>1$, on en déduit que $a+1=3$;
2. si $b-1=2$, $a+1$ est pair et divise $b+1=4$ et, puisque $a+1>1$, on en déduit que $a+1=2$ ou $a+1=4$.

Les solutions (a,b) possibles sont donc $(2,2)$, $(1,3)$ et $(3,3)$. On vérifie alors ces solutions donnent respectivement $\frac{a^3b-1}{a+1}=\frac{15}{3},\frac{2}{2},\frac{80}{4}$ et $\frac{b^3a+1}{b-1}=\frac{17}{1},\frac{28}{2},\frac{82}{2}$. Les couples recherchés sont donc bien $(2,2)$, $(1,3)$ et $(3,3)$.

Solution de l'exercice 10 On pourrait regarder une par une les 35 classes de congruences modulo 35. Cela dit, il y a plus rapide, en utilisant le théorème Chinois.

En effet, puisque $35=5\times 7$, $a^3\equiv 1$ (mod. 35) si et seulement si $a^3\equiv 1$ (mod. 5) et $a^3\equiv 1$ (mod. 73). On vérifie alors à la main que $0^3\equiv 0$ (mod. 7), que $1^3\equiv 2^3\equiv 4^3\equiv 1$ (mod. 7) et que $3^3\equiv 5^3\equiv 6^3\equiv 6$ (mod. 7) ; on vérifie également $0^3\equiv 0$ (mod. 53), que $1^3\equiv 1$ (mod. 5), que $2^3\equiv 3$ (mod. 5), que $3^3\equiv 2$ (mod. 5) et que $4^3\equiv 4$ (mod. 5).

Ainsi, a est solution du problème si et seulement si $a\equiv 1$, 2 ou 4 (mod. 7), et $a\equiv 1$ (mod.5). D'après le théorème Chinois, ces conditions reviennent à dire que $a\equiv 1$, 11 ou 16 (mod. 35) Cela signifie que 35 divise a^3-1 si et seulement si a est de la forme $35\ell+1$, $35\ell+11$ ou $35\ell+16$.

Solution de l'exercice 11 Si n est strictement positif, on voit par la décomposition en facteurs premiers (par exemple) que n et $n+1$ étant premiers entre eux, ce sont tous deux des carrés. Il existe u et v des entiers tels que $n=u^2$ et $n+1=v^2$, donc $u^2+1=v^2$, donc $(v-u)(u+v)=1$, donc $v-u=u+v$, donc $v=0$ et donc $u=1$, d'où $n=1$, et 1×2 n'est pas un carré parfait. Finalement, $n=0$, qui convient. Si n est négatif, on se ramène en considérant $n-1$ au lieu de n, et on trouve que seul -1 convient, et -1 convient bien.

Solution de l'exercice 12 On peut supposer, par symétrie, que l'on a $a\leq b\leq c$. Ainsi, si $a>3$, on a $1/c\leq 1/b\leq 1/a<1/3$, d'où $1/a+1/b+1/c<1$. Ainsi, on a $a\leq 3$.

— Si $a=3$, on a soit $b=3$, et alors $c=3$, ce qui donne la solution $(3,3,3)$, qui convient, soit $b\geq 4$, d'où $1/a+1/b+1/c\leq 1/3+1/4+1/4<1$.
— Si $a=2$, on a $1/b+1/c=1/2$. Si $b>4$, on obtient $1/b+1/c<1/2$. On a donc $b=4$ ou $b=3$. Si $b=4$, alors $c=4$. Si $b=3$, alors $c=6$.

Finalement, les solutions sont $(a,b,c)=(3,3,3)$ ou $(2,4,4)$ ou $(2,3,6)$ et leurs permutations.

Solution de l'exercice 13 On regarde les restes des puissances de 7 modulo 100. C'est un cycle de longueur 4. Or $9\equiv 1\pmod 4$ donc les deux derniers chiffres sont 07.

Solution de l'exercice 14 Si PGCD$(p,q)=d>1$, $\sqrt[d]{2}$ est un contre-exemple. Si PGCD$(p,q)=1$, il existe u et v tels que $pu+qv=1$ d'après le théorème de Bézout. Donc $x=(x^p)^u+(x^q)^v$ est rationnel.

Solution de l'exercice 15 Dans ce genre d'exercices, où l'on doit manipuler un grand nombre tel que 2007, il est important de rechercher des simplifications du problème, par exemple en regardant ce qui se passe modulo de petits entiers.

C'est ainsi que l'on en vient tout naturellement, après quelques essais éventuellement infructueux, à considérer l'équation dans modulo 8, où elle devient : $a^2 + b^2 + c^2 \equiv 7$ (mod. 8). Or, les carrés modulo 8 sont 0, 1 et 4.

Pour que l'équation soit vérifiée, il faut donc avoir au moins 2 carrés égaux à 4 modulo 8 (ce sans quoi leur somme vaudra ente 0 et 3 modulo 8), et alors cette somme sera égale au dernier carré, donc différente de 7 (modulo 8). Ainsi, l'équation $a^2 + b^2 + c^2 \equiv 7$ (mod. 8) n'admet aucune solution. *A fortiori*, l'équation $a^2 + b^2 + c^2 = 2007$ n'admet aucune solution en nombres entiers.

Solution de l'exercice 16 Comme 10 = 2 × 5 cela revient à calculer $\min(v_2(2014!), v_5(2014!)$. Or il y a plus de facteurs 2 que de facteurs 5. Donc on calcule $v_5(2014!)$ à l'aire de la formule de Legendre :

$$v_5(2014!) = \sum_{k=1}^{+\infty} \lfloor \frac{2014}{5^k} \rfloor = 501$$

Solution de l'exercice 17 Sachant qu'un carré est congru à 0 ou 1 modulo 4, la somme de cinq carrés d'entiers consécutifs est congrue à 2 ou 3 modulo 4.

Solution de l'exercice 18 Les diviseurs de n sont les nombres de la forme $\prod p_i^{\beta_i}$ avec $0 \leq \beta_i \leq \alpha_i$. Il y en a donc $\prod(\alpha_i + 1)$.

Solution de l'exercice 19 $P(n)^2 = \prod_{d|n} d \times \prod_{d|n} \frac{n}{d} = \prod_{d|n} n = n^{d(n)}$.

Solution de l'exercice 20 $a^b - 1$ est divisible par $a - 1$ donc nécessairement $a = 2$. De plus si $b = cd$, $2^b - 1$ est divisible par $2^c - 1$ donc $c = 1$ ou $c = b$. Donc b est premier.

Solution de l'exercice 21 On commence, comme d'habitude, par introduire $d = a \wedge b$ et écrire $a = da'$ et $b = db'$ où $a' \wedge b' = 1$.

On constate d'abord que $a = b$ est toujours solution.

On cherche les autres solutions. Sans perte de généralité (quitte à inverser les rôles de a et b), on va supposer que $a < b$. Ainsi, l'équation se réécrit

$$d^{b-a} a'^b = b'^a.$$

On voit tout de suite que $a' = 1$ car $a' \mid b'^a$ alors que $a' \wedge b'^a = 1$. Et donc $d = a$ et $b' \geqslant 2$:

$$d^{d(b'-1)} = b'^d.$$

On prend les racines d-ièmes :

$$d^{b'-1} = b',$$

et on a encore quelques cas à traiter. Si $d = 1$, alors $b' = 1$ ce qui n'est pas possible, on a exclu ce cas.

Si $d = 2$, on voit que pour $b' = 2$ on a une solution qui correspond à $a = 2, b = 4$. Ensuite, on montre (par récurrence ou par une étude de fonction) que pour $b' > 2$, alors $2^{b'-1} > b'$.

Enfin, si $d \geqslant 3$, la situation est encore plus dramatique et on montre que

$$d^{b'-1} \geqslant 3^{b'-1} > b'.$$

Ainsi, les seules solutions sont les couples (a, a), $(2, 4)$ et $(4, 2)$.

Solution de l'exercice 22

a) Tout d'abord, on note $d = \text{PGCD}(a, b)$ et $D = \text{PGCD}(n^a - 1, n^b - 1)$: on commence par montrer que $n^d - 1$ divise D. En effet, soit a' et b' deux entiers tels que $a = da'$ et $b = bd'$. Il s'ensuit que $n^a - 1 \equiv (n^d)^{a'} - 1 \equiv 1^{a'} - 1 \equiv 0$ (mod. d) et que $n^b - 1 \equiv (n^d)^{b'} - 1 \equiv 1^{b'} - 1 \equiv 0$ (mod. d). En particulier, cela signifie que d divise $n^a - 1$ et $n^b - 1$, donc divise D.
Réciproquement, montrons que D divise $n^d - 1$. Pour ce faire, on va montrer un autre résultat : si $x \geq y > 0$, alors $\text{PGCD}(n^x - 1, n^y - 1)$ divise $\text{PGCD}(n^y - 1, n^{x-y} - 1)$. Notons qu'on peut se douter qu'un tel résultat sera vrai, puisque $\text{PGCD}(x, y) = \text{PGCD}(y, x-y)$. Il nous suffit alors de montrer que $\text{PGCD}(n^x - 1, n^y - 1)$ divise $n^{x-y} - 1$, ce qui découle du fait que $n^x - 1 = n^{x-y}(n^y - 1) + (n^{x-y} - 1)$.
En remplaçant l'expression $\text{PGCD}(n^x - 1, n^y - 1)$ par $\text{PGCD}(n^{\min\{x,y\}} - 1, n^{|x-y|} - 1)$, les exposants que l'on obtient sont en fait des termes que l'on trouvera dans l'algorithme d'Euclide (sauf que, quand on a une division Euclidienne $a = bq + r$, on considère tous les couples $(b, r + kq)$ au lieu de passer directement de (a, b) à (b, r)). Ce faisant, on montre bien que $\text{PGCD}(n^a - 1, n^b - 1)$ divise $\text{PGCD}(n^d - 1, n^0 - 1) = n^d - 1$, ce qui conclut l'exercice.
PGCD$(a^m - 1, a^n - 1)$ = PGCD$(a^n(a^{m-n} - 1), a^n - 1)$ = PGCD$(a^{m-n} - 1, a^n - 1)$ car a^n et $a^n - 1$ sont premiers entre eux.

b) On applique l'algorithme des soustractions.

c) $a^m - 1 \mid a^n - 1 \Leftrightarrow$ PGCD$(a^m - 1, a^n - 1) = a^m - 1 \Leftrightarrow$ PGCD$(m, n) =$ m $\Leftrightarrow m \mid n$.

Solution de l'exercice 23 Tout d'abord, en appliquant le principe des tiroirs, il existe deux entiers naturels $u < v$ tels que $a^u \equiv a^v$ (mod. n). Cela veut dire que n divise $a^v - a^u = a^u(a^{v-u} - 1)$. Or, n est premier avec a, donc avec a^u : par théorème de Gauss, n divise $a^{v-u} - 1$, et il existe donc un plus petit entier $d > 0$ tel que $a^d \equiv 1$ (mod. n).

On note alors que, pour tout entier naturel k, $a^{dk} \equiv (a^d)^k \equiv 1^k \equiv 1$ (mod. n) : si b est un multiple de d, alors n divise $a^b - 1$. Réciproquement, si b n'est pas multiple de d, effectuons la division Euclidienne de b par d : $b = ud + v$, avec $0 < v < d$. Alors $a^b \equiv (a^d)^u a^v \equiv 1^u a^v \equiv a^v \not\equiv 1$ (mod. n), par définition de d. Cela montre bien que, si n divise $a^b - 1$, alors d divise b.

Solution de l'exercice 24 On prend $a = 4b^4$ donc $n^4 + a = (n^2 + 2b^2 + 2nb)(n^2 + 2b^2 - 2nb)$. Il suffit alors de prendre b assez grand.

Solution de l'exercice 25 $\prod_{k=0}^{n-1}(2^n - 2^k) = 2^{\frac{n(n-1)}{2}} \prod_{k=0}^{n-1}(2^k - 1)$. Or $v_2(n!) < n < \frac{n(n-1)}{2}$.

De plus, si $p \geq 3$, alors $v_p(2^k - 1) \geq a$ dès que k est un multiple de $\varphi(p^a) = (p-1)p^{a-1}$ (où φ est l'indicatrice d'Euler) : il y a au moins $\lfloor \frac{n}{(p-1)p^{a-1}} \rfloor$ tels entiers k. De manière analogue à la formule de Legendre, on sait donc que $v_p(\prod_{k=0}^{n-1}(2^k - 1)) \geq \lfloor \frac{n}{p-1} \rfloor + \lfloor \frac{n}{p(p-1)} \rfloor + \dots$ Or, $v_p(n!) = \lfloor \frac{n}{p} \rfloor + \lfloor \frac{n}{p^2} \rfloor + \dots$ (c'est la formule de Legendre), donc $v_p(n!) \leq v_p(\prod_{k=0}^{n-1}(2^k - 1))$. Cela montre bien que $n!$ divise $\prod_{k=0}^{n-1}(2^n - 2^k)$.

Solution de l'exercice 26 Pour tout $n \in [\![1, p-1]\!]$, il existe $n^{-1} \in [\![1, p-1]\!]$ tel que $n \times n^{-1} \equiv 1[p]$. De plus, $n = n^{-1}$ si et seulement si $n^2 - 1 \equiv 0$, ce qui équivaut à $n = 1$ ou $n = p - 1$.

Ainsi, calculer $(p-1)!$ modulo p revient :

— si $n \neq n^{-1}$, à grouper chaque entier n avec son inverse n^{-1} pour les multiplier, ce qui produit uniquement des facteurs 1 modulo p,

— sinon, c'est que $n = 1$ ou $n = p - 1$, ce qui rajoute un facteur 1 et un facteur -1 modulo p.

Donc : $(p-1)! \equiv 1 \times 1 \times \ldots \times 1 \times 1 \times (-1) \equiv -1[p]$.

Solution de l'exercice 27 On trouve d'abord des solutions évidentes : $(1, p)$ est toujours solution.

Si $p = 2$, et $n > 1$ alors seul $n = 2$ fonctionne et $(2, 2)$ est solution.

On suppose désormais que $p \geqslant 3$. Ainsi, n est nécessairement impair. Comme il est toujours plus simple de travailler avec des nombres premiers, soit q premier tel que $q \mid n$. Alors, les hypothèses impliquent $(p-1)^n \equiv -1[q]$, et plus généralement, $(p-1)^{an} \equiv (-1)^a[q]$. Fermat nous apprend aussi que $(p-1)^{b(q-1)} \equiv 1[q]$ car $p - 1$ n'est pas divisible par q. On résume :

$$(p-1)^{an+b(q-1)} \equiv (-1)^a[q].$$

On se demande maintenant pour quelles valeurs de a et b on peut obtenir quelquechose d'intéressant, et on pense à Bezout. Mais il faut pour l'utiliser que $q - 1 \wedge n = 1$. Pour ce faire, on suppose que q est le plus petit diviseur premier de n (qui est impair) et on prend a et b donnés par Bezout, de sorte que $an + b(q-1) = 1$. On voit immédiatement que a doit être impair, et donc

$$p - 1 \equiv -1[q]$$

soit $q \mid p$! Comme $n < 2p$ on a même que $n = p$, par minimalité de q.

On est prêt du but. En développant

$$(p-1)^p + 1 = \sum_{i=1}^{p} (-1)^{p-k} p^k \binom{p}{k} = p^2 + A,$$

on observe que A est divisible par p^3, donc $(p-1)^p + 1$ n'est pas divisible par p^3. Ainsi, on obtient que $p \leqslant 3$, soit $p = 3$ et $(3, 3)$ est bien une solution du problème, la dernière.

Solution de l'exercice 28 Il est clair que pour tout m, $d_{k-m} \leqslant n/(m+1)$. Ainsi, il vient que

$$\begin{aligned} D &\leqslant n^2\Big(\frac{1}{1\times 2} + \frac{1}{2\times 3} + \cdots + \frac{1}{(k-1)\times k}\Big) \\ &= n^2\Big(\frac{1}{1} - \frac{1}{\times 2} + \frac{1}{\times 2} - \frac{1}{\times 3} + \cdots + \frac{1}{k-1} - \frac{1}{k}\Big) \\ &= n^2\Big(1 - \frac{1}{k}\Big) < n^2. \end{aligned}$$

Pour la seconde partie de la question, on commence par remarquer que si n est premier, alors $D = d_1 d_2 = n \mid n^2$.

Si n est composé, soit $p = d_2$ les plus petit diviseur premier de n. Alors

$$n^2 > D > d_{k-1} d_k = n \times \frac{n}{p} = \frac{n^2}{p}.$$

Mais c'est alors impossible que $D \mid n^2$ car n^2/p est le plus grand diviseur strict de n^2.

Solution de l'exercice 29

Solution de l'exercice 30 On voit que $a = 0$ ou $b = 0$ sont impossibles. On réécrit l'équation comme suit :

$$7^a - 1 = 6 \times \sum_{i=0}^{a-1} 7^i = 6 \times 2^{b-1}.$$

Si $a = 1$, alors $b = 1$ est l'unique solution. Si $a = 2$ alors $b = 4$ est l'unique solution.

Supposons maintenant que $a > 2$ ce qui implique que $b > 4$. Comme la somme de gauche est paire, mais constituée d'éléments impairs, il doit y avoir un nombre pair de termes, a est donc pair. On regroupe termes pairs et impairs pour obtenir

$$(7+1)\sum_{i=0}^{a/2-1} 7^{2i} = 8 \times 2^{b-4}.$$

On simplifie, et on se rappelle que comme $b > 4$, la somme de gauche est paire mais encore constituée de termes impairs. Il y a donc un nombre pair de termes ($a/2$ est pair) et on peut recommencer la procédure :

$$(7^2+1)\sum_{i=0}^{a/4-1} 7^{4i} = 2^{b-4},$$

on aboutit à une contradiction car une puissance de 2 n'est pas divisible pas 50.

Les seules solutions sont donc $(1,1)$ et $(2,4)$.

Solution de l'exercice 31 Les nombres 2, 3, 6 doivent vous rappeler quelque chose : ils vérifient en effet $1/2+1/3+1/6 = 1$. Cette remarque peut sembler inutile puisque l'on manipule ici des nombres entiers, et que l'on ne peut pas calculer d'inverses (sauf pour 1 et -1). Mais rappelez-vous : on a aussi parlé d'inversion modulo un nombre premier. On se place donc modulo p, où p est un nombre premier. Le petit théorème de Fermat implique que $a \times a^{p-2} \equiv 1 \pmod p$ pour a un entier premier avec p. Ainsi, a^{p-2} joue le même rôle modulo p que $1/a$. Ceci nous amène donc tout naturellement à considérer $a_{p-2} = 2^{p-2} + 3^{p-2} + 6^{p-2} - 1$. Attention toutefois : si 2, 3 ou 6 ne sont pas premiers à p, i.e. $p = 2$ ou $p = 3$, il faudra raisonner différemment.

Soit donc $p > 3$ un nombre premier. On veut montrer que $p \mid a_{p-2}$. De la même façon que pour des fractions, on va essayer de calculer a_{p-2} modulo p en « mettant tout sous le même dénominateur », ou, ce qui revient au même, à tout multiplier par $2 \cdot 3 \cdot 6$, puisque $2 \cdot 3 \cdot 6$ n'est pas congru à 0 modulo p. On a alors $2 \cdot 3 \cdot 6 \cdot a_{p-2} \equiv 3 \cdot 6 + 2 \cdot 6 + 2 \cdot 3 - 2 \cdot 3 \cdot 6 \equiv 36 - 36 \equiv 0 \pmod p$ (cette avant-dernière égalité n'est pas un coup de chance, cela revient au même de dire que $1/2 + 1/3 + 1/6 = 1$). Ainsi on a bien $p \mid a_{p-2}$, comme on le voulait.

Mais à quoi tout cela va nous servir pour notre problème ? Pour alléger les notations, considérons A l'ensemble des entiers premiers à tous les termes de la suite. Soit $m \in A$. Comme souvent en arithmétique, on va essayer de se ramener à travailler avec des nombres premiers, qui ont plein de propriétés pratiques (comme justement celle que l'on vient de démontrer plus haut). Ici, c'est très naturel : la condition sur m signifie exactement que tout facteur premier p de m ne divise aucun des termes de la suite, c'est-à-dire que $p \in A$. Or comme pour tout nombre premier $q > 3$ vérifie $q \mid a_{q-2}$, on a que A ne contient aucun nombre premier, sauf éventuellement 2 et 3.

Il reste donc à traiter les cas de 2 et 3. Or on calcule : $2^1 + 3^1 + 6^1 - 1 = 10$ qui n'est pas premier avec 2, donc 2 n'appartient pas à A. De même, $2^2 + 3^2 + 6^2 - 1$ est divisible par 3, donc 3 n'appartient pas à A. Finalement, A ne contient aucun nombre premier et donc $A = \{-1, 1\}$.

3 Groupe C : inégalités et éq. fonct.

1 dimanche 23 après-midi : inégalités, Joon Kwon

On pourra se référer au cours de Guillaume Conchon-Kerjan de 2013.

2 lundi 24 matin : Gabriel Pallier

Avertissement Ce cours reprend certains éléments de celui de Pierre Bornsztein au stage de Saint-Malo 2003, que le lecteur pourra consulter avec profit s'il souhaite trouver un traitement plus abouti du vaste sujet que constitue la résolution d'équation fonctionnelles.

Rappelons la définition d'une fonction réelle de la variable réelle. $\mathbb{R}$ est l'ensemble des nombre réels ; intuitivement on l'identifie à la droite réelle munie de son origine.

Définition 152. Soit X un sous-ensemble non vide de $\mathbb{R}$. Définir une fonction de X dans $\mathbb{R}$, c'est associer à tout x élément de X, un unique nombre réel noté $f(x)$. X est appelé ensemble de définition de f. On note ceci

$$f : X \to \mathbb{R}$$

Si S est un sous-ensemble de X, on appelle restriction de f à S et on note $f_{|S}$ la fonction qui a tout $s \in S$ associe $f(s)$.

On pourra éventuellement remplacer l'ensemble d'arrivée $\mathbb{R}$ par un de ses sous-ensembles Y. On note alors $f : X \to Y$.

Définition 153. Soit $f : X \to Y$. On dit que f est injective si

$$\forall x, y \in X, \quad f(x) = f(y) \implies x = y$$

Autrement dit, deux nombres distincts ont des images distinctes.

Définition 154. Soit $f : X \to Y$. On dit que f est surjective

$$\forall y \in Y, \quad \exists x \in X \mid f(x) = y$$

Autrement dit, toutes les valeurs de Y sont atteintes.

Dans une équation fonctionnelle, la fonction est une inconnue. Elle peut être recherché dans un ensemble de fonctions de X dans $\mathbb{R}$, qui vérifie éventuellement en plus une certaine propriété (par exemple : parmi les fonctions qui ne prennent que des valeurs positives). Il peut y avoir plusieurs équations, voire plusieurs fonctions inconnues.

Beaucoup de fonctions usuelles en mathématiques (linéaires, affine, exponentielle, logarithme, fontions circulaires, factorielle...) apparaissent liées à une équation fonctionnelle particulière. On connaît d'autant mieux une fonction (ou une famille de fonctions) que l'on connaît des équations fonctionnelles qui la caractérisent.

La première équation de Cauchy

On cherche ici à caractériser toutes les fonctions f de la variable réelle telles que

$$f(x + y) = f(x) + f(y) \tag{VII.1}$$

pour tous x et y dans un sous-ensemble X de $\mathbb{R}$. Nous ne fixons pas encore X pour le moment, mais dans l'idéal on le souhaite le plus grand possible.

Remarque 155. Pour que X soit tel que l'équation de Cauchy (VII.1) ait un sens, il faut que pour tous x et y dans X, $x+y$ soit aussi dans X.

Exercice 1 Donner des sous-ensembles de $\mathbb{R}$ qui vérifient cette propriété.

Solution de l'exercice 1 On peut penser à $\{0\}$, $\mathbb{N}$, l'ensemble des entiers naturels pairs, l'ensemble des demi-entiers, l'ensemble $\mathbb{Z}$ des entiers relatifs, l'ensemble $\mathbb{Q}$ des rationnels, l'ensemble $\mathbb{R}$, l'ensemble vide $\emptyset$. Il y en a évidemment beaucoup d'autres. Remarquez que X doit être infini dès qu'il contient plus d'un élément.

Equation de Cauchy sur $\mathbb{N}$ On cherche ici à résoudre l'équation de Cauchy parmi les fonctions de $\mathbb{N} = \{0, 1, 2, \ldots\}$ dans $\mathbb{R}$. Soit $f : \mathbb{N} \to \mathbb{R}$ une solution de l'équation de Cauchy. Nous allons d'abord essayer d'obtenir quelques renseignements sur f en particularisant l'équation (VII.1), c'est-à-dire en l'appliquant en des valeurs particulières. Par exemple, en faisant $x = 0$ nous savons déjà que si f est solution alors $f(0) = 0$

Exercice 2 Montrer que pour tout n et k dans $\mathbb{N}$, nous avons

$$f(nk) = nf(k) \tag{VII.2}$$

En déduire que $f(n) = an$ pour un certain $a \in \mathbb{R}$. Vérifier que toutes les fonctions de ce type sont solutions.

Solution de l'exercice 2 On procède par récurrence sur n : Si c'est acquis au rang n l'équation de Cauchy donne

$$f((n+1)k) = f(nk) + f(k) = nf(k) + f(k) = (n+1)f(k)$$

soit, ce que l'on veut. Pour l'initialisation, il suffit de faire $x = 0$ dans l'équation de Cauchy, ce qui indique que $f(0) = 0$.

Equation de Cauchy sur $\mathbb{Z}$ On a déjà établi une équation auxilliaire (VII.2), qu'on peut souhaiter généraliser : On se donne f une solution de l'équation de Cauchy sur $\mathbb{Z}$.

Exercice 3 Montrer que pour tout $x \in \mathbb{Z}$, $f(-x) = -f(x)$. En déduire que pour tous x et y dans $\mathbb{Z}$,

$$f(xy) = xf(y)$$

En déduire les solutions de l'équation de Cauchy sur $\mathbb{Z}$

Solution de l'exercice 3 On fait $y = -x$ dans l'équation de Cauchy, ceci donne

$$f(x) + f(-x) = 0$$

d'après l'égalité $f(0) = 0$ qui a été montré plus haut. On déduit alors la solution de l'exercice précédent : si x, y sont dans $\mathbb{N}$ alors c'est bon, si $x < 0$ alors

$$f(xy) = -f(-xy) = -(-x)f(y) = xf(y)$$

Enfin, si $y < 0$ alors

$$f(xy) = -f(x(-y)) = -xf(-y) = xf(y)$$

Equation de Cauchy sur $\mathbb{Q}$ Soit f une solution de l'équation de Cauchy dans $\mathbb{Q}$.

Exercice 4 Que dire de f restreinte à $\mathbb{Z}$? Expliquer rapidement comment on pourrait montrer en reprenant les arguments précédents que pour tous $x \in \mathbb{Z}$ et $y \in \mathbb{Q}$,

$$f(xy) = xf(y)$$

En déduire les solutions de l'équation de Cauchy sur $\mathbb{Z}$.

Solution de l'exercice 4 f restreinte à $\mathbb{Z}$ vérifie l'équation de Cauchy sur $\mathbb{Z}$, qui a déjà été résolue. Nous savons ainsi que si l'on pose $a = f(1)$ alors pour tout x entier relatif, $f(x) = ax$. Maintenant, si $x = p/q$ alors on montre à l'aide de l'équation auxiliaire établie plus haut que $qf(p/q) = f(p) = pf(1)$ d'où l'on déduit

$$f(x) = xf(1)$$

pour tout $x \in \mathbb{Q}$.

Equation de Cauchy sur $\mathbb{R}$ avec condition de monotonie

Définition 156. Une fonction $f : X \to \mathbb{R}$ est croissante si pour tous x et y dans X nous avons

$$x \leqslant y \implies f(x) \leqslant f(y)$$

Elle est strictement croissante si quels que soient x et y dans X nous avons

$$x < y \implies f(x) < f(y)$$

De même, f est décroissante (strictement) si on a les inégalités auquelles on pense. Une fonction croissante ou décroissante est dite monotone.

Par exemple, la fonction linéaire $x \mapsto ax$ est croissante si, et seulement si, $a \geqslant 0$, strictement dès que $a > 0$.

On reprend l'équation (VII.1) de Cauchy sur $\mathbb{R}$, à laquelle on rajoute la condition : « f est monotone ».

Exercice 5 Montrer que sous ces conditions la fonction f est linéaire.

Solution de l'exercice 5 Posons $g(x) = xf(1)$; il s'agit alors de montrer que $f = g$, soit $f - g = 0$. La fonction $h = f - g$ est encore une solution de l'équation de Cauchy ; restreinte à $\mathbb{Q}$ elle est nulle d'après la résolution sur $\mathbb{Q}$. Si par l'absurde il existe x tel que $h(x) \neq 0$ alors quitte à prendre k un entier assez grand, nous avons $|h(kx)| > 2f(1)$. Or ceci est absurde, puisque

$$\begin{aligned} |h(kx)| &= |h(kx) - h(\lfloor kx \rfloor)| \\ &= |f(kx - \lfloor kx \rfloor) - g(kx - \lfloor kx \rfloor)| \\ &\leqslant |f(kx - \lfloor kx \rfloor)| + |g(kx - \lfloor kx \rfloor)| \\ &\leqslant 2|f(1)| \end{aligned}$$

La dernière inégalité venant de la monotonie de f et de g entre 0 et 1 et du fait que $f(0) = g(0) = 0$.

Equation de Cauchy sur $\mathbb{R}$ avec condition de multiplicativité On reprend l'équation (VII.1) de Cauchy sur $\mathbb{R}$, à laquelle on rajoute la condition :

$$f(xy) = f(x) f(y) \tag{VII.3}$$

Exercice 6 Résoudre l'équation de Cauchy sur $\mathbb{R}$ avec la conditions précédente.

Solution de l'exercice 6 D'après ce qui précède, il suffit de montrer que f est monotone. Or si x est positif, on peut écrire $x = (\sqrt{x})^2$, d'où

$$f(x) = f\left(\sqrt{x}\right)^2 \geqslant 0$$

Par conséquent, si $x \leqslant y$ alors $f(y) - f(x) = f(y - x) \geqslant 0$; f est croissante, donc f est linéaire. De plus nous avons l'équation $f(1)^2 = f(1)$ qui donne finalement les deux solutions $f(x) = 0$ ou bien $f(x) = 0$ pour tout x.

Remarque 157. Avec un vocabulaire un peu plus avancé, on dit qu'une fonction f qui vérifie (VII.1), (VII.3) et $f(1) = 1$ est un morphisme du corps $\mathbb{R}$. Nous avons montré qu'en fait, le seul morphisme du corps $\mathbb{R}$ est la fonction identité $f : x \mapsto x$. Ceci mérite d'être remarqué (par exemple, ceci ne serait pas vrai pour le corps $\mathbb{C}$ des nombres complexes).

Exercice 7 En utilisant ce qui précède, résoudre l'équation de Cauchy sur l'ensemble X des nombres de la forme $a + b\sqrt{2}$, avec a et b dans $\mathbb{Z}$.

Solution de l'exercice 7 Déjà, $\sqrt{2}$ est irrationnel donc l'écriture d'un réel donné sous la forme $a + b\sqrt{2}$, si elle existe, est unique. D'après ce qui précède, si on pose $x = f(1)$ et $y = f\left(\sqrt{2}\right)$, alors $f\left(a + b\sqrt{2}\right) = ax + by$. Toutes les fonctions de cette forme sont solutions.

solutions continues de l'équation de Cauchy L'exercice suivant demande de connaître la notion de continuité. On pourra utiliser que tout réel est limite d'une suite de nombres rationnels (autrement dit : $\mathbb{Q}$ est dense dans $\mathbb{R}$), et s'en servir pour se ramener à ce qui précède.

Exercice 8 Donner toutes les solutions continues [1] de l'équation de Cauchy sur $\mathbb{R}$.

Solution de l'exercice 8 Par passage des inégalités larges à la limite, si f est continue et si $f_{|\mathbb{Q}}$ est monotone, alors f est monotone. Or $f_{|\mathbb{Q}}$ est de la forme $x \mapsto ax$ d'après ce qui précède. Donc f est linéaire.

Conclusion La stratégie globale que nous avons mise en oeuvre ici est de résoudre l'équation sur des domaines de plus en plus grands, en tirant partie du principe que si f est solution sur $\mathbb{R}$, alors $f_{|X}$ est solution sur X. Nous n'avons cependant pas résolu l'équation de Cauchy sur $\mathbb{R}$, seulement donné une famille de solutions : les fonctions linéaires. Il existe d'autres solutions, dont la construction nécessite l'usage de l'axiome du choix.

Remarquons aussi que l'on peut parfois avoir des renseignements sur l'ensemble des solutions avant même d'en avoir une seule. Par exemple ici, si f et g sont deux solutions de l'équation de Cauchy, alors $f + g$ est solution. Si c est une constante réelle, cf est solution ; ces deux dernières propriétés disent que l'équation de Cauchy est linéaire.

1. Ce cours n'étant pas l'endroit idéal pour rencontrer la notion de continuité pour la première fois, on y fera peu appel. Voici toutefois une définition s'appuyant sur la notion de limite d'une suite qui suffira ici : $f : X \to \mathbb{R}$ est continue si pour tout $x \in X$ et toute suite x_n à valeurs dans X telle que $x_n \to x$, on a que $f(x_n) \to f(x)$.

Des équations fonctionnelles pour les fonctions affines

Les fonctions affines sont[2] les fonctions $f : \mathbb{R} \to \mathbb{R}$ vérifiant l'équation fonctionnelle de « pente constante » suivante : il existe une constante a réelle telle que pour tous x et y

$$\frac{f(x) - f(y)}{x - y} = a \tag{VII.4}$$

Equation de Jensen Voici l'équation fonctionnelle de Jensen

$$f\left(\frac{x+y}{2}\right) = \frac{f(x) + f(y)}{2} \tag{VII.5}$$

Exercice 9 Montrer qu'il s'agit d'une équation linéaire. Trouver des solutions (au moins deux).

Solution de l'exercice 9 L'équation est linéaire : si f et g sont solutions et pour tout $c \in \mathbb{R}$ alors $f + cg$ est aussi solution.

Par exemple les fonctions constantes, les fonctions linéaires sont solutions.

Remarque 158. Il est toujours instructif de commencer par chercher des solutions particulières (on dit parfois « évidentes »). Celles-ci peuvent en outre renseigner sur l'allure générale des solutions (mais pas toujours). Quoi qu'il en soit, il n'est pas efficace de passer plus de quelques minutes à rechercher des solutions évidentes.

Exercice 10 Trouver toutes les fonctions sur $\mathbb{R}$ qui sont monotones et qui vérifient l'équation fonctionnelle de Jensen

Solution de l'exercice 10 On fait le changement de fonction $g(x) = f(x) - f(0)$ et l'on s'aperçoit alors que g vérifie l'équation de Cauchy sur l'ensemble des réels dyadiques (c'est-à-dire, de la forme $k/2^n$). La monotonie impose alors que g soit linéaire, donc f est affine. Toutes les fonctions affines sont solutions.

Remarque 159. On peut se passer de la condition de monotonie dans l'équation de Jensen si on donne l'équation plus précise

$$f(tx + (1-t)y) = tf(x) + (1-t)f(y)$$

pour tous x, y dans $\mathbb{R}$ et $0 \leqslant t \leqslant 1$. Là encore, les solutions sont les fonctions affines. Une classe intéressante est constituée des fonctions f qui vérifient l'inéquation fonctionnelle

$$f(tx + (1-t)y) \leqslant tf(x) + (1-t)f(y) \tag{VII.6}$$

; celles-ci sont dites convexes. Une légère généralisation de (VII.6) donne lieu à la formule de Jensen, qui est le principe de certaines inégalités utiles dans les problèmes d'olympiades.

Une équation plus générale **Exercice 11** En utilisant la technique du changement de fonction inconnue, trouver toutes les fonctions f monotones sur $\mathbb{R}$ telles qu'il existe g et h de $\mathbb{R}$ dans $\mathbb{R}$ avec

$$f(x+y) = g(x) + h(y) \tag{VII.7}$$

2. On peut le vérifier, mais cela peut aussi être pris comme une définition

Solution de l'exercice 11 Posons $y = 0$, $g(0) = a$ et $h(0) = b$. On trouve alors les deux équations

$$\begin{aligned} g(x) &= f(x) - b \\ h(x) &= f(x) - a \end{aligned}$$

d'où $f(x+y) = f(x) + f(y) - a - b$. On fait le changement de fonctions $f_0(x) = f(x) - a - b$, ce qui redonne l'équation de Cauchy pour f_0. Conclusion : les trois fonctions sont affines, plus précisément il existe c tel que

$$\begin{aligned} g(x) &= cx + a \\ h(x) &= cx + b \\ f(x) &= cx + a + b \end{aligned}$$

Remarque 160. L'équation de Jensen est un cas particulier de (VII.7) (quelles sont g et h ?) et on pourrait déduire l'exercice 10 de l'exercice précédent.

Fonctions paires, fonctions impaires

Définition 161. Une fonction $f : \mathbb{R} \to \mathbb{R}$ est dite paire (resp. impaire) si pour tout $x \in \mathbb{R}$ on a $f(x) = f(-x)$ (resp. $f(x) = f(-x)$).

Le graphe d'une fonction paire admet une symétrie axiale (par rapport à l'axe des ordonnées) ; celui d'une fonction impaire admet une symétrie centrale par rapport à l'origine.

Exemple 162. La fonction polynômiale $x \mapsto x^n$ est paire (resp. impaire) ssi n est pair (resp. impair).

Exercice 12 Montrer que toute fonction $f : \mathbb{R} \to \mathbb{R}$ s'écrit de manière unique comme somme d'une fonction paire et d'une fonction impaire.

Solution de l'exercice 12 Pour tout x, on est amené à résoudre le système de deux équations à deux inconnues

$$\begin{cases} f_0(x) + f_1(x) = f(x) \\ f_0(x) - f_1(x) = f(-x) \end{cases}$$

Ce qui donne les solutions

$$\begin{aligned} f_0(x) &= \frac{1}{2}(f(x) + f(-x)) \\ f_1(x) &= \frac{1}{2}(f(x) - f(-x)) \end{aligned}$$

Exercice 13 Trouver toutes les fonctions $f : \mathbb{R} \to \mathbb{R}$ telles que

$$f\left(x^2 - y^2\right) = (x+y)(f(x) - f(y))$$

Solution de l'exercice 13 On commence par remarquer que $f(0) = 0$. Puis, faire $x = 0$ puis $y = 0$ donne que f est impaire :

$$\begin{aligned} f\left(-x^2\right) &= x(-f(x)) \\ f\left(x^2\right) &= xf(x) \end{aligned}$$

On remplace y par $-y$ dans l'équation initiale, cela donne :

$$\begin{aligned} f\left(x^2-(-y)^2\right) &= (x-y)\left(f(x)-f(-y)\right) \\ &= (x-y)\left(f(x)+f(y)\right) \end{aligned}$$

En développant et en comparant avec la première équation, on en déduit

$$yf(x) = xf(y)$$

$y=1$ donne que f est linéaire. Réciproquement, toutes les fonctions de la forme $x \mapsto cx$ sont solutions.

Exercice 14 Soient $f : \mathbb{N} \to \mathbb{N}$ surjective et $g : \mathbb{N} \to \mathbb{N}$ injective, telles que pour tout $n \in \mathbb{N}$ on ait $f(n) \geqslant g(n)$. Montrer que $f = g$.

Fonctions périodique

On rappelle que $f : \mathbb{R} \to \mathbb{R}$ est périodique s'il existe une constante $p \neq 0$ telle que pour tout x réel

$$f(x+p) = f(x)$$

On dit alors que p est une période de x.

Par exemple, $\sin$ et $\cos$ sont des fonctions périodiques. Leur plus petite période est 2π.

Exercice 15 Soit f telle qu'il existe $a > 0$ une constante et

$$f(x+a)\left(1-f(x)\right) = 1+f(x)$$

Montrer que f est périodique.

Exercice 16 Montrer que toutes les solutions de l'équation fonctionnelle

$$f(x+y)+f(x-y) = 2f(x)\cos y \tag{VII.8}$$

sont toutes périodiques et préciser une période ; puis résoudre cette équation.

Solution de l'exercice 14 Exploitons l'annulation de $\cos$ pour écrire

$$f\left(x+\frac{\pi}{2}\right)+f\left(x-\frac{\pi}{2}\right) = 0$$

de sorte que $f(x+\pi) = -f(x)$, et 2π est une période de f. Remarquons également que l'équation est linéaire, et $\sin$ et $\cos$ sont des solutions, de sorte que toute fonction de la forme

$$t \mapsto \lambda \sin t + \mu \cos t$$

avec λ et μ des constantes réelles, convient. Maintenant, posons $a = f(0)$ et $b = f(\pi/2)$; si l'on fait $x = 0$ dans l'équation fonctionnelle on trouve

$$\begin{aligned} f(t)+f(-t) &= 2a\cos t \\ f(2\pi+t)+f(\pi+t) &= 0 \\ f(\pi+t)+f(-t) &= -2b\sin t \end{aligned}$$

Tout ceci implique que f est bien de la forme précédente, avec $\mu = a$ et $\lambda = b$.

Exercice 17 Soient $f : \mathbb{N} \to \mathbb{N}$ surjective et $g : \mathbb{N} \to \mathbb{N}$ injective, telles que pour tout $n \in \mathbb{N}$ on ait $f(n) \geqslant g(n)$. Montrer que $f = g$.

Symétrie

Cette stratégie est applicable quand l'équation fonctionnelle fait intervenir plusieurs variables, et que l'un des membre est une expression symétrique en ces variables (c'est-à-dire, invariante quand on les permute). Par exemple, considérons l'équation fonctionnelle suivante

$$f(x+y) = x + f(y)$$

Le membre de gauche est symétrique en x et y, donc celui de droite doit l'être également. Ceci donne

$$x + f(y) = y + f(x)$$

Soit encore, $f(y) - f(x) = y - x$ et l'on se rapporte à l'équation (VII.4)

Remarque 163. Si les deux membre sont déjà symétriques (par exemple pour l'équation de Cauchy), inutile de songer à cette méthode !

Exercice 18 Montrer que l'équation fonctionnelle suivante n'admet pas de solution sur $\mathbb{R}$: $(x, y \neq 0)$

$$f\left(\frac{x}{y}\right) + f\left(\frac{y}{x}\right) = x + 3f(y)$$

Solution de l'exercice 15 Le membre de gauche est symétrique, on en déduit que pour tous x, y on doit avoir $x + 3f(y) = y + 3f(x)$. Ceci donnerait $f(x) = x/3 + c$, mais aucune constante c ne convient ; il n'y a pas de solution.

Vous verrez d'autres exemples plus élaborés en TD cet après-midi.

Remarque 164. Conclusion : attention à toujours bien effectuer la synthèse dans le raisonnement par analyse synthèse !

Principe de l'extremum, injectivité, surjectivité

Exercice 19 Soient A un ensemble fini de nombres réels et $f : A \to A$ une fonction telle que $f(x) - f(y) \geqslant x - y$ pour tous x et y dans A avec $x \geqslant y$. Montrer que f est l'identité.

Solution de l'exercice 16 Soient $x > y$. On a donc $f(x) - f(y) > y - x > 0$, et la fonction f est strictement croissante. En particulier, elle envoie le plus petit élément sur lui-même. On détermine ensuite de la même façon l'image du deuxième plus petit élément de A et ainsi de suite. Au final, f est bien l'identité.

Exercice 20 Soient $f : \mathbb{N} \to \mathbb{N}$ surjective et $g : \mathbb{N} \to \mathbb{N}$ injective, telles que pour tout $n \in \mathbb{N}$ on ait $f(n) \geqslant g(n)$. Montrer que $f = g$.

Solution de l'exercice 17 Par l'absurde : supposons que l'ensemble

$$A = \{n \mid f(n) \neq g(n)\}$$

est non vide. Alors l'ensemble $B = g(A) = \{g(n) \mid n \in A\}$ est non vide, et admet un plus petit élement : notons le $g(n_0)$, avec $n_0 \in A$. Un tel n_0 est unique puisque g est injective ; et nous avons $f(n_0) > g(n_0)$. Comme f est surjective, il existe n_1 différent de n_0 tel que $g(n_0) = f(n_1) < f(n_0)$. D'après l'injectivité de g on a alors $g(n_0) \neq g(n_1)$, donc $g(n_1) < f(n_1)$, et $n_1 \in A$. Ceci contredit la minimalité de n_0.

Un peu comme nous avions résolu un exercice précédent en commençant par remarquer que les fonctions inconnues étaient impaires, on peut commencer par chercher à montrer qu'une fonction inconnue est injective, surjective... des exemples seront traités dans le TD de cet après-midi.

Changement de fonction inconnue

Exercice 21 Trouver toutes les solutions monotones sur $\mathbb{R}_+^\times$ et qui ne s'annulent pas, de l'équation fonctionnelle

$$f(x+y) = \frac{f(x)\,f(y)}{f(x)+f(y)}$$

Solution de l'exercice 18 Supposons que f est solution, alors on vérifie que $g = 1/f$ est solution de l'équation de Cauchy. Or, f est monotone ssi g est monotone (puisque $x \mapsto 1/x$ est strictement décroissante sur l'ensemble des réels strictement positifs). Finalement les seules solutions possibles sont

$$f(x) = c/x$$

où c est une constante réelle.

3 lundi 24 après-midi : Guillaume Conchon-Kerjan

Énoncés des exercices

Exercice 1 Trouver toutes les fonctions $f : \mathbb{R} \to \mathbb{R}$ telles que pour tous réels x, y, on ait

$$f(x)f(y) + f(x+y) = xy.$$

(Olympiades africaines 2013)

Exercice 2 Trouver les fonctions $f : \mathbb{R} \to \mathbb{R}$ telles que pour tous réels x, y, on ait

$$f(x - f(y)) = 1 - x - y.$$

Exercice 3 Soit $f : \mathbb{R} \to \mathbb{R}$ telle que pour un certain $a > 0$, pour tout réel x,

$$f(x+a) = \frac{1}{2} + \sqrt{f(x) - f^2(x)}$$

Montrer que f est périodique.
(IMO 1968)

Exercice 4 Soit $f : \mathbb{R} \to \mathbb{R}$ vérifiant pour tout réel x :

$$f(x+1) + f(x-1) = \sqrt{2} f(x),$$

montrer qu'elle est périodique.

Exercice 5 Trouver toutes les fonctions de $\mathbb{R} - \{0, 1\}$ dans $\mathbb{R}$ telles que

$$f(x) + f\left(\frac{1}{1-x}\right) = x.$$

Exercice 6 Trouver les fonctions $f : \mathbb{R} \to \mathbb{R}$ telles que pour tous $x, y \in \mathbb{R}$, on ait :

$$f(\lfloor x \rfloor y) = f(x)\lfloor f(y) \rfloor$$

(IMO 2010)

Exercice 7 Trouver tous les $P \in \mathbb{R}[X]$ tels que $P(0) = 0$ et

$$P(x^2 + 1) = P(x)^2 + 1$$

pour tout réel x.

Exercice 8 Trouver toutes les fonctions $f : \mathbb{Z} \to \mathbb{Z}$ telles que pour tous réels x, y, on ait

$$f(x + f(y)) = f(x) - y.$$

(Olympiades africaines 2010)

Exercice 9 Trouver toutes les fonctions $f : \mathbb{N} \to \mathbb{N}$ telles que pour tout naturel n,

$$f(n) + f(f(n) + f(f(f(n))) = 3n.$$

Exercice 10 Trouver toutes les fonctions $f : \mathbb{N} \to \mathbb{N}$ strictement croissantes telles que $f(2) = 2$ et pour tous m, n premiers entre eux, $f(mn) = f(m)f(n)$.

Exercice 11 Soit f une fonction de $\mathbb{N}$ dans lui-même. Montrer que si pour tout naturel n,

$$f(n + 1) > f(f(n))$$

alors f est l'identité.
(IMO 1977)

Exercice 12 Existe-t-il une fonction $f : \mathbb{N} \to \mathbb{N}$ telle que pour tout entier naturel n,

$$f(f(n)) = n + 2015 \quad ?$$

(IMO 1987 - réactualisé...)

Exercice 13 Existe-t-il une fonction de $\mathbb{N}^*$ dans lui-même, strictement croissante, telle que $f(1) = 2$ et que pour tout n,

$$f(f(n)) = f(n) + n \quad ?$$

(IMO 1993)

Solutions

Solution de l'exercice 1 En prenant $x = 0$, on a $(f(0)+1)f(y) = 0$. Comme f ne peut pas être identiquement nulle (prendre $x = y = 1$ par exemple), on a $f(0) = -1$. En prenant $x = -y = 1$, on a $f(1)f(-1) = 0$.
Si $f(1) = 0$, en prenant $x = 1$, on a $f(y+1) = y$, donc la seule fonction solution possible est $x \mapsto x - 1$. On vérifie qu'elle convient.
Sinon, $f(-1) = 0$, et en prenant $x = -1$, on trouve de même $x \mapsto -1 - x$ comme unique possibilité, et elle convient également.

Solution de l'exercice 2 En prenant $x = f(y)$, on trouve $f(y) = 1 - f(0) - y$. Posons $c = 1 - f(0)$, dans l'équation initiale, on a $1 - x - y = f(x + y - c) = -(x + y - c) + c = 2c - x - y$ donc $c = \frac{1}{2}$. La seule solution possible est donc $x \mapsto \frac{1}{2} - x$, qui vérifie bien l'équation initiale.

Solution de l'exercice 3 On a $f(x) \geq \frac{1}{2}$, posons $g(x) = f(x) - \frac{1}{2}$ En élevant au carré, on obtient : $g^2(x + a) = \frac{1}{4} - g^2(x)$, ce qui donne aussi $g^2(x + 2a) = \frac{1}{4} - g^2(x + a)$. En sommant les deux relations,

$$g^2(x) = g^2(x + a)$$

or ces deux quantités sont positives, donc on a $g(x) = g(x + 2a)$ pour tout réel x, soit f et g $2a$-périodiques.

Solution de l'exercice 4 On applique à $x, x + 1$ et $x + 2$ la condition de l'énoncé :

$$\begin{aligned}
\sqrt{2}(f(x+1) + f(x-1)) &= 2f(x) \\
f(x+2) + f(x) &= \sqrt{2}f(x+1) \\
f(x) + f(x-2) &= \sqrt{2}f(x-1)
\end{aligned}$$

Il suffit alors de sommer ces trois équations pour obtenir $f(x+2) = -f(x-2)$ d'où l'on déduit que f est 8-périodique.

Solution de l'exercice 5 On exprime l'équation fonctionnelle avec les valeurs x, $\frac{1}{1-x}$ et $\frac{1}{x} - 1$, ce qui donne :

$$\begin{aligned}
f(x) + f\left(\frac{1}{1-x}\right) &= x \\
f\left(1 - \frac{1}{x}\right) + f\left(\frac{1}{1-x}\right) &= x \\
f(x) + f\left(1 - \frac{1}{x}\right) &= 1 - \frac{1}{x}
\end{aligned}$$

En sommant les première et troisième lignes puis en soustrayant la deuxième, on trouve

$$f(x) = \frac{1}{2}\left(x + 1 - \frac{1}{x} - \frac{1}{1-x}\right)$$

Solution de l'exercice 6 Posons $x = 0$ dans l'équation, on a $f(0) = f(0)\lfloor f(y) \rfloor$ pour tout réel y.
• Si $f(0) \neq 0$, alors $f(y) \in [1, 2[$ pour tout y réel. Avec $y = 0$ dans l'équation, on obtient $f(x) = f(0)$ pour tout $x \in \mathbb{R}$, donc f est constante de valeur $v \in [1, 2[$.

• Si $f(0) = 0$, on montre que f est la fonction nulle. Si pour un certain $z \in [0,1[$, $f(z) \neq 0$, on obtient avec $x = z : 0 = f(0) = f(z)\lfloor f(y) \rfloor$ donc pour tout réel y, $f(y) \in [0,1[$. Reprenons l'équation initiale avec $x = 1$ et $y = z$, on obtient $f(z) = 0$, contradiction.
Donc f est nulle sur $[0,1[$. Si maintenant $z \in \mathbb{R}$, il existe un entier $n \in \mathbb{Z}$ tel que $\frac{z}{n} \in [0,1[$. On obtient avec $x = n$ et $y = \frac{z}{n}$:

$$f(z) = f(n)\lfloor f(\frac{z}{n}) \rfloor = 0$$

donc f est bien la fonction nulle.
Réciproquement, ces fonctions satisfont toutes l'équation.

<u>Solution de l'exercice 7</u> On trouve $P(1) = 1$, $P(2) = 2$, $P(5) = 5$, etc. On définit alors la suite (a_n) par $a_0 = 0$ et $a_{n+1} = a_n^2 + 1$.
On vérifie sans difficulté qu'elle est strictement croissante, et on montre par récurrence sur n que $P(a_n) = a_n$. Ainsi, le polynôme $Q(X) = P(X) - X$ a une infinité de racines, donc c'est le polynôme nul. Autrement dit, pour tout réel x, $P(x) = x$. Réciproquement, l'identité est solution du problème.

<u>Solution de l'exercice 8</u> En posant $x = 0$, on a $f(f(y)) = f(0) - y$. Lorsque y varie dans $\mathbb{R}$, $f(0) - y$ décrit $\mathbb{R}$ donc f est surjective. Donc il existe a tel que $f(a) = 0$, ce qui donne $f(x) = f(x) - a$, donc $a = 0$ et $f(0) = 0$.
Ainsi, $x = 0$ donne $f(f(y)) = -y$. En mettant $(x, f(y))$ dans l'équation de départ, on trouve

$$f(x - y) = f(x) - f(y).$$

En appliquant $x = 0$ à cette équation, $f(-y) = -f(y)$, et en réinjectant ceci avec le couple $(x, -y)$, on trouve $f(x + y) = f(x) + f(y)$. f vérifie l'équation de Cauchy, donc il existe $a \in \mathbb{Z}$ tel que $f(x) = ax$ pour tout $x \in \mathbb{Z}$. Or $f(f(x)) = -x$ donc $a^2 = -1$, impossible. Conclusion : il n'existe pas de fonction respectant l'énoncé.

<u>Solution de l'exercice 9</u> Notons que si $f(n) = f(m)$ alors l'égalité reste vraie en composant par f, donc $3n = 3m$ donc f est injective. Montrons par récurrence forte sur n que $f(n) = n$. On initialise à $n = 1$: on a $f(1), f(f(1)), f(f(f(1))) \in \mathbb{N}^*$ et leur somme vaut 3, donc $f(1) = 1$.
Supposons le rang n, $n \geq 1$. On a $f(n + 1) \geq n + 1$ par injectivité de f. De même, $f(f(n + 1))$ et $f(f(f(n + 1)))$ ne peuvent être dans $\{1, \cdots, n\}$. Or

$$f(n + 1) + f(f(n + 1)) + f(f(f(n + 1))) = 3(n + 1)$$

donc $f(n+1) = n+1$ et ceci clôt la récurrence. L'identité est bien l'unique solution du problème (elle convient effectivement).

<u>Solution de l'exercice 10</u> Par stricte croissance de f, $f(0) = 0$ et $f(1) = 1$. Pour multiplier des nombres premiers entre eux sans utiliser 1, on aimerait bien connaître $f(3)$ par exemple. Posons $f(3) = 3 + k$, $k \geq 0$. Par encadrement successifs sur des petites valeurs, on montre que $k = 0$: en effet, $f(6) = 2k+6$ donc $f(5) \leq 2k+5$ et $f(10) \leq 4k+10$, $f(9) \leq 4k+9$, $f(18) \leq 8k+18$. Et, $f(5) \geq 5 + k$ donc $f(3 + k)(5 + k) \leq f(15) \leq f(18) - 3$ et de ceci on déduit $k = 0$.
Maintenant, montrons par récurrence sur n que $f(k) = k$ si $k \leq 2^n + 1$. On a vérifié l'initialisation à $n = 1$, et pour l'hérédité :

$$f(2^{n+1} + 2) = f(2)f(2^n + 1) = 2 = n + 1 + 2$$

donc les $f(k), 2^n + 2 \leq k \leq 2^{n+2} + 2$ sont compris entre $2^n + 2$ et $2^{n+2} + 2$ au sens large, et la stricte croissance de la fonction assure que $f(k) = k$ pour tout $k \leq 2^{n+1} + 1$. Ceci clôt la récurrence, et permet d'affirmer que f est l'identité. Réciproquement, cette fonction est évidemment solution du problème.

Solution de l'exercice 11 Montrons d'abord que f est strictement croissante : pour tout $n > 0$, $f(n) > f(f(n-1))$ donc f admet un minimum en 0 (le fait que f soit à valeurs entières et minorée par 0 assure de l'existence d'un minimum), et uniquement en 0. Cherchons la deuxième plus petite valeur de f : pour tout $n > 1$, $f(n) > f(0)$ et $f(n) > f(f(n-1))$ avec $f(n-1) \neq 0$ car $f(n-1) > 0$. Donc la deuxième plus petite valeur de f ne peut être atteinte qu'en 1. On montre en continuant ainsi que f est strictement croissante (le lecteur pourra rédiger la récurrence en question).
Comme $f(0) = 0$, on en déduit que $f(n) \geq n$ pour tout n. S'il existe m tel que $f(m) > m$, on a $f(m) \geq m + 1$ donc par croissance de f, $f(f(m)) \geq f(m+1)$, ce qui contredit l'énoncé. Donc pour tout $n \in \mathbb{N}$,

$$f(n) = n$$

Solution de l'exercice 12 Si f est solution, pour tout entier naturel n,

$$f(n + 2015) = f(n) + 2015$$

donc une récurrence immédiate montre pour tous $k, n \in \mathbb{N}$ que $f(n + 1987k) = f(n) + 1987k$. On considère g la fonction induite par f de $\mathbb{Z}/2015\mathbb{Z}$ dans lui-même. D'après l'énoncé, g^2 est l'identité. C'est donc une involution, or $\mathbb{Z}/2015\mathbb{Z}$ a un cardinal impair, donc il existe un point fixe n_0. Donc $f(n_0) = 2015 + m$ pour un certain $m \geq 0$. Et,

$$n_0 + 2015 = f(f(n_0)) = f(n_0 + 2015k) = f(n_0) + 2015k = f(n_0) + 2015 \times 2k$$

donc $k = \frac{1}{2}$, ce qui est absurde.
On peut faire différemment : on note $f(\mathbb{N})$ l'image de $\mathbb{N}$ par f, $A = \mathbb{N} - f(\mathbb{N})$, et $B = f(A)$. Il est clair que $B = f(\mathbb{N}) - f(f(\mathbb{N}))$: B est inclus dans $f(\mathbb{N})$, et si $k \in B$, alors il ne peut y avoir $k' \in \mathbb{N}$ tel que $f(f(k')) = k$ et réciproquement. A et B sont disjoints, leur union est $\mathbb{N} - f(f(\mathbb{N})) = \{0, \cdots, 2014\}$, de cardinal 2015, qui est impair. Et, f est injective, donc A et B doivent avoir même cardinal, ce qui est absurde.

Solution de l'exercice 13 La question est vicieusement piégeuse : la bonne réponse est un "oui" ingénu. On procède alors à la construction d'une fonction convenable. Puisqu'on travaille sur les entiers, on peut procéder par récurrence. $f(1) = 2$ et supposons que pour un certain $n \geq 1$, on ait construit $f(1) < \cdots < f(n)$. Pour simplifier la notation, soit $E = \{1, \cdots, n\}$.
On va essayer de définir une fonction "réciproque" de f en utilisant la croissance : soit $g(n+1)$ le plus grand entier $m \in E$ tel que $f(k) \leq n + 1$. Alors, $f(n + 1) = g(n + 1) + n + 1$. La stricte croissance de f sur E assure que $g(n + 1) \geq g(n)$ donc $f(n + 1) > f(n)$.
De plus, $f(f(n+1)) = f(n+1)+g(f(n+1))$. Or, par stricte croissance de f sur E, $f(n+1) > n+1$ (on avait aussi $f(1) > 1$). On en déduit que $g(f(n + 1)) = n + 1$, ce que l'on voulait. Ceci clôt la récurrence, et on peut ainsi construire une fonction respectant les contraintes de l'énoncé.

4 Groupe D : polynômes et inégalités

1 dimanche 23 après-midi : Guillaume Conchon-Kerjan

Énoncés

Exercice 1 Sélection roumaine 2006
Soit s et r vos rationnels préférés. Trouver toutes les fonctions $f : \mathbb{Q} \to \mathbb{Q}$ telles que pour tous rationnels x, y on ait

$$f(x + f(y)) = f(x + r) + y + s.$$

Exercice 2 Sélection roumaine 2011
Déterminer toutes les fonctions réelles telles que pour tous réels x, y :

$$2f(x) = f(x + y) + f(x + 2y).$$

Exercice 3 Olympiades balkaniques 2009
Trouver toutes les fonctions $f : \mathbb{N}^* \to \mathbb{N}^*$ telles que pour tous naturels non nuls m et n,

$$f(f^2(m) + 2f^2(n)) = m^2 + 2n^2.$$

Exercice 4 Liste courte 2005
Trouver toutes les fonctions f de $\mathbb{R}_+^*$ dans lui-même telles que pour tous x, y strictement positifs,

$$f(x)f(y) = 2f(x + yf(x)).$$

Exercice 5 Liste courte 2002
Trouver toutes les fonctions réelles vérifiant pour $x, y \in \mathbb{R}$:

$$f\left(f(x) + y\right) = 2x + f\left(f(y) - x\right).$$

Exercice 6 Sélection singapourienne 2008
Trouver toutes les fonctions réelles telles que

$$(x + y)(f(x) - f(y)) = (x - y)f(x + y).$$

Exercice 7 Olympiades balkaniques 2007
Trouver toutes les fonctions f telles que pour tous réels x, y, on ait

$$f(f(x) + y) = f(f(x) - y) + 4f(x)y.$$

Exercice 8 Olympiades balkaniques 2013
Trouver les fonctions $f : (\mathbb{R}_+^*)^3 \to \mathbb{R}_+^*$ telles que pour tous réels x, y, z, t, on ait

$$\begin{aligned} xf(x,y,z) &= zf(z,y,x) \\ f(x,ty,t^2z) &= tf(x,y,z) \\ f(1,k,k+1) &= k+1. \end{aligned}$$

Solutions

<u>Solution de l'exercice 1</u> On tente de se ramener à une équation de Cauchy. On fait $x = 0$. Puis on fait $y = f(z)$. En combinant les deux, on trouve

$$f(x + y + f(r) + s) = f(x + r) + f(y) + s$$

Si $a := f(r)-r$, on a $f(x+y+a+s) = f(x)+f(y)+s$. $y = 0$ donne ici $f(x+a+s) = f(x)+s+f(0)$, on en déduit :

$$f(x + y) = f(x) + f(y) - f(0).$$

La fonction $g = f - f(0)$ vérifie l'équation de Cauchy, donc est linéaire sur $\mathbb{Q}$, il s'ensuit que f est affine. Une vérification donne $x \mapsto x + r + s$ et $x \mapsto -x + r - s$ comme seules solutions.

<u>Solution de l'exercice 2</u> On effectue 4 substitutions : $(2x, x), (x, x), (0, x), (0, 2x)$. En les combinant, on trouve $f(x) = f(0)$, et réciproquement les fonctions constantes sont solution.

<u>Solution de l'exercice 3</u> L'injectivité est immédiate. Et, $(x+3)^2 + 2x^2 = (x+1)^2 + 2(x+2)^2$, donc $f^2(x + 3) + 2f^2(x) = f^2(x - 1)^2 + 2f^2(x + 2)$. Si on pose $u_n = f^2(n)$, on a une relation de récurrence linéaire sur cette suite :

$$u_{n+4} - 2u_{n+3} + 2u_{n+1} - u_n = 0.$$

Le polynôme associé est $X^4-2X^3+2X-1 = (X-1)^3(X+1)$. Donc $u_n = an^2+bn+c+(-1)^n d$ avec a, b, c, d des constantes. Comme $2u_1 + u_5 = 3u_3$ (prendre $m = n = 3$ et $m = 1, n = 5$ dans l'équation initiale), on a $b = 0$, puis on utilise le fait que u_n soit un carré pour en déduire (exercice !) que a est un carré et que $c = d = 0$. En injectant dans l'équation initiale, on trouve $a = 1$. Réciproquement, l'identité est bien solution.

<u>Solution de l'exercice 4</u> On pose $\varphi(x) = x + yf(x)$, on voit facilement par l'absurde que φ est injective. Si $x_1 < x_2$ et $f(x_1) > f(x_2)$, on a $\varphi(x_1) = \varphi(x_2)$ pour $y = \frac{x_1-x_2}{f(x_2)-f(x_1)}$, impossible. Donc f est croissante.

<u>Solution de l'exercice 5</u> $y = -f(x)$ offre la surjectivité. Maintenant si $f(a) = f(b)$, en prenant $f(y) = a + b$ et $x = a, b$, on voit que $a = b$. L'injectivité et $x = 0$ montrent que $f(x) = x + c$, qui convient pour tout $c \in \mathbb{R}$.

<u>Solution de l'exercice 6</u> En testant les couples $(x, 1), (x + 1, 1)$ et $(x, 2)$, on trouve et résout un système qui donne $f(x) = ax^2 + bx$. Réciproquement, ce sont des solutions du problème.

Solution de l'exercice 7 On pose $g(x) = f(x) - x^2$. On obtient $g(g(x)+x^2+y) = g(g(x)+x^2-y)$. On a alors pour tous réels x, y, z : $g(g(x)+x^2-g(y)-y^2+z) = g(g(x)+x^2+g(y)+y^2-z) = g(g(y)+y^2-g(x)-x^2+z)$. Donc $g(z) = g(2*(g(x)+x^2-g(y)-y^2)+z)$.
Si $g(x)+x^2$ est constant, on a $f = 0$, qui est solution. Sinon, g est périodique de période T, et $x = y+T$ dans l'équation précédente donne $g(z) = g(4Ty+2T^2+z)$, et comme $4Ty+2T^2$ décrit $\mathbb{R}$ lorsque y le fait aussi, g est constante. Donc $f(x) = x^2 + c$, qui est solution pour tout réel c.

Solution de l'exercice 8 On calcule $f(1, ab, b^2(a+1))$ puis $f(a, b, 1)$ puis $f(b, a, 1)$. On a ensuite $f(x, y, z) = f\left(x, \frac{y}{\sqrt{z}} \times \sqrt{z}, 1 \times \sqrt{z}^2\right) = \frac{y+\sqrt{y^2+4xz}}{2x}$. On vérifie aisément que cette fonction est solution.

2 lundi 24 matin : inégalités, Joon Kwon

Ce cours a initialement été donné au stage olympique de Montpellier en 2013. Donnons pour commencer deux références. Le cours de Pierre Bornztein sur les inégalités est une excellente référence. Il contient un chapitre consacré aux inégalités de convexité. Le lecteur intéressé par la convexité et ayant déjà un bagage mathématique solide pourra consulter l'éternel *Convex Analysis* de Rockafellar.

- Exponentielle et logarithme -

On commence par quelques rappels rapides sur l'exponentielle et le logarithme.

$$\begin{array}{rccc} \exp : & \mathbb{R} & \longrightarrow & \mathbb{R}_+^* \\ & x & \longmapsto & e^x \end{array}$$

$$\begin{array}{rccc} \ln : & \mathbb{R}_+^* & \longrightarrow & \mathbb{R} \\ & x & \longmapsto & \ln x \end{array}$$

Résumons dans un tableau leurs principales propriétés. A chaque fois, x et y appartiennent au domaine de définition de la fonction concernée et n est un entier naturel.

$\exp$	$\ln$
strict. croissante	strict. croissante
$\exp'(x) = \exp(x)$	$\ln'(x) = 1/x$
$e^{x+y} = e^x e^y$	$\ln(xy) = \ln x + \ln y$
$e^0 = 1$	$\ln 1 = 0$
$e^{nx} = (e^x)^n$	$\ln(x^n) = n \ln x$
$e^{-x} = 1/e^{-x}$	$\ln(1/x) = -\ln x$
$e^{x/n} = \sqrt[n]{e^x}$	$\ln(\sqrt[n]{x}) = \frac{1}{n} \ln x$

$\exp$ et $\ln$ sont liées par le fait qu'elles sont inverses l'une de l'autre :

$$\forall x \in \mathbb{R}_+^*,\ e^{\ln x} = x \qquad \text{et} \qquad \forall x \in \mathbb{R},\ \ln(e^x) = x.$$

Pour $a > 0$, une puissance a^x n'étant *a priori* définie que pour $x \in \mathbb{Z}$, on l'étend à tous les x réels de la manière suivante :

$$\forall x \in \mathbb{R}, \quad a^x = e^{x \ln a}.$$

- Convexité -

Définition 165. Soit I un intervalle. Une fonction $f : I \longrightarrow \mathbb{R}$ est dite convexe si :

$$\forall x, y \in I,\ \forall \lambda \in [0,1],\ f(\lambda x + (1-\lambda)y) \leqslant \lambda f(x) + (1-\lambda)f(y).$$

On dit que f est concave si $-f$ est convexe.

Théoréme 166 (Inégalité de Jensen)**.** Soit I un intervalle. Un fonction $f : I \longrightarrow \mathbb{R}$ est convexe si et seulement si pour tout $n \geqslant 1$ et tous $x_1, \ldots, x_n \in I$ et $\lambda_1, \ldots, \lambda_n \in [0,1]$ tels que $\lambda_1 + \cdots + \lambda_n = 1$, l'inégalité suivante est vérifiée :

$$f\left(\sum_{i=1}^{n} \lambda_i x_i\right) \leqslant \sum_{i=1}^{n} \lambda_i f(x_i).$$

Démonstration. Le sens indirect est acquis, puisqu'il suffit de prendre $n = 2$ pour retomber sur la définition de la convexité. Supposons donc f convexe et démontrons l'inégalité ci-dessus. On raisonne par récurrence sur n. Pour $n = 1$, elle est triviale, et pour $n = 2$ il s'agit de la définition de la convexité. Supposons le résultat acquis jusqu'à $n \geqslant 2$. Si on se donne alors $n+1$ points $x_1, \ldots, x_{n+1}$ ainsi que des coefficients positifs $\lambda_1, \ldots, \lambda_{n+1}$ tels que $\sum_{i=1}^{n+1} \lambda_i = 1$, la combinaison convexe correspondante peut s'écrire :

$$\begin{aligned}\sum_{i=1}^{n+1} \lambda_i x_i &= \sum_{i=1}^{n} \lambda_i x_i + \lambda_{n+1} x_{n+1} \\ &= (1-\lambda_{n+1}) \frac{\sum_{i=1}^{n} \lambda_i x_i}{1-\lambda_{n+1}} + \lambda_{n+1} x_{n+1} \\ &= (1-\lambda_{n+1}) y + \lambda_{n+1} x_{n+1},\end{aligned}$$

où on a posé $y = (1-\lambda_{n+1})^{-1} \sum_{i=1}^{n} \lambda_i x_i$. On est ainsi ramené à une combinaison convexe des deux points y et x_{n+1} associée aux coefficients $(1-\lambda_{n+1})$ et λ_{n+1}. On peut donc y appliquer l'hypothèse de récurrence pour $n = 2$:

$$\begin{aligned}f\left(\sum_{i=1}^{n+1} \lambda_i x_i\right) &= f\left((1-\lambda_{n+1}) y + \lambda_{n+1} x_{n+1}\right) \\ &\leqslant (1-\lambda_{n+1}) f(y) + \lambda_{n+1} f(x_{n+1}).\end{aligned}$$

Occupons-nous maintenant de $f(y)$. y peut être vu comme une combinaison convexe de n points, en effet :

$$y = \frac{1}{1-\lambda_{n+1}} \sum_{i=1}^{n} \lambda_i x_i = \sum_{i=1}^{n} \left(\frac{\lambda_i}{1-\lambda_{n+1}}\right) x_i.$$

y est donc la combinaison convexe des n points $x_1, \ldots, x_n$ associée aux coefficients $\lambda_i/(1-\lambda_{n+1})$ dont la somme vaut bien 1 :

$$\sum_{i=1}^{n} \frac{\lambda_i}{1-\lambda_{n+1}} = \frac{1}{1-\lambda_{n+1}} \sum_{i=1}^{n} \lambda_i = \frac{1}{1-\lambda_{n+1}} (1-\lambda_{n+1}) = 1.$$

On peut donc y appliquer l'hypothèse de récurrence :

$$f(y) \leqslant \sum_{i=1}^{n} \frac{\lambda_i}{1-\lambda_{n+1}} f(x_i).$$

Et finalement :

$$\begin{aligned} f\left(\sum_{i=1}^{n+1}\lambda_i x_i\right) &\leqslant (1-\lambda_{n+1})f(y) + \lambda_{n+1}f(x_{n+1}) \\ &\leqslant (1-\lambda_{n+1})\sum_{i=1}^{n}\frac{\lambda_i}{1-\lambda_{n+1}}f(x_i) + \lambda_{n+1}f(x_{n+1}) \\ &= \sum_{i=1}^{n+1}\lambda_{n+1}f(x_{n+1}). \end{aligned}$$

□

L'inégalité de Jensen n'est guère utile lorsqu'il s'agit de prouver qu'une fonction donnée est convexe. A l'inverse, lorsqu'on a une fonction qu'on sait être convexe, son application est fréquente.

Démontrons à présent une caractérisation qui porte sur les pentes des cordes.

Proposition 167. Soit I un intervalle. Une fonction $f : I \longrightarrow \mathbb{R}$ est convexe si et seulement si pour tous $x, y, z \in I$ tels que $x < y < z$:

$$\frac{f(y)-f(x)}{y-x} \leqslant \frac{f(z)-f(x)}{z-x} \leqslant \frac{f(z)-f(y)}{z-y}.$$

Démonstration. Supposons que f est convexe, et donnons-nous trois points $x < y < z$ dans I. y étant strictement compris entre x et z, il existe $\lambda \in]0,1[$ tel que :

$$y = \lambda x + (1-\lambda)z.$$

Par convexité de f, on a

$$f(y) \leqslant \lambda f(x) + (1-\lambda)f(z),$$

ce qui donne, en réarrangeant les termes :

$$\lambda(f(z)-f(x)) \leqslant f(z)-f(y).$$

Remarquons par ailleurs qu'une transformation similaire nous donne $\lambda = (z-y)/(x-z)$. En injectant cette égalité dans l'inégalité précédente, on obitent finalement :

$$\frac{f(z)-f(x)}{z-x} \leqslant \frac{f(z)-f(y)}{z-y}.$$

L'autre inégalité s'obtient de la même manière.

Réciproquement, supposons que les deux inégalités de l'énoncé sont satisfaites pour tous points $x < y < z \in I$ et montrons que f est convexe. Soient $x < z$ deux points de I et $\lambda \in [0,1]$. Si $\lambda = 0$ ou 1, l'inégalité à prouver est triviale. Supposons donc $\lambda \in]0,1[$. On pose $y = \lambda x + (1-\lambda)z$. On a par hypothèse :

$$\frac{f(z)-f(x)}{z-x} \leqslant \frac{f(z)-f(y)}{z-y}.$$

On mène alors les mêmes transformations que précédemment en sens inverse, pour retomber sur l'inégalité souhaitée :

$$f(y) \leqslant \lambda f(x) + (1-\lambda)f(z).$$

□

Voici deux caractérisations pour les fonctions dérivables.

Proposition 168. Soient I un intervalle et $f : I \longrightarrow \mathbb{R}$ une fonction dérivable. Les trois propositions suivantes sont équivalentes.

(i) f est convexe sur I.

(ii) f' est croissante sur I.

(iii) Pour tout $x_0 \in I$, la tangente en ce point est tout entière en-dessous de la fonction ; autrement dit :
$$\forall x \in I, \quad f(x_0) + (x - x_0)f'(x_0) \leqslant f(x).$$

Démonstration. (i)$\Longrightarrow$(ii). Supposons f dérivable et montrons que f' est croissante. Soient $x < y$ deux points. Montrons que $f'(x) \leqslant f'(y)$. Pour tout $z > y$, la Proposition 167 nous donne :
$$\frac{f(y) - f(x)}{y - x} \leqslant \frac{f(z) - f(y)}{z - y}.$$
En faisant tendre z vers y, on obtient, par passage des inégalités larges à la limite :
$$\frac{f(y) - f(x)}{y - x} \leqslant f'(y).$$
On se donne à présent un $x' \in I$ tel que $x < x' < y$. On a alors :
$$\frac{f(x') - f(x)}{x' - x} \leqslant \frac{f(y) - f(x)}{y - x},$$
et en faisant tendre x' vers x :
$$f'(x) \leqslant \frac{f(y) - f(x)}{y - x}.$$
En combinant les deux inégalités, on a bien $f'(x) \leqslant f'(y)$.

(ii)$\Longrightarrow$(iii). Soit $x_0 \in I$. Montrons que la tangente à f en x_0 est en-dessous du graphe de f. On pose la fonction g définie sur I par $g(x) = f(x) - (f'(x_0)(x - x_0) + f(a))$. Il s'agit donc de montrer que g est positive sur I. g est dérivable et $g'(x) = f'(x) - f'(x_0)$. f' étant croissante, g' est négative pour $x \leqslant x_0$ et positive pour $x_0 \leqslant x$. g est donc décroissante pour $x \leqslant x_0$ et croissante pour $x_0 \leqslant x$. Comme $g(x_0) = 0$, g est bien positive sur I.

(iii)$\Longrightarrow$(i). Suppsons que toutes les tangentes sont en-dessous de la fonction, et montrons que f est convexe. Soient $x, z \in I$ et $\lambda \in [0, 1]$. Notons $y = \lambda x + (1 - \lambda)z$. Notons τ la tangente à f en y :
$$\forall x' \in I, \ \tau(x') = f(y) + f'(y)(x' - y).$$
Par hypothèse, $f(x) \geqslant \tau(x)$ et $f(z) \geqslant \tau(z)$. On a donc :
$$\lambda f(x) + (1 - \lambda)f(z) \geqslant \lambda\tau(x) + (1 - \lambda)\tau(z) = \tau(y) = f(x),$$
où la première égalité se déduit facilement du fait que τ est affine, et la deuxième vient de la définition de τ. f est donc bien convexe. □

Corollaire 169. Soient I un intervalle et $f : I \longrightarrow \mathbb{R}$ une fonction deux fois dérivable. Alors f est convexe si, et seulement si $f'' \geqslant 0$.

Corollaire 170. 1. $\exp$ est convexe.

2. $\ln$ est concave.

Démonstration. Il suffit de calculer les dérivées secondes. $\forall x \in \mathbb{R},\ \exp''(x) = exp(x) \geqslant 0$, et $\forall x \in \mathbb{R}_+^*,\ \ln''(x) = -1/x^2 \leqslant 0$. □

Exemple 171. Donnons trois exemples d'inégalités classiques obtenues par la caractérisation faisant intervenir la tangente.

(i) $\forall x \in \mathbb{R},\ 1 + x \leqslant e^x$.

(ii) $\forall x \in]-1, +\infty[,\ \ln(1+x) \leqslant x$.

(iii) $\forall n \geqslant 1,\ \forall x \in [-1, +\infty[,\ 1 + nx \leqslant (1+x)^n$.

Proposition 172. Soit $f : [a, b] \longrightarrow \mathbb{R}$ une fonction convexe. Alors, f atteint son maximum en a ou en b.

Démonstration. Sans perte de généralité, supposons que $f(a) \geqslant f(b)$, et notons γ la corde entre ces deux points :

$$\gamma : x \in I \longmapsto f(a) + \frac{f(b) - f(a)}{b - a}(x - a).$$

On a clairement $\forall x \in I,\ f(x) \leqslant \gamma(x) \leqslant f(a)$. Le maximum de f existe bien et est atteint en a. □

- Exercices -

Exercice 1 Soient α, β, γ les angles d'un triangle Montrer que :

$$\sin\alpha + \sin\beta + \sin\gamma \leqslant \frac{3\sqrt{3}}{2}$$

<u>*Solution de l'exercice 1*</u> $\sin$ étant concave sur $[0, \pi]$, on peut appliquer l'inégalité de Jensen de la façon suivante :

$$\frac{1}{3}\sin\alpha + \frac{1}{3}\sin\beta + \frac{1}{3}\sin\gamma \leqslant \sin\left(\frac{1}{3}\alpha + \frac{1}{3}\beta + \frac{1}{3}\gamma\right) = \sin\frac{\pi}{3} = \frac{\sqrt{3}}{2},$$

où $\alpha + \beta + \gamma = \pi$ car il s'agit des angles d'un triangle. On conclut en multipliant par 3 de part et d'autre de cette inégalité.

Exercice 2 Soient $a, b, c > 0$ tels que $a + b + c = 1$. Montrer que

$$\left(a + \frac{1}{a}\right)^2 + \left(b + \frac{1}{b}\right)^2 + \left(c + \frac{1}{c}\right)^2 \geqslant \frac{100}{3}.$$

Solution de l'exercice 2 On pose, pour $x > 0$, $f(x) = (x+1/x)^2$. En calculant la dérivée seconde, on s'aperçoit que cette fonction est convexe. Et donc

$$\begin{aligned}\left(a+\frac{1}{a}\right)^2+\left(b+\frac{1}{b}\right)^2+\left(c+\frac{1}{c}\right)^2 &= 3\left(\frac{f(a)+f(b)+f(c)}{3}\right)\\ &\geqslant 3f\left(\frac{a+b+c}{3}\right)=3f\left(\frac{1}{3}\right)\\ &= 3\left(\frac{1}{3}+3\right)^2=\frac{100}{3}.\end{aligned}$$

Exercice 3 Soient $x_1,\dots,x_n > 0$ et $a_1,\dots,a_n \geqslant 0$ non tous nuls. On se donne aussi deux réels $0 < p < q$. Montrer qu'alors :

$$\left(\frac{\sum_{i=1}^n a_i x_i^p}{\sum_{i=1}^n a_i}\right)^{1/p} \leqslant \left(\frac{\sum_{i=1}^n a_i x_i^q}{\sum_{i=1}^n a_i}\right)^{1/q}.$$

Solution de l'exercice 3 Quitte à remplacer a_i par $a_i/\sum_{i=1}^n a_i$, on peut supposer que $\sum_{i=1}^n a_i = 1$. On considère $f(x) = x^{q/p}$ qui est convexe car $q/p \geqslant 1$. En appliquant Jensen aux x_i^p avec les coefficients a_i, on obtient :

$$\left(\sum_{i=1}^n a_i x_i^p\right)^{q/p} \leqslant \sum_{i=1}^n a_i (x_i^p)^{q/p} = \sum_{i=1}^n a_i x_i^q.$$

On conclut en prenant la racine q-ième des deux côtés.

Exercice 4 Soient $0 < a \leqslant b \leqslant c \leqslant d$. Montrer que $a^b b^c c^d d^a \geqslant b^a c^b d^c a^d$. *Solution de l'exercice 4*

En passant au logarithme de part et d'autre, il vient :

$$b\ln a + c\ln b + d\ln c + a\ln d \geqslant a\ln b + b\ln c + c\ln d + d\ln a.$$

En réarrangeant les termes, on obtient :

$$\frac{\ln c - \ln a}{c-a} \geqslant \frac{\ln d - \ln b}{d-b}.$$

Cette inégalité se prouve en appliquant l'inégalité des pentes à $\ln$ concave aux points (a,b,c) puis (b,c,d).

Exercice 5 Soit $x_1,\dots,x_n$ et $a_1,\dots,a_n$ des réels appartenant à $[0,1]$ tels que $\sum_{i=1}^n a_i = 1$. Montrer que pour tout $s \in \mathbb{R}$,

$$\ln\left(\sum_{i=1}^n a_i e^{sx_i}\right) \leqslant (e^s-1)\sum_{i=1}^n a_i x_i.$$

Solution de l'exercice 5 Observons que pour tout $x \in [0,1]$:

$$e^{sx} = e^{xs+(1-x)\cdot 0} \leqslant xe^s + (1-x)e^0 = xe^s + (1-x),$$

par convexité de l'exponentielle. Ainsi :

$$\begin{aligned}\sum_{i=1}^{n} a_i e^{sx_i} &\leqslant \sum_{i=1}^{n} a_i \left(x_i e^s + (1-x_i)\right) \\ &= e^s \sum_{i=1}^{n} a_i x_i + \sum_{i=1}^{n} a_i - \sum_{i=1}^{n} a_i x_i \\ &= 1 + (e^s - 1) \sum_{i=1}^{n} a_i x_i\end{aligned}$$

Car par hypothèse, $\sum_{i=1}^{n} a_i = 1$. En appliquant l'inégalité $1+x \leqslant e^x$ à cette dernière expression :

$$1 + (e^s - 1) \sum_{i=1}^{n} a_i x_i \leqslant \exp\left((e^s - 1) \sum_{i=1}^{n} a_i x_i\right).$$

On obtient donc :

$$\sum_{i=1}^{n} a_i e^{sx_i} \leqslant \exp\left((e^s - 1) \sum_{i=1}^{n} a_i x_i\right).$$

On trouve le résultat souhaité en prenant le logarithme des deux côtés de cette inégalité.

Exercice 6 Soient $x_1, \ldots, x_n \geqslant 1$. Montrer que :

$$\frac{1}{x_1+1} + \frac{1}{x_2+1} + \cdots + \frac{1}{x_n+1} \geqslant \frac{n}{1 + (x_1 x_2 \ldots x_n)^{1/n}}.$$

Solution de l'exercice 6 On effectue le changement de variable $x_i = e^{y_i}$. Posons $f(y) = \frac{1}{1+e^y}$ pour $y \geqslant 0$. En dérivant deux fois, on constate que f est convexe sur $\mathbb{R}_+$. Ainsi, l'inégalité demandée revient simplement à appliquer Jensen aux y_i avec coefficients $1/n$.

Exercice 7 Soient $a, b, c \in [0,1]$. Montrer que :

$$\frac{a}{b+c+1} + \frac{b}{c+a+1} + \frac{c}{a+b+1} + (1-a)(1-b)(1-c) \leqslant 1.$$

Solution de l'exercice 7 Demandons-nous pour quels $(a,b,c) \in [0,1]^3$ le membre de gauche atteint sa valeur maximale. Pour $b, c \in [0,1]$ fixés, considérons la fonction :

$$f(a) = \frac{a}{b+c+1} + \frac{b}{c+a+1} + \frac{c}{a+b+1} + (1-a)(1-b)(1-c).$$

On vérifie aisément que cette fonction est convexe. Cette fonction atteint son maximum en $a = 0$ ou $a = 1$. Avec un raisonnement analogue pour b et c, on voit que nécessairement a, b et c doivent appartenir à $\{0,1\}$ lorsque la quantité considérée est maximale. On conclut en remarquant qu'en chacun des triplets $(a,b,c) \in \{0,1\}^3$, la quantité vaut 1.

Exercice 8

1. Soit $x, y > 0$ et $p, q \in [1, +\infty[$ tels que $1/p + 1/q = 1$. Montrer que :

$$xy \leqslant \frac{x^p}{p} + \frac{y^q}{q}.$$

2. Soient $x_1, \dots, x_n$ et $y_1, \dots, y_n$ des réels strictement positifs. On se donne $p, q \in [1, +\infty[$ tels que $1/p + 1/q = 1$. Montrer que :

$$\sum_{i=1}^{n} x_i y_i \leqslant \left(\sum_{i=1}^{n} x_i^p\right)^{1/p} \left(\sum_{i=1}^{n} y_i^q\right)^{1/q}.$$

3. Montrer que :

$$(1 + x^2 y + x^4 y^2)^3 \leqslant (1 + x^3 + x^6)^2 (1 + y^3 + y^6).$$

Solution de l'exercice 8

1. On utilise la convexité de l'exponentielle :

$$\begin{aligned} xy &= \exp\left(\ln(xy)\right) = \exp\left(\ln x + \ln y\right) \\ &= \exp\left(\frac{1}{p}\ln(x^p) + \frac{1}{q}\ln(y^q)\right) \\ &\leqslant \frac{1}{p} e^{\ln(x^p)} + \frac{1}{q} e^{\ln(y^q)} = \frac{x^p}{p} + \frac{y^q}{q}. \end{aligned}$$

2. On applique la question précédente de la manière suivante :

$$\begin{aligned} \sum_{i=1}^{n} \frac{x_i}{\left(\sum_{j=1}^{n} x_j^p\right)^{1/p}} \cdot \frac{y_i}{\left(\sum_{j=1}^{n} y_j^q\right)^{1/q}} &= \frac{1}{p} \sum_{i=1}^{n} \frac{x_i^p}{\sum_{i=1}^{n} x_j^p} + \frac{1}{q} \sum_{i=1}^{n} \frac{y_i}{\sum_{j=1}^{n} y_j^q} \\ &= \frac{1}{p} + \frac{1}{q} \\ &= 1. \end{aligned}$$

   On conclut en multipliant de part et d'autre par $\left(\sum_{j=1}^{n} x_j^p\right)^{1/p} \left(\sum_{j=1}^{n} y_j^q\right)^{1/q}$

3. Il s'agit d'une application directe de la question précédente.

3 lundi 24 après-midi : inégalités, Matthieu Piquerez

Ce TD-cours a pour but de résumer les différentes inégalités qu'il faut connaître et de présenter quelques inégalités très générales. Il s'agit d'un résumé donc beaucoup de points ne seront pas détaillés. Il suffira le plus souvent de regarder dans ce polycopié ou dans ceux des années précédentes pour avoir plus d'informations. De plus ce résumé est bien loin d'être exhaustif, mais quelqu'un sachant résoudre les exercices proposés, avec l'aide des indications, peut déjà résoudre un nombre non négligeable d'exercices présentés aux différentes olympiades. Dans la suite, les techniques et inégalités très utiles à retenir sont écrites en gras. Enfin, même si le lecteur sait résoudre un exercice, nous lui conseillons de lire tout de même la solution dans laquelle il pourra peut-être apprendre une autre méthode de résolution.

Durant tout ce cours, sauf indication contraire, n sera un entier strictement positif quelconque.

- Inégalité arithmético-géométrique et autres -

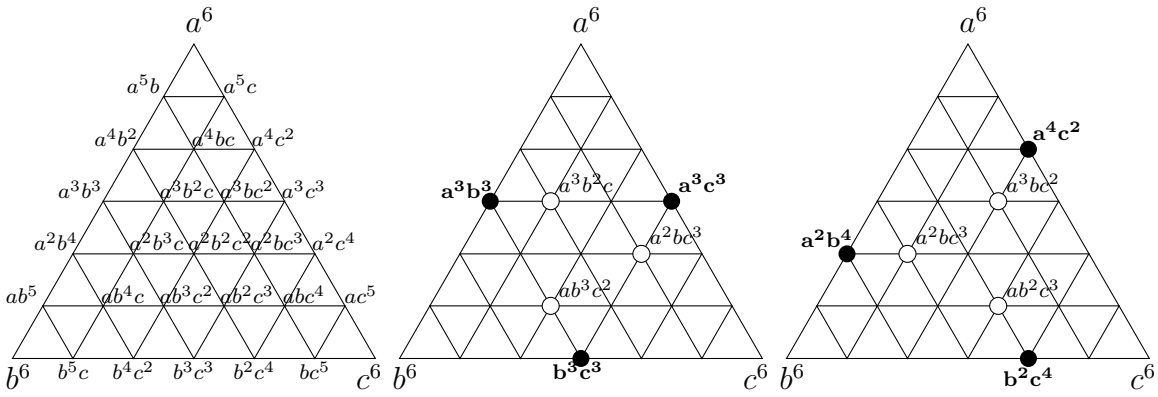
Exercice 1 Montrer que pour tous réels a, b, c :

$$\begin{aligned}\frac{ab}{c^2}+\frac{bc}{a^2}+\frac{ac}{b^2} &\geqslant \frac{a}{c}+\frac{b}{a}+\frac{c}{b},\\ \frac{a^2}{b^2}+\frac{b^2}{c^2}+\frac{c^2}{a^2} &\geqslant \frac{a}{b}+\frac{b}{c}+\frac{c}{a}.\end{aligned}$$

Solution de l'exercice 1 Un grand nombre d'exercices peuvent être résolus rien qu'en développant l'inégalité et en utilisant l'**inégalité arithmético-géométrique** (IAG) de manière systématique en utilisant la "**méthode du triangle**". Cette dernière peut être utilisée dès que l'on a une inégalité homogène à trois variables réelles positives. Prenons l'exemple des inégalités ci-dessus. En multiplant par $a^2b^2c^2$ et en développant cela revient à démontrer la positivité de :

$$\begin{aligned}a^3b^3+b^3c^3+a^3c^3-a^3b^2c-ab^3c^2-a^2bc^3 \text{ et de}\\ a^4c^2+a^2b^4+b^2c^4-a^3bc^2-a^2b^3c-ab^2c^3.\end{aligned}$$

L'expression est homogène d'ordre 6. On place donc des points sur un triangle de taille 6 comme ci-dessous (en noir les termes positifs et en blanc les termes négatifs) :



Pour plus de rigueur, le terme $a^\alpha b^\beta c^\gamma$ est placé au point de coordonnées barycentriques (α, β, γ) par rapport aux sommets du triangle. Il n'est pas nécessaire de comprendre les coordonnées barycentriques pour la suite.

Pour la première inégalité, on se rend par exemple compte que le point blanc a^3b^2c a pour coordonnées barycentriques $(2/3, 1/3)$ par rapport aux points noirs a^3b^3 et a^3c^3 (c'est-à-dire que le point blanc est entre les deux points noirs et deux fois plus près du premier que du deuxième). On utilise donc l'IAG comme suit :

$$\frac{2}{3}a^3b^3+\frac{1}{3}a^3c^3=\frac{a^3b^3+a^3b^3+a^3c^3}{3}\geqslant\sqrt[3]{a^3b^3a^3b^3a^3c^3}=a^3b^2c.$$

On fait de même pour les deux autres points noirs et l'on obtient l'inégalité voulue.

Pour la seconde inégalité, les coefficients à utiliser ne sont pas aussi évidents. Pour ceux qui ont l'habitude des coordonnées barycentriques, ils trouveront facilement. Pour les autres, il est préférable de poser un système d'équations. On a l'IAG

$$\frac{\alpha b^2c^4+\beta a^4c^2+\gamma a^2b^4}{3}\geqslant a^{\frac{2}{3}(2\beta+\gamma)}b^{\frac{2}{3}(\alpha+2\gamma)}c^{\frac{2}{3}(2\alpha+\beta)},$$

donc on cherche à résoudre pour le premier terme négatif

$$\frac{2}{3}(2\beta+\gamma)=3, \qquad \frac{2}{3}(\alpha+2\gamma)=1, \qquad \frac{2}{3}(2\alpha+\beta)=2.$$

On trouve $\beta=2, \alpha=1/2, \gamma=1/2$. On obtient bien

$$\frac{b^2c^4+4a^4c^2+a^2b^4}{6} \geqslant a^3bc^2.$$

On fait de même pour les autres points blancs et l'on obtient l'inégalité souhaitée.

Dans certains cas, pour aller plus vite, on peut utiliser l'**inégalité de Muirhead**.

Proposition 173. (Inégalité de Muirhead) Soient $x_1 \leqslant x_2 \leqslant \cdots \leqslant x_n$ et $y_1 \leqslant y_2 \leqslant \cdots \leqslant y_n$ des nombres réels positifs, $a_1 \leqslant \cdots \leqslant a_n$ et $b_1 \leqslant \cdots \leqslant b_n$ des entiers positifs tels que pour tout entier p entre 1 et n

$$\begin{aligned} a_1+\cdots+a_p &\leqslant b_1+\cdots+a_p, \text{ et} \\ a_1+\cdots+a_n &= b_1+\cdots+b_n, \end{aligned}$$

alors, avec $\mathfrak{S}$ l'ensemble des permutations de $\{1,\ldots,n\}$,

$$\sum_{\sigma\in\mathfrak{S}} x_1^{a_{\sigma(1)}}\ldots x_n^{a_{\sigma(n)}} \geqslant \sum_{\sigma\in\mathfrak{S}} y_1^{b_{\sigma(1)}}\ldots y_n^{b_{\sigma(n)}}.$$

Nous n'allons pas démontrer cette inégalité ici car la méthode du triangle et l'IAG permettent de toute façon de démontrer chaque cas particulier. Si le lecteur souhaite une preuve, il peut se référer au livre *Les olympiades de mathématiques, Réflexes et stratégies* de Tarik Belhaj Soulami.

Exercice 2 Montrer que pour tout réels positifs a, b, c

$$(a+b-c)(b+c-a)(c+a-b) \leqslant abc.$$

Solution de l'exercice 2 L'inégalité ci-dessus est une forme particulière de l'**inégalité de Schur** pour $r=1$ dont l'énoncé est ci-dessous.

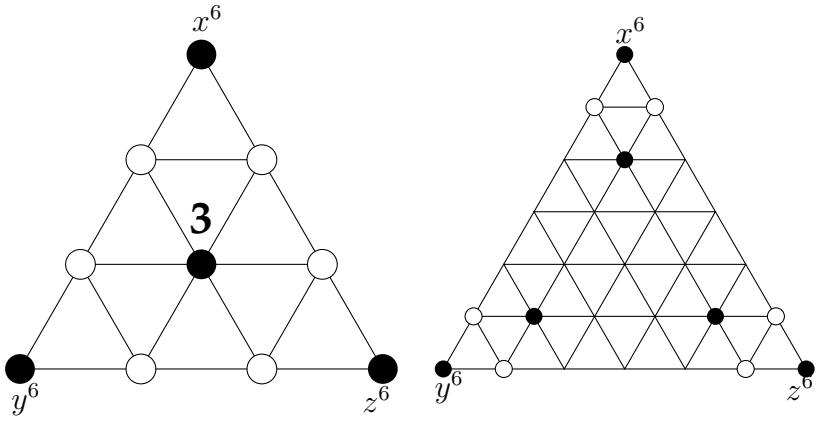
Proposition 174. (Inégalité de Schur) Soient x, y, z des réels positifs et r un nombre réel. Alors

$$x^r(x-y)(x-z)+y^r(y-x)(y-z)+z^r(z-x)(z-y) \geqslant 0,$$

l'égalité étant atteinte lorsque $x=y=z$, ou bien lorsque deux réels parmi x, y, z sont égaux et le troisième est nul.

Démonstration. L'inégalité étant symétrique en x, y, z, on peut supposer $x \geqslant y \geqslant z$. **Ordonner** des variables lorsque l'expression est symétrique se révèle souvent utile. Le premier et le troisième terme sont positifs. En ce qui concerne le deuxième, si $r \geqslant 0$ alors $x^r \geqslant y^r$ et $x-z \geqslant y-z$ et si $r<0$ alors $z^r \geqslant y^r$ et $z-x \geqslant y-x$, donc la somme des deux premiers termes, pour r positif, ou des deux derniers termes, pour r négatif, est positive ce qui conclut (le cas d'égalité est à présent facile). □

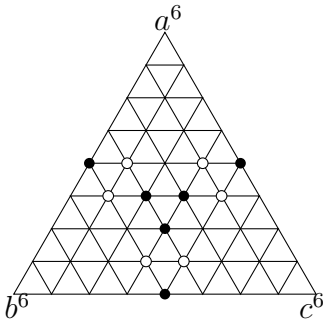
Il est bon de connaître cette inégalité car elle ne se démontre pas directement avec l'IAG et elle peut prendre de multiples formes. La façon la plus simple de la reconnaître est de dessiner le triangle (lorsque r est un entier positif). Elle prend alors la forme suivante (pour $r = 1$ et $r = 4$)



Exercice 3 Montrer que pour tous réels positifs a, b, c :

$$\sum_{\text{cyc}} a^3b^3(ab - ac - bc + c^2) \geqslant 0.$$

Solution de l'exercice 3 On dessine le triangle :



On reconnaît l'inégalité de Schur dans le triangle de sommets a^4b^4, a^4c^4, b^4c^4, mais on ne peut pas l'exploiter directement. Il faut faire un **changement de variable** en posant $x = \sqrt[8]{b^4c^4}, y = \sqrt[8]{a^4c^4}, z = \sqrt[8]{a^4b^4}$ pour "remettre le triangle à l'endroit". On obtient alors le terme de gauche

$$\sum_{\text{cyc}} z^8 - z^6y^2 - z^6x^2 + z^4x^2y^2 = \sum_{\text{cyc}} z^4(z^2 - x^2)(z^2 - y^2),$$

et l'on conclut avec l'inégalité de Schur.

Pour l'exercice suivant, démontrer d'abord le cas $p = n - 1$. L'idée principale du reste de la preuve est importante. Quant aux détails, ils sont intéressants mais s'éloignent du cadre des inégalités.

Exercice 4 (Inégalités de Maclaurin et de Newton) Soient $n \geqslant 2$ un entier et $x_1, \ldots, x_n$ des réels strictement positifs. Si p est un entier tel que $1 \leqslant p \leqslant n$, on pose :

$$d_p = \frac{1}{\binom{n}{p}} \sum_{\text{sym}} x_1x_2 \cdots x_p.$$

Montrer que :

1. si $1 \leqslant p < q \leqslant n$ alors $d_p^{1/p} \geqslant d_q^{1/q}$,
2. si $p \in \{1, \dots, n-1\}$ alors $d_p^2 \geqslant d_{p-1} d_{p+1}$.

Solution de l'exercice 4 Montrons donc la première inégalité pour $p = n-1$ et $q = n$. En élevant le tout à la puissance $n-1$ on doit donc démontrer que

$$\frac{\sum_{\text{sym}} x_1 \dots x_{n-1}}{n} \geqslant \sqrt[n]{x_1^{n-1} \dots x_n^{n-1}},$$

ce qui est l'IAG.

Pour la deuxième inégalité avec $p = n-1$, en multipliant par $n^2(n-1)/(x_1 \dots x_n)^2$ on obtient

$$(n-1)\left(\sum_{i=1}^{n} \frac{1}{x_i}\right)^2 \geqslant 2n \sum_{1 \leqslant i < j \leqslant n} \frac{1}{x_i x_j}.$$

En développant le membre de gauche et en simplifiant les termes identiques, l'inégalité équivaut à

$$\begin{aligned} (n-1)\sum_{i=1}^{n} \frac{1}{x_i^2} &\geqslant 2 \sum_{1 \leqslant i < j \leqslant n} \frac{1}{x_i x_j}, \text{ ou encore à} \\ \sum_{1 \leqslant i < j \leqslant n} \frac{1}{x_i^2} + \frac{1}{x_j^2} &\geqslant \sum_{1 \leqslant i < j \leqslant n} 2\frac{1}{x_i x_j}, \end{aligned}$$

ce qui est clairement vraie.

Traitons maintenant le cas général par **récurrence**. Pour cela nous allons utiliser des propriétés sur les polynômes, notamment le théorème de Rolle. Le cas traité ci-dessus prouve l'initialisation $n = 2$ pour la première inégalité et $n = 3$ pour la seconde. Pour l'hérédité, supposons les inégalités vérifiées au rang $n-1$. Soit $P(X)$ le polynôme unitaire de racines $x_1, \dots, x_n$. On a :

$$P(X) = X^n + nd_1X^{n-1} + \binom{n}{2} d_2 X^{n-2} + \dots + d_n.$$

On dérive ce polynôme pour obtenir

$$P'(X) = n\left(X^{n-1} + (n-1)d_1X^{n-2} + \binom{n-1}{2} X^{n-3} + \dots + d_{n-1}\right).$$

On remarque alors que $d_i = d_i'$ pour i allant de 1 à $n-1$ et où les d_i' sont définis comme les d_i mais par rapport aux $n-1$ racines de P'. Or, il y a au moins une racine de P' entre deux racines de P (théorème de Rolle) donc les racines de P' sont toutes réelles strictement positives. On conclut avec l'hypothèse de récurrence et avec le cas étudié ci-dessus.

Exercice 5 Soient a, b, c les longueurs des trois côtés d'un triangle. Démontrer que

$$a^2c(a-b) + b^2a(b-c) + c^2b(c-a) \geqslant 0.$$

Solution de l'exercice 5 Lorsqu'il s'agit des longueurs des côtés d'un triangle, on peut utiliser la **transformation de Ravi**. Soient x, y, z les nombres réels strictement positifs tels que

$$a = y + z, \qquad b = x + z, \qquad c = x + y.$$

On obtient que le membre de gauche égale

$$\sum_{\text{cyc}} (y+z)^2(x+y)(y-x).$$

Puis on conclut en développant et en utilisant la méthode du triangle.

Exercice 6 (IMO 12, 2) Soit $n \geqslant 3$ un nombre entier et soient $a_2, a_3, \ldots, a_n$ des nombres réels positifs tels que $a_2 a_3 \cdots a_n = 1$. Montrer que

$$(1+a_2)^2(1+a_3)^3 \cdots (1+a_n)^n > n^n.$$

Solution de l'exercice 6 La méthode du triangle est efficace car elle explicite comment **découper les termes** pour utiliser l'IAG. Parfois il faut se débrouiller seul. Pour i compris entre 2 et n, on a

$$\begin{aligned} 1 + a_i &= \frac{1}{i-1} + \cdots + \frac{1}{i-1} + a_i \\ &\geqslant i\sqrt[i]{\left(\frac{1}{i-1}\right)^{i-1} a_i} \\ (1+a_i)^i &\geqslant \frac{i^i}{(i-1)^{i-1}} a_i. \end{aligned}$$

De plus l'inégalité est stricte pour au moins l'un des a_i (sinon $a_i = \frac{1}{i-1}$ pour tout i ce qui contredit la condition). On obtient alors

$$(1+a_2)^2(1+a_3)^3 \cdots (1+a_n)^n > \frac{2^2}{1^1} a_2 \frac{3^3}{2^2} a_3 \ldots \frac{n^n}{(n-1)^{n-1}} a_n = n^n.$$

- Cauchy-Schwarz -

Exercice 7 (**Cauchy-Schwarz**) Soient $x_1, \ldots, x_n, y_1, \ldots, y_n$ des nombres réels. Montrer que

$$|x_1 y_1 + \cdots + x_n y_n| \leqslant \sqrt{x_1^2 + \cdots + x_n^2}\sqrt{y_1^2 + \ldots y_n^2}.$$

Avec égalité si et seulement si $(x_1, \ldots, x_n)$ est proportionnel à $(y_1, \ldots, y_n)$.

L'inégalité de **Cauchy-Schwarz**, qu'il faut absolument connaître, admet plusieurs preuves dont une très simple qui consiste à mettre au carré, à simplifier et à utiliser l'IAG. Une seconde preuve intéressante est l'**interprétation géométrique**, qui est aussi un bon moyen mémotechnique : la valeur absolue du produit scalaire de deux vecteurs est inférieure au produit des normes. Le lecteur pourra trouver une définition plus générale de produit scalaire, et donc

une inégalité plus générale, dans le cours d'inégalité de Vincent Jugé du stage de Montpellier 2014. Nous allons voir ici une autre preuve qui présente une technique de démonstration intéressante.

Solution de l'exercice 7 Soit λ une variable réelle. Étudions le produit scalaire suivant :

$$(x-\lambda y)\cdot(x-\lambda y) = \left(\sum_{i=1}^{n} y_i^2\right)\lambda^2 - 2\left(\sum_{i=1}^{n} x_i y_i\right)\lambda + \sum_{i=1}^{n} x_i^2.$$

On obtient un polynôme du second degré en λ qui ne s'annule jamais sauf si x et y sont colinéaires. Donc le discriminant est négatif, ou nul dans le second cas :

$$4\left(\sum_{i=1}^{n} x_i y_i\right) - 4\left(\sum_{i=1}^{n} y_i^2\right)\left(\sum_{i=1}^{n} x_i^2\right) \leqslant 0.$$

On obtient bien l'inégalité de Cauchy-Schwarz.

Il est aussi utile d'avoir en tête la reformulation suivante de Cauchy-Schwarz (parfois appelée **inégalité des mauvais élèves**, ou lemme de T2), qui facilite l'application de Cauchy-Schwarz dans certains cas.

Exercice 8 (Inégalité des mauvais élèves) Soient $a_1, \ldots, a_n$ et $x_1, \ldots, x_n$ des réels strictement positifs. Montrer que

$$\frac{a_1^2}{b_1} + \ldots + \frac{a_n^2}{b_n} \geqslant \frac{(a_1 + \ldots + a_n)^2}{b_1 + \ldots + b_n},$$

avec égalité lorsque les vecteurs $(a_1, \ldots, a_n)$ et $(b_1, \ldots, b_n)$ sont colinéaires.

Pour démontrer cette inégalité, on peut utiliser la "**seconde forme**" de l'inégalité de Cauchy-Schwarz : si $x_1, \ldots, x_n, y_1, \ldots, y_n$ sont des réels positifs, alors

$$\left(\sum_{i=1}^{n} x_i\right)^2 \leqslant \left(\sum_{i=1}^{n} \frac{x_i}{y_i}\right)\left(\sum_{i=1}^{n} x_i y_i\right).$$

Elle se démontre en utilisant l'inégalité de Cauchy-Schwarz avec les facteurs $\sqrt{x_i/y_i}$ et $\sqrt{x_i y_i}$.

Solution de l'exercice 8 Il ne reste qu'à appliquer cette seconde forme pour $x_i = a_i$ et $y_i = b_i/a_i$.

Exercice 9 Soient a, b, c trois nombres réels strictement positifs. On suppose en outre que $abc = 1$. Montrer que

$$\frac{a^2}{b+c} + \frac{b^2}{c+a} + \frac{c^2}{a+b} \geqslant \frac{3}{2}.$$

Solution de l'exercice 9 C'est un cas particulier de l'inégalité des mauvais élèves :

$$\begin{aligned}\frac{a^2}{b+c} + \frac{b^2}{c+a} + \frac{c^2}{a+b} &\geqslant \frac{(a+b+c)^2}{2(a+b+c)} \\ &\overset{\text{(IAG)}}{\geqslant} \frac{3\sqrt[3]{abc}}{2} = \frac{3}{2}.\end{aligned}$$

Voici une généralisation de l'inégalité de Cauchy-Schwarz (pour résoudre cet exercice on pourra supposer p et q rationnels) :

Exercice 10 (Inégalité de Hölder) Soient $p, q \geqslant 0$ tels que $p+q=1$ et $x_1, \ldots, x_n > 0$ et $y_1, \ldots, y_n > 0$. Montrer que

$$x_1^p y_1^q + \cdots + x_n^p y_n^q \leqslant (x_1 + \cdots + x_n)^p (y_1 + \cdots + y_n)^q.$$

Généraliser au cas de kn variables avec $k \geqslant 2$.

Solution de l'exercice 10 L'expression est homogène en les x_i et en les y_i. L'idée est de la **déshomogénéiser**. On pose, sans perte de généralité (quitte à diviser les x_i par $(x_1 + \cdots + x_n)^p$), $x_1 + \cdots + x_n = 1$. De même on pose $y_1 + \cdots + y_n = 1$. On utilise maintenant l'IAG (on peut s'appuyer sur la rationnalité de p et q pour cela ou, pour le cas général, utiliser l' IAG généralisée ci-dessous). Pour tout i entre 1 et n :

$$x_i^p y_i^q \leqslant p x_i + q y_i.$$

En sommant tout on obtient

$$x_1^p y_1^q + \cdots + x_n^p y_n^q \leqslant p(x_1 + \cdots + x_n) + q(y_1 + \cdots + y_n) = 1.$$

On peut généraliser l'inégalité de la manière suivante. Soient k un entier supérieur à 2, $x_{j,i}$, pour i allant de 1 à n et j allant de 1 à k, et $p_1, p_2, \ldots p_k$ des réels positifs tels que $p_1 + \cdots + p_k = 1$, alors

$$\sum_{i=1}^{n} x_{1,i}^{p_1} \ldots x_{k,i}^{p_k} \leqslant \prod_{j=1}^{k} \left(x_{j,1} + \cdots + x_{j,n}\right)^{p_j}.$$

Nous laissons la preuve, facile par récurrence, au lecteur.

L'exercice suivant est un corollaire de l'inégalité de Hölder. Voici une indication pour résoudre cet exercice :

$$(a+b)^p = (a+b)(a+b)^{p-1}.$$

Exercice 11 (Inégalité de Minkowski) Soient p, $x_1, \ldots, x_n$ et $y_1, \ldots, y_n$ des réels strictement positifs tels que $p \geqslant 1$, montrer que

$$\left(\sum_{i=1}^{n} (x_i + y_i)^p\right)^{1/p} \leqslant \left(\sum_{i=1}^{n} x_i^p\right)^{1/p} + \left(\sum_{i=1}^{n} y_i^p\right)^{1/p}.$$

Solution de l'exercice 11 On a

$$\sum_{i=1}^{n} (x_i + y_i)^p = \sum_{i=1}^{n} (x_i + y_i)(x_i + y_i)^{p-1}$$

Coupons cette somme en deux et appliquons Hölder avec $1/p$ et $(p-1)/p$:

$$\sum_{i=1}^{n} x_i (x_i + y_i)^{p-1} \leqslant \left(\sum_{i=1}^{n} x_i^p\right)^{\frac{1}{p}} \left(\sum_{i=1}^{n} (x_i + y_i)^p\right)^{\frac{p-1}{p}}$$

On obtient donc, en sommant les deux parties,

$$\sum_{i=1}^{n}(x_i+y_i)(x_i+y_i)^{p-1} \leqslant \left(\left(\sum_{i=1}^{n}x_i^p\right)^{1/p}+\left(\sum_{i=1}^{n}y_i^p\right)^{1/p}\right)\left(\sum_{i=1}^{n}(x_i+y_i)^p\right)^{\frac{p-1}{p}}$$

On simplifie pour conclure.

- Autres inégalités -

L'**inégalité de Nesbitt** ci-dessous apparaît fréquemment :

Exercice 12 (Inégalité de Nesbitt) Soient $a, b, c > 0$ des réels. Montrer que

$$\frac{a}{b+c}+\frac{b}{c+a}+\frac{c}{a+b} \geqslant \frac{3}{2},$$

avec égalité si et seulement si $a = b = c$.

Solution de l'exercice 12 L'inégalité est symétrique en a, b et c. On peut donc ordonner les variables : $a \geqslant b \geqslant c$. On a alors $\frac{1}{b+c} \geqslant \frac{1}{a+c} \geqslant \frac{1}{a+b}$. En utilisant l'**inégalité de réordonnement**, on obtient

$$\begin{aligned}\frac{a}{b+c}+\frac{b}{c+a}+\frac{c}{a+b} &\geqslant \frac{b}{b+c}+\frac{c}{c+a}+\frac{a}{a+b}, \text{ et}\\ \frac{a}{b+c}+\frac{b}{c+a}+\frac{c}{a+b} &\geqslant \frac{c}{b+c}+\frac{a}{c+a}+\frac{b}{a+b}.\end{aligned}$$

En sommant ces deux inégalités et en divisant par deux on obtient le résultat voulu.

Exercice 13 Soient a, b, c des réels positifs tels que $abc = 1$. Montrer que

$$\frac{a}{ab+1}+\frac{b}{bc+1}+\frac{c}{ca+1} \geqslant \frac{3}{2}.$$

De nombreuses inégalités olympiques font intervenir des variables $a_1, \ldots, a_n$ soumises à une condition du type $a_1 \ldots a_n = 1$. Une méthode très utile pour aborder ce genre d'inégalités consiste à **se débarrasser de cette contrainte** tout en **homogénéisant** en opérant un **changement de variables du type**

$$a_1 = \left(\frac{x_2}{x_1}\right)^{\alpha},\ a_2 = \left(\frac{x_3}{x_2}\right)^{\alpha}, \ldots, a_n = \left(\frac{x_1}{x_n}\right)^{\alpha},$$

où α est un réel à choisir, souvent pris égal à 1.

Solution de l'exercice 13 La substitution la plus simple $a = \frac{x}{y}$, $b = \frac{y}{z}$, $c = \frac{z}{x}$ (obtenue en prenant par exemple $x = 1 = abc$, $y = bc$, $z = c$) transforme le côté gauche en

$$\frac{\frac{x}{y}}{\frac{x}{z}+1}+\frac{\frac{y}{z}}{\frac{y}{x}+1}+\frac{\frac{z}{x}}{\frac{z}{y}+1} = \frac{zx}{xy+yz}+\frac{xy}{yz+zx}+\frac{yz}{zx+xy}.$$

On applique l'inégalité de Nesbitt pour conclure.

Exercice 14 Soit a, b et c trois réels strictement positifs. Montrer que

$$\frac{ab}{a+b}+\frac{bc}{b+c}+\frac{ca}{c+a}\leqslant\frac{3(ab+bc+ca)}{2(a+b+c)}.$$

Solution de l'exercice 14 L'inégalité équivaut à

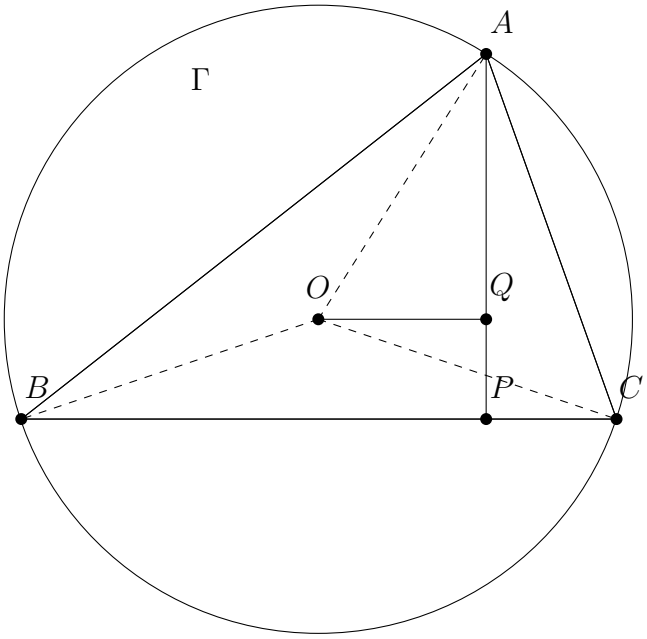
$$\left(\frac{ab}{a+b}+\frac{bc}{b+c}+\frac{ca}{c+a}\right)((a+b)+(b+c)+(c+a))\leqslant 3(ab+bc+ca).$$

Il reste à diviser par 9 et ordonner les variables (sans perdre de généralité par symétrie), $a\geqslant b\geqslant c$, pour obtenir l'**inégalité de Tchebychev**.

Beaucoup d'inégalités aux Olympiades Internationales sont des inégalités géométriques. Elles relèvent généralement plus de la géométrie que des inégalités. Nous proposons tout de même les deux exercices suivants pour présenter des techniques utiles.

Exercice 15 (IMO 01, 1) Soit ABC un triangle strictement acutangle. Soient P le pied de la hauteur issue de A et O le centre du cercle circonscrit au triangle ABC. Montrer que si $\widehat{ACB}\geqslant\widehat{ABC}+30^\circ$ alors $\widehat{BAC}+\widehat{COP}<90^\circ$.

Solution de l'exercice 15 On ajoute le projeté orthogonal Q de O sur $[AP]$. Une simple chasse



aux angles donne $\widehat{PCO}=90^\circ-\widehat{BAC}$ et $\widehat{OAP}=\widehat{BCA}-\widehat{ABC}$. Donc l'énoncé nous donne $\widehat{OAP}\geqslant 30^\circ$ et l'on veut montrer $\widehat{PCO}>\widehat{POC}$. Or, la loi des sinus nous montre que **les angles d'un triangle sont dans le même ordre que les longueurs des côtés opposés respectifs**. Donc cette dernière inégalité équivaut à $OP>PC$. Or on a $OQ/OA=\sin(\widehat{OAP})$ donc $OQ\geqslant R/2$ où R est le rayon du cercle circonscrit. D'un autre côté, on a $OQ+PC<OC=R$ donc

$$OP>OQ\geqslant R/2\geqslant R-OQ>PC,$$

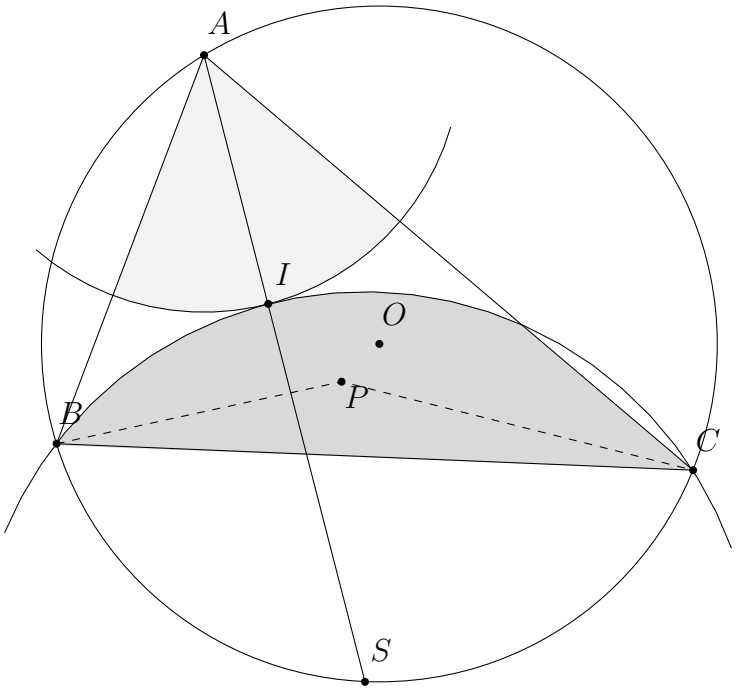
ce qui conclut.

Exercice 16 (inspiré de IMO 06, 1) Soient ABC un triangle et I le centre de son cercle inscrit. Soit P un point à l'intérieur du triangle tel que

$$\widehat{PBA} + \widehat{PCA} \geqslant \widehat{PBC} + \widehat{PCB}.$$

Montrer que $AP \geqslant AI$, et qu'il y a égalité si et seulement si $P = I$.

Solution de l'exercice 16 On ajoute le "pôle Sud" S issu de A c'est-à-dire l'intersection de la bissectrice de l'angle $\widehat{BAC}$ avec le cercle circonscrit à ABC. On a



$$\widehat{PBA} + \widehat{PCA} + \widehat{PBC} + \widehat{PCB} = \widehat{ABC} + \widehat{ACB} = 2(90^\circ - \frac{\widehat{BAC}}{2}),$$

donc la condition de l'énoncé revient à $\widehat{PBC} + \widehat{PCB} \leqslant 90^\circ - \frac{\widehat{BAC}}{2}$ ou encore à

$$\widehat{BPC} \geqslant 90^\circ + \frac{\widehat{BAC}}{2} = \widehat{BIC}$$

On en déduit que P est dans la zone grise foncée qui est délimitée par le cercle passant par B, I et C à cause de **l'inégalité reliant les angles inscrits à un cercle à ceux internes au disque et à ceux externe au disque**. Or $AP \leqslant AI$ si et seulement si P est dans la zone grise claire délimitée par le cercle de centre A et de rayon AI. De plus, il est bien connu que le cercle passant par B, I et C a pour centre S. A, I et S sont alignés donc le cercle de centre A et celui de centre S sont tangants en I. Le seul point appartenant aux deux zones est le point I, ce qui conclut l'inégalité.

- Preuves analytiques -

Les méthodes utilisées dans cette partie font appel à l'analyse : fonctions convexes et multiplicateurs de Lagrange. Ce sont des outils puissants mais à utiliser en faisant très attention aux conditions d'utilisation des théorèmes.

Exercice 17 Montrer que si $0 \leqslant a, b, c \leqslant 1$ alors

$$\frac{a}{bc+1} + \frac{b}{ac+1} + \frac{c}{ab+1} \leqslant 2.$$

Solution de l'exercice 17 Le membre de gauche est deux fois dérivable en chaque variable de dérivées secondes positives. Donc la fonction est convexe en chaque variable. Or, le **maximum global d'une fonction convexe** définie sur un espace fermé borné est atteint en un point extrémal. Attention, ici nous savons seulement que la fonction est convexe en chaque variable (ce qui est strictement plus faible). Nous pouvons tout de même en déduire que le maximum est atteint au bord, et même, comme le domaine est un cube de côtés parallèles aux axes, le maximum est atteint en l'un des sommets. Ces derniers ont pour coordonnées, à l'ordre des coordonnées près, $(0,0,0), (0,0,1), (0,1,1)$ et $(1,1,1)$. Les valeurs en ces points sont respectivement $0, 1, 2$ et $3/2$, ce qui conclut.

Exercice 18 Soient a, b, c et d des réels strictement positifs. Montrer que

$$\sum_{\text{cyc}} \frac{a}{b+2c+3d} \geqslant \frac{2}{3}.$$

Solution de l'exercice 18 L'inégalité est homogène (de degré 0). On peut la déshomogénéiser sans perdre de généralité en posant $a+b+c+d=1$. La fonction $f(x) = 1/x$ est convexe sur $\mathbb{R}_+^*$. On peut appliquer l'inégalité de Jensen :

$$\begin{aligned} \sum_{\text{cyc}} a f(b+2c+3d) &\geqslant f\left(\sum_{\text{cyc}} a(b+2c+3d)\right) \\ \sum_{\text{cyc}} \frac{a}{b+2c+3d} &\geqslant \frac{1}{4\sum_{\text{sym}} ab} \end{aligned}$$

Or, d'après l'inégalité de Maclaurin :

$$\sqrt{\frac{\sum_{\text{sym}} ab}{\binom{4}{2}}} \leqslant \frac{a+b+c+d}{4} = \frac{1}{4},$$

ce qui permet de conclure.

Exercice 19 (Inégalité de la moyenne généralisée) Soient $x_1, \ldots, x_n, w_1, \ldots, w_n$ des réels strictement positifs tels que $w_1 + \ldots + w_n = 1$, et p un réel non nul. Soient :

$$\begin{aligned} N_p &= \left(\sum_{i=1}^n w_i x_i^p\right)^{1/p}, \\ N_0 &= \prod_{i=1}^n x_i^{w_i}, \\ N_{+\infty} &= \max(x_1, \ldots, x_n), \\ N_{-\infty} &= \min(x_1, \ldots, x_n). \end{aligned}$$

Montrer que si p, q appartiennent à $\mathbb{R}\cup\{-\infty;+\infty\}$ et vérifient $p > q$ alors $N_p \geqslant N_q$ avec égalité si et seulement si les x_i sont tous égaux.

Les cas à retenir de cette inégalité très générale sont $p, q \in \{+\infty; 2; 1; 0; -1; -\infty\}$ c'est-à-dire concernant respectivement **le maximum, la moyenne quadratique, la moyenne arithmétique, la moyenne géométrique, la moyenne harmonique et le minimum**.

Solution de l'exercice 19 Soient p et q dans $\mathbb{R} \cup \{-\infty; +\infty\}$ tels que $p > q$. On traite différents cas :

- si $p = +\infty$ ou $q = -\infty$ l'inégalité est triviale.
- si $p > 1$ et $q = 1$. La fonction $f(x) = x^p$ est strictement convexe sur $\mathbb{R}^+$ donc l'inégalité de Jensen donne $N_p \geqslant N_1$ avec égalité si et seulement si les x_i sont tous égaux.
- si $p, q > 0$, on se ramène au cas précédent avec le changement de variable $y_i = x_i^q$ et en élevant à la puissance q.
- si $p = 1, q = 0$, on passe au logarithme, qui est strictement convexe, et on obtient l'inégalité de Jensen.
- si $p > 0, q = 0$ on se ramène au cas précédents avec le changement de variable $y_i = x_i^p$ et en élevant à la puissance p.
- si $p \leqslant 0$ et $q < 0$ on se ramène aux cas précedent en posant $y_i = 1/x_i$ et en passant à l'inverse.
- si $p > 0$ et $q < 0$ on compare N_p et N_q à N_0.

Dans tout les cas, l'inégalité et le cas d'égalité sont vérifiés.

Il est à noter que $N_{+\infty}$, N_0 et $N_{-\infty}$ sont les limites de N_p lorsque p tend respectivement vers $+\infty$, 0 et $-\infty$. La démonstration dépasse le cadre de ce cours. Cette propriété nous permet d'éviter beaucoup de cas ci-dessus.

Exercice 20 (Inégalité des mauvais élèves plus générale) Soient $a_1, \ldots, a_n$ des réels positifs ou nuls et $x_1, \ldots, x_n$ et r des réels strictement positifs. Montrer que

$$\frac{a_1^{r+1}}{x_1^r} + \ldots + \frac{a_n^{r+1}}{x_n^r} \geqslant \frac{(a_1 + \ldots + a_n)^{r+1}}{(x_1 + \ldots + x_n)^r},$$

avec égalité lorsque les vecteurs $(a_1, \ldots, a_n)$ et $(x_1, \ldots, x_n)$ sont colinéaires.

Cette inégalité peut être prouvée en utilisant l'inégalité de Hölder. Nous allons ici utiliser la méthode **des multiplicateurs de Lagrange**.

Solution de l'exercice 20 Si tous les a_i sont nuls l'inégalité est triviale. Supposons maintenant qu'ils ne sont pas tous nuls. Travaillons par récurrence sur n. L'initialisation $n = 1$ est triviale. Supposons l'inégalité vraie au rang $n - 1$. Si l'un des a_i est nul, disons a_n, on obtient par hypothèse de récurrence

$$\frac{a_1^{r+1}}{x_1^r} + \ldots + \frac{a_n^{r+1}}{x_n^r} = \frac{a_1^{r+1}}{x_1^r} + \ldots + \frac{a_{n-1}^{r+1}}{x_{n-1}^r} \geqslant \frac{(a_1 + \ldots + a_{n-1})^{r+1}}{(x_1 + \ldots + x_{n-1})^r} > \frac{(a_1 + \ldots + a_n)^{r+1}}{(x_1 + \ldots + x_n)^r}.$$

Donc, dans ce cas, l'inégalité est stricte. Traitons maintenant le cas où les a_i sont tous non nuls. L'inégalité est homogène en les a_i et en les x_i. On peut donc ajouter les contraintes $a_1 + \cdots +$

$a_n = x_1 + \cdots + x_n = 1$. Lorsque les x_i sont fixés, en utilisant la méthode du multiplicateur de Lagrange avec les variables a_i, le minimum du membre de gauche est éventuellement atteint, hors du bord, seulement si $((r+1)\frac{a_1^r}{x_1^r}, \ldots, (r+1)\frac{a_n^r}{x_n^r})$ est proportionnel à $(1, \ldots, 1)$, c'est-à-dire seulement si $(a_1, \ldots, a_n)$ est proportionnel à $(x_1, \ldots, x_n)$. Dans ce cas on trouve bien

$$\frac{a_1^{r+1}}{x_1^r} + \ldots + \frac{a_n^{r+1}}{x_n^r} = \frac{(a_1 + \ldots + a_n)^{r+1}}{(x_1 + \ldots + x_n)^r} = 1.$$

Le cas du bord est déjà traité (c'est lorsque l'un des a_i vaut 0) et montre de plus que nous avons bien trouvé le minimum global du membre de gauche. L'inégalité et le cas d'égalité sont donc démontrés.

Exercice 21 (Inégalité de Karamata) Soit f une fonction convexe de $\mathbb{R}$ dans $\mathbb{R}$. Soient $x_1 \leqslant x_2 \leqslant \cdots \leqslant x_n$ et $y_1 \leqslant y_2 \leqslant \cdots \leqslant y_n$ tels que pour tout entier p entre 1 et n :

$$\begin{aligned} x_1 + \cdots + x_p &\leqslant y_1 + \cdots + y_p \text{ et} \\ x_1 + \cdots + x_n &= y_1 + \cdots + y_n. \end{aligned}$$

Montrer que

$$f(x_1) + \cdots + f(x_n) \geqslant f(y_1) + \cdots + f(y_n).$$

Solution de l'exercice 21 Cette inégalité s'appuie sur l'"**inégalité des pentes**" dans une fonction convexe f : si $x \leqslant y \leqslant z$ alors

$$\frac{f(y) - f(x)}{y - x} \leqslant \frac{f(z) - f(x)}{z - x} \leqslant \frac{f(z) - f(y)}{z - y}.$$

On pose $a_i = \frac{f(x_i) - f(y_i)}{x_i - y_i}$. Comme les x_i et les y_i sont par ordre croissant, les a_i le sont aussi. On a

$$f(x_1) - f(y_1) + \cdots + f(x_n) - f(y_n) = a_1(x_1 - y_1) + \cdots + a_n(x_n - y_n).$$

Maintenant on note $U_i = x_1 + \cdots + x_i - y_1 - \cdots - y_i$ et $U_0 = 0$. On a

$$\begin{aligned} f(x_1) - f(y_1) + \cdots + f(x_n) - f(y_n) &= a_1(U_1 - U_0) + \cdots + a_n(U_n - U_{n-1}) \\ &= -a_1 U_0 + (U_1(a_1 - a_2) + \cdots + U_{n-1}(a_{n-1} - a_n)) + U_n a_n. \end{aligned}$$

Cette série d'égalité s'appelle la transformation d'Abel. Or, $U_0 = U_n = 0$, les $a_i - a_{i+1}$ sont négatifs et les U_i sont négatifs par hypothèse. Donc la somme ci-dessus est positive ce qui permet de conclure.

VIII. Mardi 25 matin : Test de fin de parcours

Contenu de cette partie

1 Groupe A

1 Enoncé

Exercice 1
Montrer que la fraction

$$\frac{21n+4}{14n+3}$$

est irréductible pour tout entier n.

Exercice 2
Soit ABC un triangle, I le centre de son cercle inscrit et O celui de son cercle circonscrit. On définit respectivement A', B' et C' comme les centres des cercles circonscrits aux triangles IBC, ICA et IAB. Montrer que O est le centre du cercle circonscrit du triangle $A'B'C'$.

Exercice 3
Trouver tous les entiers positifs x et y tels que

$$x^2 - y! = 2015$$

Exercice 4
Soient d et d' deux droites parallèles. Un cercle Γ est tangent à d en A et intersecte d' en C et D. La tangente à Γ en D recoupe d en B. Enfin, soient E l'intersection de (BC) avec Γ et I de (DE) avec d. Montrer que I est le milieu de $[AB]$.

2 Solution

Solution de l'exercice 1

Soit $d \in \mathbb{N}^*$ un diviseur commun de $21n+4$ et de $14n+3$. On a :

$$d \mid 2 \times (21n+4) - 3 \times (14n+3) = -1,$$

donc $d = 1$.

La fraction $\frac{21n+4}{14n+3}$ est donc bien irréductible.

Solution de l'exercice 2

Une première possibilité est de reconnaître en A', B', C' les pôles sud du triangle, qui sont par définition sur le cercle.

On peut aussi procéder par chasse aux angles :

$$\widehat{BIC} = 90^\circ + \frac{1}{2}\widehat{BAC},$$

d'où :

$$\widehat{BA'C} = 360^\circ - 2\widehat{BIC} = 180^\circ - \widehat{BAC},$$

d'où A, B, C, A' cocycliques.

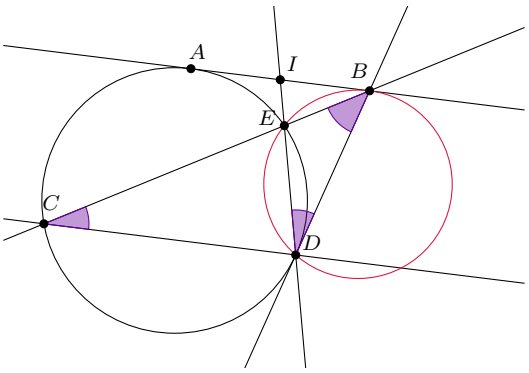
On montre de même que B' et C' sont sur le cercle circonscrit à ABC, qui est par définition de centre O.

Solution de l'exercice 3

On regarde modulo 3 : si $y \geq 3$, $y! \equiv 0\ [3]$. De plus, un carré est toujours congru à 0 ou 1 modulo 3. Or 2015 est congru à 2 modulo 3, ce qui nous amène à une contradiction !

Donc $y = 1$ ou $y = 2$, et on vérifie dans les deux cas que $2015 + y!$ n'est pas un carré (il est strictement compris entre 44^2 et 45^2).

Solution de l'exercice 4



On montre tout d'abord que le cercle circonscrit à BDE est tangent à (d) en B : $\widehat{EBA} = \widehat{BCD}$ car ce sont des angles alternes-internes, et $\widehat{BCD} = \widehat{EDB}$ car (BD) est tangente au cercle circonscrit à ACD en D.

Donc I est le point d'intersection d'une tangente commune aux deux cercles et de leur axe radical. Donc $IA^2 = IB^2$, d'où I milieu de $[AB]$.

2 Groupe B

1 Enoncé

Exercice 1
Trouver tous les nombres premiers p et r tels que

$$p^2 + p = 15r$$

Exercice 2
Soient A, B, C et D quatre points cocycliques. On note respectivement A' et C' les projetés orthogonaux de A et C sur (BD), et B' et D' les projetés orthogonaux de B et D sur (AC). Montrer que A', B', C' et D' sont également cocycliques.

Exercice 3
Soit ABC un triangle acutangle. On note respectivement D, E, F les pieds des hauteurs sur les côtés $[BC], [CA], [AB]$. Soit P un point d'intersection de (EF) avec le cercle circonscrit à ABC. Soit Q le point d'intersection des droites (BP) et (DF). Montrer que $AP = AQ$.

Exercice 4
Trouver tous les nombres premiers p, q et r tels que

$$3p^4 - 5q^4 - 4r^2 = 26$$

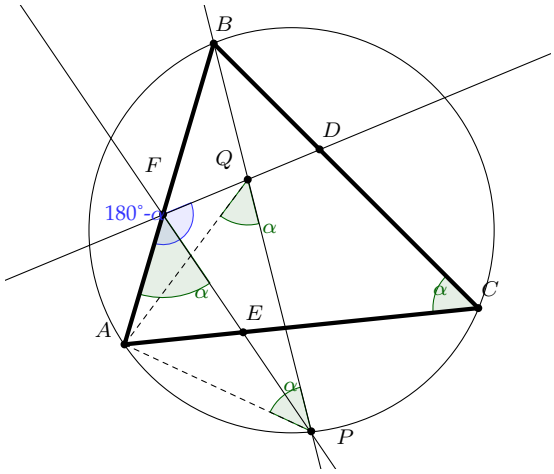
2 Solution

Solution de l'exercice 1 $p^2 + p = 15r$, or $p^2 + p = p(p+1)$ est toujours pair, donc $15r$ l'est aussi, donc $r = 2$. On a donc $p^2 + p = 30$, donc $p|30$, donc p vaut 2,3 ou 5. Finalement, seul 5 convient, donc l'unique solution est $r = 2$ et $p = 5$.

Solution de l'exercice 2 Puisque $\widehat{AD'D} = \widehat{AA'D} = 90$, le théorème de l'angle inscrit permet d'affirmer que A, D, A' et D' sont cocycliques. On obtient de la même façon que B, C, B' et C' sont cocycliques.

On en déduit alors que $(DA', DA) = (D'A', D'A)$ car A, D, A' et D' sont cocycliques et que $(CB, CB') = (C'B, C'B')$ car B, C, B' et C' sont cocycliques. Or, A, B, C et D étant cocycliques, nous savons que $(DB, DA) = (CB, CA)$ et l'alignement des points D, A' et B d'une part et de C, B' et A d'autre part fait que cette dernière égalité se réécrit $(DA', DA) = (CB, CB')$. Finalement, on en conclut que $(D'A', D'A) = (C'B, C'B')$ soit $(D'A', D'B') = (C'A', C'B')$, ce qui démontre que A', B', C' et D' sont cocycliques.

Solution de l'exercice 3



Pour montrer que $AP = AQ$, on va plutôt montrer $\widehat{AQP} = \widehat{APQ}$

Posons $\widehat{APB} = \alpha$. Par cocyclicité des points A, B, C, P, on a $\widehat{BCA} = \alpha$. Comme (AD) et (CF) sont des hauteurs, les points A, C, D, F sont cocycliques et donc $\widehat{AFD} = 180° - \alpha$. Donc $\widehat{AFD} + \widehat{APQ} = 180°$, ce qui implique que les points A, P, Q, F sont cocycliques.

On a alors $\widehat{AFE} = 180° - \widehat{EFB} = \alpha$ (car E, F, B et C sont cocycliques dans cet ordre). A, P, Q et F sont cocycliques, donc $\widehat{AQP} = \widehat{AFP} = \alpha$ donc AQP est isocèle en A, d'où $AP = AQ$.

<u>*Solution de l'exercice 4*</u> L'idée majeure de la preuve est d'utiliser les modulos pour en déduire que pour un entier n connu, n divise p, q ou r, et que donc $n = p$, q ou r.

L'équation modulo 3 est $q^4 + 2r^2 \equiv 2 \mod 3$. Or, on a :
— si $n \equiv 0 \mod 3$ alors $n^2 \equiv 0 \mod 3$
— si $n \equiv 1 \mod 3$ alors $n^2 \equiv 1 \mod 3$
— si $n \equiv 2 \mod 3$ alors $n^2 \equiv 1 \mod 3$

Supposons que q et r ne soient pas divisibles par 3. Alors $q^4 + 2r^2 \equiv 1^2 + 2x1 \mod 3$, c'est-à-dire $q^4 + 2r^2 \equiv 0 \mod 3$, ce qui est une contradiction. Donc q ou r est divisible par 3, et comme q et r sont premiers, alors q ou r vaut 3. Si $r = 3$, alors $q^4 \equiv 2 \mod 3$, ou $(q^2)^2 \equiv 2 \mod 3$, ce qui est impossible. Donc $q = 3$.

L'équation modulo 5 est $3p^4 + r^2 \equiv 1 \mod 5$. Or, on a :
— si $n \equiv 0 \mod 5$ alors $n^4 \equiv 0 \mod 5$
— si $n \equiv 1 \mod 5$ alors $n^4 \equiv 1 \mod 5$
— si $n \equiv 2 \mod 5$ alors $n^4 \equiv 1 \mod 5$
— si $n \equiv 3 \mod 5$ alors $n^4 \equiv 1 \mod 5$
— si $n \equiv 4 \mod 5$ alors $n^4 \equiv 1 \mod 5$

On remarque que $n^4 \equiv 1 \mod 5$ si n n'est pas divisible par 5. Supposons que p ne soit pas divisible par 5. Alors $3 + r^2 \equiv 1 \mod 5$, c'est-à-dire $r^2 \equiv 3 \mod 5$. Or, on a :
— si $n \equiv 0 \mod 5$ alors $n^2 \equiv 0 \mod 5$
— si $n \equiv 1 \mod 5$ alors $n^2 \equiv 1 \mod 5$
— si $n \equiv 2 \mod 5$ alors $n^2 \equiv 4 \mod 5$
— si $n \equiv 3 \mod 5$ alors $n^2 \equiv 4 \mod 5$
— si $n \equiv 4 \mod 5$ alors $n^2 \equiv 1 \mod 5$

Il est donc impossible que $r^2 \equiv 3 \mod 5$. Donc p est divisible par 5, comme p est premier, alors $p = 5$. On reporte $p = 5$ et $q = 3$ dans l'équation de départ, ce qui donne après un rapide

calcul $r = 19$, qui est bien premier. La seule solution à cette équation est $p = 5$, $q = 3$ et $r = 19$.

3 Groupe C

1 Enoncé

Exercice 1

Trouver tous les entiers naturels m, n, k tels que

$$3^n + 4^m = 5^k.$$

Exercice 2

Soient $x_1, x_2, \ldots, x_n$ et $y_1, y_2, \ldots, y_n$ des réels strictement positifs, et $z_1, z_2, \ldots, z_n$ des réels tels que pour tout $i \in \{1, \ldots, n\}$, $x_i y_i - z_i^2 > 0$. Montrer que :

$$\left(\left(\sum_{i=1}^{n} x_i\right)\left(\sum_{i=1}^{n} y_i\right) - \left(\sum_{i=1}^{n} z_i\right)^2\right) \times \sum_{i=1}^{n} \frac{1}{x_i y_i - z_i^2} \geq n^3.$$

Exercice 3

Trouver toutes les fonctions $f : \mathbb{R} \to \mathbb{R}$ telles que pour tous réels x, y, on ait :

$$f(f(x) + y) = 2x + f(f(y) - x).$$

Exercice 4

Trouver le plus grand diviseur commun à tous les nombres de la forme $a^{25} - a$ avec $a \in \mathbb{Z}$.

2 Solution

Exercice 1

Il est clair que $k > 0$.
• Si $n = 0$, alors $1 + 4^m = 5^k$. Si $k = 1$, $m = 1$ est la seule solution. Sinon, $1 + 1^m \equiv (-1)^k \pmod 3$. Donc k est impair, $k = 2k' + 1$ avec $k' \geq 1$. Donc $4^m - 4 = 5(25^{k'} - 1)$. On a $m > 0$ donc 8 ne divise pas $4^m - 4$ or $25^{k'} - 1$ est divisible par $25 - 1 = 3 \times 8$. Donc pas de solution.
• Si $m = 0$, $3^n + 1 = 5^k$, soit $3^n = 5^k - 1$. Donc 3^n est multiple de $5 - 1 = 4$, impossible.
• Si $m, n, k > 0$, on a $(-1)^n \equiv 1 \pmod 4$ donc $n = 2n'$, $n' \in \mathbb{N}^*$. Et $1 \equiv (-1)^k \pmod 3$ donc $k = 2k'$, $k' \in \mathbb{N}^*$. Donc

$$4^m = (5^{k'})^2 - (3^{n'})^2 = (5^{k'} + 3^{n'})(5^{k'} - 3^{n'}).$$

Donc $5^{k'} + 3^{n'}$ et $5^{k'} - 3^{n'}$ sont des puissances de 2. Et $5^{k'} + 3^{n'} > 5^{k'} - 3^{n'} > 1$ d'après le paragraphe précédent. Si $5^{k'} - 3^{n'} \geq 4$, les deux facteurs sont multiples de 4 donc $2 \times 3^{n'}$ est

multiple de 4, impossible. Donc $5^{k'} - 3^{n'} = 2$, et $3^{n'} = 2^{2m-2} - 1 = (2^{m-1}+1)(2^{m-1}-1)$. Donc $(2^{m-1}+1)$ et $(2^{m-1}-1)$ sont des puissances de 3, or leur différence vaut 2. La seule solution est alors $2^{m-1}+1 = 3$ donc $m = 2$ et $n' = 1$ donc $n = 2$, on a alors $k = 2$, on retrouve le triplet pythagoricien bien connu.
Conclusion : les seules solutions sont $k = m = 1$ et $n = 0$, et $k = m = n = 2$.

Exercice 2

Soit R le membre de gauche de l'équation. D'après Cauchy-Schwarz,

$$\left(\sum_{i=1}^{n} x_i\right)\left(\sum_{i=1}^{n} y_i\right) \geq \left(\sum_{i=1}^{n} \sqrt{x_i y_i}\right)^2,$$

donc

$$R \geq \left(\sum_{i=1}^{n} \sqrt{x_i y_i} - z_i\right)\left(\sum_{i=1}^{n} \sqrt{x_i y_i} + z_i\right) \sum_{i=1}^{n} \frac{1}{x_i y_i - z_i^2}.$$

Posons $a_i = \sqrt{x_i y_i} - z_i$ et $b_i = \sqrt{x_i y_i} + z_i$, on a $a_i > 0$ et $b_i > 0$, et il suffit de montrer que $\sum a_i \sum b_i \sum \frac{1}{a_i b_i} \sum 1 \geq n^4$. En appliquant Cauchy-Schwarz, $\sum a_i \sum b_i \geq \left(\sum \sqrt{a_i b_i}\right)^2$ et $\sum \frac{1}{a_i b_i} \sum 1 \geq \left(\sum \frac{1}{\sqrt{a_i b_i}}\right)^2$. Il suffit donc de montrer que

$$\left(\sum \sqrt{a_i b_i}\right)\left(\sum \frac{1}{\sqrt{a_i b_i}}\right) \geq n^2.$$

Une fois n'est pas coutume, Cauchy-Schwarz fonctionne, mais l'inégalité du réordonnement aussi.

Exercice 3

En posant $y = -f(x)$, on a $f(f(y) - x) = f(0) - 2x$ et on voit que f est surjective. Montrons l'injectivité : soit $a, b \in \mathbb{R}$ tels que $f(a) = f(b)$, on a $f(f(a) + y) = f(f(b) + y)$ donc $2a + f(f(y) - a) = 2b + f(f(y) - b)$. Par surjectivité, on peut prendre y tel que $f(y) = a + b$, donc $2a + f(b) = 2b + f(a)$ donc $2a = 2b$ et f est injective.
En faisant $x = 0$ dans l'équation initiale, $f(f(0) + y) = f(f(y))$ et l'injectivité donne $f(y) = y + f(0)$. Réciproquement, on vérifie que les fonctions $x \mapsto x + c$, avec $c \in \mathbb{R}$, conviennent.

Exercice 4

Soit d ce pgcd. On a $2^{25} - 2 = 2(2^{12} - 1)(2^{12} + 1) = 2(2^6 - 1)(2^6 + 1)(2^4 + 1)(2^8 - 2^4 + 1)$, donc $2^{25} - 2 = 2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 241$. D'après le petit théorème de Fermat, si p est un nombre premier tel que $p - 1$ divise 24, p divisera $a^{25} - a$ pour tout entier relatif a, car si $pgcd(a, p) = 1$ $a^{25} \equiv a \times a^{k(p-1)} \equiv a \times 1^k \equiv a \pmod{p}$, et sinon p divise a. Et $2, 3, 5, 7, 13$ vérifient cette condition, donc $d = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot d'$ avec $d' | 3 \cdot 17 \cdot 241$. Prendre $a = 3$ montrent que d n'est pas divisible par 9, donc $d' | 17 \cdot 241$: il ne reste plus qu'à tester 17 et 233 (qui est premier, si si).
On a $3^{25} - 3 = 3(3^{12} - 1)(3^{12} + 1) = 3(3^6 - 1)(3^6 + 1)(3^4 + 1)(3^8 - 3^4 + 1) = 3 \cdot 728 \cdot 730 \cdot 82 \cdot 6481$.
On vérifie qu'aucun de ces facteurs n'est divisible par 17 ou 241.
Conclusion : $d = 2730$.

4 Groupe D

1 Enoncé

Exercice 1

Soient x, y, z des nombres réels strictement positifs tels que

$$\sum_{\text{cyc}} x^2y^2 = 6xyz.$$

Montrer que

$$\sum_{\text{cyc}} \sqrt{\frac{x}{x+yz}} \geqslant \sqrt{3}.$$

Exercice 2

Trouver toutes les fonctions f de $\mathbb{R}$ dans $\mathbb{R}$ telles que, pour tous réels x et y :

$$f(x^2 + y + f(y)) = 2y + f(x)^2$$

Exercice 3

Dans cet exercice, on considère qu'un point qui est sur un côté d'un triangle **n'est pas** à l'intérieur du triangle.

Soit $n \geq 3$. Trouver le plus petit entier k vérifiant la propriété suivante :

Pour tout ensemble S de n points du plan, trois quelconques jamais alignés, il existe un ensemble T de k points tel que pour tous A, B et C dans S deux à deux distincts, il y a au moins un point de T à l'intérieur du triangle ABC.

2 Solution

Exercice 1

Il y a beaucoup de manières de résoudre cette inégalité. Une méthode consiste à utiliser l'inégalité de Jensen. La condition nous donne

$$\sum_{\text{cyc}} \frac{xy}{z} = 6.$$

On obtient alors, par convexité de la fonction $\left(x \mapsto \frac{1}{1+\sqrt{x}}\right)$,

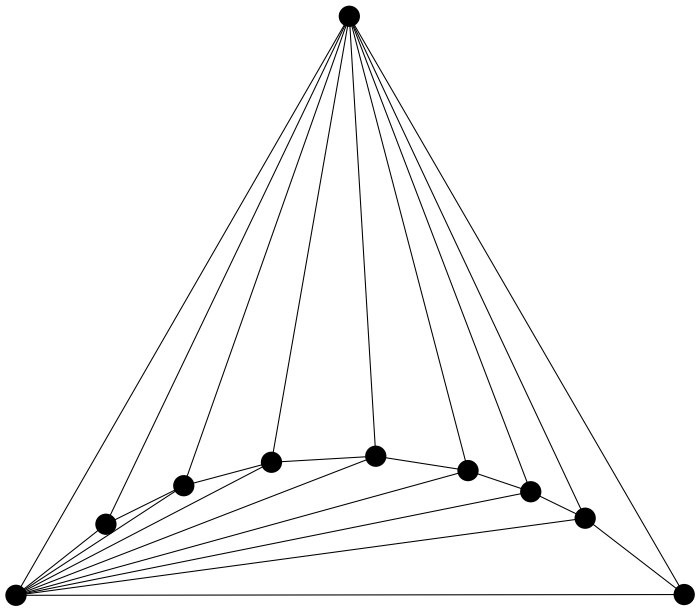
$$\begin{aligned}
\sum_{\text{cyc}} \sqrt{\frac{x}{x+yz}} &= \sum_{\text{cyc}} \frac{1}{\sqrt{1+\frac{yz}{x}}} \\
&\underset{\text{(Jensen)}}{\geqslant} 3\frac{1}{\sqrt{1+\frac{1}{3}\sum_{\text{cyc}} \frac{yz}{x}}} \\
&\geqslant \sqrt{3}.
\end{aligned}$$

Exercice 2

f est clairement surjective. On essaie d'abord $(0,0),(f(0),0)$ et $(0,f(0))$ pour trouver $f(0)=0$ ou $1<f(0)<2$. Dans le second cas, on construit une suite $x_n=x_{n-1}^2+1$ qui tend vers $+\infty$ et telle que $f(x_n)=0$. En prenant $y>0$ et x tel que $x^2+y+f(y)=x_n$ pour un certain $n\in\mathbb{N}^*$, on obtient une contradiction. Donc $f(0)=0$.
Et, $f(x^2)=f(x)^2$ $(*)$. Cela sert à montrer que seul $-\frac{f(0)^2}{2}=0$ a pour image 0. On montrer encore que f est injective (si $a=b$, tester les couples $(a,-\frac{f(a)^2}{2})$ et $(b,,-\frac{f(a)^2}{2})$, qui donne déjà $a^2=b^2$). Puis que f est positive sur les positifs, et enfin qu'elle vérifie l'équation de Cauchy sur les réels positifs, les deux derniers éléments montrant qu'elle est linéaire sur $\mathbb{R}^+$ puis sur $\mathbb{R}$ par injectivité et $(*)$.

Exercice 3

On va montrer que la réponse est $2n-5$. La figure suivante (pour $n=10$) montre qu'il est possible de trouver S tel que les points de S forment $2n-5$ triangles d'intérieur disjoints (il y a $n-2$ triangles en haut et $n-3$ en bas). Il nous faut donc au moins $2n-5$ points.



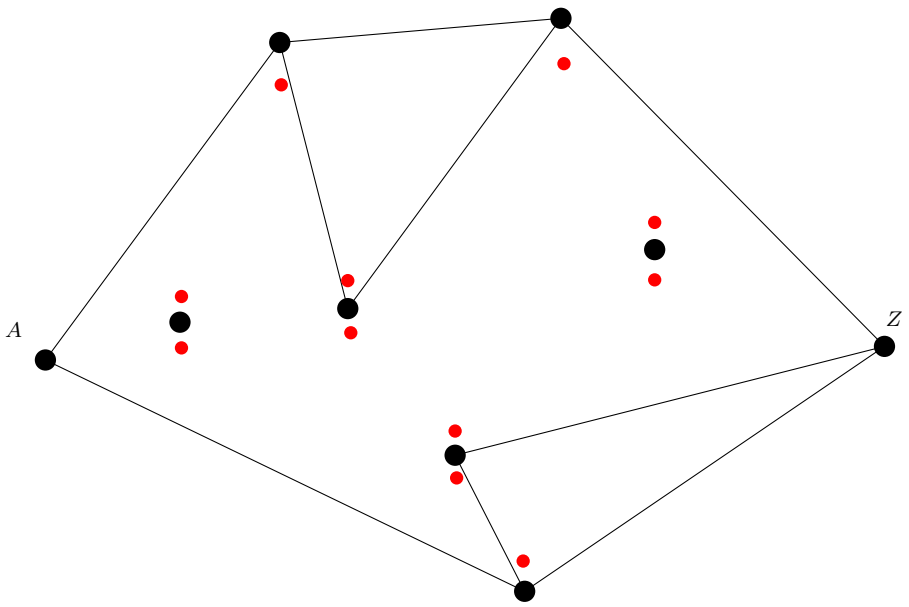
Il reste à montrer qu'on peut toujours trouver T de cardinal $2n-5$ vérifiant la condition voulue. Pour cela, on choisit T comme suit : notons A le point le plus à gauche de S (qui est unique quitte à "tourner" la figure) et Z le plus à droite. On on note ∂S le bord de l'enveloppe convexe de S.

— Si $X\in S$ n'est pas sur ∂S, on prend dans T un point X' "juste au-dessus" de X et un point X'' "juste en-dessous", où "juste au-dessus" signifie assez proche pour que le segment $[XX']$ n'intersecte aucun segment entre deux points de S.

— Si $X \in \partial S$ est sur l'arc de ∂S au-dessus de A et Z, on prend dans T un point "juste en-dessous" de X.
— Si $X \in \partial S$ est sur l'arc de ∂S en-dessous de A et Z, on prend dans T un point "juste au-dessus" de X.

On a donc pris 2 points par éléments de S, moins 2 points pour A, 2 points pour Z et encore un point par élément de ∂S différent de A et Z. Comme ∂S contient au moins un point différent de A et Z on a $|T| \leq 2n - 5$.

Enfin, soient A, B et C dans S. On peut supposer qu'ils sont ordonnés par abscisse croissante. Il y a alors à l'intérieur du triangle ABC un petit segment issu de B partant vers le haut ou vers le bas. Si de plus B est sur l'arc haut de ∂S, ce segment part forcément vers le bas, ce qui assure qu'on ait sur ce segment un point de T. La construction est plus claire sur la figure suivante (les points de T sont en rouge) :



IX. Dernière période

Contenu de cette partie

1 Groupe A

1 mercredi 26 matin : Félix Lequen

Ce texte n'a pas encore été intégré.

2 mercredi 26 après-midi : Cécile Gachet

Ce cours présentait les bases de la théorie des graphes. Pour plus de détails, il est conseillé de se référer à l'excellent polycopié de Pierre Bornzstein à ce sujet.

2 Groupe B

1 mercredi 26 matin : groupes, Eva Philippe

Quelques groupes

L'intérêt de cette modeste introduction aux groupes était surtout de présenter des exemples (ensemble de nombres, transformations géométriques du plan ou laissant invariante une certaine figure, permutations) et comprendre ce que cela signifie pour deux ensembles d'avoir la même structure de groupe.

Il n'y a pas de plan très construit car je m'appuie sur ce qui a été fait à l'oral. Je vous encourage très vivement à approfondir vos recherches par vous-mêmes si le sujet vous intéresse.

Définition 175. Soit G un ensemble et $\star : G \times G \to G$ une loi de composition interne sur G (associe à deux éléments de G un autre élément de G).

$(G, \star)$ est un groupe si :

— pour tous $x, y, z \in G$, $(x \star y) \star z = x \star (y \star z)$ (on dit que la loi $\star$ est associative)

— il existe $e \in G$, nommé élément neutre, tel que pour tout $x \in G$, $e \star x = x \star e = x$

— pour tout $x \in G$, il existe $y \in G$, appelé inverse de x, tel que $x \star y = y \star x = e$

Quelques propriétés très simples :

— L'élément neutre est unique.

— Tout élément de G possède un unique inverse pour la loi $\star$.

Démonstration.

— Soient e_1 et e_2 deux éléments neutres de G. On a par définition de e_1, $e_1 \star e_2 = e_2$ et par définition de e_2, $e_1 \star e_2 = e_1$, d'où $e_1 = e_2$.

— Soit $x \in G$ et $y_1, y_2 \in G$ tels que $x \star y_1 = y_1 \star x = e$ et $x \star y_2 = y_2 \star x = e$. Alors $(y_1 \star x) \star y_2 = y_2$ et $y_1 \star (x \star y_2) = y_1$, d'où $y_1 = y_2$.

□

Des exemples de groupes :

— $(\mathbb{Z}, +)$

— $(\mathbb{R}, +)$

— $(\mathbb{R}^\star, \times)$

— $(\mathbb{Z}/n\mathbb{Z}, +)$

— permutations du Rubik's cube avec la loi de composition

— homothéties de centre commun

— isométries (transformations du plan qui conservent les distances, aussi appelées similitudes)

...

Des exemples de non-groupes :

— $(\mathbb{N}, +)$ (l'opposé d'un entier naturel n'est pas un entier naturel)

— $(\mathbb{R}, \times)$ (0 n'a pas d'inverse)

...

Proposition 176. Certains des groupes cités ci-dessus (comme $(\mathbb{Z}, +)$, $(\mathbb{R}^\star, \times)$, ...) sont dits commutatifs (on dit aussi abéliens) car ils possèdent la propriété suivante :

pour tous $x, y \in G$, $x \star y = y \star x$.

Attention, ce n'est en général pas le cas, en particulier pour les transformations géométriques ou $\mathfrak{S}_n$ pour $n \geq 3$.

Définition 177. $(H, \star)$ est un sous-groupe de $(G, \star)$ si $H \subset G$ et H est un groupe.

Pour vérifier qu'un sous-ensemble H de G est un sous-groupe, il suffit de vérifier que H est non vide, la loi est interne et tout inverse d'un élément de H est également dans H (ces deux dernières conditions se résument en : pour tous $x, y \in H$, $x \star y^{-1} \in H$).

Par exemple, l'ensemble des rotations et des translations est un sous-groupe des isométries du plan. En revanche, l'ensemble des symétries axiales n'en est pas un car la composée de deux symétries axiales est une rotation et non une symétrie axiale.

Définition 178. Un groupe $(G, \star)$ est dit *fini* si l'ensemble G possède un nombre fini d'éléments. On appelle *ordre* du groupe G ce nombre d'éléments (qui est aussi le cardinal de l'ensemble G).

Le groupe symétrique forme l'un des meilleurs exemples de groupe fini.

Permutations

Rappelons quelques notions avant de parler de permutations.

Définition 179. Soient E, F deux ensembles et $f : E \to F$ une application.

(i) On dit que f est *injective* si pour tous $x, y \in E$ avec $x \neq y$, $f(x) \neq f(y)$, ce qui revient à dire que les éléments de F ont au plus un antécédent par f

(ii) On dit que f est *surjective* si pour tout $y \in F$, il existe $x \in E$ tel que $f(x) = y$ (tout élément de F a au moins un antécédent par f.

(iii) On dit que f est *bijective* (ou est une *bijection*) si elle est injective et surjective, i.e tout élément de F a exactement un antécédent par f. On peut dans ce cas construire la fonction $f^{-1} : H \to F$ qui associe à tout élément de H son antécédent par f et vérifie $f \circ f^{-1} = f^{-1} \circ f = Id$.

L'ensemble des permutations de l'ensemble des entiers de 1 à n forme un groupe d'ordre $n!$, noté $\mathfrak{S}_n$ (groupe symétrique d'ordre n).

Pour plus de détails je vous renvoie vers la conférence de Joseph Najnudel que vous trouverez un peu plus loin dans ce poly.

Tables de Cayley

Pour visualiser le résultats de la loi d'un groupe fini G, on peut dessiner ce qu'on appelle une table de Cayley et qui fonctionne exactement sur le même principe que les tables de multiplication ou d'addition habituelles : on écrit en en-tête des lignes et des colonnes tous les éléments $g_1, g_2, \cdots$ de G et dans la case à l'intersection de la ligne i et de la colonne j on écrit le résultat du produit $g_i \star g_j$ (attention, l'ordre est important pour un groupe non commutatif). Comme on a un groupe, chaque élément de G doit apparaître exactement une fois dans chaque ligne et dans chaque colonne (un peu comme un sudoku).

En exemple, essayez d'établir la table de Cayley d'un groupe quelconque d'ordre 3. Vous constaterez qu'il n'y en a qu'une seule possible (sans compter les différents noms qu'on peut donner à nos éléments bien sûr).

Deux groupes qui ont les mêmes tables de Cayley sont dits isomorphes. Plus précisément, un morphisme de groupes entre $(G, \star)$ et $(H, \circ)$ est une application $\phi : G \to H$ telle que :
pour tous $x, y \in G$, $\phi(x \star y) = \phi(x) \circ \phi(y)$
(en gros les opérations sont bien conservées).
Si ce morphisme est bijectif, on l'appelle un *isomorphisme*.

Un exemple de morphisme non bijectif est la signature, qui va de $\mathfrak{S}_n$ dans $-1, 1$ (je vous renvoie encore à la conférence de Joseph, vous comprendrez en plus pourquoi on ne peut

pas résoudre un jeu de Taquin truqué) ou le morphisme trivial qui envoie tout élément d'un groupe sur l'élément neutre (bon, celui là est franchement sans intérêt).

On peut également montrer que $\mathfrak{S}_3$ est isomorphe à l'ensemble des transformations qui laissent invariant un triangle équilatéral (groupe constitué de l'identité, les trois symétries axiales selon les médianes, les rotations de $\frac{2\pi}{3}$ et $\frac{4\pi}{3}$). En effet, si on numérote les sommets de notre triangle, une transformation correspond effectivement à une permutation des sommets.

Deux groupes de même ordre ne sont pas nécessairement isomorphes loin de là. Par exemple $(\mathbb{Z}/4\mathbb{Z}, +)$ n'est pas isomorphe au groupe des transformations laissant invariant un rectangle (aussi appelé groupe de Klein ou V_4 et qui est en revanche isomorphe à $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$).

Pour s'en convaincre, il suffit de s'apercevoir que toutes les symétries du rectangle sont leur propre inverse mais ce n'est pas le cas de tous les éléments de $\mathbb{Z}/2\mathbb{Z}$ puisque $1+1 = 2 \neq 0 \mod 4$.

2 mercredi 26 après-midi : Joon Kwon

Ce cours porte sur la théorie des graphes reprend celui des groupes A et B qu'on peut trouver dans le polycopié du stage de 2013.

3 Groupe C

1 mercredi 26 matin : Matthieu Piquerez

- Introduction à l'axiome du choix : entre évidences et paradoxes -

Dans tout ce TD, on supposera l'axiome du choix.

Dans l'hôtel de Hilbert, il y a une infinité de chambres numérotées 0, 1, …. L'hôtel est rempli. Un nouveau client arrive. Hilbert décide alors de décaler le locataire de la chambre 0 dans la chambre 1, celui de la chambre 1 dans la chambre 2, etc. Le nouveau client peut donc aller dans la chambre 0. Mais un bus infini arrive. Hilbert a une idée, il met le locataire de la chambre n dans la chambre $2n$ et le $n^{\text{ème}}$ arrivant dans la chambre $2n-1$. Mais il existe des bus trop gros où les arrivants ne pourront pas rentrer dans l'hôtel.

Définition 180. Une application $f : E \longrightarrow F$ est dite
- *injective* si deux éléments distincts de E ont des images distinctes par f (i.e. f "sépare" les éléments de E)
- *surjective* si tout élément de F a un antécédent par f (i.e. f "recouvre" F tout entier)
- *bijective* si elle est injective et surjective (i.e. f "couple" les éléments de E avec ceux de F).

Définition 181. Dans ce cours, nous dirons qu'un ensemble A est dénombrable s'il existe une injection de A dans $\mathbb{N}$.

Exercice 1 Montrer que $\mathbb{Z}$, $\mathbb{Q}$ et $\mathbb{Q}[X]$, l'ensemble des polynômes à coefficients rationnels, sont dénombrables mais pas $\mathbb{R}$.

Indication : Pour le cas de $\mathbb{R}$, on pourra supposer par l'absurde que l'on a énuméré les nombres réels par $u_0, u_1, \ldots$ et considérer la $i^{\text{ème}}$ décimale de u_i.

Exercice 2 (Cantor-Bernstein) Soient E et F deux ensembles tels qu'il existe une injection de E dans F et une injection de F dans E. Montrer qu'il existe une bijection entre E et F.

Exercice 3 (Lemme de König) Montrer que tout arbre infini à branchement fini a une branche infinie.

Exercice 4 (Théorie de Ramsey infinie) Soit G un graphe complet de taille infinie. Montrer que si l'on colorie les arêtes de G avec un nombre fini de couleurs, alors G contient un sous-graphe infini monochrome.

Indication : L'idée est de construire une suite de sommets distincts $(u_n)_{n\in N}$ et une suite de couleurs (où une couleur peut apparaître plusieurs fois) $(c_n)_{n\in N}$ possédant la propriété suivante : si $p > q$ alors l'arête entre u_p et u_q est de couleur c_q.

En suivant la même idée de démonstration mais en prenant des ensembles et suites finis suffisamment grands au lieu d'infinis, on peut démontrer la théorie de Ramsey finie : pour tous k et c des entiers strictement positifs, il existe n entiers positifs tels que pour tout graphe complet de taille n dont les arêtes sont coloriées avec c couleurs différentes, il existe un sous-graphe complet monochrome de taille k.

Sans le savoir, pour résoudre les exercices précédents, nous avons utilisé l'axiome du choix. Celui-ci affirme que l'on peut faire une infinité de choix arbitraires simultanément. Soient I un ensemble d'indices, souvent très gros, et $(E_i)_{i\in I}$ une famille d'ensembles non vides. Selon l'axiome du choix, on peut choisir une famille $(x_i)_{i\in I}$ d'éléments telle que $x_i \in E_i$ pour tout i. Remarquez que ci-dessus nous avons fait une infinité de choix consécutifs, et non simultanés. A-t-on le droit ?

Exercice 5 Montrer que "axiome du choix simultané" implique "axiome du choix consécutif".

Cet axiome, c'est-à-dire une propriété que l'on accepte telle quelle et qui est à la base de toute démonstration, n'apparaît pas dans l'axiomatique de base couramment utilisée. Ainsi, si l'on ne l'ajoute pas, les deux exercices précédents, bien qu'intuitifs, ne sont plus nécéssairement vrais. Pourquoi les mathématiciens ne l'ajoutent-t-ils pas toujours à l'axiomatique ? Parce que cet axiome implique l'existence d'objets non explicites et parfois paradoxaux pour le sens commun, comme le paradoxe de Banach-Tarski que nous verrons ci-dessous.

Pour ce familiariser avec l'axiome du choix, commençons par un exercice typique.

Exercice 6 Montrer qu'il existe un sous-ensemble A de $\mathbb{R}^*$ tel que :

$$\forall x \in \mathbb{R}^*, \exists!(\lambda, a) \in \mathbb{Q} \times A, \quad x = \lambda a.$$

On appelle un tel ensemble A un ensemble de représentants du quotient $\mathbb{R}^*/\mathbb{Q}$.

Maintenant voyons quelques énigmes paradoxales.

Exercice 7 Un matheux a réussi à enchaîner une infinité dénombrable de Lo Jac' le pirate sur une galère. Il leur a mis à chacun un chapeau sur la tête. Chaque chapeau est d'une certaine couleur parmi 10 couleurs différentes. La chaîne est faite telle que les Lo Jac' sont alignés mais ne peuvent pas tourner la tête. Ainsi, le premier Lo Jac' voit tous les chapeaux sauf le sien, le deuxième les voit tous sauf celui du premier ni le sien, etc. Chaque Lo Jac' à son tour va chuchoter un nom de couleur dans l'oreille du matheux. Si il n'y a qu'un nombre fini de Lo Jac' qui n'ont pas dit la couleur de leur propre chapeau, ils sont tous libérés. Sinon, c'est la galère à perpétuité. Lo Jac' peu(ven)t-il(s) s'en sortir ?

Indication : Montrer qu'il existe un ensemble A tel que pour tout nombre réel x, il existe un unique nombre y dans A dont le développement décimal propre coïncide avec celui de x à partir d'un certain rang.

Exercice 8 Pour se venger, Lo Jac' enferme 63 matheux sur son bateau. Il possède une infinité (dénombrable, il a un petit bateau) de tonneaux contenant chacun un nombre réel. Pour être libérés, les mathématiciens doivent réussir l'épreuve suivante : chacun d'eux passe dans la cale et ouvre autant de tonneaux qu'il souhaite (y compris une infinité), mais pas toutes. Quand il le décide, il annonce un nombre réel en désignant un tonneau encore fermé. Le but est que ce nombre soit dans ce tonneau. Lo Jac' referme les tonneaux entre deux passages. Les mathématiciens ont le droit à au plus une erreur en tout sinon ils seront tous dévorés par les requins. Trouver une stratégie pour les aider. On admettra que des mathématiciens sont capables de faire une infinité de choix simultanément.

Indication 1 : Adapter l'indication de l'exercice précédent à l'ensemble des suites de réels.

Indication 2 : Résoudre l'énigme plus simple : il n'y a plus que 63 tonneaux et chaque mathématicien doit dire un nombre plus grand que tous les nombres présents dans les tonneaux non ouverts. Ils ont de nouveau le droit à une seule erreur.

Indication 3 : Séparer les tonneaux en 63 ensembles infinis de tonneaux.

Regardons maintenant un énoncé plus spectaculaire : le paradoxe de Banach-Tarski stipule que l'on peut couper une boule en un nombre fini de morceaux (5 au minimum pour être exact) et les déplacer sans les superposer pour obtenir deux boules identiques à la précédente.

L'intuition rejette une telle proposition car l'on crée en quelque sorte du volume uniquement en déplaçant des objets. La réalité est que lorsque l'on accepte l'axiome du choix, il existe des objets desquels on ne pas parler de volume. Mais commençons par voir comment on pourrait définir un volume (que l'on appelle en mathématique une mesure), ici dans $\mathbb{R}$. La mesure puissante la plus intuitive est la mesure de Lebesgue.

Définition 182. Une tribu sur un ensemble E est un ensemble $\mathcal{M}$ de sous-ensembles de E vérifiant :

— $\emptyset \in \mathcal{M}$ et $E \in \mathcal{M}$.
— Si $(A_n) \in \mathcal{M}^{\mathbb{N}}$ alors $\cup_{n=0}^{\infty} A_n \in \mathcal{M}$.
— Si $A \in \mathcal{M}$ alors $(E \setminus A) \in \mathcal{M}$.

Nous pouvons maintenant définir un espace mesuré.

Définition 183. Un espace E est mesuré s'il est muni d'une tribu $\mathcal{M}$, dont les éléments sont appelés ensembles mesurables, et d'une fonction μ de $\mathcal{M}$ dans $\mathbb{R}_+ \cup \{+\infty\}$, appelée mesure, telles que :

— $\mu(\emptyset) = 0$.
— (Sigma-additivité) si $(A_n) \in \mathcal{M}^{\mathbb{N}}$ est une suite d'ensembles deux à deux disjoints alors $\mu(\cup_{n=0}^{\infty} A_n) = \sum_{n=0}^{+\infty} \mu(A_n)$.

Nous pouvons maintenant définir la mesure de Lebesgue. Notons $\mathcal{I}$ l'ensemble des unions dénombrables d'intervalles ouverts disjoints (c'est-à-dire d'intervalles de la forme $]a\,;b[$ pour $a, b \in \mathbb{R} \cup \{-\infty, +\infty\}$ et $a < b$).

Définition 184. Notons $\mathcal{B}(\mathbb{R})$, appelée tribu des boréliens de $\mathbb{R}$, la plus petite tribu incluant $\mathcal{I}$.

Définition 185. La mesure de Lebesgue μ est définie sur $\mathcal{B}(R)$ par

— pour $a, b \in \mathbb{R} \cup \{-\infty, +\infty\}$ et $a < b$, $\mu(]a\,;b[) = b - a$.

— pour $I \in \mathcal{I}$, $\mu(I)$ est définie par sigma-additivité.
— pour $A \in \mathcal{B}(\mathbb{R})$ quelconque,

$$\mu(A) = \min \{\mu(I) | I \in \mathcal{I}, A \subset I\} .$$

Montrer que cette définition est cohérente est assez difficile et a été effectué pour la première fois par Lebesgue lui-même. Commençons par nous familiariser avec cette mesure.

Exercice 9 (Calculs de mesures de Lebesgue)

1. Montrer qu'un point est de mesure nulle.
2. Quelle est la mesure de $[0\,;1[\cap]3/2\,;4]$?
3. Quelle est la mesure de $\cup_{n=0}^{\infty}[2^{-2n}\,;2^{-2n-1}]$?
4. Monter que $\mathbb{Q}$ est de mesure nulle.
5. Quelle est la mesure de l'ensemble des nombres dont la partie entière est paire ?
6. Montrer que la mesure est invariante par translation.
7. Montrer que l'ensemble des nombres dont l'écriture décimale ne contient pas de 9 est de mesure nulle.
8. Montrer que si A est un ensemble mesurable et λ un nombre réel, alors $\lambda A := \{\lambda x | x \in A\}$ a pour mesure λ fois la mesure de A.

La mesure de Lebesgue peut facilement être prolongée à des ensembles plus gros que les boréliens. On peut même poser en axiome que tous les sous-ensembles de $\mathbb{R}$ sont mesurables. Mais dans ce dernier cas, on ne peut plus supposer l'axiome du choix qui devient faux. En effet, l'axiome du choix implique l'existence d'ensembles non mesurables.

Exercice 10 (Un exemple d'ensemble non mesurable) Trouver un ensemble non mesurable.

Indication : Prendre un ensemble particulier de représentants du quotient $\mathbb{R}^*/\mathbb{Q}$.

Maintenant nous allons essayer de comprendre pourquoi le paradoxe de Banach-Tarski peut être vrai en prenant l'exemple du cercle. Dans ce cours nous dirons qu'un ensemble E est décomposable en un ensemble F si l'on peut découper E en un nombre fini de morceaux et les déplacer pour former F. On dit que E est n-décomposable en F si n morceaux suffisent. On remarquera que la décomposabilité est une relation d'équivalence.

Exercice 11

1. Montrer qu'un cercle est 2-décomposable en un cercle privé d'un point.
2. Montrer qu'un cercle est 2-décomposable en un cercle privé d'un ensemble non mesurable (on adapte naturellement la mesure sur $\mathbb{R}$ en une mesure le cercle).

Indication : Considérer un angle θ tel que $\pi/\theta \notin \mathbb{Q}$.

En réalité, un cercle (ou un disque) n'est pas décomposable en deux cercles (ou deux disques). Toutefois, la même idée est utilisée pour démontrer le paradoxe. On sépare la boule en deux moitiés. Chacune des moitiés est de nouveau séparée en deux morceaux selon l'idée de l'exercice précédent (sauf que l'on utilise deux rotations au lieu d'une) est l'un des morceaux après rotation va boucher le trou laissé par l'autre moitié. Aprés avoir complété les quelques trous restants, nous obtenons les deux boules souhaitées. Généralisons maintenant ce résultat.

Exercice 12 Adapter le théorème de Cantor-Berstein pour montrer que si E et F sont deux ensembles tels que l'on peut décomposer E en une partie de F et F en une partie de E alors on peut décomposer E en F.

Exercice 13 En déduire que tout ensemble borné de l'espace incluant une boule peut être décomposé en une boule de rayon 1 et donc en tout autre ensemble borné de l'espace incluant une boule.

Enfin un dernier exercice :
Exercice 14 Connaissez-vous un anagramme de Banach-Tarski ?

Solution de l'exercice 1 Pour les trois premiers ensembles, nous avons les injections suivantes :

1. pour $n \in \mathbb{Z}$, si n est positif, on l'envoie sur $2n$, sinon sur $2|n| - 1$.
2. pour $r \in \mathbb{Q}$, si $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$ est un couple tel que p est premier avec q et $r = \frac{p}{q}$ alors on envoie r sur $2^p 3^q$ si r est positif et sur $2^{|p|} 3^q 5$ sinon.
3. pour $P \in \mathbb{Q}[X]$, si P est nul on l'envoie sur 1 et sinon si P est de degré d, il existe des nombres rationnels $a_0, a_1, \ldots, a_d$ tels que $P = a_d X^d + \cdots + a_1 X + a_0$. Soit φ la fonction injective de $\mathbb{Q}$ dans $\mathbb{N}$ décrite ci-dessus, alors on envoie P sur $p_0^{\varphi(a_0)} p_1^{\varphi(a_1)} \ldots p_d^{\varphi(a_d)}$ où p_i désigne le $(i+1)^{\text{ème}}$ nombre premier.

Supposons par l'absurde qu'il existe une fonction injective φ de $\mathbb{R}$ dans $\mathbb{N}$. Dans ce cas, on note u_i pour $i \in \mathbb{N}$ l'antécédant de i par φ s'il existe et 0 sinon. On note x_i la $i^{\text{ème}}$ décimale propre de u_i (u_i admet un unique développement décimal qui ne termine pas par une infinité de 9 nommé développement décimal propre). Soit y_i un chiffre nul si x_i est non nul et valant 1 sinon. Soit y le nombre réel compris entre 0 et 1, 0 inclus, tel que la $i^{\text{ème}}$ décimale propre de y soit y_i. Alors y diffère de $u_{\varphi(y)}$ (car la $(\varphi(y))^{\text{ème}}$ décimale diffère) ce qui est absurde. On a ici utilisé l'argument diagonal de Cantor qui est utile pour démontrer d'autres résultats.

Solution de l'exercice 2 On cherche à construire une bijection φ de E dans F. Soit f l'injection de E dans F et g celle de F dans E. Une idée est de partir de f. On décrète que φ vaut f sur E. Il existe alors des points de B non atteints par φ : les points y hors de $f(E)$, pour eux on a envie de se servir de g, par exemple dire que, $\varphi(g(y)) = y$. Le problème, c'est qu'après cette modification le point $f(g(y))$ n'est plus atteint par φ, il faudrait donc trouver un moyen de répéter à volonté le processus.

Une façon de faire cela proprement est d'introduire des « chaînes ». Soit x dans E, on définit la chaîne de x comme étant la suite (x_n) définie par récurrence par $x_{2k+1} = f(x_{2k})$ et $x_{2k} = g(x_{2k-1})$. Si cette suite revient sur x, on dit que la chaîne de x est une boucle. Si ce n'est pas une boucle, on l'étend le plus possible sur les entiers négatifs : si x a un antécédent y par g, il n'en a qu'un, et on pose $x_{-1} = y$. Puis on cherche un antécédent de x_{-1} par f, et ainsi de suite. Si ce processus bloque au bout d'un moment (si on tombe sur un élément n'ayant pas d'antécédent), on dit que la chaîne a une origine, sinon on dit qu'elle est infinie.

On va définir φ directement sur les chaînes : si la chaîne de x est une boucle ou est infinie, on prend pour $\varphi(x)$ l'élément suivant x dans la chaîne (c'est-à-dire $f(x)$). Si la chaîne a une origine et que cette origine est dans E, on prend pour $\varphi(x)$ l'élément suivant x dans la chaîne, mais si l'origine de la chaîne est dans F, on prend pour $\varphi(x)$ l'élément précédent x dans la chaîne (si on ne faisait pas cela, l'origine de la chaîne n'aurait pas d'antécedent par φ). On vérifie qu'une telle définition fonctionne.

Solution de l'exercice 3 Soit u_0 la racine de l'arbre. Comme l'arbre est infini, u_0 possède au moins un fils qui est la racine d'un sous-arbre infini. Notons ce fils u_1. Par le même raisonnement, u_1 possède un fils u_2 racine d'un sous-arbre infini. On construit ainsi une suite de

noeuds $(u_n)_{n\in\mathbb{N}}$ qui forment une branche infinie de l'arbre ce qui démontre le lemme de König.

Solution de l'exercice 4 Nous allons reprendre l'idée de la preuve du lemme de König pour construire les suites de l'indication par récurrence. Nous allons construire en plus une suite d'ensembles notée $(A_n)_{n\in\mathbb{N}}$ telle que pour tous $p > q$ et pour tout sommet s dans A_p, l'arête reliant u_q à s est de couleur c_q. Pour u_0 nous prenons un sommet quelconque du graphe et pour A_0 l'ensemble des sommets privé de u_0. Supposons u_n et A_n construits pour un certain entier positif n. u_n est nécessairement incident à une infinité d'arêtes de même couleur dont les seconds extrémités sont dans A_n. Notons cette couleur c_n et A_{n+1} l'ensemble, infini, des secondes extrémités de ces arêtes. Enfin, choisissons un sommet quelconque u_{n+1} dans A_{n+1}. Nous pouvons maintenant poursuivre notre construction par récurrence.

Supposons maintenant les suites (u_n) et (c_n) construites. Il existe un sous-ensemble infini E de $\mathbb{N}$ tel que toutes les couleurs c_n pour $n \in E$ soient identiques. Le sous-graphe de G de sommets $\{u_n | n \in E\}$ est alors monochrome.

Solution de l'exercice 5 En fait, il suffit de faire tous les choix simultanément avant. Prenons l'exemple du lemme de König. Pour chaque noeud racine d'un sous-arbre infini, on choisit un fils qui est racine d'un sous-arbre infini. A présent, à partir de la racine, on suit le choix déjà fait.

Solution de l'exercice 6 Si x est un élément de $\mathbb{R}^*$, on note $\overline{x}$ l'ensemble $y \in \mathbb{R}^* | \frac{x}{y} \in \mathbb{Q}\}$. On remarque que si $y \in \overline{x}$ alors $\overline{x} = \overline{y}$. Un tel ensemble est appelé une classe d'équivalence. $\mathbb{R}^*$ est alors partitionné par l'ensemble des classes d'équivalence (ce qui signifie que $\mathbb{R}^*$ est l'union de ces classes et que deux classes différentes sont disjointes). L'axiome du choix nous autorise à choisir un élément dans chacune des classes ce qui nous donne A.

Solution de l'exercice 7 Si x est un nombre réel, on note $\overline{x}$ l'ensemble des nombres réels dont le développement décimal propre coïncide avec celui de x à partir d'un certain rang : c'est la classe d'équivalence de x. Comme dans l'exercice précédent, ces classes partitionnent $\mathbb{R}$. Les mathématiciens peuvent donc se mettre d'accord sur un ensemble de représentants A. On associe à chaque chiffre une couleur. La suite des couleurs des chapeaux des mathématiciens définit ainsi le développement décimal d'un nombre réel a. Chaque mathématicien voit la fin de se développement, il peut donc en déduire le nombre b de A qui représente la classe $\overline{a}$. Il chuchote alors à Lo Jac' la couleur de la décimale de b lui correspondant. Tous les mathématiciens à partir du rang où coïncide a et b disent la bonne couleur. Les mathématiciens seront sauvés !

Solution de l'exercice 8 On numérote les mathématiciens entre 1 et 63. Les mathématiciens se mettent d'accord sur un ensemble A de suites de réels tel que chaque suite de réels coïncide à partir d'un certain rang avec une unique suite de A. On partitionne l'ensemble des tonneaux en 63 ensembles infinis et l'on associe à la $i^{\text{ème}}$ suite, notée (u_i), la suite (v_i) correspondante dans A. On note k_i le rang à partir duquel (u_i) et (v_i) coïncident. Lorsque le $n^{\text{ème}}$ mathématicien passe, il ouvre tous les tonneaux des 63 suites exceptés ceux de la $n^{\text{ème}}$ suite. Il a donc accès aux nombres u_i sauf à u_n ainsi qu'aux nombres (v_i) et k_i correspondants. Maintenant, si K_n est le maximum des k_i pour i différent de n, le mathématicien ouvre tous les tonneaux de la $n^{\text{ème}}$ suite à partir du rang $K_n + 1$. Il obtient la fin d'une suite qu'il peut associer à la suite (v_n) de A. Il dit alors à Lo Jac' le K_n^{me} terme de cette suite tout en désignant le $K_n^{\text{ème}}$ tonneau de la $n^{\text{'eme suite}}$.

Si k_n est strictement plus grand que tous les autres k_i, ce qui arrive à au plus un mathématicien, ce mathmaticien a de grandes chances de faire une erreur. Sinon, $K_n \geqslant k_n$. Dans ce cas, la suite u_n coïncide avec la suite v_n à partir du rang K_n (ou même avant) ce qui fait que la prédiction du mathématicien sera correcte. De nouveau, les mathématiciens seront sauvés.

Solution de l'exercice 9 On note μ la mesure de Lebesgue. On a

1. soit x un nombre réel. On a

$$\begin{aligned} \mu(]x-1\ :x+1[) &= \mu(]x-1\,;x[)+\mu(\{x\})+\mu(]x\,;x+1[) \\ 2 &= 1+\mu(\{x\})+1 \end{aligned}$$

   Donc la mesure d'un point est nulle. Ou encore, pour tout $n \geqslant 1$ entier,

$$\mu(\{x\}) \leqslant \mu(]x-\frac{1}{n}\,;x+\frac{1}{n}[) = \frac{2}{n},$$

   donc $\mu(\{x\}) = 0$.

2. les deux intervalles sont disjoints donc

$$\begin{aligned} \mu([0;1[\cap]3/2;4]) &= \mu([0;1[)+\mu([3/2;4[) \\ &= \mu(\{0\})+\mu(]0\,;1[)+\mu(\{3/2\})+\mu(]3/2;4[) \\ &= 1+1/2 \\ \mu([0;1[\cap]3/2;4]) &= 3/2. \end{aligned}$$

3. Tous les intervalles sont disjoints donc

$$\begin{aligned} \mu(\cup_{n=0}^{\infty}[2^{-2n};2^{-2n+1}]) &= \sum_{n=0}^{\infty}\mu([2^{-2n};2^{-2n+1}]) \\ &= \sum_{n=0}^{\infty}4^{-n} \\ &= 4/3. \end{aligned}$$

4. $\mathbb{Q}$ est une union dénombrable de points, qui sont de mesure nulle, donc est de mesure nulle.
5. L'ensemble des nombres dont la partie entière est paire est une union infinie d'intervalles disoints de longueur 1 donc est de mesure infinie.
6. Clairement, si I est un intervalle ouvert $]a\,;b[$ et t un réel alors, avec $I+t=]a+t\,;b+t[$ le translaté de I, $\mu(I) = b-a = (b+t)-(a+t) = \mu(I+t)$. Cette propriété se prolonge directement à tout $\mathcal{I}$. Si A est un ensemble mesurable quelconque, on a

$$\begin{aligned} \mu(A) &= \min(\mu(I)|I\in\mathcal{I}, A\subset I) \\ &= \min(\mu(I+t)|(I+t)\in\mathcal{I}, (A+t)\subset(I+t)) \\ &= \mu(A+t). \end{aligned}$$

7. Traitons d'abord le cas de l'ensemble I des nombres de $[0\,;1[$ ne contenant pas de 9 dans leur développement décimal. Si n est un entier positif, cette ensemble est inclus

dans l'ensemble des nombres ne contenant pas de 9 jusqu'à la n^{me} décimale noté I_n. Si l'on note A_n l'ensemble des nombres entiers positifs strictement inférieurs à 10^n qui ne contienne pas le chiffre 9, on a

$$I_n = \cup_{a \in A_n} [\frac{a}{10^n} ; \frac{a+1}{10^n}$$

On en déduit que

$$\begin{aligned} \mu(I_n) &= \frac{\text{card}(A_n)}{10^n} \\ &= \frac{9^n}{10^n}. \end{aligned}$$

Or, cette dernière valeur tend vers 0 lorsque n tend vers l'infini. Donc l'ensemble I est de mesure nulle. L'ensemble de départ est une union dénombrable de translatés de I et est donc lui aussi de mesure nulle.

8. Par le même raisonnement que pour la translation, si I est un intervalle ouvert et λ un réel positif, $\mu(\lambda I) = \lambda \mu(I)$. Cette propriété se prolonge directement à $\mathcal{I}$ puis à $\mathcal{B}(\mathbb{R})$ par la même série de calculs que pour la translation.

Solution de l'exercice 10 Soit un ensemble A de représentants du quotient $\mathbb{R}^*/\mathbb{Q}$, comme ci-dessus, avec la contrainte supplémentaire que A est inclus dans $[0;1]$. Par construction de A, si r et s sont deux nombres rationnels non nuls différents, rA et sA sont disjoints.

Supposons par l'absurde A mesurable. On pose

$$B = \cup_{n=3}^{\infty} \frac{1}{n} A \cup \frac{n-1}{n} A.$$

On a

$$\mu(B) = \sigma_{n=3}^{\infty} \mu(\frac{1}{n} A \cup \frac{n-1}{n} A) = \sigma_{n=3}^{\infty} \mu(A)$$

Or B est inclus dans $[0;1]$ donc B ne peut être de mesure infinie donc A est de mesure nulle. Or, toujours par construction de A

$$\mathbb{R}^* = \cup_{r \in \mathbb{Q}^*} rA.$$

Donc $\mathbb{R}^*$ est union disjointe d'un nombre dénombrable d'ensembles de mesure nulle donc est de mesure nulle. Contradiction. Donc A n'est pas mesurable.

Solution de l'exercice 11 Soit θ un nombre tel que $\pi/\theta \notin \mathbb{Q}$. On prend comme premier morceau A les points d'angle $k\theta$ pour tout k entier positif ou nul, le second morceau est le complémentaire. On effectue une rotation d'angle θ sur A. Pour chaque k, le point d'angle $k\theta$ remplace le point d'angle $(k+1)\theta$. Le seul point qui n'est pas remplacé est le point d'angle 0. En effet, sinon on aurait $(k+1)\theta$ est un multiple de π ce qui contredit l'hypothèse sur θ. Pour la deuxième partie, si x est un nombre réel, on note $\overline{x}$ l'ensemble des nombres réels y tels qu'il existe a et b entiers tels que $x = y + a\pi + b\theta$. Comme précedemment, l'axiome du choix nous permet de trouver un ensemble X de représentants. On prend pour premier morceau A l'ensemble des points d'angle $x + k\theta$ pour tous k entier positif ou nul et x dans X. De nouveau, en tournant A d'un angle θ nous obtenons le cercle privé de X. X n'est pas mesurable car le cercle est l'union

dénombrable et disjointe des rotations de X par un multiple de θ. On utilise alors le même argument que précédemment.

Solution de l'exercice 12 La décomposition de E dans une partie de F induit une injection de E dans F. Notons-la f. Réciproquement on note g l'injection de F dans E induite par la décomposition de F dans E. En reprenant la démonstration de Cantor-Bernstein ci-dessus, nous avions séparé E en deux sous-ensembles. Le premier ensemble, que nous appellerons E_1, sur lequel la bijection φ coïncide avec f et le second, E_2, sur lequel φ coïncide avec la réciproque partielle de g. Maintenant, si l'on effectue la décomposition de E en restreignant les morceaux à E_1 et la décomposition inverse de F en restreignant les morceaux à E_2, nous obtenons bien F tout entier. Donc nous avons décomposé E en F.

Solution de l'exercice 13 On peut découper l'ensemble en un nombre fini de sous-ensembles de boules de rayon 1. En utilisant le paradoxe de Banach-Tarski, on peut rassembler ces parties de boule deux à deux pour former de nouvelles parties de boule et continuer jusqu'à ce qu'il ne reste plus qu'une partie de boule de rayon 1. Maintenant, si la boule incluse dans l'ensemble de départ est de rayon r, en utilisant la même méthode, on peut découper la boule de rayon 1 en parties de boule de rayon r et les rassembler pour finalement obtenir une partie de boule de rayon r et donc une partie de l'ensemble de départ. En utilisant l'adaptation du théorème de Cantor-Bernstein, l'ensemble est donc décomposable en la boule. On conclut par équivalence de la décomposabilité.

Solution de l'exercice 14 Banach-Tarski Banach-Tarski.

2 mercredi 26 après-midi : théorie des graphes, Gabriel Pallier

Ce cours n'est pas à proprement parler un cours de préparation olympique et les exercices sont plutôt conçus pour entraîner des discussions en classe ; il n'y a pas toujours de correction. Ce cours est aussi ouvert, dans une certaine mesure ; ainsi, par exemple, on s'autorisera à faire évoluer les définitions [1] au gré de leurs rencontres avec les propositions et les théorèmes. Voici quelques références qui ont inspiré ce cours :

1. L'ouvrage de I.Lakatos, *Preuves et réfutations* autour de la relation d'Euler.
2. Le livre *Raisonnements divins* (Aigner, Ziegler) disponible dans la salle de la muraille, pour le lemme du petit degré et le théorème des six couleurs.
3. Les images du film mathématique *Dimensions* d'E. Ghys et J. Leys pour la projection stéréographique.

Les problèmes suivants sont des invitations à la théorie des graphes.

Problème A (Enigme des trois maisons) Dans le plan, est-il possible de relier 3 maisons A, B et C à une arrivée d'eau, de gaz et d'électricité sans que deux canalisations ne se croisent ?

1. Il faut dire qu'on bénéficie d'un certain flou juridique concernant les définitions en théorie des graphes : Bourbaki n'est pas passé par là.

Problème B Combien de couleurs au minimum faut-il pour colorier les pays sur une carte du monde de sorte que deux pays qui ont une frontière commune sont colorés de manières différente ?

Nous cherchons ici à établir une théorie permettant de répondre (au moins en partie...) à ces problèmes.

Notion de graphe

Une première définition Voici une première définition pour démarrer :

Définition 186. Un graphe (simple, non orienté) est la donnée d'un ensemble V de sommets et d'un ensemble E de paires d'éléments de V, appelés arêtes.

On s'interessera aujourd'hui aux graphes finis (c'est-à-dire que V est fini, ce qui implique automatiquement que E est fini). On peut dessiner un graphe fini sur une feuille de papier ou un tableau : les sommets sont des points, et on relie deux sommets v et w quand et seulement quand $\{v, w\} \in E$. **Exercice 1** $G = (V, E)$ avec $V = \{1, 2, 3, 4, 5, 6, 7\}$ et pour tous $i \neq j$, $\{i, j\} \in E \iff i \mid j$ ou $j \mid i$. Dessiner le graphe G ; combien possède-t-il d'arêtes ?

Dessinons quelques graphes. Manifestement certains sont d'un seul tenant (c'est le cas de G), d'autres non. On dira que les graphes d'un seul tenant sont les graphes connexes. Voici une définition rigoureuse :

Définition 187. On dit qu'un graphe est connexe si pour tout couple (v, w) de sommets il existe une suite d'arêtes $\{e_1, \dots e_\ell\}$ telle que $e_i \cap e_{i+1}$ est non vide, $v \in e_1$ et $w \in e_n$.

Définition 188. Si $G = (V, E)$ est un graphe si $V' \subset V$ et $E' \subset E$ sont deux sous-ensembles tels que

$$\forall e \in E,\ e \in E' \implies e \subset V'$$

alors on dit que $G' = (V', E')$ est un sous-graphe de E.

Remarque 189. L'intérêt de la condition dans la définition précédente, est de s'assurer que l'on ne peut pas mettre dans le sous-graphe d'arête pointant vers un sommet situé hors de ce sous-graphe.

Pour finir, le degré d'un sommet v, noté $d(v)$ est le nombre d'arêtes auquel ce sommet appartient. D'après un exercice bien connu (lemme des poignées de mains, voir par exemple le cours du groupe B sur les invariants), il existe un nombre pair de sommets ayant des degrés impairs. On a aussi la formule obtenue par double comptage

$$2|E| = \sum_{v \in V} d(v) \tag{IX.1}$$

Exemples fondamentaux On décrit ici des familles d'exemples que nous rencontrerons par la suite.

Graphe complet K_n est le graphe complet à n sommets. $V = \{1, \dots, n\}$ et toute paire $\{i, j\}$ est une arête.

Graphe bipartite $K_{m,n}$ est le graphe bipartite sur m et n sommets. On décompose V est la réunion disjointe de V_0 à m éléments et V_1 à n éléments, et les arêtes sont les paires qui possèdent un élément dans V_0 et un dans V_1.

Graphe linéaire L_n est le graphe linéaire à n sommets. $V = \{1, \dots, n\}$ et $\{i, j\} \in E \iff |i - j| = 1$

Graphe cyclique ($n \geqslant 3$) C_n est le graphe cyclique à n sommets (on dit aussi n-cycle). $V = \mathbb{Z}/n\mathbb{Z}$ et pour tous $x \neq y$ $\{x, y\} \in E \iff x - y \in \left\{\overline{-1}, \overline{1}\right\}$ **Exercice 2** Peut-on définir les graphes C_1 et C_2 et si oui, comment ? Proposer un changement dans la définition de graphe qui permette d'intégrer le cas de C_1 et C_2. *Solution de l'exercice 1* On pourrait encore appliquer la définition donnée plus haut avec 1 et 2, ce qui donnerait que C_1 et C_2 sont respectivement L_1 et L_2, mais cela n'est pas entièrement satisfaisant : l'aspect cyclique est perdu. Si l'on autorise les arêtes multiples et les boucles, on arrive à former des graphes qui correspondent mieux à l'idée que l'on se fait de C_1 et C_2.

On propose la définition plus large suivante.

Définition 190. Un graphe (non orienté) est la donné d'un ensemble fini $V = \{v_1, \dots v_n\}$ de sommets, d'un ensemble fini E d'arêtes et d'une fonction $\gamma : E \to V \times V$ telle que $\gamma(e) = (v_i, v_j)$ avec $i \leqslant j$.

Avec cette définition, $G = (V', E')$ est un sous-graphe si $e \in V' \implies \gamma(e) \subset E'$. Les graphes de l'ancienne définition sont encore naturellement des graphes pour la nouvelle définition. Nous dirons que les graphes vérifiant l'ancienne définition sont les graphes simples. Un graphe est simple s'il ne contient aucun sous-graphe de la forme C_1 ou C_2.

Pour que IX.1 continue d'être valable, nous conviendrons que le sommet de C_1 est de degré 2.

Cycles, arbres Un cycle est la donnée d'un sous-graphe cyclique. Sa longueur est son nombre de sommets. **Exercice 3** Combien y a-t-il de cycles de longueur ℓ dans le graphe K_n ? Dans le graphe $K_{n,m}$? *Solution de l'exercice 2* (Exercice corrigé en classe par Yakob Kahane) K_n et $K_{n,m}$ sont simples, donc déjà il n'y a pas de 1-cycle ni de 2-cycles, on supposera $\ell \geqslant 3$. Dans K_n, un cycle est la donnée de ses sommets, et d'un ordre de parcours de ces sommets, sachant que le choix du premier point et sens du parcours ne comptent pas. On en déduit que le nombre de ℓ-cycles est

$$N = \binom{n}{\ell} \cdot \ell! \cdot \frac{1}{\ell} \cdot \frac{1}{2} = \frac{(\ell - 1)!}{2} \binom{n}{\ell}$$

Dans $K_{n,m}$ il n'y a pas de ℓ-cycle si ℓ est impair (puisque par exemple, si l'on est parti de V_0, on sera dans V_1 après avoir suivi un nombre impair d'arêtes). En revanche, si ℓ est pair, écrivons $\ell = 2\ell'$; alors le choix d'un ℓ-cycle revient à celui de ℓ' éléments dans V_0, de ℓ' éléments dans V_1, puis d'un ordre de parcours de sorte que

$$N = \frac{1}{2} \binom{n}{\ell'} \binom{m}{\ell'} \frac{(\ell'!)^2}{\ell'^2} = \frac{(\ell - 1)!^2}{2} \binom{n}{\ell'} \binom{m}{\ell'}$$

On a vu dans l'exercice précédent qu'un graphe bipartite ne contient pas de 3-cycle. En fait, le graphe bipartite $K_{n,n}$ est, parmi les graphes simples sans 3-cycles ayant autant de sommets, celui qui a le plus d'arêtes. Ce résultat constitue le théorème de Mantel [2]. Au sujet des graphes connexes simples qui n'ont pas de 4-cycle, signalons le beau théorème de l'amitié (ou du politicien) qui est démontré dans le livre Raisonnements Divins.

Définition 191. On dit qu'un graphe est un arbre s'il est connexe et ne possède pas de cycle.

Proposition 192. Si $G = (E, V)$ est un arbre non vide alors

$$|E| = |V| - 1 \tag{IX.2}$$

Démonstration. Soit G est un arbre à n sommets, prenons $v_0 \in V$. Puisque G est connexe, pour chaque $v \in V \setminus \{v_0\}$ il existe un chemin de v_0 à v formé d'arêtes distinctes ; ce chemin est unique car G n'a pas de cycle, on le note $\Gamma_{v_0 \to v}$. On vérifie alors que l'application f qui à v associe la dernière arête de $\Gamma_{v_0 \to v}$ est une bijection de $V \setminus \{v_0\}$ sur E :

- f est injective : si deux chemins $\Gamma_{v_0 \to v}$ et $\Gamma_{v_0 \to v'}$ terminent par la même arête et si $v_0 \neq v'$, alors on pourrait former un cycle en recollant ces deux chemins.

- f est surjective : soit $e \in E$; posons $\gamma(e) = (v, v')$; alors si $e \neq f(v)$, $\Gamma_{v_0 \to v'}$ s'obtient en ajoutant e à la fin de $\Gamma_{v_0 \to v}$. □

Remarque 193. On pourrait généraliser la proposition précédente : si p est le nombre de composantes connexes (c'est-à-dire de sous-graphes connexes maximaux) alors

$$|E| - |V| + p \geqslant 0 \tag{IX.3}$$

avec égalité si et seulement si G est sans cycle.

Soit G un graphe connexe. On dit qu'un sous-graphe G' de G est couvrant si G' est connexe et $E' = E$. **Exercice 4** Montrer que tout graphe fini possède un arbre couvrant. *Solution de l'exercice 3*

Tant qu'il existe un cycle, on peut retirer l'une de ses arêtes sans perdre la connexité (puisque l'arête retirée faisait partie d'un cycle). A la fin le graphe obtenu est couvrant, connexe et acyclique : c'est un arbre couvrant.

Les graphes planaires et la formule d'Euler

Graphes planaires et polyèdres convexes.

Définition 194. On dit que G est planaire s'il possède un dessin dans le plan où aucune de ses arêtes ne se croisent.

Par exemple, les graphes cycliques, le graphe K_4 est planaire.

2. Pour une preuve, on pourra consulter le polycopié de Pierre Bornzstein concernant les graphes. Une autre preuve à partir de l'inégalité de Cauchy-Schwarz est rapportée par Roger Mansuy dans Quadrature, numéro 87 (juillet 2015).

Remarque 195. Pour le moment on ne sait pas encore s'il existe des graphes non planaires ; toutefois, remarquons que si un graphe est planaire, alors tous ses sous-graphes le sont aussi. Par conséquent pour montrer qu'un graphe est non planaire, il suffi(rai)t de trouver un sous-graphe non planaire.

Une famille fondamentale de graphes planaires est donnée par les polyèdres convexes. Si P est un polyèdre convexe, on peut lui associer un unique graphe planaire Γ_P dont les sommets sont les sommets et les arêtes sont les arêtes. Le dessin de ce graphe planaire sans intersection associé au polyèdre peut s'obtenir à l'aide d'une projection stéréographique. **Exercice 5** Dessiner les graphes de l'octaèdre, du cuboctaèdre, du dodécaèdre, du rhombicosidodécaèdre (voir dessins). Un polyèdre possède des faces, et elles sont encore bien visibles sur son graphe. Il est également assez clair qu'un dessin plan d'un graphe planaire possède encore des faces. L'une d'entre elle est "infinie" (c'est-à-dire qu'elle n'est pas limitée dans le plan).

Théoréme 196. [Formule d'Euler] Soit G un graphe planaire à n sommets, m arêtes. Alors, si f est le nombre de faces sur un dessin plan de G, on a la relation

$$n - m + f = 2 \tag{IX.4}$$

Puisqu'un polyèdre s'identifie à un graphe planaire, on en déduit le

- Correction -

Soit P un polyèdre convexe possédant S sommets, A arêtes et F faces. Alors

$$S - A + F = 2$$

Remarque 197. Mais qu'est-ce qu'une face, au juste ? Si les faces sont faciles à identifier sur un dessin sans intersection du graphe, il ne s'agit pas là d'une définition intrinsèque (qui dépende seulement du graphe et pas de ses dessins). Cependant la formule d'Euler nous dit qu'il y aura toujours le même nombre de faces, quel que soit le dessin. De plus, si l'on effectue plusieurs dessins d'un même graphe, les mêmes arêtes semblent border les mêmes faces. Il y a là une difficulté, que nous ne faisons qu'effleurer.

Le degré d'une face est le nombre d'arêtes qui la bordent. De même qu'une arête pointe vers deux sommets, elle borde deux faces, de sorte que si F est l'ensemble des faces alors

$$\sum_{\nu \in F} \deg(\nu) = 2\,|E| \tag{IX.5}$$

Attention, si une arête a une même face de ses deux côtés, alors elle compte double dans le calcul du degré de cette face.

Dual d'un graphe planaire

Définition 198. Soit G un graphe planaire ; son graphe dual, noté $G^\star$ est défini comme suit :

- Les sommets de $G^\star$ sont les faces de G.
- Dans $G^\star$ il y a une arête entre les faces μ et ν pour chaque arête bordante en commun.

Exercice 6 Donner une condition nécessaire et suffisante sur G pour que $G^\star$ soit un graphe simple. *Solution de l'exercice 4* Pour que $G^\star$ n'ait respectivement pas de boucles ni d'arêtes

double il faut que les sommets de G aient des degrés différents de 1 et 2 respectivement. Pour autant ceci ne suffit pas, il faut rajouter la condition que G reste connexe si on lui enlève au plus une arête.

On admettra ici la

Proposition 199. Le graphe dual $G^\star$ est planaire, et $G^{\star\star}$ s'identifie à G.

On appelle dual d'un polyèdre convexe, le polyèdre obtenu comme enveloppe convexe[3] des centres de ses faces. On peut vérifier que le graphe du dual de P est le dual du graphe de P.

Preuve de la formule d'Euler Soit G un graphe planaire. On se donne T un arbre couvrant de G (on sait qu'il existe) et $T^\star$ le sous-graphe de $G^\star$ formé sur l'ensemble des faces $V^\star$ en prenant toutes les arêtes qui ne correspondent pas à $T^\star$. On vérifie alors que :

1. $T^\star$ est sans cycle : s'il possédait un cycle, celui-ci séparerait deux sommets de V, l'un dans son intérieur, l'autre à l'exterieur. Mais ceci n'est pas possible puisque T est connexe.
2. $T^\star$ est connexe ; dans l'hypothèse du contraire, on voit que $T^{\star\star} = T$ devrait posséder un cycle.

On en déduit que $T^\star$ est un arbre couvrant de $G^\star$. Le nombre total d'arêtes de G est

$$m = n_T + n_{T^\star} = s - 1 + f - 1 = s + f - 2$$

La formule d'Euler est démontrée.

Applications de la formule d'Euler

Les graphes K_5 et $K_{3,3}$ et le théorème de Kuratowski

Proposition 200. K_5 et $K_{3,3}$ ne sont pas des graphes planaires.

En particulier, la proposition répond au problème des trois maisons donné dans l'introduction. On se propose de la démontrer sous forme d'exercice :

Exercice 7 On note $\overline{d}$ (resp $\overline{c}$) le degré moyen des sommets (resp. le nombre moyen de côtés des faces). Montrer les formules suivantes :

$$\begin{aligned} \overline{d} &= 2e/s \\ \overline{c} &= 2e/f \end{aligned}$$

Interpréter à l'aide de la dualité. *Solution de l'exercice 5* Ces formules proviennent directement

de IX.1 et IX.5 démontrées plus haut.

3. Pour prendre l'enveloppe convexe d'un ensemble Π de points de l'espace, on prend un ballon de baudruche qui est de diamètre nul quand il est dégonflé ; on le gonfle assez pour y faire rentrer tout Π, puis on le laisse se dégonfler. A la fin, les points dans le ballon forment l'enveloppe convexe.

Exercice 8 En utilisant l'exercice précédent, montrer que si K_5 était planaire, il ne serait pas simple. Conclure.

Solution de l'exercice 6 Supposons que K_5 est planaire. Alors, il possède des faces. Puisque K_5 possède 5 sommets et $\binom{5}{2} = 10$ arêtes, d'après la formule d'Euler il doit y avoir 7 faces. D'après l'exercice précédent, leur nombre moyen de côté est $\bar{c} = \frac{20}{7} \simeq 2.85$. En particulier, une face possède strictement moins de 3 côtés. Ceci est absurde puisque K_5 est un graphe simple, il ne peut donc pas posséder de 2-cycle. Conclusion, K_5 n'est pas planaire

Exercice 9 Montrer que si $K_{3,3}$ était planaire alors il posséderait un triangle. Conclure.

Solution de l'exercice 7 Supposons que K_5 est planaire. Alors, il possède des faces. Puisque K_5 possède 5 sommets et $\binom{5}{2} = 10$ arêtes, d'après la formule d'Euler il doit y avoir 7 faces. D'après l'exercice précédent, leur nombre moyen de côté est $\bar{c} = \frac{20}{7} \simeq 2.85$. En particulier, une face possède strictement moins de 3 côtés. Ceci est absurde puisque K_5 est un graphe simple, il ne peut donc pas posséder de 2-cycle.

En corollaire de la proposition, G n'est pas planaire dès qu'il contient un sous-graphe de la forme $K_{3,3}$ ou $K_{5,5}$. **Exercice 10** Donner une condition nécessaire et suffisante sur n et m pour que $K_{n,m}$ soit planaire. *Solution de l'exercice 8* On peut supposer $n \leqslant m$. Si $n \geqslant 3$, alors $K_{n,m}$ possède $K_{3,3}$ comme sous-graphe ; il n'est pas planaire. sinon, on peut dessiner $K_{1,m}$ et $K_{2,m}$ sans intersection en plaçant les m sommets sur une droite.

G n'est toujours pas planaire si c'est une expansion de $K_{3,3}$ ou $K_{5,5}$, c'est-à-dire obtenu par ajout de sommets sur des arêtes et passage à un sur-graphe. De manière assez surprenante, $K_{3,3}$ et K_5 suffisent pour décider si un graphe est planaire. Ceci constitue le théorème de Kuratowski (que nous ne démontrerons pas ici) :

Théoréme 201. Soit G un graphe connexe. Alors G est non planaire si et seulement si, G est une expansion de $K_{3,3}$ ou K_5.

Exercice 11 Montrer que l'on peut dessiner $K_{3,3}$ sans intersection des arêtes sur un tore. Est-ce possible pour K_5 ? Sur le tore, toute la théorie est donc à refaire ! Mais Wagner a conjecturé en 1937 qu'il existait un analogue du théorème de Kuratowski sur toutes les surfaces "raisonnables" ; c'est-à-dire pour chaque surface un nombre fini de graphes interdits minimaux, dont les autres se déduisent par expansion. Robertson et Seymour ont démontré cette conjecture (sous une forme légèrement différente) en 2004. Leur preuve n'est pas constructive, c'est-à-dire que l'on ne peut pas en déduire les graphes interdits.

Caractéristique d'Euler Il est légitime de se demander s'il existe une généralisation de la formule d'Euler pour les graphes que l'on peut dessiner sans intersection sur un tore, et plus généralement sur une surface S. La réponse est oui, en voici un énoncé informel :

Proposition 202. Soit S une surface qui n'est pas infinie ; on dit que le dessin d'un graphe sans intersection sur S est une triangulation si toutes les faces qu'ils délimite sont "sans trou". Il existe un entier $\chi(S)$ tel que pour toute triangulation de S on a

$$n - m + f = \chi(S) \tag{IX.6}$$

En particulier, si S est un tore à g trous alors $\chi(G) = 2 - 2g$.

Par "sans trou", nous entendons que tout lacet peut être déformé sans cassure pour se concentrer en un point (on pourra revoir le résumé de la conférence de Xavier pour plus de détails). Les graphes planaires sont les triangulation de la sphère S^2, qui est le tore à 0 trou de sorte que la relation d'Euler s'inscrit dans la proposition précédente. On peut vérifier que les dessins de $K_{3,3}$ et K_5 sur le tore forment une triangulation de sorte qu'ils ont respectivement 3 et 5 faces.

Le lemme du petit degré Il s'agit d'un lemme combinatoire bien utile pour les résultats qui suivent.

Lemme 203. Soit G un graphe planaire simple à n sommets. Alors G possède un sommet de degré au plus 5.

Démonstration. On note f_k le nombre de faces à k côtés. G est simple donc $f_2 = 0$. On a donc

$$\begin{aligned} f &= f_3 + f_4 + \cdots \\ 2e &= 3f_3 + 4f_4 + \cdots \end{aligned}$$

D'où : $2e - 3f \geq 0$. Si par l'absurde chaque sommet a un degré $\geqslant 6$ alors

$$\begin{aligned} s &= s_6 + s_7 + \cdots \\ 2e &= 6s_6 + 7s_7 + \cdots \end{aligned}$$

D'où : $2e - 6s \geqslant 0$. On en déduit :

$$6(e - s - f) \geqslant 0$$

L'addition des deux inégalités précédente donne $e \geq s + f$ ce qui contredit la formule d'Euler. □

Les polyèdres réguliers

Définition 204. Soit P un polyèdre convexe. On dit que P est régulier s'il existe p et q deux entiers $\geqslant 3$ tels que ses faces sont toutes des p-gones réguliers, et si elles se rencontrent en même nombre q en chaque sommet.

Les entiers p et q suffisent à décrire complètement[4] un polyèdre régulier : reportant $sq = fp = 2e$ dans la formule d'Euler, on trouve $s - \frac{sq}{2} + \frac{sq}{p} = 2$, ce qui permet d'accéder au nombre de sommets, puis de faces et d'arêtes. Le dual d'un polyèdre régulier étant lui aussi régulier, on doit avoir $3 \leqslant p, q \leqslant 5$ d'après le lemme du petit degré. Ceci laisse a priori 9 possibilités simplement par des arguments de théorie des graphes ; on va utiliser un argument géométrique pour finir. La somme des angles en un sommet doit être inférieure strictement à 2π, ce qui donne $\frac{1}{p} + \frac{1}{q} > \frac{1}{2}$; les 5 possibilités restantes sont dans le tableau suivant :

4. Disons, à similitude près

$\{p,q\}$	polyèdre	sommets	arêtes	faces
$\{3,3\}$	tétraèdre	4	6	4
$\{4,3\}$	cube (hexaèdre)	8	12	6
$\{3,4\}$	octaèdre	6	12	8
$\{5,3\}$	dodécaèdre	20	30	12
$\{3,5\}$	icosaèdre	12	30	20

Le théorème des six couleurs (et moins si affinités...)

Théoréme 205. Soit G un graphe planaire simple fini. Alors six couleurs suffisent pour colorier les sommets de G de telle sorte que deux sommets d'une arête commune sont toujours de deux couleurs différentes.

Exercice 12 Démontrer le théorème des six couleurs à l'aide du lemme du petit degré.

Solution de l'exercice 9 On procède par récurrence sur le nombre n de sommets. Si $n \leqslant 6$ la conclusion est manifestement valable. Sinon, prenons un sommet v_0 de degré $\leqslant 5$ dont l'existence est fournie par le lemme. D'après l'hypothèse de récurrence, le graphe formé sur $V \setminus \{v_0\}$ est colorable avec 6 couleurs de sorte que deux d'entre elles ne colorent jamais deux sommets voisins. Les voisins de v_0 ont au plus 5 couleurs différentes ; on peut donc choisir la couleur de v_0 d'une manière compatible.

En réalité, le théorème n'est pas optimal, puisque l'on peut se contenter de quatre couleurs. La preuve a été obtenue en 1979 seulement, et a fait débat à l'époque, puisqu'il s'agit de l'une des premières preuves qui fait en partie appel à des calculs menés sur ordinateur (bien que les idées menant à sa résolution soient bien plus anciennes).

Le théorème de Sylvester-Gallai Pour finir, nous donnons ci-dessous une démonstration du théorème de Sylvester-Gallai faisant appel à la formule d'Euler et à un soupçon de dualité projective.

Théoréme 206. Etant donné un ensemble fini de $n \geqslant 2$ points du plan non alignés, il existe toujours une droite qui en contient exactement deux.

Une première démonstration de ce théorème (faisant appel à un principe extremal) est à trouver dans le TD de stratégies de bases du groupe B.

Etape 1 Quitte à projeter le plan sur une sphère à partir du centre de la sphère, les points du plan sont ramenés à des bipoints (couples de points antipodaux sur la sphère) et les droites à des grands cercles.

Sur la sphère, étant donné un ensemble fini de n couples de points antipodaux qui ne sont pas tous sur un même grand cercle, il existe un grand cercle qui contient exactement 2 couples de ces points.

Etape 2 (Passage au problème dual) Sur la sphère, on a une correspondance

$$\{\text{bipoints antipodaux}\} \longleftrightarrow \{\text{grands cercles}\}$$

qui à un bipoint fait correspondre l'ensemble des points équidistants ; et à un grand cercle, les pôles nord et sud si l'on identifie ce grand cercle à l'équateur. Trois bipoints sont alors sur un même grand cercle si, et seulement si, les trois grands cercles associés sont concourants (c'est-à-dire qu'ils ont un bipoint en commun).

Etape 3 Via l'étape précédente on est ramené à montrer que parmi n grands cercles non tous concourants il existe un bipoint ou exactement 2 se croisent. Les grands cercles dessinent un graphe sur la sphère ; il s'agit d'un graphe planaire, et d'après le lemme du petit degré, il possède un sommet de degré $\leqslant 4$. Or le degré d'une intersection de k grands cercles est exactement $2k$; donc il existe un sommet de degré 4 où exactement deux grands cercles s'intersectent.

4 Groupe D

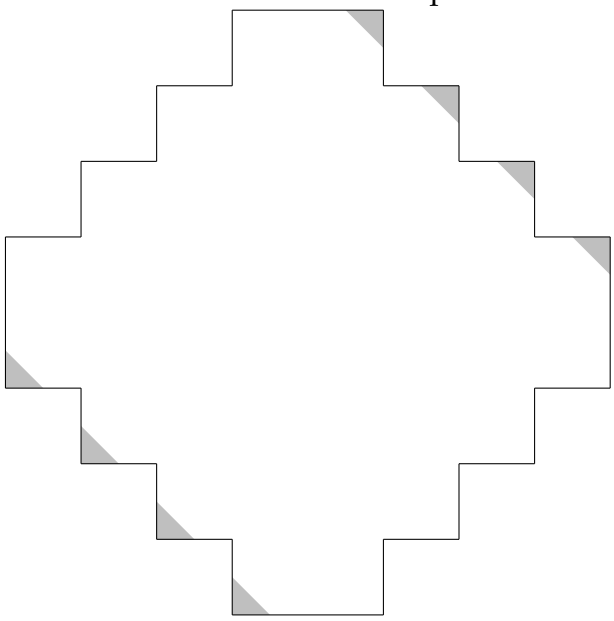
1 mercredi 26 matin : Guillaume Conchon-Kerjan et Thomas Budzinski

Le diamant aztèque

Un peu de Mexicologie

Définition 207. Sur un réseau carré, le *diamant aztèque* d'ordre n est constitué des $2n(n+1)$ petits carrés dont les coordonnées (x, y) des centres vérifient $|x| + |y| \leq n$.

On colorie ces carrés (ou cases) à la manière d'un damier d'échecs, de sorte que le bord droit du haut soit constitué de n cases noires. Cela donne 4 types de dominos selon l'orientation horizontale ou verticale et la position de la case blanche.



Lemme de Lindström-Gessel-Viennot

On considère un graphe G fini, orienté et acyclique (mais il peut y avoir un cycle qui ne respecte pas l'orientation). On suppose qu'entre deux sommets, il n'existe qu'on nombre fini

de chemins. Soit $n \geq 1$, on fixe des sommets $(s_1, \cdots, s_n)$ appelés *sources*, et des sommets $(p_1, \cdots, p_n)$ appelés *puits*.

Définition 208. Une famille de chemins non intersectants associée aux sources (s_i) et puits (p_i) est un n-uplet $C = (C_1, \cdots, C_n)$ tel que pour tout i, C_i est un chemin orienté entre s_i et un p_j, et aucun sommet du graphe n'est sur deux C_i à la fois.

On peut donc associer une permutation $\sigma(C) \in S_n$ à C telle que pour tout i, C_i relie s_i à $p_{\sigma(i)}$, et sa signature $\varepsilon(C)$.

Théoréme 209. Sur un tel graphe, on a

$$\sum_{\sigma \in S_n} \prod M_{i,\sigma(i)} = \sum_{C} \varepsilon(C),$$

où la somme porte sur les familles de chemins non intersectants.

Démonstration. Il suffit de montrer que la contribution de chaque configuration intersectante est nulle. Si on prend une telle configuration C, on note i_0 le plus petit i tel que C_i intersecte un autre chemin, et C_{j_0} le dernier chemin qu'il intersecte. On construit C'_{i_0} un chemin qui suit C_{i_0} jusqu'au croisement, puis C_{j_0} ensuite, et C'_{j_0} de manière similaire. Cela donne une nouvelle famille, dont la signature est opposée à C, car on a effectué une transposition. Et, cette opération définit une involution sur les familles intersectantes, d'où le résultat. □

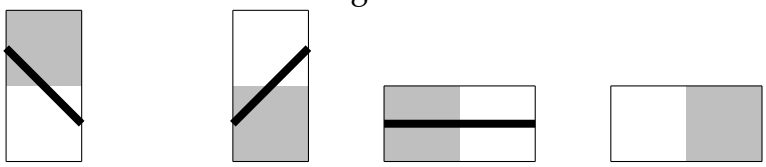
Corollaire 210. Lorsque pour tous $i_1 \leq i_2$ et $j_1 \leq j_2$, tout chemin de s_{i_1} à p_{j_2} intersecte tous ceux de s_{i_2} à p_{j_1}, le membre de droite est égal au nombre de familles non intersectantes.

Remarque 211. Le membre de gauche est le **déterminant** de la matrice $(M_{i,j})$. C'est un objet difficilement contournable en algèbre linéaire.

Remarque 212. Ce lemme se généralise lorsqu'on pondère les arêtes du graphe.

Pavage du diamant

On introduit une bijection entre les pavages du diamant aztèque et une famille de chemins non intersectante traversant celui-ci. Pour cela, on insère des arêtes dans les quatre types de dominos comme sur la figure suivante.



Définition 213. On appelle *chemin de Schröder* dans un réseau carré un chemin reliant deux points de l'axe des abscisses distants de pas, en restant toujours sur ou au-dessus de celui-ci, et en autorisant seulement les pas suivants : avancer de deux cases horizontalement, monter d'une case en diagonale vers le haut, ou descendre d'une case en diagonale vers le bas.
On note s_n le nombre de tels chemins dont les extrémités sont séparées de n pas.

Théoréme 214. Il y a une bijection entre les pavages du diamant aztèque et les familles de chemins de Schröder non intersectantes reliant les sources de coordonnées $(-\frac{1}{2} - i, -n)$ avec $1 \leq i \leq n$ et les puits $(\frac{1}{2} + j, -n)$ avec $1 \leq j \leq n$ familles de chemins du diamant non intersectantes reliant les sources de coordonnées $(\frac{1}{2} - i, i - n)$ [bord inférieur gauche du diamant] et les puits $(\frac{1}{2} - j, n - j)$ [bord inférieurs droit].

Démonstration. On remarque une bijection entre ces familles et les familles C' de chemins du diamant non intersectantes reliant les sources de coordonnées $(\frac{1}{2}-i, i-n)$ [bord inférieur gauche du diamant] et les puits $(\frac{1}{2}-j, n-j)$ [bord inférieurs droit] (il suffit de prolonger judicieusement ces derniers). Un pavage du diamant induit clairement un unique graphe. Pour montrer qu'il s'agit d'une famille C', on constate d'abord qu'on ne peut obtenir de sommet de degré au moins 3 en utilisant notre traçage des arêtes dans les dominos. En regardant les arêtes dans les dominos, il est clair que n chemins partent des cases du bord inférieur gauche, que ces chemins sont obligés d'aller vers la droite à chaque pas et ne qu'ils ne peuvent s'arrêter sur un domino au milieu du diamant. Ces chemins ont donc n points d'arrivée qui sont nécessairement blancs en regardant nos 4 types de dominos. C'est donc le bord inférieur droit du diamant (on voit aisément qu'on ne peut monter assez pour arriver sur le bord supérieur gauche).
Et, si on trace une famille non intersectante, elle induit un pavage : on peut paver les chemins sans intersection avec les dominos des 3 premiers types, il reste à combler les "trous" avec le quatrième type de domino. Pour cela, on considère deux chemins qui relient $(\frac{1}{2}-i, i-n)$ à $(\frac{1}{2}-i, n-i)$ et $(\frac{1}{2}-i+1, i-1-n)$ à $(\frac{1}{2}-i+1, n-i+1)$ (d'autres liaisons ne respecteraient pas la non intersection). On vérifie à chaque pas que l'espace entre les deux est pavable. Pour l'espace éventuel au-dessus du chemin le plus haut, on introduit un chemin fictif (qui pourrait figurer dans le diamant de taille $n+1$) qui longe les bords supérieurs gauche et droit par le dessus. □

Théoréme 215. Il existe $A_n = 2^{\binom{n+1}{2}}$ pavages du diamant aztèque.

Démonstration. D'après le lemme LGV et le théorème 1, $A_n = \sum\limits_{\sigma\in S_n} \prod s_{i,+\sigma(i)}$.
On introduit t_n le nombre de chemins de Schröder entre deux points distants de n pas et qui ne font pas de mouvement horizontal sur l'axe des abscisses. On montre par récurrence que $s_n = \sum s_{n-1-k}s_k$, et $t_n = \sum t_{n-1-k}s_k$ donc que $s_n = 2t_n$.
De plus, il y a une bijection entre les n chemins de Schröder et les $n+1$ chemins de Schröder positifs donc $\sum\limits_{\sigma\in S_n} \prod r_{s,+\sigma(i)} = \sum\limits_{\sigma\in S_{n+1}} \prod t_{i,+\sigma(i)}$. Ainsi, $A_{n+1} = 2^n A_n$ et le résultat en découle. □

Remarque 216. Ce théorème peut se prouver par récurrence, en "dilatant" le diamant de taille n (par des mouvements sur les dominos) pour obtenir un diamant troué de taille $n+1$, les trous étant n carrés 2×2 disjoints. [1]

Autre fait amusant : il y a exactement $\binom{n(n+1)/2}{k}$ pavages avec $2k$ dominos horizontaux.

Le cercle arctique

Quand n tend vers $+\infty$, et qu'on prend un pavage au hasard, on obtient avec grande probabilité une configuration où chaque coin est monochrome, le disque inscrit sur les côté du carré étant au contraire très mélangé. Le bord de cette zone s'appelle "cercle arctique".

Sources

[1] Random Domino Tilings and the Arctic Circle Theorem, W. Jokush, J. Propp, P. Shor, 1995

La bijection de Schaefer

Err 404 texte tapé not found.

2 mercredi 26 après-midi : Louise Gassot

- Qu'est-ce qu'un entier p-adique ? -

C'est un peu comme un nombre réel, mais au lieu d'avoir un nombre infini de décimales à droites de la virgule, un nombre p-adique a un nombre infini de décimales à gauche...

Dans toute la suite, p sera un nombre premier.

Définition 217 (Entier p-adique)**.** Soit p un nombre premier.
On appelle p-cimale un entier a tel que $0 \leq a \leq (p-1)$.
Un entier p-adique est une suite $(a_i)_{i\in\mathbb{N}}$ de p-cimales. On le note de la façon suivante :

$$\dots a_n \dots a_1 a_0.$$

Remarque 218 (Décomposition de Hensel)**.** Si $x = \dots a_n \dots a_1 a_0$ est un entier p-adique, on écrit : $x = \sum_{k=0}^{+\infty} a_k p^k$. Cette écriture est appelée décomposition canonique de Hensel.

Exemple 219. $\dots 1 \dots 11$ est un entier 3-adique.
17 est aussi un entier 3-adique, il s'écrit $\dots 0 \dots 00122$.

Remarque 220. Pour les entiers naturels, la décomposition de Hensel correspond à la décomposition en base p. De plus, un entier naturel est caractérisé par le fait qu'il possède un nombre fini de p-cimales (penser à $\mathbb{R}$!).

Remarque 221. Quel est le lien avec la valuation p-adique ?

C'est très simple : si x est un entier relatif non nul, il a une décomposition de Hensel de la forme $x = \sum_{k=k_0}^{+\infty} a_k p^k$, avec $k_0 \geq 0$ et $a_{k_0} \neq 0$, et alors $v_p(x) = k_0$.

- Opérations élémentaires -

On va maintenant définir les opérations usuelles (addition, soustraction, multiplication, division) entre les entiers p-adiques.

Définition 222 (Addition)**.** L'addition est analogue à celle de $\mathbb{R}$.
Par exemple, dans $\mathbb{Z}_5$:

$$\begin{array}{r} \overset{1}{\dots}\overset{1}{2}\overset{}{4}\overset{1}{3}14 \\ + \dots 13422 \\ \hline \dots 43241 \end{array}$$

Ceci fonctionne bien car les n derniers chiffres du nombre $a+b$ ne dépendent que des n derniers chiffres de a et de b.

Définition 223 (Multiplication)**.** La multiplication est aussi analogue à la multiplication de réels.
Par exemple, dans $\mathbb{Z}_5$:

$$\begin{array}{r} \dots 222 \\ \times \dots 333 \\ \hline \dots 221 \\ + \dots 210 \\ + \dots 100 \\ + \dots 000 \\ \hline \dots 031 \end{array}$$

Ceci fonctionne bien car les n derniers chiffres du nombre $a+b$ ne dépendent aussi que des n derniers chiffres de a et de b.

Exercice 1 Comment s'écrit -1 en p-adiques ?

Solution de l'exercice 1

$$\begin{array}{rccccc} & \ldots & (p-1) & (p-1) & (p-1) \\ + & \ldots & 0 & 0 & 1 \\ \hline & \ldots & 0 & 0 & 0 \end{array}$$

On en déduit qu'en p-adiques, $-1 = \ldots(p-1)\ldots(p-1)$.

La soustraction fonctionne également comme celle que nous utilisons habituellement.

Exercice 2 Comment caractériser les entiers strictement négatifs en fonction de leur écriture en p-adiques ?

Solution de l'exercice 2 Ce sont exatement les entiers p-adiques dont toutes les p-cimales, sauf un nombre fini, sont égales à $(p-1)$.

Proposition 224. $\mathbb{Z}_p$ est un anneau commutatif.

Pour justifier que ces opérations sont licites, on a définir la notion de limite en p-adiques :

Définition 225 (Limite)**.** Soit $(a_n)_{n\geq 1}$ une suite de nombres p-adiques. On dit que cette suite a pour limite le nombre p-adique b si, pour tout nombre k de p-cimales, il existe un rang N tel que, pour tout $n \geq N$, les k dernières p-cimales de a_n sont les mêmes que celles de b.

On voit alors que, comme les p-cimales de droite sont déterminées une fois pour toutes à partir d'un certain moment lorsque nous effectuons une opération, le résultat que nous obtiendront "à la fin du calcul" a bien un sens.

Nous avons vu comment additionner, soustraire, multiplier... mais peut-on faire des divisions en p-adiques ?

Nous allons voir que c'est un peu plus compliqué...

- Division et nombres p-adiques -

Exemple 226. p (qui s'écrit $\ldots 0\ldots 010$) n'a pas d'inverse dans $\mathbb{Z}_p$.

$$\begin{array}{rc} & \ldots??? \\ \times & \ldots 010 \\ \hline & \ldots??0 \\ + & \ldots??0 \\ + & \ldots?00 \\ \hline & \ldots??0 \end{array}$$

Néanmoins, on se doute que seule la division par p pose un problème dans les entiers p-adiques, les autres nombres premiers étant premiers avec p...

Proposition 227. Tous les entiers p-adiques dont la valuation p-adique est nulle possède un inverse dans $\mathbb{Z}_p$.

Démonstration. On commence par les entiers p-adiques α dont la dernière p-cimale (qui correspond a_0 dans la définition) vaut 1.

On pose $\alpha = 1 + \beta$. Alors la dernière p-cimale de β est nulle, et alors pour tout $i \geq 1$, les i dernières p-cimales de β^i sont nulles. Considérer le nombre $1 - \beta + \beta^2 - \beta^3 + \ldots$ a donc bien un sens, et en admettant que les propriétés de l'addition sont préservées pour les sommes infinies,

$$(1+\beta)(1-\beta+\beta^2-\beta^3+\ldots) = 1+\beta-\beta-\beta^2+\beta^2+\cdots = 1$$

Maintenant, si la dernière p-cimale de α vaut $d \neq 0$, on considère d' l'inverse de d modulo p. Alors la dernière p-cimale de $d'\alpha$ est 1 donc on sait calculer son inverse. On a alors $\alpha = \frac{d'}{d'\alpha}$ et il suffit ensuite d'effectuer une multiplication.

Exercice 3 Calculer $\frac{1}{3}$ dans $\mathbb{Z}_5$.

Solution de l'exercice 3 On trouve les coefficients de Bézout (en utilisant par exemple l'algorithme d'Eulclide étendu) pour progresser de décimale en décimale :

$$1 = 3 \times 2 - 5 \times 1$$

donc

$$\frac{1}{3} = 2 + 5 \times \frac{-1}{3}.$$

Or on sait $\frac{-1}{3}$ est un entier p-adique donc la première décimale de $\frac{1}{3}$ est 2. De même,

$$-1 = 3 \times 3 - 5 \times 2 \text{ donc } \frac{-1}{3} = 3 + 5 \times \frac{-2}{3},$$

$$-2 = 3 \times 1 - 5 \times 1 \text{ donc } \frac{-2}{3} = 1 + 5 \times \frac{-1}{3}.$$

Or on a est déjà tombés sur $\frac{-1}{3}$, on a donc une périodicité.
On en déduit : $\frac{1}{3} = \ldots 13 \ldots 13132$.

Exercice 4 Caractériser les nombres rationnels en fonction de leur écriture p-adique.

Solution de l'exercice 4 x est rationnel si, et seulement si son développement p-adique est périodique à partir d'un certain rang.

Si x est rationnel, on peut écrire $x = \frac{a}{b}$ avec a et b premiers entre eux. On pose alors $x_0 = a$ et on écrit la relation de Bézout : $x_n = u_n p + b v_n$, où quitte à faire une division euclidienne par p on peut supposer $0 \leq v_n < p$. Alors, si $u_n = bq_n + x_{n+1}$, avec $0 \leq x_{n+1} < b$, on a

$$\frac{x_n}{b} = (\frac{x_{n+1}}{b} + q_n)p + v_n.$$

Les n premières décimales de x sont alors déterminées à partir des v_n et des q_n.
Comme les x_n sont bornés pas b, la suite (x_n) est périodique à partir d'un certain rang. On va alors retomber sur les mêmes v_n et q_n, donc le développement est périodique à partir d'un certain rang.

Réciproquement, si le développement de x est périodique à partir d'un certain rang, on peut écrire

$$x = a + \sum_{n \geq N} \frac{b}{(p^k)^n}$$

avec a rationnel et b entier. On a alors

$$x = a + \frac{bp^{kN}}{1 - p^k}.$$

Proposition 228. $\mathbb{Q}_p$ est un corps.

Maintenant, nous allons définir l'ensemble $\mathbb{Q}_p$ des nombres p-adiques à partir de $\mathbb{Z}_p$ de la même façon que nous définissons $\mathbb{Q}$ à partir de $\mathbb{Z}$. Pour construire les rationnels, on ajoute à $\mathbb{Z}$ les quotients d'un nombre entier par un nombre entier non nul. Ceci revient à ajouter un inverse pour chaque nombre premier. Dans le cas de $\mathbb{Q}_p$, nous n'aurons besoin d'ajouter un inverse qu'à p.

Définition 229 (Nombre p-adique)**.** Un nombre p-adique est une suite $(a_i)_{i\in\mathbb{Z}}$ de p-cimales telle que $a_i = 0$ pour i assez petit, i.e., telle qu'il existe i_0 tel que $a_i = 0$ pour $i < i_0$. On le note de la façon suivante :

$$\dots a_n \dots a_1 a_0, a_{-1} \dots a_{i_0}$$

Remarque 230. Le nombre p-adique $\dots 00,1$ correspond alors à $\frac{1}{p}$.
La décomposition de Hensel devient alors, avec les notations précédentes,

$$\sum_{k=i_0}^{+\infty} a_k p^k.$$

Remarque 231. Quitte à multiplier d'abord par des puissances de p pour faire les opérations dans $\mathbb{Z}_p$ puis à se ramener à des éléments quelconques de $\mathbb{Q}_p$ en re-divisant par une puissance de p, on remarque que l'on sait toujours faire des additions, soustractions, multiplications et divisions "à virgule" (i.e. dans $\mathbb{Q}_p$).

Remarque 232 (Et si p n'était pas premier ?- Le problème des diviseurs de zéro)**.** Lorsque p est premier, il n'existe pas de nombres p-adiques $a, b \neq 0$ tels que $ab = 0$. En revanche, par exemple si on étudie les décadiques (la définition est la même que pour les p-adiques, mais avec $p = 10$), il existe des diviseurs de zéro...

Proposition 233. $\mathbb{Z}_p$ n'est pas dénombrable.

Démonstration. Il suffit de montrer que l'ensemble des suites binaires est non dénombrable. On utilise l'argument de Cantor. Si on considère une suite $(u^n)_{n\in\mathbb{N}}$ de suites binaires, notons alors $u^n = (u^n_k)_{k\in\mathbb{N}}$ pour tout $n \in \mathbb{N}$. On pose alors $u = (1 - u^k_k)_{k\in\mathbb{N}}$. Le $n^{\text{ème}}$ bit de la suite u sera différent de celui de la suite u^n. Par conséquent, la suite binaire u n'est pas présente dans cette indexation.

Proposition 234. $\mathbb{Z}_p$ est compact, c'est-à-dire que de toute suite d'entiers p-adiques on peut extraire une sous-suite convergente.

Démonstration. Soit $(u_n) \in (\mathbb{Z}_p)^{\mathbb{N}}$. On considère d'abord la première décimale des éléments de la suite. Comme elle ne peut prendre qu'un nombre fini de valeurs, il existe une sous-suite extraite $(u_{\varphi_1(n)})$ d'éléments ayant tous la même première décimale. De cette suite extraite, on extrait une sous-suite $(u_{\varphi_1(\varphi_2(n))})$ d'éléments ayant tous les mêmes deux premières décimales.

On pose alors $v_n = u_{\varphi_1\circ\varphi_2\circ\dots\varphi_n(n)}$. C'est une suite extraite de (u_n) et à partir du rang n, tous les éléments de cette suite ont les mêmes n premières décimales. Cette suite est donc convergente dans les p-adiques.

- Approche analytique aux nombres p-adiques -

On va construire le corps $\mathbb{Q}_p$ à partir des rationnels de la même façon que l'on peut construire $\mathbb{R}$ à partir des rationnels, à partir d'une valeur absolue.

Définition 235 (Valeur absolue)**.** Une valeur absolue sur un corps $\mathbb{K}$ est une aplication $|.| : \mathbb{K} \to \mathbb{R}^*_+$ telle que :

1. $\forall x \in K,\ |x| = 0 \iff x = 0$
2. $\forall (x, y) \in K^2,\ |x \times y| = |x| \times |y|$
3. $\forall (x, y) \in K^2,\ |x + y| \leq |x| + |y|$

Définition 236. On définit la valeur absolue p-adique par :
$\forall x \in \mathbb{Q}$, $|x|_p = (\frac{1}{p})^{v_p(x)}$ ($|0| = 0$)

Proposition 237. La valeur absolue p-adique ainsi définie est une valeur absolue ! Elle vérifie même

$$\forall (x, y) \in \mathbb{Q}^2,\ |x + y| \leq \max(|x|, |y|)$$

On parle de valeur absolue ultramétrique, ou non archimédienne (et cela conduit à plein de propriétés rigolotes !).

Remarque 238. Tout entier p-adique a une valeur absolue inférieure ou égale à 1.

Définition 239 (Construction de $\mathbb{Q}_p$)**.** De la valeur absolue p-adique, on déduit une distance d sur $\mathbb{Q}$ par :
$d(x, y) = |x - y|_p$
$\mathbb{Q}_p$ est alors $\mathbb{Q}$ auquel on a ajouté les limites des suites dites "de Cauchy" pour cette valeur absolue (avec les décimales, ce sont les suites qui finissent par avoir les mêmes décimales à partir d'un certain rang...). Pour comparaison, $\mathbb{R}$ peut être construit de la même manière, mais avec la valeur absolue usuelle.

Remarque 240. La notion de limite que nous avons définie précédemment (i.e. le fait que les dernières décimales ne changent pas), se réécrit en termes de valeur absolue de la façon suivante : la suite (u_n) a pour limite l si

$$|u_n - l|_p \underset{n \to +\infty}{\longrightarrow} 0\ .$$

Théoréme 241 (Ostrowski)**.** Les valeurs absolues sur $\mathbb{Q}$ sont toutes associées à l'une des trois valeurs absolues suivantes :

1. La valeur absolue triviale, définie par
$$|x| = \begin{cases} 0 & \text{si } x = 0 \\ 1 & \text{si } x \neq 0. \end{cases}$$
2. La valeur absolue usuelle, définie par
$$|x| = \begin{cases} x & \text{si } x \geq 0 \\ -x & \text{si } x < 0. \end{cases}$$
3. La valeur absolue p-adique pour un nombre premier p fixé.

- Lemme de Hensel -

Ceux qui ont parcouru le poly d'arithmétique disponible sur le site d'Animath auront certainement rencontré le lemme de Hensel sous la forme suivante :

Théoréme 242 (Lemme de Hensel, première forme)**.** S'il existe $x \in \mathbb{Z}$ tel que

$$P(x) \equiv 0[p] \quad \text{et} \quad P'(x) \not\equiv 0[p],$$

alors il existe $y \in \mathbb{Z}$ tel que

$$P(y) = 0[p^n] \quad \text{et} \quad y \equiv x[p].$$

Exercice 5 Montrer qu'il existe $\alpha \in \mathbb{Z}$ tel que $\alpha^2 \equiv 2[7^3]$ et $\alpha \equiv 3[7]$.

Solution de l'exercice 5 On applique le lemme de Hensel à $P(X) = X^2 - 2$ et $x = 3$. On a alors $P(x) = 7 \equiv 0[7]$ et $P'(x) = 6 \not\equiv 0[7]$.

Nous allons nous intéresser à un rafinement p-adique de ce lemme :

Théoréme 243 (Lemme de Hensel p-adique)**.** Soit $P \in \mathbb{Z}[X]$. On suppose qu'il existe $x \in \mathbb{Z}_p$tel que $|P(x)|_p < |P'(x)|_p^2$. Alors il existe $y \in \mathbb{Z}_p$, racine de P, vérifiant : $|y - x|_p < |P'(x)|_p$ et $|P'(y)|_p = |P'(x)|_p$.

Démonstration. On applique la méthode de Newton p-adique. On pose $a_1 = x$ et on considère la suite (a_n) définie par :

$$a_{n+1} = a_n - \frac{P(a_n)}{P'(a_n)}.$$

On justifiera l'existence de cette suite par récurrence, en montrant de plus les trois conditions suivantes :

1. $|a_n|_p \leq 1$
2. $|P'(a_n)|_p = |P'(a_1)|_p$
3. $|P(a_n)|_p \leq |P'(a_1)|_p^2 t^{2^{n-1}}$ où $t = \frac{|P(x)|_p}{|P'(x)^2|_p} < 1$

Les conditions sont évidemment respectées pour $n = 1$.
Supposons les conditions respectées au rang n.

1. $|P'(a_n)|_p = |P'(a_1)|_p > 0$ donc $P'(a_n) \neq 0$: a_{n+1} est bien défini. De plus, $\frac{|P(a_n)|_p}{|P'(a_n)|_p} \leq |P'(a_1)|_p t^{2^{n-1}} \leq 1$ donc a_{n+1} est un entier p-adique.
2. Pour un polynôme $F \in \mathbb{Z}_p[X]$, comme $X - Y | X^i - Y^i$ pour tout i, il existe un polynôme $G \in \mathbb{Z}_p[X, Y]$ tel que $F(X) - F(Y) = (X - Y)G(X, Y)$. En appliquant ce résultat à P', on en déduit que
$$P'(a_{n+1}) - P'(a_n) = (a_{n+1} - a_n)z$$
avec $z \in \mathbb{Z}_p$. Par conséquent,
$$|P'(a_{n+1}) - P'(a_n)|_p \leq |a_{n+1} - a_n|_p = \frac{|P(a_n)|_p}{|P'(a_n)|_p} < |P'(a_1)|_p.$$
Comme $|P'(a_n)|_p = |P'(a_1)|_p$, on en déduit que $|P'(a_{n+1})|_p = |P'(a_1)|_p$.
3. Pour tout polynôme $F \in \mathbb{Z}_p[X]$, il existe un polynôme $G \in \mathbb{Z}_p[X, Y]$ tel que $F(X + Y) = F(X) + F'(X)Y + G(X, Y)Y^2$. Appliqué à P, cela donne l'existence de $z \in \mathbb{Z}_p$ tel que
$$P(a_{n+1}) = P(a_n) + P'(a_n)\left(-\frac{P(a_n)}{P'(a_n)}\right) + z\left(-\frac{P(a_n)}{P'(a_n)}\right)^2,$$

ce qui donne

$$P(a_{n+1}) = z\left(\frac{P(a_n)}{P'(a_n)}\right)^2.$$

On en déduit que

$$|P(a_{n+1})|_p \leq \left(\frac{|P(a_n)|_p}{|P'(a_n)|_p}\right)^2 \leq |P'(a_1)|_p^2 t^{2^n}.$$

Ce qui achève la récurrence.

Enfin, on a

$$|a_{n+1} - a_n|_p = \frac{|P(a_n)|_p}{|P'(a_n)|_p} \leq |P'(a_1)|t^{2^{n-1}} \underset{n\to+\infty}{\longrightarrow} 0.$$

Dans $\mathbb{Z}_p$, cette condition implique que la suite (a_n) a une limite, que nous noterons y. Les conditions ci-dessus impliquent que $|P'(y)|_p = |P'(x)|_p$ et que $P(y) = 0$.

De plus, grâce au caractère ultramétrique de la valeur absolue,

$$|y - x|_p \leq \sup_{n\geq 1} |a_{n+1} - a_n|_p < |P'(a_1)|_p.$$

Exercice 6 Montrer que $P(X) = X^4 - 7X^3 + 2X^2 + 2X + 1$ a une racine y dans $\mathbb{Z}_p$ telle que $|y - 2|_3 < \frac{1}{3}$ (ses deux dernières décimales sont donc $\ldots 02$).

Solution de l'exercice 6 $P(2) = -27$ et $P'(2) = -42$ donc $|P(2)|_3 = \frac{1}{27}$ et $|P'(2)|_3 = \frac{1}{3}$. On a donc bien $|P(2)|_3 < |P'(2)|_3^2$, et il suffit alors d'appliquer le lemme de Hensel.

Théoréme 244 (Lemme de Hensel, deuxième (troisième) version)**.** Soit $f \in \mathbb{Z}_p[X]$ et $\overline{f} \in \mathbb{Z}/p\mathbb{Z}[X]$ sa classe modulo p. Si $\overline{f} = \overline{g}\overline{h}$, où $\overline{g} \in \mathbb{Z}/p\mathbb{Z}[X]$ et $\overline{h} \in \mathbb{Z}/p\mathbb{Z}[X]$ sont premiers entre eux, il existe $g, h \in \mathbb{Z}_p[X]$ tels que $g \in \overline{g}$, $h \in \overline{h}$ et $f = gh$

Démonstration. Soient $f^*, g^*, h^* \in \mathbb{Z}[X]$ des représentants respectifs des polynômes $\overline{f}, \overline{g}$ et $\overline{h}$, et de même degré qu'eux.

On dira qu'un polynôme $P \in \mathbb{Z}_p[X]$ est congru à zéro modulo p^n si tous ses coefficients ont une valuation p-adique supérieure ou égale à n.

On construit deux suites de polynômes $(g_n)_{n\geq 1} \in (\mathbb{Z}_p[X])^{\mathbb{N}}$ et $(h_n)_{n\geq 1} \in (\mathbb{Z}_p[X])^{\mathbb{N}}$ de la façon suivante :

$$\begin{cases} g_1 = g^* \\ h_1 = h^* \end{cases}$$

et vérifiant les relations suivantes, pour tout $n \geq 2$:

$$(*)\begin{cases} g_n \equiv g_{n-1}[p^{n-1}] \\ h_n \equiv h_{n-1}[p^{n-1}] \\ \operatorname{pgcd}(g_n, h_n) \equiv 1[p] \\ f \equiv g_n h_n[p^n] \\ \deg(f - g_n h_n) < \deg f \end{cases}$$

En posant $g_0 = X^{\deg f}$, $h_0 = a_0$ où a_0 est le coefficient dominant de f, les conditions sont réalisées pour $n = 1$.

Supposons avoir construit ces deux suites jusqu'au rang n. Posons

$$\phi_n = \frac{f - g_n h_n}{p^n}.$$

On a alors : $\phi_n \in \mathbb{Z}_p[X]$ et $\deg \phi_n < \deg f$.
De plus, comme $\mathrm{pgcd}(g_n, h_n) = 1$, d'après le théorème de Bézout dans $\mathbb{Z}/p\mathbb{Z}[X]$, il existe deux polynômes $u_n, v_n \in \mathbb{Z}_p[X]$, tels que $\deg u_n < \deg g_n$, $\deg v_n < \deg h_n$ et

$$u_n h_n + v_n g_n \equiv \phi_n[p].$$

On pose alors

$$\begin{cases} g_{n+1} = g_n + u_n p^n \\ h_{n+1} = h_n + v_n p^n \end{cases}$$

Alors

$$g_{n+1} h_{n+1} \equiv g_n h_n + \phi_n p^n [p^{n+1}]$$

donc

$$f - g_{n+1} h_{n+1} \equiv f_n - g_n h_n - \phi_n p^n \equiv 0[p^{n+1}].$$

De plus, $g_{n+1} \equiv g_1[p]$ et $h_{n+1} \equiv h_1[p]$ donc $\mathrm{pgcd}(g_{n+1}, h_{n+1}) \equiv 1[p]$.
Enfin, $\deg(f - g_{n+1}h_{n+1}) < \deg f$, donc les conditions $(*)$ sont réalisées à l'ordre $n+1$.

Les polynômes g_n et h_n sont de degré fixe, de plus la condition $(*)$ implique que leurs coefficients convergent dans $\mathbb{Z}_p$. On en déduit que les polynômes g_n et h_n convergent vers des polynômes $g, h \in \mathbb{Z}_p[X]$ de même degré tels que $f = gh$.

- Les nombres p-adiques, à quoi ça sert ? -

Un intérêt des nombres p-adiques réside dans l'étude des équations diophantiennes. Une équation diophantienne est de la forme $P(X_1, \ldots, X_n) = 0$, où $P(X_1, \ldots, X_n) \in \mathbb{Z}[X_1, \ldots, X_n]$. Nous allons nous intéresser aux solutions entières $(x_1, \ldots, x_n) \in \mathbb{Q}^n$ de ces équations. Le théorème de Hasse-Minkowski, énoncé ci-dessous, a été démontré dans les années 1920 par Hasse et constitue le premier résultat significatif illustrant l'utilité des nombres p-adiques.

Théoréme 245 (Hasse-Minkowski)**.** Un polynôme de degré au plus 2 $P(X_1, \ldots, X_n) \in \mathbb{Q}[X_1, \ldots, X_n]$ (ou a valeurs dans une extension finie de $\mathbb{Q}$) a un point d'annulation $(x_1, \ldots, x_n) \in \mathbb{Q}^n$ si, et seulement si il a un point d'annulation réel et un point d'annulation dans $\mathbb{Q}_p$ pour tout p premier.

Exercice 7 Montrer que l'équation $x^2 - 2$ n'a pas de solution dans $\mathbb{Q}_5$. En déduire que $\sqrt{2}$ est irrationnel.

Solution de l'exercice 7 Si a est une solution de cette équation, alors $|a|_p^2 = |2|_p = 1$ donc $|a|_p = 1$. De plus, la dernière décimale de a^2 est un 2. Or 2 n'est pas un carré modulo 5.
L'irrationnalité de $\sqrt{2}$ se déduit alors du théorème de Hasse-Minkowski.

- Théorème de Skolem-Mahler-Lech -

Définition 246. Une suite complexe $(u_n)_{n\in\mathbb{N}}$ est appelée suite récurrente linéaire d'ordre m s'il existe des nombres complexes $a_0, \ldots, a_m \in \mathbb{C}$ tels que $a_0, a_m \neq 0$ telles que, pour tout $n \in \mathbb{N}$,

$$a_0 u_n + \cdots + a_m u_{n+m} = 0.$$

Exemple 247. La suite de Fibonacci est une suite récurrente linéaire d'ordre 2. Elle est en effet définie par la relation :

$$u_n + u_{n+1} - u_{n+2} = 0$$

pour tout $n \in \mathbb{N}$, avec les conditions initiales $u_0 = u_1 = 1$.

Nous allons nous intéresser dans cette partie au théorème suivant :

Théoréme 248 (Théorème de Skolem-Mahler-Lech)**.** Soit $(u_n)_{n\in\mathbb{N}}$ une suite récurrente linéaire. Alors les n tels que $u_n = 0$ sont, sauf peut-être un nombre fini d'entre eux, les termes d'un nombre fini de progressions arithmétiques de même raison. Formellement, il existe $N \in \mathbb{N}^*$, un ensemble fini T et un ensemble $S \subset \{0, 1, \ldots, N-1\}$ (S peut être vide) tels que

$$u_n = 0 \Leftrightarrow n \in T \cup (S + N\mathbb{Z})$$

Ce théorème a été montré par Skolem en 1934 pour les suites récurentes linéaires rationnelles. Mahler l'a étendu aux extensions finies de $\mathbb{Q}$ en 1935, et Lech à tout corps de caractéristique 0 en 1953.

Nous présenterons la démonstration dans ses grandes lignes.

D'abord, nous aurons besoin d'un résultat classique sur les suites récurrentes linéaires :

Proposition 249. S'équivalent :

1. (u_n) est une suite récurrente linéaire d'ordre m, définie par les relations, pour tout $n \in \mathbb{N}$, $a_0u_n + \cdots + a_mu_{n+m} = 0$.
2. Pour tout n, $u_n = \sum_{i=1}^{s} P_i(n)\lambda_i^n$ pour certains nombres distincts deux à deux $\lambda_1, \ldots, \lambda_s \in \mathbb{C}$ et certains polynômes $P_1, \ldots, P_s \in \mathbb{C}[X]$ tels que $(\deg P_i+1) \leq m_i$, pour certains entiers m_i. Avec la notation du 1., les nombres λ_i sont les racines du polynôme $a_0 + a_1X + \cdots + a_mX^m$ et m_i est la multiplicité de la racine λ_i pour tout i.

Nous aurons aussi besoin de quelques résultats sur les séries entières :

Définition 250. Une fonction $f : D(a, r) \to K$, où K est une extension finie de $\mathbb{Q}_p$, et $D(a, r)$ le disque de centre a et de rayon r dans $\mathbb{Q}_p$, est une série entière si $f(z) = \sum_{k=0}^{+\infty} \alpha_k(z - a)^k$ (et que cette somme est bien définie) pour tout $z \in D(a, r)$.

Proposition 251. Les zéros d'une série entière non identiquement nulle à valeurs dans K sont isolés. En d'autres termes, si $f(x) = 0$, il existe ρ tel que, pour tout $y \in D(a, r)$ tel que $|y - x|_p \leq \rho$, alors $f(y) \neq 0$.

On déduit de la compacité de $\mathbb{Z}_p$ le résultat suivant :

Corollaire 252. Une série entière sur $\mathbb{Z}_p$ non identiquement nulle a un nombre fini de zéros.

L'idée de la preuve est la suivante :

On écrit la suite récurrente linéaire (u_n) sous la forme $u_n = P_1(n)\lambda_1^n + \cdots + P_s(n)\lambda_s^n$. Pour p premier bien choisi, on se place dans une extension de $\mathbb{Q}_p$, contenant $\lambda_1, \ldots, \lambda_n$, munie d'une valeur absolue $|.|$ étendant $|.|_p$, et tel qu'il existe un entier m tel que $\log \lambda_i^m$ soit défini pour tout i (admis). On peut alors considérer, pour tout entier $0 \leq h \leq m - 1$,

$$f_h(z) = \sum_{i=1}^{s} P_i(h + mz)\lambda_i^h\lambda_i^{mz}.$$

f_h est alors une série entière convergeant pour tout $z \in \mathbb{Z}_p$.
On vérifie que $f_h(k) = u_{h+mk}$ pour tout entier k.
Il y a alors deux cas, selon les valeurs de h :

1. f_h est identiquement nulle : alors $u_{h+mk} = 0$ pour tout k, cela correspond à $h \in S$.
2. f_h a un nombre fini de zéros : les indices correspondants sont alors dans T.

X. Les soirées

Contenu de cette partie

1 mardi 18 : Xavier Caruso

- Dessine-moi une planète -

Comment peut-on se rendre compte que la Terre est une boule (et pas un disque ou un plan infini) ? Plus généralement, comment peut-on déterminer la forme de la planète sur laquelle on vit ? Bien entendu, une possibilité est la regarder « de loin » après s'être échappé dans l'espace... mais sans cela, est-ce encore possible ? Ou même encore, peut-on déterminer la forme de la planète sur laquelle on vit en n'utilisant aucune donnée venant de l'espace [1] ? Cette dernière hypothèse peut paraître beaucoup trop forte mais elle prend tout son sens lorsque l'on cherche à connaître non pas la forme d'une planète mais plutôt celle de l'univers tout entier. Les dernières théoriques physiques en vogue laissent penser qu'il possède une géométrie très complexe et il est évident, par définition même de l'univers, que le physicien ne peut compter sur aucune information extérieure pour l'aider à appréhender cette géométrie.

Le but de cet exposé est de présenter quelques techniques de nature mathématique pour répondre à la question posée ci-dessus dans le cas des surfaces (donc des planètes, plutôt que de l'univers).

Reconnaître la forme

Voici quelques exemples de surfaces, que nous allons chercher à distinguer entre elles :

1. Par exemple, sans utiliser le Soleil ou la Lune, si l'on parle de la Terre.

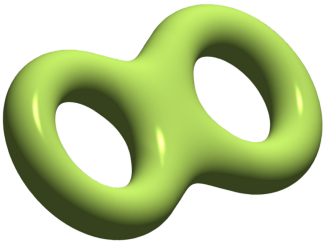
— le disque :

— la sphère :

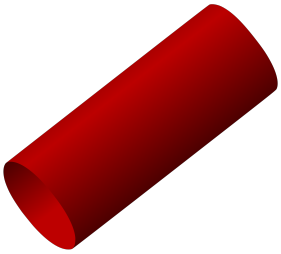
— la bouée, connue sous le nom mathématique de *tore* :

(X.1)

— le tore à deux trous :



— le cylindre :



— le ruban de Moebius, qui s'obtient en recollant les deux petits bords d'une bande de

papier, le coin du haut sur celui du bas et *vice et versa* :

Le bord d'une surface. Un premier élément qui permet de distinguer deux surfaces est l'existence ou l'inexistence d'un bord [2]. Sur les exemples sus-cités, cela permet de mettre d'un côté la sphère et les tores (qui ne possèdent pas de bord) et d'un autre côté le disque, le cylindre et le ruban de Moebius (qui en possèdent un).

La méthode peut en fait s'affiner car elle permet également de distinguer deux surfaces qui auraient des bords différents. Par exemple, le bord du cylindre est la réunion de deux cercles alors que celui de la sphère est formé d'un unique cercle. La sphère et le cylindre sont donc des surfaces différentes. Il est à noter toutefois que le bord du ruban de Moebius est lui aussi formé d'un unique cercle. L'argument présenté ici ne permet donc pas de la distinguer du disque.

L'orientabilité d'une surface. Pour distinguer la disque du ruban de Moebius, une possibilité est de faire intervenir l'orientation. La définition mathématique est assez complexe mais l'intuition est plutôt simple : si un habitant d'une planète en forme de ruban de Moebius fait une fois le tour de sa planète pour revenir à son point de départ, il se retrouve la tête en bas et les pieds en haut — ou encore, la main gauche à droite et la main droite à gauche (comme dans un miroir). On dit que le ruban de Moebius est *non orientable*. Par contre, le disque, lui, l'est : un habitant d'une planète en forme de disque ne verra jamais sa gauche et sa droite inversées. De la même manière, la sphère, le cylindre et les tores sont *orientables*.

Géométrie des lacets. Un outil particulièrement puissant pour distinguer les surfaces entre elles consiste à dessiner des lacets sur celle-ci puis, éventuellement, à les déformer. Mathématiquement, un lacet est défini comme une courbe fermée (tracée sur la surface) dont un certain point, que l'on appelle traditionnellement l'*origine*, est distingué.

Sur une sphère, un lacet sépare la surface en deux parties bien déterminées. Typiquement, si l'on enferme un terrien à l'intérieur d'une courbe fermée, il ne pourra pas rejoindre une personne qui vit à l'extérieur de la courbe sans traverser cette dernière. Or, ceci n'est pas automatique sur le tore : en effet, si on trace un lacet qui entoure la bouée, deux habitants qui sont *a priori* de part et d'autre du lacet pourront toujours se rejoindre en faisant le tour par l'autre côté.

Un autre moyen de distinguer la sphère du tore est d'étudier la déformation des lacets. Si un lacet est tracé sur la sphère (et fixée en une origine), il est toujours possible de le déformer

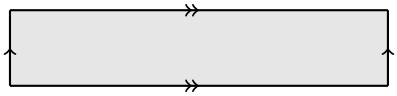
2. Mathématiquement, le bord d'une surface S est défini comme l'ensemble des points M de S au voisinage desquels la surface ressemble à un demi-disque (et non pas à un disque entier).

jusqu'à ce qu'il ne soit plus qu'un point. Par contre, ceci n'est pas possible avec tous les lacets du tore, un exemple étant le lacet déjà considéré précédemment. Cette dernière méthode permet aussi de distinguer le tore à un trou du tore à deux trous, mais ceci est plus compliqué.

Représentation plane des surfaces.

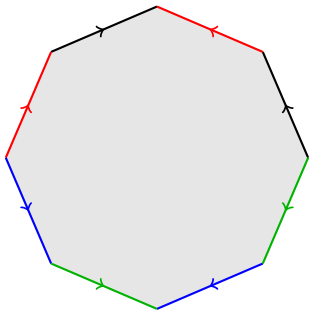
Beaucoup de surfaces s'obtiennent à partir d'une surface plane (typiquement une feuille de papier) en recollant certains côtés sur certains autres. Souvent, plutôt que de dessiner la surface comme nous l'avons fait jusqu'alors, il est plus commode de dessiner la surface plane et d'indiquer sur les recollements celles-ci. Typiquement, le ruban de Moebius peut être représenté ainsi :

La partie coloriée représente la surface, tandis que les flèches indiquent que l'on recolle les deux bords verticaux. Le fait que les flèches pointent dans des directions opposées signifie que l'on recolle le haut du bord gauche sur le bas du bord droit et *vice et versa*. Le cylindre, quant à lui, possède une représentation similaire dans laquelle les flèches pointent dans la même direction. Plus intéressant : le tore, lui aussi, admet une représentation de ce type que voici :

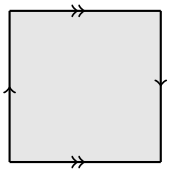


(X.2)

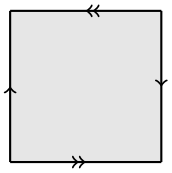
la notation indiquant que les deux côtés portant une flèche simple sont recollés entre eux, de même que les deux côtés portant une double flèche. Pour le tore à deux trous, on a [3] :



Ceci permet d'imaginer tout un éventail de nouvelles surfaces. En restant sur une base carrée, en voici deux nouvelles :



Bouteille de Klein



Plan projectif réel

3. On laisse en exercice au lecteur le soin de s'en convaincre... ainsi que de généraliser la construction afin d'obtenir le tore à g trous.

On peut démontrer (exercice laissé au lecteur) que le plan projectif réel s'obtient également des deux manières suivantes :

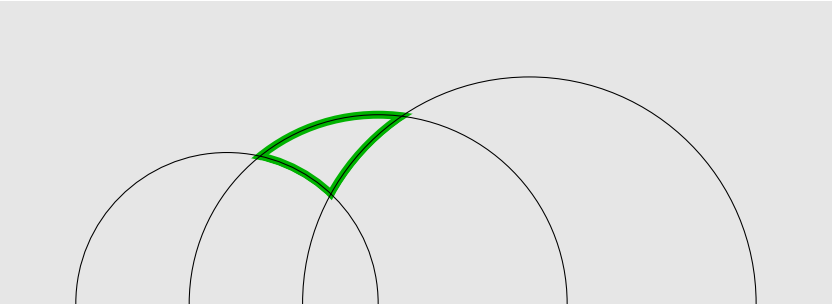
— soit en collant un disque sur le bord d'un ruban de Moebius (qui, on le rappelle, est un cercle),
— soit en identifiant dans une sphère les points antipodaux.

Le lien entre ces deux descriptions se fait en remarquant que le ruban de Moebius correspond à une petite bande autour d'un grand cercle (*e.g.* l'équateur) de la sphère. Étudier la déformation des lacets sur le plan projectif réel aboutit à quelques surprises. Par exemple, sur la représentation sphérique, on constate qu'un grand cercle définit un lacet qui est déformable en un point (puisqu'il l'est déjà sur la sphère). Par contre, un demi grand cercle définit lui aussi un lacet, mais celui-ci n'est pas déformable en un point. Autrement dit, dans le plan projectif réel, il existe un lacet qui n'est pas déformable mais qui le devient lorsqu'il est parcouru deux fois ! Cette propriété permet, par exemple, de distinguer le plan projectif des tores.

Considérations métriques

Jusqu'à présent, nous avons travaillé uniquement sur la « forme » des surfaces mais pas encore sur les distances ou les angles. Or, pour se représenter la planète sur laquelle on vit, un moyen naturel est de réaliser des mesures et d'observer d'éventuelles aberrations. C'est ainsi, par exemple, que nous, humains, pouvons ainsi nous rendre compte que la Terre sur laquelle nous vivons n'est pas plate mais ronde. En effet, sur une Terre plate, la somme des angles d'un triangle doit toujours être égale à $180°$. Or ceci n'est pas le cas sur notre Terre [4] : par exemple, un triangle dont un sommet se situe au pôle nord et les deux autres sur l'équateur possède deux angles droits et un troisième angle pouvant prendre n'importe quelle valeur entre $0°$ et $90°$. En réalité, sur Terre, la somme des angles d'un triangle non aplati excède toujours $180°$, cet excès étant directement proportionnel à l'aire du triangle.

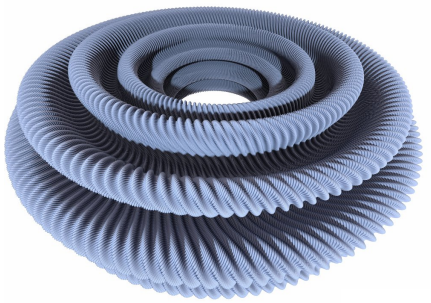
Il existe également des surfaces sur lesquelles les triangles voient la somme de leurs angles strictement inférieure à $180°$. Un exemple typique est ce que l'on appelle le *plan hyperbolique* qui peut être défini comme un demi-plan sur lequel les distances s'allongent lorsque l'on s'approche du bord [5]. Dans cette géométrie, les droites — c'est-à-dire les chemins les plus courts entre deux points — sont les demi-cercles perpendiculaires au bord du demi-plan et les triangles ressemblent à cela :



4. Bien que, sauf à dessiner des triangles immenses, il faille des instruments très précis pour s'en apercevoir...
5. Précisément, si le demi-plan en question est mis en bijection avec l'ensemble des nombres complexes de partie réelle strictement positive, la distance entre les points d'affixe z_1 et z_2 est donnée par la formule $\log \frac{|z_1-\bar{z}_2|+|z_1-z_2|}{|z_1-\bar{z}_2|-|z_1-z_2|}$.

Si l'on préfère, il est aussi possible de constater des aberrations sur les distances. Par exemple, sur une sphère, il n'est *pas* vrai que le périmètre d'un cercle de rayon $r > 0$ est $2\pi r$; il est, en réalité, toujours strictement inférieur à cette valeur, la différence étant d'autant plus ténue que r est petit par rapport au rayon de la sphère. Pour illustrer ceci, regardons l'équateur sur Terre. Son périmètre est $2\pi R$ où R désigne le rayon de la Terre. Par ailleurs, il consiste exactement en l'ensemble des points dont la distance (sur Terre !) au pole nord est $\frac{\pi R}{2}$. Il apparaît ainsi comme un cercle de rayon $\frac{\pi R}{2}$ et a bel et bien un périmètre qui est strictement inférieur à ce qu'il devrait être si la Terre était plate, à savoir $\pi^2 R$.

Il se trouve que, de la même manière, il est possible de distinguer par des arguments métriques le tore bombé (la bouée) représenté en (X.1) du tore plat obtenu par recollement comme indiqué en (X.2) : sur le tore plat, les cercles de rayon r (suffisamment petit pour éviter les chevauchements) ont un périmètre exactement égal à $2\pi r$ tandis que celui-ci est légèrement inférieur à $2\pi r$ sur le tore bombé ! Malgré tout, il est possible de compenser la courbure afin de représenter le tore plat dans l'espace ambiant. Voici ce que l'on obtient [6] :



2 mercredi 19 : Les Olympiades de Mathématiques

Le but de la soirée était de présenter aux élèves les différentes olympiades de mathématiques auxquelles la France participe, et de faire intervenir les nombreux élèves qui ont été à une ou plusieurs de ces olympiades.

Les IMO (International Mathematical Olympiad) :

C'est l'olympiade la plus connue et la plus ancienne. Elle a lieu tous les ans depuis 1959 en été, et une centaine de pays y participent actuellement. Chaque pays envoie une équipe de 6 élèves maximum (la seule condition étant qu'ils ne soient pas inscrits dans un établissement d'enseignement supérieur), accompagnés d'un chef de délégation et d'un chef de délégation adjoint. Le chef de délégation arrive sur place un peu avant le reste de l'équipe, et ne les rejoint qu'à la fin des épreuves, car il participe à la sélection des problèmes. Les épreuves durent deux fois quatre heures et demie, et sont reparties sur deux matinées consécutives. Il y a trois problèmes chaque jour, de difficulté croissante, chaque problème étant noté sur 7. Après les épreuves, pendant que les copies sont corrigées et notées par les chefs de délégation, des activités et des sorties sont organisées pour les élèves. L'olympiade se termine par une cérémonie de clôture à laquelle des médailles sont distribuées : sur environ 600 participants, 50 personnes reçoivent une médaille d'or, 100 une médaille d'argent et 150 une médaille de

6. Cette figure a été obtenue récemment par V. Borelli, S. Jabrane, F. Lazarus, D. Rohmer, B. Thibert.

bronze. Ceux qui n'ont pas obtenu de médaille mais ont eu la note maximale (c'est-à-dire 7) à au moins un problème obtiennent une mention honorable.

Cette année, les IMO ont eu lieu au Chiang-Mai, en Thaïlande. La délégation française était composée de Vincent Bouis, Félix Breton, Colin Davalo, Florent Noisette, Adrien Lemercier et Julien Portier. Les élèves ont remporté trois médailles d'argent (Vincent, Florent et Adrien) et autant de bronze (Félix, Colin et Julien). Au classement des nations, la France arrive en 14ème position, son meilleur résultat depuis 1992 !

Avis aux amateurs d'exotisme : les IMO 2016 auront lieu à Hong-Kong !

Les JBMO (Junior Balkan Mathematical Olympiad) :

Cette olympiade se tient tous les ans au mois de juin dans un pays des Balkans. La France y participe en tant que pays invité depuis 2013. Le principe est à peu près le même qu'à l'IMO, sauf que cette olympiade est destinée aux élèves très jeunes : il faut avoir moins de 15 ans et demi le jour de l'épreuve. La spécificité de cette compétition est qu'il n'y a qu'une journée d'épreuves, consistant en quatre problèmes à faire en quatre heures et demie, notés chacun sur 10.

Les JBMO 2015 ont eu lieu à Belgrade, en Serbie. La délégation française était composée de Pierre-Alexandre Bazin, Romain Caplier, Thomas Fusellier, Yakob Kahane, Juraj Rosinsky et Jean Zablocki. Pierre-Alexandre, Romain, Thomas, Yakob et Juraj ont remporté une médaille de bronze.

Les EGMO (European Girls' Mathematical Olympiad) :

Cette olympiade est une création récente, puisqu'elle n'existe que depuis 2012. Elle fonctionne essentiellement de la même façon que les IMO, mais les délégations sont composées de quatre personnes maximum, qui doivent toutes être des filles. L'olympiade a lieu tous les ans au mois d'avril. Une autre différence est le fait que la séparation entre les chefs de délégation et les équipes soit beaucoup moins stricte : pendant les deux olympiades auxquelles la France a déjà participé, tout le monde était dans le même hôtel, et nous pouvions passer du temps ensemble, à condition bien sûr de ne pas parler de maths ! Cette olympiade a connu un succès grandissant depuis sa création, regroupant cette année 22 pays européens et 7 pays invités (dont les États-Unis).

En 2015, les EGMO ont eu lieu à Minsk, en Biélorussie. La délégation française était composée de Albertine Devillers, Clara Ding, Myriam Qrichi Aniba et Lucie Wang. Clara Ding et Lucie Wang ont remporté une médaille d'argent.

L'an prochain, la compétition se déroulera à Busteni, en Roumanie.

Comment participer ? L'OFM, mode l'emploi

L'OFM (Olympiade Française de Mathématiques) est une préparation à toutes ces compétitions internationales. Elle se fait par correspondance : les élèves sélectionnés reçoivent approximativement tous les mois des *envois*, c'est-à-dire des feuilles d'exercices, à faire et à renvoyer. Ils récupèrent leurs copies plus tard pour avoir un retour sur leur travail. Cette préparation est complétée par un stage pendant les vacances d'hiver, ainsi que quelques tests en temps limité qui visent en particulier à sélectionner les équipes pour les différentes olympiades internationales.

Afin de rejoindre l'OFM, il faut participer au test d'entrée, qui s'effectue chaque année début octobre.

Pour plus d'informations et pour s'inscrire, une seule adresse :

`www.animath.fr`

3 samedi 22 : Joseph Najnudel

- Échanger des choses au hasard, qu'est-ce que ça donne ? -

Le groupe symétrique

Imaginons que l'une personne ait n paires de chaussettes rangées dans n tiroirs numérotés de 1 à n, une par tiroir. Supposons qu'après s'être habillée un certain nombre de fois, cette personne se retrouve à nouveau avec une paire de chaussette dans chacun des n tiroirs. Cependant, les places des chaussettes ont pu changer. La chaussette initialement dans le tiroir 1 se retrouve dans un des n tiroirs, dont le numéro sera noté ici $\sigma(1)$, la chaussette initialement dans le tiroir 2 se retrouve dans un autre tiroir, numéro $\sigma(2)$, et ainsi de suite jusqu'à la chaussette du tiroir n qui se retrouve dans le tiroir $\sigma(n)$. Les entiers $\sigma(1), \sigma(2), \ldots, \sigma(n)$ sont exactement les entiers $1, 2, \ldots, n$, pris dans un ordre quelconque.

L'action qui consiste à mettre dans le tiroir $\sigma(j)$ la chaussette initialement dans le tiroir j, pour tout j entre 1 et n, s'appelle une *permutation*. Elle est codée par la bijection σ de $\{1, \ldots, n\}$ dans $\{1, \ldots, n\}$: pour cette raison, on identifiera cette permutation à σ.

Si on met la chaussette du tiroir j dans le tiroir $\sigma(j)$ pour tout j, et ensuite la chaussette du tiroir k dans le tiroir $\tau(k)$ pour tout k, σ, τ étant deux bijections de $\{1, \ldots, n\}$ dans $\{1, \ldots, n\}$, la chaussette initialement dans le tiroir j se retrouve à la fin dans le tiroir $\tau(\sigma(j)) = \tau \circ \sigma(j)$ pour tout j.

Ainsi, effectuer des permutations successives revient à composer les bijections de $\{1, \ldots, n\}$ correspondantes.

L'ensemble de toutes les bijections de $\{1, \ldots, n\}$, muni de l'opération de composition des bijections $(\sigma, \tau) \mapsto \sigma\tau := \sigma \circ \tau$, forme ce qu'on appelle un *groupe*, ce qui signifie que les propriétés suivantes sont vérifiées :

— La composition des bijections est associative (si on compose trois permutations, le résultat ne dépendent pas de la manière dont on regroupe deux d'entre elles).
— Elle admet un élément neutre Id, correspondant à la fonction identié de $\{1, \ldots, n\}$: cette permutation revient à laisser chacune des chaussettes dans son tiroir.
— Toute permutation σ admet une bijection réciprique σ^{-1} (consistant à remettre les chaussettes dans les tiroirs où ils étaient au départ), qui est un inverse de σ pour la composition, c'est-à-dire que $\sigma\sigma^{-1} = \sigma^{-1}\sigma = Id$.

Le groupe des permutations de $\{1, \ldots, n\}$ est aussi appelé *groupe symétrique* de degré n : il est noté $\mathfrak{S}_n$.

Pour choisir une bijection de $\{1, \ldots, n\}$, on a n choix possibles pour l'image de 1, puis une fois cette image fixée, $n-1$ choix pour l'image de 2, puis une fois cette deuxième image fixée, $n-2$ choix pour l'image de 3, $n-3$ pour l'image de 4, ..., 2 choix pour l'image de $n-1$, puis un seul choix pour l'image de n (qui est imposée par le choix des images de $1, \ldots, n-1$). Au

total, il y a donc $n(n-1)(n-2)\dots 2.1 = n!$ choix possibles pour une permutation de $\{1,\dots,n\}$, c'est-à-dire que le groupe symétrique $\mathfrak{S}_n$ a $n!$ éléments (on dit également que ce groupe est d'*ordre* $n!$).

Exemple : Le groupe $\mathfrak{S}_5$ a 120 éléments, dont σ tel que $\sigma(1)=3, \sigma(2)=2, \sigma(3)=1, \sigma(4)=5, \sigma(5)=4$ et τ tel que $\tau(1)=1, \tau(2)=2, \tau(3)=4, \tau(4)=5, \tau(5)=3$. On vérifie alors que $\sigma^2 = Id$ et donc que $\sigma^{-1}=\sigma$. D'autre part, τ^{-1} laisse fixe 1 et 2, et envoie respectivement $3,4,5$ sur $5,3,4$; on vérfie alors que $\tau^2=\tau^{-1}$ et donc que $\tau^3 = Id$. Enfin $\sigma\tau = \sigma\circ\tau$ envoie $1,2,3,4,5$ respectivement sur $3,2,5,4,1$ (dans ce cas, on applique d'abord τ, puis σ), et $\tau\sigma$ envoie $1,2,3,4,5$ sur $4,2,1,3,5$ (on applique σ, puis τ). Ceci prouve que la loi du groupe symétrique n'est pas commutative en général : on vérifie que $\mathfrak{S}_n$ n'est un groupe commutatif que pour $n=1$ et $n=2$.

Décomposition en cycles des permutations

Dans l'exemple précédent, si on suit les images successives de 1 obtenues en itérant σ, on trouve $1,3,1,3,\dots$. Les images successives de 4 sont $4,5,4,5,\dots$. Enfin 2 est un point fixe de la permutation. Ainsi, chacun des ensembles $\{1,3\}$, $\{2\}$ et $\{4,5\}$ est globalement invariant par σ, et au sein de chacun des ensembles $\{1,3\}$ et $\{4,5\}$, les deux éléments sont échangés par σ. Autrement dit, σ est le produit, dans n'importe quel ordre, des deux premutations échangeant respectivement 1 et 3, 4 et 5. On notera $\sigma=(13)(45)$, ou $\sigma=(13)(2)(45)$ pour bien préciser que 2 est un point fixe de σ.

Pour τ, 1 et 2 restent fixes, et les images successives de 3 sont $3,4,5,3,4,5,\dots$. Ainsi, τ permute circulairement, dans cet ordre, les élément $3,4$ et 5 : on dit que τ est un *cycle de longueur* 3, ou un 3-*cycle*. On pourra noter $\tau=(345)$, ou alors $\tau=(1)(2)(345)$ pour bien préciser que 1 et 2 sont des points fixes. Les ensembles $\{1\}$, $\{2\}$ et $\{3,4,5\}$ sont alors globalement invariants par τ. On a $\tau^2=\tau^{-1}=(354)\neq\tau=(345)$ (donc l'ordre des éléments est important dans un cycle de longueur 3 ou plus), et on vérifie, d'après les calculs précédents, que $\sigma\tau = (135) = (135)(2)(4)$ et que $\tau\sigma=(143)=(143)(2)(5)$, donc ces deux produits sont des 3-cycles.

D'une manière générale, on peut montrer que toute permutation peut être décomposée de manière unique en un produit de cycles dont les supports sont disjoints. Par exemple, la permutation μ de $\{1,\dots,15\}$ envoyant $1,2,\dots,15$ respectivement sur 3, 4, 5, 9, 8, 7, 11, 14, 10, 12, 6, 2, 1, 13, 15 peut s'écrire comme le produit de cycles $(1,3,5,8,14,13)(2,4,9,10,12)(6,7,11)(15)$, 15 étant l'unique point fixe de μ.

L'écriture d'une permutation comme produit (commutatif dans ce cas particulier) de cycles à supports disjoints est très pratique pour étudier ses puissances, et en particulier la plus petite puissance qui est égale à l'identité (l'exposant de cette puissance est ce qu'on appelle l'*ordre* de la permutation dans le groupe symétrique). Par exemple, du fait que la puissance k d'un k-cycle est égale à l'identité, on peut calculer :

$$\begin{aligned}\mu^{2015} &= (1,3,5,8,14,13)^{2015}(2,4,9,10,12)^{2015}(6,7,11)^{2015}\\ &= (1,3,5,8,14,13)^{-1}(2,4,9,10,12)^{0}(6,7,11)^{-1} = (1,13,14,8,5,3)(6,11,7)\\ &= (1,13,14,8,5,3)(2)(4)(6,11,7)(9)(10)(12)(15).\end{aligned}$$

La puissance n de μ est égale à l'identité si et seulement si chacun des cycles de la décomposition précédente devient l'identité après élévation à la puissance n, donc si et seulement si n est divisible par 6, 5 et 3. On en déduit que la permutation μ est d'ordre 30.

D'une manière générale, l'ordre d'une permutation est le plus petit commun multiple des longueurs des cycles impliqués dans la décomposition en produit de cycles à supports disjoints.

Exemple (battage parfait d'un jeu de cartes) : On bat un jeu de 32 cartes de la manière suivante : on divise le jeu en deux tas de 16 cartes, et ensuite on alterne les cartes des deux tas de manière parfaitement rigoureuse. Si on numérote de 1 à 32 la position des cartes, on vérifie que le battage correspond à la permutation envoyant les éléments de 1 à 32 respectivement sur $1, 3, 5, 7, 9, \ldots, 31, 2, 4, 6, \ldots, 32$. Les éléments 1 et 32 restent donc fixes. Pour le autres, on peut vérifier que pour tout k entre 1 et 30, $k+1$ est envoyé sur $\overline{2k}+1$, $\overline{2k}$ désignant le reste de $2k$ modulo 31. En itérant la permutation, on en déduit que tous les cycles de la décomposition précédente, autres que les points fixes 1 et 32, sont de la forme $(k+1, \overline{2k}+1, \overline{4k}+1, \overline{8k}+1, \overline{16k}+1)$, puisque $\overline{32k}+1 = k+1$. Ces cycles sont de longueur 5, et donc la permutation est également d'ordre 5. Ainsi, si on bat parfaitement 5 fois un jeu de 32 cartes, on retombe sur l'ordre initial. Plus généralement, pour un jeu de $2m$ cartes, l'ordre de la permutation est l'ordre de 2 modulo $2m-1$, en particulier, comme $2^8 - 1 = 51 \times 5$, le battage d'un jeu de 52 cartes redonne la situation initiale au bout de 8 coups seulement.

Signature d'une permutation

Soit σ une permutation de $\mathfrak{S}_n$. Pour toute paire $\{i,j\}$ $(i \neq j)$, le ratio

$$R_\sigma(\{i,j\}) := \frac{\sigma(j)-\sigma(i)}{j-i}$$

ne dépend pas de l'ordre dans lequel on prend les éléments de la paire : si on échange i et j, le numérateur et le dénominateur sont tous deux changés de signe, et donc le quotient reste le même. On peut alors considérer ce qu'on appelle la *signature* de la permutation σ, notée $\epsilon(\sigma)$, définie comme étant le produit des $R_\sigma(\{i,j\})$ pour toutes les $n(n-1)/2$ paires $\{i,j\}$ d'élements de $\{1,\ldots,n\}$. On a donc

$$\epsilon(\sigma) = \prod_{1\leq i<j\leq n} \frac{\sigma(j)-\sigma(i)}{j-i}.$$

Pour $\sigma, \tau \in \mathfrak{S}_n$, on a

$$\epsilon(\sigma\tau) = \prod_{1\leq i<j\leq n} \frac{\sigma(\tau(j))-\sigma(\tau(i))}{j-i} = \prod_{1\leq i<j\leq n} \frac{\sigma(\tau(j))-\sigma(\tau(i))}{\tau(j)-\tau(i)} \prod_{1\leq i<j\leq n} \frac{\tau(j)-\tau(i)}{j-i}$$

soit

$$\epsilon(\sigma\tau) = \epsilon(\tau) \prod_{1\leq i<j\leq n} R_\sigma(\{\tau(i),\tau(j)\}).$$

Or il n'est pas difficile de vérifier que lorsque $\{i,j\}$ parcourt l'ensemble des paires d'éléments de $\{1,\ldots,n\}$, il en est de même pour $\{\tau(i),\tau(j)\}$. On en déduit

$$\epsilon(\sigma\tau) = \epsilon(\tau) \prod_{1\leq i<j\leq n} R_\sigma(\{i,j\})$$

soit

$$\epsilon(\sigma\tau) = \epsilon(\sigma)\epsilon(\tau).$$

Du fait de cette égalité, et comme la signature d'une permutation est un réel non nul, on dit que ϵ est un *morphisme de groupe* de $\mathfrak{S}_n$ vers $\mathbb{R}^*$.

On peut être plus précis sur les valeurs possibles de $\epsilon(\sigma)$. En effet, si on prend la valeur absolue de cette signature, on obtient au numérateur le produit de $|\sigma(j) - \sigma(i)|$ pour toutes les paires $\{i, j\}$ de $\{1, \dots, n\}$, et au dénominateur le produit de $|j - i|$. On vérifie que les deux produits sont identiques à ordre près des facteurs, ce qui implique que $|\epsilon(\sigma)| = 1$. Par ailleurs, le signe du facteur $(\sigma(j) - \sigma(i))/(i - j)$ est positif si σ conserve l'ordre des éléments i et j, et négatif si σ change cet ordre.

On dit qu'on a une *inversion* pour chaque paire $\{i, j\}$ telle que σ renverse l'ordre des éléments i et j. On a alors le résultat suivant : $\epsilon(\sigma) = 1$ si σ a un nombre pair d'inversions, et $\epsilon(\sigma) = -1$ si σ a un nombre impair d'inversions. Dans le premier cas, on dit que σ est une *permutation paire* et dans le deuxième, que σ est une *permutation impaire*.

On peut alors dire que ϵ est un morphisme de $\mathfrak{S}_n$ vers le groupe $\{-1, 1\}$ muni de la multiplication. Cette propriété de morphisme implique le résultat suivant : la parité d'un produit fini de permutations est égale à la somme des parités des permutations formant le produit.

Exemples : Considérons la permutation $\sigma \in \mathfrak{S}_5$ introduite précédemment, envoyant 1, 2, 3, 4, 5 sur 3, 2, 1, 5, 4. Les éléments 1 et 2 sont envoyés respectivement sur 3 et 2 donc la paire $\{1, 2\}$ donne une inversion. Les éléments 1 et 3 donnent 3 et 1, d'où une autre inversion. Pour 1 et 4, on obtient 3 et 5, donc pas d'inversion car l'ordre des éléments est conservé. Pour 1 et 5, on obtient 3 et 4 donc pas d'inversion non plus. En regardant les autres paires, on vérifie que celles qui donnent une inversion sont $\{2, 3\}$ et $\{4, 5\}$. Il y a donc 4 inversions en tout, et la permutation est paire.

On peut faire le même calcul pour τ, pour laquelle les inversions sont données par les paires $\{3, 5\}$ et $\{4, 5\}$, soit deux inversions et une permutation paire.

Comme σ et τ sont des permutations paires, tous les produits qu'on peut former avec σ, τ et leurs inverses sont des permutations paires.

Un cas particulier très important de permutations sont les *transpositions*, qui sont par définition les cycles de longueur 2. On vérifie que les inversions de la transposition (ij) pour $i < j$ sont $\{i, k\}$ et $\{k, j\}$ pour $i < k < j$, et $\{i, j\}$. Il y en a donc $2(j - i) - 1$: toute transposition est une permutation impaire.

Un des points justifiant l'importance des transpositions est le fait qu'elles engendrent tout le groupe symétrique, c'est à dire que toute permutation peut être écrite comme un produit de transpositions. En effet, pour toute permutation $\sigma \in \mathfrak{S}_n$, soit $\sigma(n) = n$, soit $\sigma(n) = j < n$, et dans ce cas $\sigma = (jn)\sigma'$ où $\sigma'(n) = n$. Dans les deux cas, on se ramène à la décomposition d'une permutation laissant n fixe, et donc pour $n \geq 2$, on raméne le problème de la décomposition d'une permutation de $\{1, \dots, n\}$ à celui de la décomposition d'une permutation de $\{1, \dots, n - 1\}$. L'existence d'une décomposition en produit de transpositions est alors déduite par récurrence sur n.

La décomposition d'une permutation en produit de transpositions n'est pas unique si $n \geq 2$ (par exemple $Id = (12)^2$), mais sa parité l'est, car elle doit être nécessairement égale à celle de la permutation.

On peut facilement calculer la parité d'une permutation en fonction de sa décomposition en cycles à supports disjoints. En effet, tout cycle a une parité opposée à celle de sa longueur, puisque pour $k \geq 2$, le k-cycle $(j_1, \dots, j_k)$ peut être décomposé en le produit, dans cet ordre, des $k - 1$ transpositions $(j_1, j_2), (j_2, j_3), \dots, (j_{k-1}, j_k)$. On en déduit également que la parité d'une permutation est celle de n moins le nombre total de cycles dans la décomposition pré-

cédente, points fixes compris.

Exemples : La permutation précédente μ est le produit d'un 6-cycle (impair), d'un 5-cycle (pair) et d'un 3-cycle (pair). La permutation μ est donc impaire. On peut également voir cela en observant qu'il y a 4 cycles en tout (le point fixe 15 compris), et que $15 - 4 = 11$.

Le battage d'un jeu de 32 cartes est donné par un produit de six cycles de longueur 5 (avec deux points fixes), donc c'est une permutation paire. Pour le battage d'un jeu de 52 cartes, de l'arithmétique modulo 51 que nous ne détaillons pas ici permet de vérifier qu'il y a deux points fixes 1 et 52, un 2-cycle $(18, 35)$ et six 8-cycles. Cela fait en tout 9 cycles, et la permutation est impaire car $52 - 9 = 43$.

Le jeu du taquin : Sam Loyd, à la fin du dix-neuvième siècle, a proposé le jeu suivant : on dispose d'un cadre carré composé de 15 petits carreaux numérotés de 1 à 15, pouvant glisser parallèlement aux côtés du cadre, et d'une case vide. A chaque mouvement, on fait glisser vers la case vide un des petits carreaux qui lui est adjacent. Dans la configuration de départ, les carreaux sont dans l'ordre suivant, ligne par ligne : $(1, 2, 3, 4)$, $(5, 6, 7, 8)$, $(9, 10, 11, 12)$, $(13, 15, 14)$, la case vide étant en bas à droite. Le but du jeu est d'obtenir la même position qu'au début, sauf pour les carreaux 14 et 15 qui sont remis dans l'ordre (14 à gauche de 15).

Le but de ce jeu est impossible à atteindre. En effet, supposons qu'on ait une solution. Si on colorie les cases du jeu comme un échiquier, la couleur de la case vide change à chaque mouvement. Comme la case vide reprend sa place initiale à la fin, on doit faire un nombre pair de mouvements. Mais par ailleurs, si on note 16 la case vide, chaque mouvement revient à faire une transposition (de la forme $(j, 16)$ pour $1 \leq j \leq 15$). Comme la permutation obtenue à la fin est impaire (c'est la transposition $(14, 15)$), il doit y avoir un nombre impair de mouvements. On a donc une contradiction.

Ce raisonnement reste valable pour toute permutation impaire des éléments de 1 à 15. Il ne prouve pas que toutes les permutations paires sont possibles à atteindre, cependant on peut montrer que c'est bien le cas.

Le groupe alterné : Tout produit de permutations paires et de leurs inverses est une permutation paire. On en déduit que l'ensemble des permutations paires forment un groupe. Ce groupe est appelé *groupe alterné*, et pour les permutations de $\{1, \dots, n\}$, il est noté $\mathcal{A}_n$. Si $n = 1$, $\mathcal{A}_n = \mathcal{S}_n$ est le groupe à un seul élément. Si $n \geq 2$, l'application $\sigma \mapsto (12)\sigma$ est une bijection de $\mathcal{A}_n$ vers son complémentaire $\mathcal{A}_n^c$, la bijection réciproque de $\mathcal{A}_n^c$ dans $\mathcal{A}_n$ étant donnée par la même formule. On en déduit qu'exactement la moitié des permutations de $\mathcal{S}_n$ sont dans $\mathcal{A}_n$: ce dernier groupe est donc de cardinal $n!/2$ pour tout $n \geq 2$.

Le cardinal de $\mathcal{A}_1$ et de $\mathcal{A}_2$ est égal à 1 : ces groupes ne contiennent que la permutation identité. Le cardinal de $\mathcal{A}_3$ est égal à 3 : ce groupe contient l'identité et les deux cycles de longueur 3. Il est isomorphe au groupe des entiers modulo 3 : les isomorphismes sont obtenus en associant 0 à l'identité, 1 à un des 3-cycles et 2 à l'autre. On voit en particulier que $\mathcal{A}_n$ est commutatif pour $n \leq 3$: ce n'est plus le cas pour $n \geq 4$.

Que peut-on dire si on prend une permutation aléatoire ?

Dans cette section, nous allons fixer $n \geq 1$ et tirer au hasard, uniformément, une permutation σ de degré n, c'est à dire un élément de $\mathfrak{S}_n$. Chaque permutation a donc une chance sur $n!$ d'être tirée. On peut se poser la question suivante : quelle est la "structure typique" de σ.

Nous venons de voir que pour $n \geq 2$, il y avait exactement une chance sur deux que la permutation soit paire.

On peut étudier d'autres caractéristiques de la permutation σ, plus précisément de sa structure en produit de cycles.

Nombre moyen de points fixes : On peut se poser la question suivante : si un groupe de personnes s'échangent leurs chapeaux au hasard, combien en moyenne se retrouvent à garder celui qu'ils avaient au départ ? Cela revient à calculer le nombre moyen de points fixes de la permutation aléatoire σ introduite ci-dessous.

Il se trouve que le calcul donne un résultat très simple (ce calcul correspond à l'exercice 1 des IMO 1987, année où la médaille d'or nécessitait 42 points...). En effet, pour chaque $j \in \{1, 2, \dots, n\}$, la probabilité que j soit un point fixe est égal à $1/n!$ fois le nombre de permutations laissant j fixe. Or choisir une telle permutation revient à choisir une permutation des $n-1$ éléments restants après avoir retiré j. Cela fait $(n-1)!$ permutations donc une probabilité $(n-1)!/n! = 1/n$ que j soit fixe. Ainsi chaque $j \in \{1, \dots, n\}$ donne en moyenne $1/n$ point fixe, donc comme il y n choix pour j, le nombre moyen de points fixes de σ est simplement égal à 1. Ainsi, en moyenne une personne retrouve son chapeau...

Nombre moyen de k-uplets de points fixes : Un calcul un peu plus difficile est celui du nombre moyen de k-uplets de points fixes distincts pour tout $k \geq 1$. Il est clair que pour $n < k$, ce nombre est nul (il n'y a pas assez de nombres pour faire un k-uplet). Si $n \geq k$, on raisonne comme suit. Pour un k-uplet donné $(j_1, \dots, j_k)$ d'éléments distincts entre 1 et n, une permutation laissant fixes tous ces éléments correspond à une permutation des $n-k$ éléments restants, ce qui donne $(n-k)!$ possibilités (avec la convention $0! = 1$ si $n = k$). La probabilité qu'un k-uplet donné soit fixe est donc $(n-k)!/n!$. Or il y a $n(n-1)\dots(n-k+1) = n!/(n-k)!$ choix possibles pour le k-uplet (si on tient compte de l'ordre des éléments) : n choix pour le premier, $n-1$ pour le deuxième, ..., $n-k+1$ pour le k-ième. Il y a donc $n!/(n-k)!$ k-uplets donnant chacun en moyenne $(n-k)!/k!$ k-uplets de points fixes. Le nombre total de k-uplets de points fixes est donc, quel que soit $k \geq 1$, égal en moyenne à 0 si $n < k$ et à 1 si $n \geq k$.

Par ailleurs, si N_f est le nombre de points fixes de la permutation aléatoire σ, le nombre de k-uplets de points fixes est égal au produit $N_f(N_f-1)\dots(N_f-k+1)$ (N_f choix pour le premier point fixe, $N_f - 1$ pour le deuxième, ...). La moyenne, qu'on appelle en probabilités *l'espérance* (d'où la notation $\mathbb{E}$ ci-dessous), de ce produit est donc calculée par le raisonnement précédent :

$$\mathbb{E}[N_f(N_f-1)\dots(N_f-k+1)] = 1_{n \geq k},$$

où $1_{n \geq k}$ vaut 1 si $n \geq k$ et 0 sinon.

Loi limite du nombre de points fixes : Pour k fixé et n suffisamment grand, on a

$$\mathbb{E}[N_f(N_f-1)\dots(N_f-k+1)] = 1.$$

Il se trouve qu'il existe une unique loi de probabilité sur les entiers positifs telle que si N suit cette loi, on a

$$\mathbb{E}[N(N-1)\dots(N-k+1)] = 1.$$

Cette loi est appelée *loi de Poisson* de paramètre 1, et elle est caractérisée par la formule

$$\mathbb{P}[N = m] = \frac{1}{m!e}$$

valable pour tout entier $m \geq 0$. La constante e est la base de la fonction exponentielle. Elle est nécessaire pour que la somme des probabilités précédentes soit égale à 1 :

$$e = \frac{1}{0!} + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \dots \simeq 2,7182818284590.$$

On peut montrer que c'est la loi limite du nombre de points fixes de σ quand n tend vers l'infini, ce qui signifie que $\mathbb{P}[N_f = m]$ tend vers $\mathbb{P}[N = m] = 1/(m!e)$ quand n tend vers l'infini.

Ainsi, si on revient à l'exemple des chapeaux, la probabilité que personne ne retrouve son chapeau tend vers $1/e \simeq 36,79\%$ quand le nombre de personnes tend vers l'infini, la probabilité qu'exactement une pesonne retrouve son chapeau tend vers la même limite, pour deux personnes, on trouve $1/(2e) \simeq 18,39\%$, pour trois personnes, $1/(6e) \simeq 6,13\%$.

Le nombre de ℓ-cycles : On peut se poser les questions précédentes pour le nombre de ℓ-cycles dans la décomposition en cycles à supports disjoints. Nous n'allons pas refaire les détails : le raisonnement est similaire bien qu'un peu plus compliqué. On trouve que le nombre moyen de ℓ-cycles est égal à $1/\ell$ si $\ell \geq n$ et à 0 sinon, et plus généralement que le nombre moyen de k-uplets de ℓ-cycles distincts est égal à $1/\ell^k$ si $\ell \geq nk$ et à 0 sinon. La loi limite du nombre de ℓ-cycles est alors la loi de Poisson de paramètre $1/\ell$, donnant une probabilité $1/(\ell^m m! e^{1/\ell})$ à l'entier m.

La taille du cycle contenant un élément donné : Nous venons de voir qu'une permutation aléatoire uniforme contient "peu de petits cycles" puisque leur nombre moyen n'augmente plus avec n dès que n est suffisamment grand. Une permutation typique est donc "dominée par les grands cycles". Il se trouve que la loi de la taille du cycle contenant un élément donné j_1 est particulièrement simple. Pour la calculer, on considère les images successives de j_1 par la permutation σ.

— L'image de j_1 par σ vaut j_1 avec probabilité $1/n$, et une autre valeur, qu'on peut noter j_2, avec probabilité $(n-1)/n$.

— Dans le deuxième cas, l'image de j_2 est différente de j_2 qui est l'image de j_1, parmi les $n-1$ valeurs possibles, on trouve j_1 avec probabilité $1/(n-1)$ et une autre valeur $j_3 \neq j_1, j_2$ avec probabilité $(n-2)/(n-1)$.

— Dans le dernier cas, l'image de j_3 peut prendre toutes les valeurs sauf j_2 et j_3 qui sont les images de j_1 et j_2, on trouve donc j_1 avec probabilité $1/(n-2)$ et une autre valeur $j_4 \neq j_1, j_2, j_3$ avec probabilité $(n-3)/(n-2)$.

On peut continuer ce processus jusqu'à ce qu'une image retombe sur j_1, ce qui ferme le cycle contenant j_1. Si on refait ensuite le processus pour obtenir les autres cycles, cela correspond à ce qu'on appelle le *couplage de Feller*, mais ici nous ne nous intéressons qu'au cycle de j_1. La probabilité que le cycle soit fermé en k étapes, ce qui donne une longueur égale à k, est obtenue en multipliant les probabilités qu'on ne ferme pas le cycle les $k-1$ premières fois et qu'on le referme la k-ième, ce qui donne :

$$\frac{n-1}{n} \cdot \frac{n-2}{n-1} \cdots \frac{n-k+1}{n-k+2} \cdot \frac{1}{n-k+1} = \frac{1}{n}.$$

Autrement dit, la taille du cycle contenant un élément donné est simplement une variable aléatoire uniforme sur toutes les valeurs possibles $1, 2, 3, \ldots, n$.

La loi de la taille du plus grand cycle : La loi complète de la taille du plus grand cycle n'est pas simple et nous n'allons pas la calculer entièrement. Cependant, nous allons pouvoir calculer la probabilité que le plus grand cycle ait une taille m, lorsque m est strictement plus grand que $n/2$. Le raisonnement est le suivant : pour chaque élément j de $\{1, \ldots, n\}$, la probabilité qu'il appartienne à un m-cycle est égale à $1/n$ d'après le calcul précédent. En ajoutant ces probabilités pour toutes les valeurs de j, on en déduit que le nombre moyen d'éléments compris dans un m-cycle est égal à 1, ce qui implique que le nombre moyen de m-cycles est

égal à $1/m$ (nous avons d'ailleurs vu ce résultat précédemment). Or comme $m > n/2$, il ne peut y avoir qu'au plus un m-cycle, donc la probabilité qu'il y ait effectivement un m-cycle est $1/m$. Dans ce cas, ce cycle est nécessairement le plus grand : autrement dit, pour $m > n/2$, il y a une chance sur m que le plus grand cycle ait une taille exactement égale à m.

La probabilité qu'il y ait un cycle strictement plus grand que $n/2$ est obtenue en ajoutant les probabilités précédentes : on obtient donc la somme des $1/m$ pour $n/2 < m \leq n$. On peut montrer que cette somme tend vers $\ln 2 \simeq 0.6931$ quand n tend vers l'infini ($\ln 2$ est le logarithme népŕien de 2, soit l'unique y tel que $e^y = 2$, e étant le nombre introduit précédemment). On en déduit que pour n assez grand, entre 69 et 70 pourcent des permutations de taille n ont un cycle occupant plus de la moitié des entiers de 1 à n. Ceci illustre la "domination des grands cycles" dans une permutation typique.

Un problème de prisonniers : Cent prisonniers sont enfermés dans une pièce, où ils ont le droit de communiquer librement entre eux. Ensuite, le gardien appelle (dans un ordre aléatoire) successivement chacun des cent prisonniers. Lorsqu'un prisonnier est appelé, il est envoyé dans une deuxième pièce, où il ne peut plus communiquer avec les autres. Dans cette deuxième pièce sont alignés cent tiroirs, chacun d'entre eux comportant un papier avec le nom d'un des prisonniers (chaque prisonnier ayant son nom dans un et un seul tiroir, la permutation correspondante étant choisie uniformément par les gardiens). Le prisonnier appelé ouvre un tiroir de son choix et regarde le nom indiqué sur le papier contenu dedans. Ensuite, il remet le papier dans le tiroir et referme le tiroir. S'il a tiré son propre nom, il est envoyé dans une troisième pièce où la communication avec les prisonniers encore dans la première pièce est impossible. S'il n'a pas tiré son nom, il recommence la procédure en choisissant un deuxième tiroir, et continue ainsi jusqu'à ce qu'il ait soit fini par tirer son nom, soit encore échoué après cinquante tentatives. Dans ce dernier cas, les cent prisonniers sont réunis puis tous exécutés. La question posée est la suivante : quelle stratégie doivent adopter les prisonniers pour avoir le plus de chance de survivre ? On suppose que les prisonniers savent à l'avance le contenu de l'épreuve qui les attend.

La méthode la plus naïve consiste pour les prisonniers à choisir les tiroirs aléatoirement. Dans ce cas, la probabilité de trouver son nom au bout de 50 essais ou moins est de $1/2$, on en déduit une probabilité de $1/2^{100}$ pour l'ensemble des 100 prisonniers, et donc une probabilité de survie de $1/2^{100}$. Ce n'est pas encourageant !

Il est naturel de supposer qu'on puisse améliorer cette probabilité, mais assez surprenant qu'on puisse l'augmenter jusqu'à plus de 30% ! Rappelons en effet que le premier prisonnier n'ayant aucune information sur la manière dont les papiers sont répartis dans les tiroirs, il a nécessairement déjà une probabilité d'échec de 50%. De plus, le taux de succès de 30% reste atteignable même si le nombre de prisonniers augmente. La stratégie considérée (il est possible de montrer qu'elle est optimale, mais on ne vas pas le faire ici) est la suivante : les prisonniers conviennent d'une bijection entre les noms et les nombres entre 1 et 100, et conviennent également d'une numérotation des tiroirs. Soit alors $\sigma \in \mathfrak{S}_{100}$ la permutation qui à j associe le numéro du prisonnier dont le nom est sur le papier du tiroir j. Lorsque le prisonnier k est appelé, son but est alors d'ouvrir le tiroir numéro $\sigma^{-1}(k)$. Sa stratégie est la suivante : il ouvre d'abord le tiroir numéro k. Le papier contient alors le nom du prisonnier numéro $\sigma(k)$. Le prisonnier appelé connaît donc $\sigma(k)$ et peut donc ouvrier le tiroir correspondant, qui contient le nom du prisonnier $\sigma^2(k)$. Ensuite, il ouvre le successivement les tiroirs $\sigma^2(k)$, $\sigma^3(k)$, etc., jusqu'à obtenir son nom. Si le cycle de σ contenant k a une taille ℓ, le nombre d'essais nécessaires pour trouver le bon tiroir est ℓ : le prisonnier doit ouvrir successivement les tiroirs

$k, \sigma(k), \ldots, \sigma^{\ell-1}(k) = \sigma^{-1}(k)$. L'épreuve est réussie si et seulement si le cycle contenant k est de taille inférieure ou égale à 50. La probabilité que tous les prisonniers réussissent l'épreuve, et donc survivent, est la probabilité que tous les cycles aient une taille inférieure ou égale à 50, ce qui donne, d'après ce qui précède :

$$1 - \frac{1}{51} - \frac{1}{52} - \frac{1}{53} - \cdots - \frac{1}{100}.$$

On s'attend à ce que cette quantité soit proche de $1 - \ln 2 \simeq 30,69\%$, un calcul exact donne environ $31,18\%$.

4 dimanche 23 : ITYM et le TFJM²

Cette conférence consistait en une présentation succinte du TFJM² (Tournoi Français des Jeunes Mathématiciennes et Mathématiciens), et de son homologue international, l'ITYM (International Tournament of Young Mathematicians).

Le Tournoi Français des Jeunes Mathématiciennes et Mathématiciens (TFJM²) existe depuis 2011. Il est organisé par le département de mathématiques de l'université Paris-Sud et l'association Animath. Il est l'étape française du tournoi international "International Tournament of Young Mathematicians" (ITYM), créé en 2009, qui fonctionne sur le même principe. Cette année ont eu lieu des tournois régionaux à Paris, Palaiseau, Rennes, Strasbourg et Toulouse, et les douze meilleures équipes se sont affrontées lors de l'épreuve nationale à l'École Polytechnique.

Il s'agit d'une compétition destinée aux élèves de lycée (1ère et Terminale S notamment). Il se distingue d'autres compétitions comme les olympiades en proposant des problèmes ouverts à chercher équipe. Guidées par des encadrantes et encadrants, elles auront plus d'un mois et demi pour travailler. Pendant le tournoi, les élèves participant présenteront leurs résultats sous forme de débats avec quatre rôles : défenseur, opposant, rapporteur et observateur.

Les problèmes proposés sont inhabituels pour la plupart des élèves, car ils n'admettent, à la connaissance du jury, pas de solution complète. Pour les équipes, il s'agit donc de comprendre le problème, de résoudre des cas particuliers, de repérer les difficultés... La liste des problèmes proposés est, en totalité ou en partie, la même que celle pour l'ITYM. Les problèmes abordés dans le tournoi recouvrent les domaines de l'algèbre, l'analyse, la combinatoire, la géométrie et la théorie des nombres.

Les principaux objectifs du tournoi sont :

— stimuler l'intérêt pour les mathématiques et leurs applications,
— développer la pensée scientifique des élèves, leurs talents de communication, et leur capacité à travailler en équipe,
— permettre l'échange d'expérience entre enseignants et étudiants.

Les équipes gagnantes sont invitées au tournoi international des jeunes mathématiciens (ITYM).

Pour rendre compte du caractère ô combien théâtral de ce tournoi, un tour blanc a été présenté aux élèves, reprenant des prestations du TFJM² passé. Henry Bambury a présenté une solution pour le problème 5, le Fils du Polygone. L'opposant, Gabriel Pallier, a non seulement fait preuve d'esprit critique en pointant des erreurs et des imprécisions dans cette présentation, mais il a aussi élargi le débat en posant la question des généralisations du problème. Le

rapporteur, Cécile Gachet a fait la synthèse du débat précédent, pointant également du doigt une erreur importante que l'opposant avait omis de mentionner, mais qui a heureusement pu être corrigée.

Pour plus de détails sur le tournoi en lui-même comme sur le contenu mathématique de la présentation donnée, le lecteur est invité à se rendre sur les sites officiels : www.tfjm.org et itym.org.

En outre, il fut question au début de la soirée du concours de cryptanalyse Al Kindi, lancé cette année à l'échelle nationale pour tous les élèves de de 2nde. Les concurrent(e)s, seul(e)s ou en équipe, auront des épreuves ludiques à surmonter en ligne, comme le codage et le décodage de messages cryptés.
La compétition est entièrement gratuite, et aucune notion de programmation n'est requise. Pour se renseigner et s'inscrire, une seule adresse : www.concours-alkindi.fr !

XI. La muraille

Contenu de cette partie

1 Présentation

Une muraille de 142 exercices était affichée dans la bibliothèque - la plus petite des cinq salles à notre disposition. Les exercices 1 à 42 sont de niveau 1, 43 à 96 de niveau 2, 97 à 142 de niveau 3. Un exercice est décoré de n étoiles lorsqu'il est resté sans solution à la muraille de n stages.

Les élèves du groupe A cherchent les exercices de niveau 1 (ou au dessus). Les élèves du groupe B, les exercices de niveau 2 et les exercices étoilés de niveau 1 (ou au dessus). Les élèves du groupe C, ceux de niveau 3 et ceux étoilés de niveau 2 (ou au dessus). Les élèves du groupe D, ceux de niveau 3. Certains exercices ont été résolus avant la constitution des groupes lundi soir.

Une fois un exercice résolu, la solution doit etre rédigée et donnée à une animatrice ou un animateur. La première solution correcte d'un exercice est reproduite dans ce polycopié. Il est possible de résoudre les exercices à plusieurs. Le but est d'avoir tout résolu à la fin du stage !

Tous les deux exercices résolus (individuellement ou bien par équipe d'au plus deux personnes), une glace est offerte. La distribution des glaces a été retardée car les premiers jours nous n'avions pas accès au frigidaire. A la fin du stage, quatre Grands Prix Mystère seront décernés aux quatre élèves ayant obtenu le plus de points en résolvant des exercices de la muraille, dans chacun des quatre groupes A, B, C, D. Un autre Grand Prix Mystère est décerné à l'équipe (constituée d'au moins deux élèves et d'au plus quatre élèves) ayant obtenu le plus de points en résolvant des exercices de la muraille.

Barème : un exercice à x étoiles résolu rapporte $x+1$ points (sauf pour les élèves du groupe B qui résolvent des exercices étoilés de niveau 1 et les élèves du groupe C qui résolvent des exercices étoilés de niveau 2, pour lesquels un exercice à x étoiles rapporte x points).

2 Enoncés

Exercice 1 (*) Soit $l_1, l_2, \ldots, l_n$ des réels strictement positifs tels qu'il existe un polygone dont les côtés sont de longueurs respective $l_1, l_2, \ldots, l_n$. Montrer qu'il existe un polygone

convexe (avec éventuellement des angles plats) dont les côtés sont de longueurs respective $l_1, l_2, \ldots, l_n$.

Exercice 2 On se donne $2n+1$ nombres tels que la somme de n nombres quelconques d'entre eux soit inférieure à la somme des $n+1$ autres. Montrer que tous ces nombres sont positifs.

Exercice 3 Soit ABC un triangle équilatéral et P un point à l'intérieur de ce triangle. Soient D, E et F les pieds des perpendiculaires de P sur $[BC], [CA]$ et $[AB]$ respectivement. Montrer que

1. $AF + BD + CE = AE + BF + CD$ et que
2. $|APF| + |BPD| + |CPE| = |APE| + |BPF| + |CPD|$,

où $|XYZ|$ désigne l'aire du triangle XYZ.

Exercice 4 (*) Déterminer tous les nombres réels a et b vérifiant l'égalité suivante :

$$2a^2 + 2b^2 + 2(b - a - ab) + 2 = 0.$$

Exercice 5 Sophie choisit au hasard un polynôme P dont tous les coefficients sont des entiers naturels. Thomas a le droit de demander à Sophie la valeur prise par P en un nombre a donné, puis, en tenant éventuellement compte de la première réponse de Sophie, en un autre nombre b. Thomas doit ensuite deviner le polynôme P. Comment faire ?

Exercice 6 (**) Le nombre 10^{2013} est écrit au tableau. Alexandra et Béatrice jouent au jeu suivant à tour de rôle, où à chaque tour il est permis de faire l'une des deux opérations suivantes :

- remplacer un nombre x écrit au tableau par deux entiers $a, b > 1$ tels que $ab = x$.
- effacer un ou deux nombres égaux écrits au tableau.

Celle qui ne peut plus jouer a perdu.

Alexandra joue en premier. Est-elle sure de gagner ?

Exercice 7 (**) Montrer qu'il existe une infinité de nombres premiers dont le dernier chiffre n'est pas 1.

Exercice 8 Trouver tous les entiers relatifs x et y tels que

$$x^2y + 7x = x^2 + 3xy + 3y + 4$$

Exercice 9 (***) Soit k un entier supérieur ou égal à 2. Trouver tous les entiers x et y tels que :

$$y^k = x^2 + x.$$

Exercice 10 (**) Soit $[EF]$ un segment inclus dans le segment $[BC]$ tel que le demi-cercle de diamètre $[EF]$ est tangent à $[AB]$ en Q et à $[AC]$ en P. Prouver que le point d'intersection K des droites (EP) et (FQ) appartient à la hauteur issue de A du triangle ABC.

Exercice 11 (***) Soit $ABCD$ un carré, et $PQRS$ un petit carré placé à l'intérieur de $ABCD$ de telle sorte que les segments $[AP]$, $[BQ]$, $[CR]$, $[DS]$ ne s'intersectent pas entre eux, et n'intersectent pas $PQRS$. Prouver que la somme des aires des quadrilatères $ABQP$ et $CDSR$ est égale à la somme des aires des quadrilatères $BCRQ$ et $DAPS$.

Exercice 12 * Trouver tous les entiers a, b et m tels que

$$4a^b + 1 = m^2.$$

Exercice 13 Soit ABC un triangle. Soit I un point du segment $[AB]$. Montrer que la droite (CI) est la bissectrice intérieure issue de C si et seulement si $CA/CB = IA/IB$.

Exercice 14 * Montrer que $\sqrt{2} + \sqrt{5} + \sqrt{13}$ est irrationnel.

Exercice 15 Montrer que tous les termes de la suite (a_n) définie par

$$\begin{cases} a_1 = a_2 = a_3 = 1 \\ a_{n+1} = \frac{1+a_{n-1}a_n}{a_{n-2}} \end{cases}$$

sont des entiers.

Exercice 16 ** On a un polyèdre convexe, dont les faces sont des triangles. Les sommets du polyèdre sont coloriés avec trois couleurs.

Montrer que le nombre de triangles dont les sommets ont trois couleurs distinctes est pair.

Exercice 17 Existe-t-il une suite (u_n) d'entiers naturels non nuls telle que u_n et u_m sont premiers entre eux ssi $|n - m| = 1$?

Exercice 18 Alexandre et Béatrice jouent au jeu suivant : sur un rectangle quadrillé de taille 4×2015, chacun place à son tour un pentomino **T**, qui ne recouvre pas les précédents. Le premier joueur qui ne peut plus poser de pentomino a perdu. Montrer que le premier joueur à commencer possède une stratégie gagnante.

Exercice 19 (*) Trouver l'ensemble des entiers naturels égaux au carré de leur somme des chiffres.

Exercice 20 (*) Trouver les entiers naturels n tels que $n^4 + 4^n$ soit premier.

Exercice 21 Montrer que pour tous réels strictement positifs a et b et pour tout entier n,

$$\left(1 + \frac{a}{b}\right)^n + \left(1 + \frac{b}{a}\right)^n \geq 2^{n+1}.$$

Exercice 22 (**) Trouver les entiers strictement positifs a et b tels que $\frac{a^{2b+1}b-1}{a+1}$ et $\frac{b^a a+1}{b-1}$ soient des entiers.

Exercice 23 (**) On considère $ab + 1$ condylures (avec a, b des entiers positifs) telles que si l'on considère 2 quelconques d'entre eux, alors soit l'un descend de l'autre, soit ils n'ont aucune lien de parenté. Montrer que l'on peut en trouver $a + 1$ qui descendent les uns des autres ou bien $b + 1$ qui n'ont aucun lien de parenté entre eux.

Exercice 24 (**) Soient m, n des entiers positifs. À quelle condition existe-t-il un entier positif N tel que pour tout entier $r \geq N$ il existe deux entiers positifs a et b tels que $r = am+bn$? Estimer la valeur minimale de N aussi précisément que possible.

Exercice 25 Montrer que 2015 n'est pas une somme de trois cubes d'entiers naturels.

Exercice 26 (***) Soit $x_0, x_1, x_2, \ldots$ une suite de nombres réels. On dit que la suite $x_0, x_1, \ldots$ est convexe si :

$$\text{pour tout entier } n \geq 0, \frac{x_{n-1} + x_{n+1}}{2} \geq x_n$$

et qu'elle est log-convexe si :

$$\text{pour tout entier } n \geq 0, x_{n+1}x_{n-1} \geq x_n^2$$

On suppose que pour tout nombre réel $a > 0$, la suite $x_0, ax_1, a^2x_2^2, a^3x_3^3, \ldots$ est convexe. Prouver que la suite $x_0, x_1, \ldots$ est log-convexe.

Exercice 27 Un troupeau est constitué de 25 vaches pesant chacune entre 500 et 1000 kg. Montrer qu'il existe dans ce troupeau deux sous-troupeaux contenant au moins une vache, et sans aucune vache en commun, dont la masse est égale au gramme près.

Exercice 28 (***) Soit ABC un triangle isocèle en C. On considère un point P sur le cercle circonscrit au triangle ABC situé entre A et B (et P n'est pas du même côté que C par rapport à la droite (AB)). Soit D un point de la droite (PB) tel que les droites (CD) et (PB) soient perpendiculaires. Prouver que $PA + PB = 2 \cdot PD$.

Exercice 29 (***) Soient $x, y > 0$, et soit $s = min(x, y + 1/x, 1/y)$. Quelle est la valeur maximale possible de s ? Pour quels x, y est-elle atteinte ?

Exercice 30 (***) Trouver les nombres premiers p pour lesquels il existe des entiers positifs x et y tels que :

$$x(y^2 - p) + y(x^2 - p) = 5p.$$

Exercice 31 (****) On place $2n$ points dans le plans et on trace $n^2 + 1$ segments entre ces points.

Montrer que l'on peut trouver 3 points reliés deux à deux.

Exercice 32 (***) Soit $\mathcal{P} = A_1 \ldots A_{2n}$ un $2n-$gone convexe dans le plan. Soit P un point intérieur à $\mathcal{P}$, non situé sur une diagonale. Prouver que P est contenu dans un nombre pair de triangles à sommets parmi les A_i.

Exercice 33 (*) En joignant chaque milieu d'un côté d'un rectangle d'aire 1 aux sommets du côté opposé, on obtient un octogone au centre du rectangle (une figure est conseillée). Quelle est son aire ?

Exercice 34 (*) Trouver tous les entiers strictement positifs x, y, z tels que

$$\frac{1}{x} + \frac{2}{y} - \frac{3}{z} = 1.$$

Exercice 35 (⋆) On demande à Guillaume d'additionner deux fractions irréductibles. Hélas, l'étourdi les multiplie. Heureusement, le résultat est le même : une fraction dont le dénominateur est 2007. Quel peut être le numérateur ?

Exercice 36 (⋆) Trouvez 7 entiers strictement positifs, tous différents, tels que chacun divise leur somme, et que cette somme soit la plus petite possible.

Exercice 37 (⋆⋆⋆) Soit ABC un triangle isocèle en A tel que $\widehat{BAC} < 60^\circ$. Les points D et E sont des points du côté $[AC]$ tels que $EB = ED$ et $\widehat{ABD} = \widehat{CBE}$. Soit O le point d'intersection des bissectrices des angles $\widehat{BDC}$ and $\widehat{ACB}$. Trouver la valeur de l'angle $\widehat{COD}$.

Exercice 38 (⋆⋆⋆) Trouver tous les entiers positifs a, b, c tels que

$$2^a 3^b + 9 = c^2.$$

Exercice 39 (⋆⋆⋆) Soit ABC un triangle dont tous les angles sont aigus. On note Γ son cercle circonscrit. On suppose que La tangente en A à Γ coupe la droite (BC) en un point P. Soit M le milieu de $[AP]$ et soit R le deuxième point d'intersection de la droite (BM) avec le cercle Γ. La droite (PR) recoupe le cercle Γ en S.

Prouver que les droites (AP) et (CS) sont parallèles.

Exercice 40 (⋆) On considère 2014 tas de jetons, le i-ème tas contenant p_i jetons, où p_i est le i-eme nombre premier (notamment $p_1 = 2$). On a le droit de fusionner deux piles puis d'ajouter 1 jeton a la nouvelle pile, ou de diviser une pile en deux autres (pas forcément de meme taille), puis d'ajouter 1 jeton à l'une des deux nouvelles piles crées. Pourra-t-on avoir 2014 piles de 2014^{2014} jetons ?

Exercice 41 (⋆) Soient ABC un triangle équilatéral et M un point situé à l'intérieur de ce triangle. Montrer que la somme des distances de M aux trois côtés du triangle est indépendante de M.

Exercice 42 (⋆) Alceste et Brunehilde jouent au jeu suivant : on commence par dessiner un carré de côté 1. Ensuite les joueurs jouent tour à tour, sachant que chaque coup consiste à dessiner un carré ne se superposant pas à la figure déjà dessinée, et tel que l'un de ses côtés coïncide exactement avec l'un des côtés de la figure déjà dessinée (en particulier, cette dernière est toujours un rectangle). Le gagnant est celui qui arrive à une figure d'aire un multiple de 5. On suppose qu'Alceste commence. L'un des deux joueurs a-t-il une stratégie gagnante ?

Exercice 43 Existe-t-il un triangle rectangle ayant des côtés de longueur rationnelle et dont l'aire vaut 1 ?

Exercice 44 Soit $\mathcal{P}$ la parabole d'équation $y = x^2$. Trouver une condition nécessaire et suffisante pour que des points de $\mathcal{P}$ d'abscisse a, b, c et d soient cocycliques.

Exercice 45 (⋆) Pour quels entiers $n \geq 1$ existe-t-il une bijection $\sigma : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ de sorte que $|\sigma(i) - i| \neq |\sigma(j) - j|$ si $i \neq j$?

Exercice 46 (⋆⋆) Considérons un triangle ABC tel que $AB = BC$ et $\widehat{ABC} = 80^\circ$. Soit P le point de l'intérieur de ABC tel que $\widehat{PAC} = 40^\circ$ et $\widehat{PCA} = 30^\circ$. Calculer l'angle $\widehat{BPC}$.

Exercice 47 (***) Soit $n > 2$ un entier naturel, T la transformation $\mathbb{R}^n \to \mathbb{R}^n, (x_1, \ldots, x_n) \mapsto (\frac{x_1+x_2}{2}, \frac{x_2+x_3}{2}, \ldots, \frac{x_{n-1}+x_n}{2}, \frac{x_n+x_1}{2})$. On part d'un $n-uplet$ $(a_1, \ldots, a_n)$ d'entiers deux à deux distincts. Prouver que pour $k \in \mathbb{N}$ assez grand, $T^k(a_1, \ldots, a_n) \notin \mathbb{N}^n$.

Exercice 48 (**) On considère un triangle acutangle ABC avec $\widehat{A} = 60°$. Déterminer les points $M \in (AB)$ et $N \in (AC)$ qui minimisent la somme $|CM| + |MN| + |BN|$.

Exercice 49 Soit P un point de l'espace et $r > 0$. Montrer qu'il existe 8 sphères disjointes de même rayon r qui cachent le point P, c'est-à-dire que toute demi-droite issue de P rencontre au moins l'une des sphères. On supposera que les centres des sphères sont tous à des distances $> r$ de P.

Exercice 50 Parmi les quadrilatères de côtés a,b,c,d, caractériser géométriquement celui qui a la plus grande aire.

Exercice 51 (***) Soit P un point à l'intérieur d'un polygone régulier à n côtés tel que quel que soit un côté du polygone, P se projette orthogonalement sur l'intérieur du côté. Ces n projections orthogonales partagent les n côtés du polygone en $2n$ segments. On numérote ces segments de 1 à $2n$, en commençant par un segment arbitraire, puis en tournant dans le sens direct le long du polygone. Prouver que la somme des longueurs des segments de numéros pairs est égale à la somme des longueurs des segments de numéros impairs.

Exercice 52 Soit P un point à l'intérieur d'un cercle de rayon R, d une droite passant par P et d' la perpendiculaire à d en P. On fait tourner les droites d et d' d'un angle ϕ autour de P. Montrer que quelle que soit la position du point P, l'aire balayée par d et d' à l'intérieur du cercle (qui a la forme d'une croix) vaudra $\pi R^2 \frac{4\phi}{360}$.

Exercice 53 (*) Trouver toutes les fonctions $f : \mathbb{R} \to \mathbb{R}$ telles que pour tous réels x, y, z, t,

$$(f(x) + f(y))(f(z) + f(t)) = f(xz + yt) + f(xt - yz).$$

Exercice 54 (**) Soit ABC un triangle, D le milieu de $[AB]$, M le milieu de $[CD]$. On suppose que les droites (BM) et (AC) sont sécantes, en un point que l'on nomme N. Enfin, soit Γ le cercle circonscrit au triangle BCN. Montrer que AB est tangente à Γ si et seulement si

$$\frac{BM}{MN} = \frac{(BC)^2}{(BN)^2}.$$

Exercice 55 (**) Soit n un entier relatif. Montrer qu'il existe un unique polynôme P à coefficients dans $\{0, 1\}$ tel que $P(-2) = n$.

Exercice 56 (***) Si A est un ensemble d'entiers naturels non vide, on note $PGCD(A)$ le plus grand diviseur commun à tous les éléments de A.

Trouver le plus petit entier naturel non nul n vérifiant la propriété suivante : pour toute partie A de $\{1, 2, ..., 2012\}$, il existe une partie B de A de cardinal inférieur ou égal à n telle que $PGCD(B) = PGCD(A)$.

Exercice 57 Alice et Bob sont complices et opposés à Eve. Dans une salle est disposé un échiquier avec sur chaque case une pièce de monnaie en position pile ou face. Au départ, seuls Eve et Bob sont dans la pièce ; ce dernier observe Eve retourner l'une des pièces. Ensuite, Eve

s'en va et Bob a le droit de retourner au plus une pièce avant de partir lui aussi. Finalement, Alice entre dans la salle. Elle observe l'échiquier et doit déterminer la pièce retournée par Eve. Expliquer comment Alice et Bob peuvent se concerter à l'avance pour qu'Alice retrouve à coup sûr la pièce retournée par Eve.

Exercice 58 (⋆) Soit ABC un triangle rectangle isocèle en C, D et E des points de $[AC]$ et $[BC]$ tels que $CE = CD$. Les perpendiculaires à (AE) passant par D et C coupent (AB) respectivement en K et L. Montrer que $KL = LB$.

Exercice 59 (⋆) Démontrer que pour tout nombre réel $x \in]0, \pi/2[$ on a l'inégalité suivante :

$$\left(1 + \frac{1}{\cos^{10}(x)}\right)\left(1 + \frac{1}{\sin^{10}(x)}\right) \geq 1089.$$

Exercice 60 On considère n entiers $a_1, \dots a_n$ dans $\{1, \dots 2015\}$ tels que le ppcm de deux d'entre eux est toujours > 2015. Montrer que

$$\frac{1}{a_1} + \cdots + \frac{1}{a_n} < 2.$$

Exercice 61 (⋆) Déterminer tous les couples de polynômes non constants P et Q unitaires, de degré n et admettant n racines positives ou nulles (non nécessairement distinctes) tels que

$$P(x) - Q(x) = 1.$$

Exercice 62 (⋆⋆) On appelle I l'ensemble des points du plan tels que leur abscisse et leur ordonnée soient des nombres irrationnels, et R celui des points dont les deux coordonnées sont rationnelles. Combien de points de R au maximum peuvent se situer sur un cercle de rayon irrationnel dont le centre appartient à I ?

Exercice 63 (⋆) On se donne un nombre entier $n > 1$. Deux joueurs R et B colorient tour à tour des points sur un cercle, R coloriant en rouge et B en bleu. Une fois que chacun a placé n points, le jeu s'arrête, et chaque joueur cherche sur le cercle l'arc de cercle le plus long ayant pour extrémités des points de sa couleur, et ne contenant aucun autre point coloré. Le joueur dont l'arc de cercle sélectionné est le plus long gagne (s'ils sont de même longueur, ou bien s'il n'y a aucun tel arc, on dit que la partie est nulle). L'un des deux joueurs a-t-il une stratégie gagnante ?

Exercice 64 (⋆) Pour chaque nombre premier p, trouver le plus grand entier k tel que $(p!)^k$ divise $(p^2)!$.

Exercice 65 (⋆) Soit $a_1, a_2, \dots$ une suite infinie strictement croissante d'entiers naturels telle que pour tout n, le terme a_n soit égal soit à la moyenne arithmétique, soit à la moyenne géométrique des deux termes a_{n-1} et a_{n+1}. Cette suite est-elle nécessairement toujours arithmétique ou toujours géométrique à partir d'un certain rang ?

Exercice 66 (⋆) On partitionne un carré en un nombre fini (supérieur à 2) de rectangles de côtés parallèles aux côtés du carré. Parmi les segments joignant les centres de deux rectangles de la partition, en existe-t-il toujours un n'intersectant aucun autre rectangle ?

Exercice 67 (***) Soient ABC un triangle, H le pied de la hauteur issue de B, M le milieu de $[AB]$ et N le milieu de $[BC]$. Les cercles circonscrits aux triangles AHN et CHM se recoupent au point P. Prouver que la droite (PH) coupe le segment $[MN]$ en son milieu.

Exercice 68 (**) On considère trois nombres réels x, y, z qui ne sont pas tous égaux. On suppose que

$$x + \frac{1}{y} = y + \frac{1}{z} = z + \frac{1}{x} = k.$$

Trouver toutes les valeurs possible de k.

Exercice 69 Soient a, b et c les longueurs des côté d'un triangle. Montrer que

$$a^2b\,(a-b) + b^2c\,(b-c) + c^2a\,(c-a) \geqslant 0$$

Quel est le cas d'égalité ?

Exercice 70 Soit ABC un triangle équilatéral de côté a et P un point à l'intérieur de ce triangle. On construit un triangle XYZ de côtés de longueur PA, PB et PC et on note F son point de Fermat. Montrer que $FX + FY + FZ = a$.

Exercice 71 (**) Une droite passant par un point A coupe un cercle $\mathcal{C}$ en B et C. On suppose que B est situé entre A et C. Les deux tangentes à $\mathcal{C}$ passant par A sont tangentes à $\mathcal{C}$ en S et en T. On note P le point d'intersection de (ST) et (AC). Montrer que $\frac{AP}{PC} = 2\frac{AB}{BC}$

Exercice 72 (*) Trouver toutes les fonctions f de $\mathbb{N}$ dans $\mathbb{N}$ telles que pour tous entiers $m, n \geq 0$ on ait

$$f(m + f(n)) = f(f(m)) + f(n).$$

Exercice 73 (***) Une ampoule est placée sur chaque case d'un échiquier 2011×2012. Initialement, 4042111 ampoules sont allumées. On a le droit d'éteindre une ampoule si elle appartient à un bloc 2×2 dont les trois autres ampoules sont éteintes. Peut-on éteindre toutes les ampoules ?

Exercice 74 (**) Soit ABC un triangle dont le cercle inscrit est noté ω. Soient I le centre de ω et P un point tel que les droites (PI) et (BC) soient perpendiculaires et les droites (PA) et (BC) parallèles. Soient finalement Q et R deux points tels que $Q \in (AB)$, $R \in (AC)$, les droites (QR) et (BC) soient parallèles et finalement (QR) soit tangente à ω.

Prouver que $\widehat{QPB} = \widehat{CPR}$.

Exercice 75 Montrer que pour tous entiers m et n non nuls et strictement positifs,

$$\frac{1}{\sqrt[n]{1+m}} + \frac{1}{\sqrt[m]{1+n}} \geq 1$$

Exercice 76 (***) Soit p un nombre premier congru à 2 modulo 3 et a et b des entiers tels que p divise $a^2 + ab + b^2$. Montrer que p divise a et b.

Exercice 77 (**) Trouver tous les polynômes $P(x)$ à coefficients réels tels que

$$xP\left(\frac{y}{x}\right) + yP\left(\frac{x}{y}\right) = x + y$$

pour tous nombres réels non nuls x, y.

Exercice 78 (***) Soit n un entier non nul. Montrer que

$$\lfloor \sqrt{n} \rfloor + \lfloor \sqrt[3]{n} \rfloor + \ldots + \lfloor \sqrt[n]{n} \rfloor = \lfloor \log_2 n \rfloor + \lfloor \log_3 n \rfloor + \ldots + \lfloor \log_n n \rfloor.$$

On rappelle que $\lfloor x \rfloor$ désigne le plus grand entier inférieur ou égal à x, et que $\lfloor \log_k n \rfloor$ est égal au plus grand exposant a tel que $k^a \leq n$.

Exercice 79 (**) Trouver tous les nombres premiers p, q tels que $p^2 - pq - q^3 = 1$.

Exercice 80 (*) Trouver tous les polynômes P à coefficients réels tels que $P(0) = 0$ et tels que $P(X^2 + 1) = P(X)^2 + 1$.

Exercice 81 Trouver tous les polynômes P à coefficients réels tels que, pour tout $n \in \mathbb{N}$, il existe un rationnel r tel que $P(r) = n$.

Exercice 82 (*) Soit $(x_n)_{n \geq 0}$ une suite de nombre réels telle que pour tout entier positif $n \geq 0$ on ait

$$\sum_{i=0}^{n} x_i^3 = \left(\sum_{i=0}^{n} x_i \right)^2.$$

Montrer que pour tout entier $n \geq 0$, il existe un entier $m \geq 0$ tel que

$$\sum_{i=0}^{n} x_i = \frac{m(m+1)}{2}.$$

Exercice 83 Montrer que pour tous réels strictement positifs x, y et z,

$$\frac{x}{x + 2y + 3z} + \frac{y}{y + 2z + 3x} + \frac{z}{z + 2x + 3y} \geq \frac{1}{2}$$

Exercice 84 (**) Trouver tous les couples (p, n), où p est un nombre premier et n un entier strictement positif, tels que p^n divise $(p-1)! + 1$.

Exercice 85 (*) On définit une suite u_n ainsi : u_1 et u_2 sont des entiers entre 1 et 10000 (au sens large), et u_{k+1} est la plus petite valeur absolue des différences deux à deux des termes précédents. Montrer que $u_{21} = 0$.

Exercice 86 Soit ABC un triangle acutangle, avec $AC > BC$. On note H son orthocentre, O le centre de son cercle circonscrit et M le milieu de $[AC]$. Soit F le pied de la hauteur issue de C, et P le symétrique de A par rapport à F. On note X l'intersection de (PH) avec (BC), Y l'intersection de (FX) avec (OM), et Z l'intersection de (OF) avec (AC). Montrer que F, M, Y et Z sont cocycliques.

Exercice 87 Soit P un polynôme à coefficients entiers. Existe-t-il des entiers distincts a, b et c tels que

$$P(a) = b$$
$$P(b) = c$$
$$P(c) = a$$

Exercice 88 (⋆) Hyacinthe et Hippolyte jouent au jeu suivant : sur un échiquier $m \times n$, on place une tour sur une case c. Tour à tour, chacun la déplace (d'un nombre arbitraire de cases selon les lignes ou colonnes, comme aux échecs). On perd lorsqu'on est obligé de revenir sur une case où la tour s'est déjà arrêtée. Qui gagne ?

Exercice 89 (⋆⋆) On considère un cercle $\mathcal{C}_1$ du plan, d'équation $(x-4)^2 + y^2 = 1$, ainsi qu'une droite l de pente positive qui passe par l'origine et qui est tangente à $\mathcal{C}_1$ en P_1. Le cercle $\mathcal{C}_2$ est tangent à l'axe des abscisse en P_2, passe par P_1 et son centre appartient à l.

Le cercle $\mathcal{C}_3$ est tangent à l en P_3, passe par P_2 et son centre appartient à l'axe des abscisses. Le cercle $\mathcal{C}_4$ est tangent à l'axe des abscisses en P_4, passe par P_3 et son centre appartient à l.

On construit de la même manière les cercles $\mathcal{C}_5, \mathcal{C}_6$, etc. Pour $n \geq 1$, on note S_n l'aire du cercle $\mathcal{C}_n$.

Lorsque N tend vers l'infini, vers quoi converge la somme

$$\sum_{n=1}^{N} S_n \qquad ?$$

Exercice 90 ⋆⋆Soit $n \geq 0$ un entier naturel. Montrer qu'il existe un disque dans le plan contenant exactement n points à coordonnées entières.

Exercice 91 (⋆) Al et Xandre communiquent via un réseau peu fiable : lorsqu'Al envoie un message de n caractères, Xandre reçoit k d'entre eux (dans le même ordre). Sachant que tant que certaines sous-suites du message original ne sont pas sorties, le réseau ne renvoie pas une sous-suite déjà obtenue par Xandre, combien de fois Al doit-il envoyer son message (dont tous les caractères sont distincts) pour être sûr que Xandre puisse le décoder ?

Exercice 92 (⋆) Soit un ensemble de n points (a_i, b_i) dans le carré $[0,1]\times[0,1]$, les a_i différant deux à deux, les b_i aussi, et contenant les points $(0,0)$ et $(1,1)$. Sissi la suave sauterelle veut aller du premier au second, et s'astreint à respecter la règle suivante : si elle est en (a_i, b_i) , elle peut sauter en (a_j, b_j) si et seulement si :

-$a_i < a_j$, $b_i < b_j$,

-il n'y a aucun a_k entre a_i et a_j ou aucun b_k entre b_i et b_j .

Pour la piéger, Arabelle l'araignée acharnée décide de mettre en place une configuration où un tel trajet est impossible. Quelle est la valeur minimale de n pour qu'elle puisse arriver à ses fins ?

Exercice 93 (⋆) Soit $n \geq 4$ un entier. On considère des entiers strictement positifs $a_1, \ldots, a_n$ placés sur un cercle. On suppose que chaque terme a_i ($1 \leq i \leq n$) divise la somme de ses deux voisins, c'est-à-dire qu'il existe un entier k_i tel que

$$\frac{a_{i-1} + a_{i+1}}{a_i} = k_i$$

, avec la convention $a_0 = a_n$ et $a_{n+1} = a_1$. Montrer que

$$2n \leq k_1 + k_2 + \cdots k_n < 3n.$$

Exercice 94 Soit $n \in \mathbb{N}$. Montrer que si $2 + 2\sqrt{28n^2 + 1}$ est un entier, alors c'est un carré parfait.

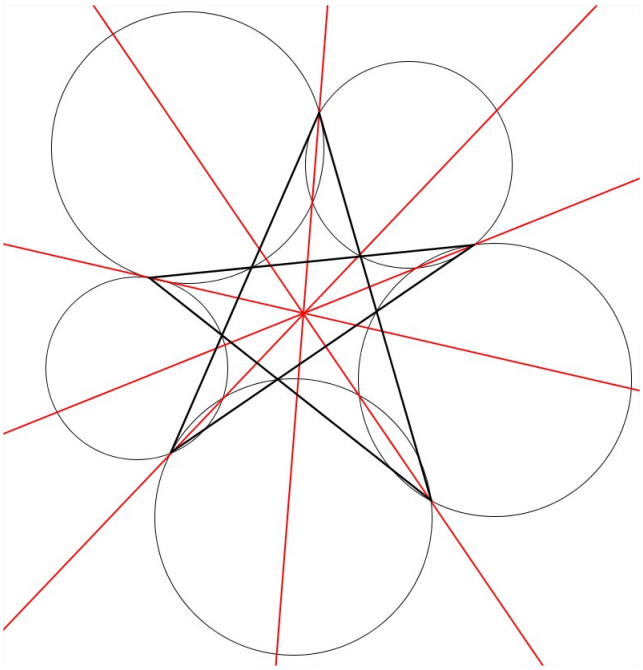
Exercice 95 On écrit un nombre premier $p = a_k a_{k-1} ... a_0$ en base 10 et on pose

$$Q_p(x) = a_k x^k + a_{k-1} x^{k-1} + ... + a_1 x + a_0$$

Montrer que Q_p n'a pas de racines entières sauf pour 4 valeurs de p que l'on déterminera.

Exercice 96 Soit P un polynôme de degré 2015 tel que $P(0) = 0$, $P(1) = 1$, ..., $P(2014) = 2014$ et $P(2015) = 2016$. Combien vaut $P(2016)$?

Exercice 97 Montrer que les droites rouges sur la figure ci-dessous sont concourantes (on part de 5 points du plan formant un pentagone convexe) :



Exercice 98 Soit ABC un triangle d'orthocentre H. On prend un point P sur $[BC]$ et on appelle D le projeté orthogonal de H sur $[AP]$. On trace la parallèle à (BC) passant par D : elle recoupe $(AB$ en E, (AC) en F, le cercle circonscrit à ADB en X et le cercle circonscrit à ADC en Y. Enfin, soit Z l'intersection de (XB) et (YC). Montrer que $ZE = ZF$ si et seulement si P est le milieu de $[BC]$.

Exercice 99 Soit ABC un triangle, D, E, F les points de tangence du cercle inscrit aux côtés $[BC]$, $[CA]$, $[AB]$. Soit Δ la parallèle à (BC) (différente de (BC)) tangente au cercle inscrit. La droite Δ intersecte (AB) et (AC) respectivement en P et Q. Soit T l'intersection de (BC) et (EF), et M le milieu de $[PQ]$. Montrer que (TM) est tangente au cercle inscrit.

Exercice 100 Montrer qu'il existe une infinité d'entiers positifs n tels que $n^2 + 1$ n'ait que 1 et lui-même comme diviseur de la forme $k^2 + 1$.

Exercice 101 (⋆) Soit u_n le nombre de résidus différents, modulo n, des entiers de la forme $k(k+1)/2$ avec $k \geq 0$. Calculer u_n.

Exercice 102 (⋆) Il y a 2014 députés dans une assemblée. Chacun d'eux déteste exactement trois autres députés, sachant que le fait de détester n'est pas nécessairement réciproque : A peut détester B sans que B déteste A. Quel est le plus petit n tel que l'on puisse repartir les 2014 députés en n comités, de sorte qu'aucun député ne se retrouve dans le même comité avec quelqu'un qu'il déteste ?

Exercice 103 (⋆⋆) Soit ABC un triangle dont le cercle circonscrit est noté ω, le centre du cercle inscrit ω_1 est noté I et le centre du cercle exinscrit ω_2 tangent au côté $[BC]$ est noté I_A. Les cercles ω_1 et ω_2 sont tangents à $[BC]$ respectivement en D et en E. Soit finalement M le milieu de l'arc $\widehat{BC}$ qui ne contient pas A. On considère un cercle tangent à ω en un point T et à la droite (BC) en D. Soit S l'intersection de (TI) avec Ω. Prouver que les droites (SI_A) et (ME) se coupent sur ω.

Exercice 104 (⋆⋆) Soient a, b, c des réels strictement positifs tels que

$$a + b + c = a^{1/7} + b^{1/7} + c^{1/7}.$$

Prouver que

$$a^a b^b c^c \geq 1.$$

Exercice 105 (⋆⋆⋆⋆) Alice et Bob jouent sur un échiquier plan infini. Alice commence par choisir une case et la colorie en rouge, puis Bob choisit une case non encore coloriée et la colorie en vert, et ainsi de suite. Alice gagne la partie si elle réussi à colorier en rouge quatre cases dont les centres forment les sommets d'un carré de côtés parallèles à ceux des cases.

a) Prouver qu'Alice possède une stratégie gagnante.

b) Qu'en est-il si Bob a, lui, le droit de colorier deux cases en vert à chaque coup ?

Exercice 106 Soit ABC un triangle et N son point de Nagel. Soit Δ une droite qui passe par N. La droite Δ recoupe (BC), (CA) et (AB) en D, E et F respectivement. Soit X le symétrique de D par rapport au milieu de $[BC]$. On définit de même Y et Z.

(i) Montrer que X, Y et Z sont alignés.

(ii) Montrer que la droite passant par XYZ est tangente au cercle inscrit de ABC.

Exercice 107 (⋆) Soit n un nombre parfait, c'est-à-dire un entier tel que

$$\sum_{d|n} d = 2n.$$

On factorise n sous la forme d'un produit de nombres premiers :

$$n = \prod_{i=1}^{k} p_i^{\alpha_i},$$

avec $p_1 < p_2 < \ldots < p_k$. Montrer que α_1 est pair.

Exercice 108 On place quatre points dans le plan, et on suppose que les six distances qui les relient entre eux sont toutes entières. Montrer qu'alors au moins une d'entre elles est divisible par 3.

Exercice 109 (**) Soit $ABCD$ un quadrilatère tel que $AC = BD$. Soit P le point d'intersection des diagonales (AC) et (BD). On note ω_1 le cercle circonscrit de ABP. Soit O_1 le centre de ω_1. On note ω_2 le cercle circonscrit de CDP. Soit O_2 le centre de ω_2. On note S et T les intersections respectives de ω_1 et ω_2 avec $[BC]$ (autres que B et C). Soient M et N les milieux respectifs des arcs $\widehat{SP}$ (ne contenant pas B) et $\widehat{TP}$ (ne contenant pas C). Prouver que les droites (MN) et (O_1O_2) sont parallèles.

Exercice 110 Soit ABC un triangle. Soit K l'intersection des tangentes au cercle circonscrit de ABC en B et en C, et soit A' le second point d'intersection de (AX) avec le cercle circonscrit de ABC. On définit similairement B' et C' de manière cyclique. Soit P est un point quelconque. On définit les secondes intersections de (AP), (BP) et (CP) avec le cercle circonscrit de ABC comme étant A'', B'' et C''. Soit X l'intersection de (BC) et de $(A'A'')$, et on définit similairement Y et Z de manière cyclique. Montrer que X, Y et Z sont alignés.

Exercice 111 (****) L'ensemble $\{1, 2, \ldots, 3n\}$ est partitionné en trois ensembles A, B et C de n éléments chacun.

Montrer qu'il est possible de choisir un élément dans chacun de ces trois ensembles, tels que la somme de deux d'entre eux soit égale au troisième.

Exercice 112 Soient a, b et c les côtés entiers et premiers entre eux d'un triangle rectangle. Montrer que si c est un carré parfait, alors l'aire du triangle est divisible par 84.

Exercice 113 (*****) Les élèves d'une classe sont allés se chercher des glaces par groupe d'au moins deux personnes. Il y a eu $k > 1$ groupes en tout. Deux élèves quelconques sont partis ensemble exactement une fois.

Prouver qu'il n'y a pas plus de k élèves dans la classe.

Exercice 114 (*) Soit m et n deux entiers naturels non nuls. On note $\phi(m, n)$ le cardinal de l'ensemble $\{k : 1 \leq k \leq n, \mathrm{PGCD}(k, m) = 1\}$. Trouver tous les entiers $m \geq 1$ tels que $n\phi(m, m) \leq m\phi(m, n)$ pour tout $n \in \mathbb{N}^*$.

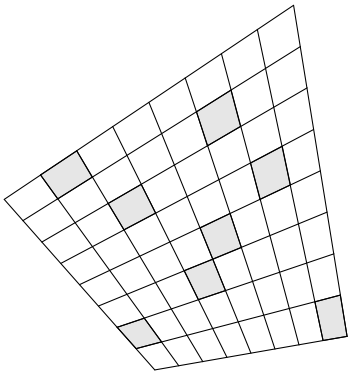
Exercice 115 (**) Trouver toutes les fonctions $f : \mathbb{R}_+ \to \mathbb{R}_+$ telles que pour tous $a > b > c > d > 0$ vérifiant $ad = bc$ on ait

$$f(a + d) + f(b - c) = f(a - d) + f(b + c).$$

Exercice 116 Trouver tous les entiers x et y tels que

$$y^2 = x^3 + (x + 4)^2.$$

Exercice 117 (***) On prend un quadrilatère convexe $ABCD$, et on divise chacun de ses côtés en N portions égales. On relie ensuite ces différentes portions de façon à former un quadrillage $N \times N$, comme sur la figure. On sélectionne ensuite N quadrilatères de ce quadrillage, de telle sorte qu'il n'y en ait pas deux sur la même ligne ou sur la même colonne du quadrillage. Calculer l'aire totale de tous ces quadrilatères.



Exercice 118 (****) Une suite croissante $(s_n)_{n\geq 0}$ est dite super-additive si pour tout couple (i,j) d'entiers on a $s_{i+j} \geq s_i + s_j$. Soient (s_n) et (t_n) deux telles suites super-additives. Soit (u_n) la suite croissante d'entiers vérifiant qu'un nombre apparaît autant de fois dans (u_n) que dans (s_n) et (t_n) combinées.

Montrer que (u_n) est elle aussi super-additive.

Exercice 119 (****) Soit ABC un triangle, soit $A'B'C'$ un triangle directement semblable à ABC de telle sorte que A appartienne au côté $B'C'$, B au côté $C'A'$ et C au côté $A'B'$. Soit O le centre du cercle circonscrit à ABC, H son orthocentre et H' celui de $A'B'C'$.

Montrer qu'on a $OH = OH'$.

Exercice 120 Trouver le plus petit réel M tel que

$$|(a-b)(a-c)(b-c)(a+b+c)| \leq M(a^2+b^2+c^2)^2$$

pour tous nombres réels a, b, c.

Exercice 121 (*) Soit $k \geq 6$ un entier et P un polynôme à coefficients entiers tel qu'il existe k entiers distincts $x_1, \ldots, x_k$ tels que pour tout $i \in \{1, \ldots, k\}$, $P(x_i) \in \{1, \ldots, k-1\}$. Montrer que $P(x_1) = \ldots = P(x_k)$.

Exercice 122 (*) Soient $k \geq 2$ un entier et $a \geq k-1$ un nombre réel. Montrer que pour tout n-uplet de nombres réels strictement positifs $(x_1, \ldots, x_n)$ on a

$$\frac{x_1 + \cdots + x_n}{1+a} \leq \frac{x_1^{k+1}}{x_1^k + ax_2^k} + \cdots + \frac{x_n^{k+1}}{x_n^k + ax_1^k}.$$

Exercice 123 (*) On considère une ligne de n carrés. On note $S(n)$ le nombre minimal de carrés à colorier en bleu tels que chacun des $n-1$ traits séparant deux cases voisines soit à égale distance de deux cases bleues. Montrer que

$$\lfloor 2\sqrt{n-1} \rfloor + 1 \leq S(n) \leq \lfloor 2\sqrt{n} \rfloor + 1.$$

Exercice 124 Soit $n \geq 3$ un nombre entier et $x_1, \ldots, x_n$ des nombres réels strictement positifs. Montrer que

$$\frac{x_1}{x_2+x_3} + \frac{x_2}{x_3+x_4} + \ldots + \frac{x_n}{x_1+x_2} \geq \frac{5}{12}.$$

Exercice 125 (⋆) Soit $k \geq 1$ un entier. Trouver tous les polynômes P à coefficients entiers tels que $P(n)$ divise $(n!)^k$ pour tout entier $n \geq 1$.

Exercice 126 (⋆) On dit qu'une permutation $a_1, \ldots, a_n$ des entiers $1, 2 \ldots, n$ est *sympathique* s'il existe au moins un carré parfait parmi les entiers $a_1, a_1 + a_2, \ldots, a_1 + a_2 + \cdots + a_n$. Trouver tous les entiers n tels que toutes les permutations de $1, 2 \ldots, n$ soient sympatiques.

Exercice 127 (⋆⋆⋆⋆) On considère un ensemble de $2n + 1$ droites du plan, deux jamais parallèles ni perpendiculaires et trois jamais concourantes. Trois droites forment donc toujours un triangle non-rectangle.

Déterminer le nombre maximal de triangles aigus qui peuvent ainsi être formés.

Exercice 128 (⋆⋆) Soit n un entier. Dans les lignes d'un tableau de 2^n lignes et n colonnes on place tous les n-uplets formés de 1 et de -1. Ensuite, on efface certains de ces nombres, et on les remplace par des 0. Prouver que l'on peut trouver un ensemble de lignes dont la somme est nulle (i.e., tel que, pour tout i, la somme des nombres appartenant à la colonne i d'une ligne de notre ensemble soit nulle).

Exercice 129 Soit X un point à l'intérieur du triangle ABC tel que $XA.BC = XB.CA = XC.AB$. Soient I_1, I_2, I_3 les centre des cercles inscrits respectifs de BXC, AXC et AXB. Montrer que les droites AI_1, BI_2 et CI_3 sont concourantes.

Exercice 130 (⋆⋆⋆) Soit ABC un triangle, et O un point à l'intérieur de ce triangle. Quel est le point M minimisant la quantité $AM + BM + CM + OM$?

Exercice 131 (⋆) Soient a, b, c des nombres réels strictement positifs tels que $a + b + c = 3$. Prouver que

$$\frac{a}{1 + (b + c)^2} + \frac{b}{1 + (a + c)^2} + \frac{c}{1 + (a + b)^2} \leq \frac{3(a^2 + b^2 + c^2)}{a^2 + b^2 + c^2 + 12abc}.$$

Exercice 132 (⋆) Soit ABC un triangle non isocèle. Son cercle inscrit, de centre I, touche le côté $[BC]$ en D. Soit X un point de l'arc $\widehat{BC}$ du cercle circonscrit de ABC tel que si E, F sont respectivement les projetés orthogonaux de X sur (BI) et (CI) et M le milieu de $[EF]$, alors $MB = MC$. Prouver que $\widehat{BAD} = \widehat{CAX}$.

Exercice 133 (⋆⋆⋆⋆⋆) Soit E un ensemble de $n \geq 2$ points du plan. On désigne respectivement par D et d la plus grande et la plus petite distance entre deux points distincts de E.

Prouver que :

$$D \geq \frac{\sqrt{3}}{2}(\sqrt{n} - 1)d.$$

Exercice 134 (⋆⋆⋆⋆) Soit S un ensemble infini de points du plan tel que si A, B et C sont trois points quelconques dans S, la distance de A à la droite (BC) soit un entier.

Prouver que les points de S sont tous alignés.

Exercice 135 (***) Soient $a, b, c > 0$ des nombres réels tels que $a + b + c = 3$. Prouver que :

$$\frac{ab}{b^3+1} + \frac{bc}{c^3+1} + \frac{ca}{a^3+1} \leq \frac{3}{2}.$$

Exercice 136 (*****) Trouver toutes les fonctions continues $f : \mathbb{C} \to \mathbb{C}$ vérifiant :

$$f(x+y)f(x-y) = f(x)^2 - f(y)^2.$$

Exercice 137 Soit ABC un triangle, I son centre du cercle inscrit. Soient D, E et F ses projetés sur les côtés de ABC. Soient P et Q les intersections de la droite (EF) avec le cercle circonscrit de ABC. Soient O_1 et O_2 les centres des cercles circonscrits de AIB et de AIC. Montrer que le centre du cercle circonscrit de DPQ est sur la droite (O_1O_2).

Exercice 138 (**) Soient P, Q deux polynômes non nuls à coefficients entiers tels que $\deg P > \deg Q$. On suppose que le polynôme $p \cdot P + Q$ possède une racine rationnelle pour une infinité de nombre premiers p. Montrer qu'au moins une racine de P est rationnelle.

Exercice 139 (***) Soient P et Q deux polynômes à coefficients entiers, premiers entre eux. Pour tout entier n, posons $u_n = PGCD(P(n),\ Q(n))$. Montrer que la suite (u_n) est périodique.

Exercice 140 (****) On veut colorier certains des points de l'ensemble $E_n = \{(a, b)/a, b$ entiers et $0 \leq a, b \leq n\}$ de sorte que tout carré $k \times k$ dont les sommets sont dans E_n contienne au moins un point colorié sur son bord. On note $m(n)$ le nombre minimum de points à colorier pour que la condition désirée soit satisfaite.

Prouver que

$$\lim_{n\to+\infty} \frac{m(n)}{n^2} = \frac{2}{7}.$$

Exercice 141 (*) Soit Γ le cercle circonscrit d'un triangle acutangle ABC. Le point D est le centre de l'arc $\widehat{BC}$ contenant A, et I est le centre du cercle inscrit de ABC. La droite (DI) coupe (BC) en E et recoupe Γ en F. Soit P un point de la droite (AF) tel que (PE) et (AI) soient parallèles. Prouver que (PE) est la bissectrice de l'angle $\widehat{BPC}$.

Exercice 142 Soit ABC un triangle. On note D, E, F les points de tangence du cercle inscrit de centre I de ABC avec les côtés de ABC. Soit X le point de $[AB]$ tel que (XD) et (EF) soient perpendiculaires. Soit Y le second point d'intersection des cercles AEF et ABC. Montrer que le triangle XYF est rectangle.

3 Solutions des élèves

Solution de l'exercice 1 (Résolu par Sylvain Procope-Mamert et Solal Gaudin) On découpe la liste des longueurs $l_1 \leq \cdot \leq l_n$ en 3 paquets. Initialement, le premier paquet P_1 contient l_n, P_2 contient le reste et P_3 contient le reste. Tant que $P_2 > P_1 + P_3$ on transfère une longueur de P_2 vers P_3. Il arrive un moment où pour une certaine longueur x, $P_2 > P_1 + P_3$ et $P_2 - x \leq$

$P_1 + P_3 + x$. L'hypothèse de l'énoncé donne $P_1 \leq P_2 + P_3$, et $P_3 + x \leq P_2 - P_1 + x \leq P_2 - x + P_1$ car l_n est la plus grande longueur. On obtient donc un triangle (éventuellement plat) qui est un n-gone convexe.

Solution de l'exercice 2 (Résolu par Étienne Massart et Arthur Léonard)

Supposons par l'absurde qu'il existe un nombre négatif $-x$, avec $x > 0$. Alors, on peut isoler cet élément négatif et partitionner les $2n$ nombres restants en deux groupes de n nombres de somme S_1 et S_2. Si on exploite la condition de l'énoncé en regroupant l'élément négatif dans le groupe de somme S_1, on sait que

$$S_1 - x \geq S_2$$

Si on fait de même en mettant cette fois-ci l'élément négatif avec le groupe de somme S_2 on obtient

$$S_2 - x \geq S_1$$

En combinant ces deux dernières inégalités, il vient

$$(S_2 - x) - x \geq S_1 - x \geq S_2$$

Ainsi $S_2 - 2x \geq S_2$. Contradiction.

Solution de l'exercice 4 (Résolu par Théodore Fougereux et Arthur Léonard) L'égalité se réécrit

$$(a-b)^2 + (a-1)^2 + (b+1)^2 = 0.$$

Un carré étant toujours positif, on doit avoir $a = b$, $a = 1$ et $b = -1$, ce qui est impossible. Il n'y a donc pas de solution.

Solution de l'exercice 6 (Résolu par Théodore Fougereux) Alexandra sépare 10^{2013} en 2^{2013} et 5^{2013} au premier coup. Le jeu est ainsi "séparé" en deux parties (tout nombre ayant une unique décomposition en facteurs premiers, on ne peut obtenir un même entier > 1 à partir de 2^{2013} et de 5^{2013}), qui sont identiques (on part d'un nombre premier à la puissance 2013). Quoique fasse Béatrice dans l'une, Alexandra fait la même chose dans l'autre. Béatrice finira par être bloquée car il n'y a qu'un nombre fini de décompositions ou suppressions faisables. Donc elle perdra.

Solution de l'exercice 7 (Résolu par Solal Gaudin) Supposons qu'il existe un nombre fini de premiers ne se terminant pas par 1. On prend leur produit (en mettant 2 et 5 de côté). Si le résultat termine par 3, on multiplie par 7 et réciproquement, et s'il termine par 9 on multiplie par 9. On rajoute 2, et le nouveau nombre termine par 3. Il a un facteur premier qui ne se termine pas par 1, et différent de tous les précédents car premier avec eux. Contradiction.

Solution de l'exercice 9 (Résolu par Antoine Stark) On a $y^k = x(x+1)$, or x et $x+1$ sont premiers entre eux. Il existe donc $u, v \in \mathbb{N}$ tels que $x = u^k$ et $x + 1 = v^k$. Comme $k \geq 2$, $v^k \geq (u+1)^k \geq u^k + 1$ sauf si $u = 0$. Ainsi, la seule solution est $(x, y) = (0, 0)$.

Solution de l'exercice 11 (Résolu par Sylvain Procope-Mamert et Solal Gaudin) Soit A_1 et A_2 les deux quantités à comparer. On pose $x = AB, y = PQ$ et $z = BD$. $A_1 = Aire(ABP) + Aire(DRC) + Aire(BPQ) + Aire(DSR)$, donc $A_1 = Aire(ABP) + Aire(DRC) + PQ \times \left(\frac{BD-PQ}{2}\right) = Aire(ABP) + Aire(DRC) + \frac{y(z-y)}{2}$. On peut inscrire $PQRS$ dans un carré dont les bords sont

parallèles à ceux du grand. Notons d son côté, on a $2A_1 = x(x-d) + y(z-y)$. On obtient la même chose pour A_2, exercice résolu !

Solution de l'exercice 12 (Résolu par Antoine Stark) On doit résoudre $4a^b = (m-1)(m+1)$. m doit être impair. Posons $x = \frac{m-1}{2}$. Le problème se ramène à $a^b = x(x+1)$. Comme dans l'exercice 9, x et $x+1$ sont des puissances b-èmes. On trouve comme solutions $a = 0, m = 1$ et $b \in \mathbb{N}^*$, ou bien $b = 1$, m impair quelconque et $a = \frac{m^2-1}{4}$ (a est toujours entier car un carré impair vaut 1 modulo 4).

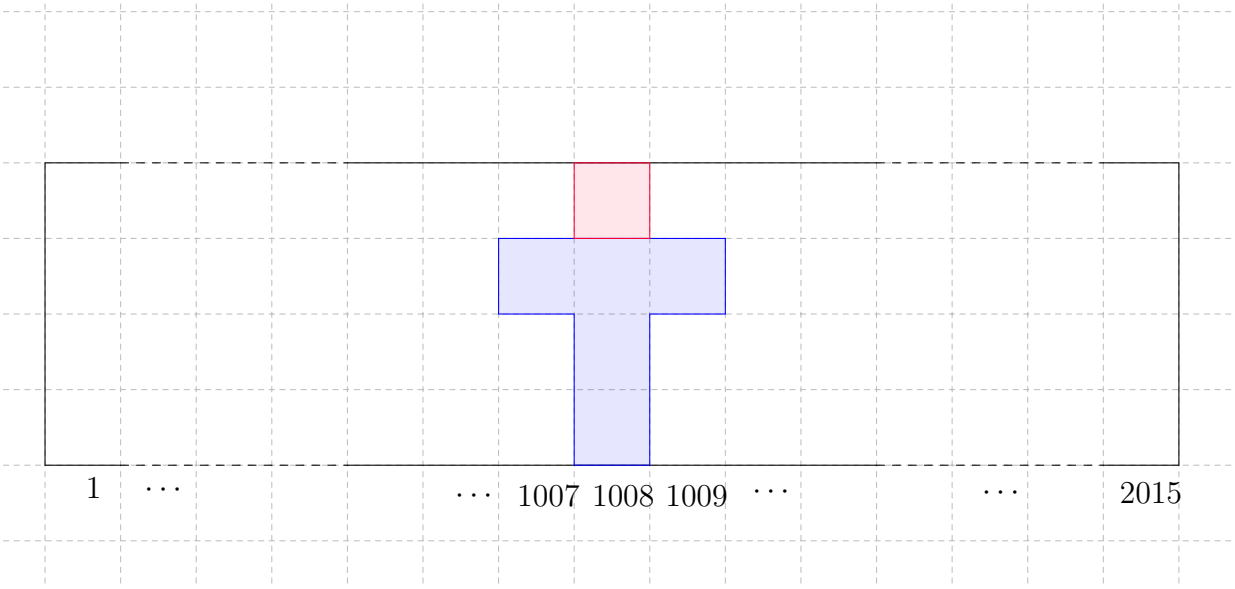
Solution de l'exercice 14 (Résolu par Antoine Stark) On a $r - \sqrt{13} = \sqrt{2} + \sqrt{5}$. On met au carré, on développe, on isole les racines d'un côté de l'équation. On remet au carré et on trouve

$$\frac{r^4 - 40r^2 - 4}{840} = \sqrt{130}.$$

Si r était rationnel, $\sqrt{130}$ le serait aussi. Or 130 n'est pas un carré parfait donc $\sqrt{130}$ est irrationnel [comme pour $\sqrt{2}$, cela peut se prouver par l'absurde en regardant la valuation 2-adique), impossible.

Solution de l'exercice 16 (Résolu par Sylvain Procope-Mamert) On prend P un sommet du polyèdre. On fait le tour de ses voisins dans le sens trigonométrique. Il y a un triangle équilatéral lorsqu'il y a un changement de couleur. Comme on revient sur la couleur dont on était parti, il y a un nombre pair de changements de couleur. Soit n le nombre de triangles équilatéraux. En sommant les nombres de changements de couleur par sommet, on obtient $3n$, qui est donc pair. On en déduit que 2 divise n, ce qu'on voulait démontrer.

Solution de l'exercice 18 (Résolu par Théodore Fougereux) Le premier joueur commence par placer le pentomino en position verticale sur la 1008ème colonne comme sur le dessin suivant.



Le deuxième joueur est obligé de placer ses pentominos soit à gauche, soit à droite, et ne peut pas recouvrir la case en rouge. Le premier joueur n'a ensuite plus qu'à jouer le coup symétrique, ainsi il pourra toujours jouer quelque chose, jusqu'à ce que le second joueur se retrouve bloqué.

Solution de l'exercice 19 (Résolu par Théodore Fougereux et Étienne Massart) Le nombre a le même résidu modulo 9 que la somme de ses chiffres, donc ce résidu doit être égal à son carré,

soit 0 ou 1. On teste donc les carrés congrus à 0 ou 1 modulo 9 entre 0 et 729, et seuls $0, 1, 81$ vérifient l'énoncé.
Or si le nombre a 3 chiffres, sa somme des chiffres est au plus $9+9+9 = 27 = \sqrt{729}$. Donc une autre solution aurait au moins 4 chiffres. Le carré de sa somme des chiffres serait au plus 1296, donc ce nombre comporte "au mieux" un 1 et 3 9 donc sa somme des chiffres serait finalement majorée par $28 = \sqrt{784}$. Donc il faudrait au moins 5 chiffres.
Le carré de la somme des chiffres d'un nombre à n chiffres vaut au plus $81n^2$. Une récurrence rapide donne $81n^2 \leq 10^n$ pour $n \geq 5$. Donc les 3

Solution de l'exercice 21 (Résolu par Arthur Léonard)
D'après la formule du binôme de Newton,

$$\left(1+\frac{a}{b}\right)^n + \left(1+\frac{b}{a}\right)^n = \sum_{i=0}^{n} \binom{n}{i} \left(\frac{a^i}{b^i} + \frac{b^i}{a^i}\right)$$

Or, on sait d'après l'inégalité arithmético-géométrique que $\left(\frac{a^i}{b^i} + \frac{b^i}{a^i}\right) \geq 2$.
Donc

$$\left(1+\frac{a}{b}\right)^n + \left(1+\frac{b}{a}\right)^n \geq 2\sum_{i=0}^{n} \binom{n}{i}$$

Puisque $\sum_{i=0}^{n} \binom{n}{i} = 2^n$, on obtient la conclusion cherchée.

Solution de l'exercice 23 (Résolu par Solal Gaudin) On appelle une famille un ensemble de condylures qui ont deux-à-deux un lien de parenté. On voit aisément qu'une famille est constituée d'une suite de bestioles descendant les unes des autres. S'il n'y a qu'au plus b familles différentes, par principe des tiroirs, il y en a une ayant au moins $a+1$ membres. D'après la remarque initiale, elle descendent les unes des autres.

Solution de l'exercice 25 (Résolu par Arthur Léonard et Théodore Fougereux) Un des cubes doit être supérieur à $2015/3$. Les seules possibilités sont $729, 1000, 1331$ et 1728. Dans chaque cas, on teste toutes les possibilités pour les deux autres entiers (qui sont plus petits que $\sqrt[3]{2015}$), et aucun ne fonctionne. Il n'y a donc pas de solution.

Autre solution en raisonnant modulo 2 Remarquons que 2015 est impair et pour tout $x \in \mathbb{N}$ $x^3 \equiv x\,(2)$. Dans la suite on suppose que $x_1^3 + x_2^3 + x_3^3 = 2015$, les x_i dans $\mathbb{N}$, avec $x_1 \leqslant x_2 \leqslant x_3$.

Comme $13^3 > 2015$, les x_i impairs sont inférieurs à 11, et comme $2 \times 11^3 > 2015$, il y a au plus une fois 11. On fait une disjonction selon le nombre de x_i impairs (il y en a un ou trois) :

1. Un seul des x_i est impair. Il est congru à 7 modulo 8 et plus petit que 11, c'est donc 7. On calcule alors $2015 - 7^3 = 1672$, dont il s'agit de montrer que ce n'est pas une somme de deux cubes pairs. Si c'était le cas, alors le plus grand des deux serait 10 et 672 n'est pas un cube.

2. Les x_i sont tous impairs. Puisque $7^3 + 7^3 + 9^3 = 729 + 686 < 2015$, nécessairement $x_3 \geqslant 9$, et si $x_3 = 9$ alors $x_2 = 9$; mais on a les encadrements assez faciles à vérifier

$$7^3 + 9^3 + 9^3 < 2015 < 3 \times 9^3$$

Donc nécessairement $x_3 = 11$, et il reste à voir que $2015 - 11^3 = 754$ n'est pas somme de deux cubes. Puisque $754 > 686 = 2 \times 7^3$, l'un des deux serait 9, et $754 - 729 = 35$ n'est pas un cube.

Solution de l'exercice 27 (Résolu par Étienne Massart et Théodore Fougereux) On a $2^{25} - 1$ groupes non vides, ce qui est bien plus que le nombre de sommes différentes de masses (moins que 25000000). On a donc deux groupes différents non vides de même masse. On retire les vaches en commun à ces groupes et il reste deux groupes non vides de même masse.

Solution de l'exercice 30 (résolu par Sylvain Procope-Mamert) On ne peut pas avoir $x = 0$ car sinon $-yp = 5p$ ce qui n'est pas possible. De même pour y donc, $x, y > 0$. L'équation de départ est équivalente à $xy(x + y) = p(5 + x + y)$. Le nombre p doit diviser xy ou $x + y$.

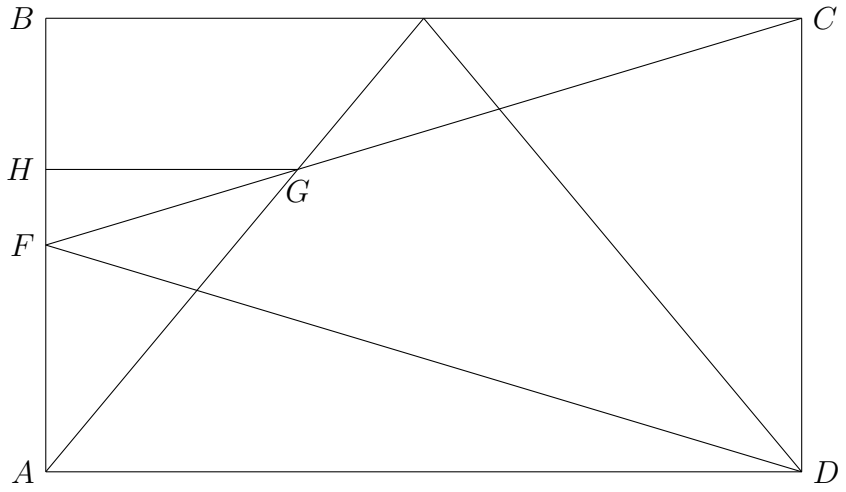
Cas $p|xy$: Soit $k = xy/p$, on doit avoir $kp(x + y) = p(5 + x + y)$, soit $(k - 1)(x + y) = 5$. Comme $x + y \geq 2$, on a $k = 2$ et $x + y = 5$. Ceci donne les solutions $(x, y) = (2, 3)$ ou $(3, 2)$, $p = 3$, et $(x, y) = (1, 4)$ ou $(4, 1)$, $p = 2$.

Cas $p|(x+y)$: Soit $k = (x+y)/p$. On doit avoir $kxy = 5+x+y = 5+kp$, donc k doit diviser 5. Si $k = 5$, on obtient $xy = 1 + p$ d'où $x + y \leq 2 + p$. Or on a aussi $x + y = 5p$, ce qui donne une contradiction puisque $p \geq 2$. On a donc $k = 1$, puis $x + y = p$, $xy = p + 5$. Si $p = 2$, la première équation donne $x = y = 1$ ce qui contredit la deuxième. On a donc p impair, soit $p = 2n + 1$ avec $n \geq 1$. Il existe alors $m \geq 0$ tel que $x = n + 1 + m$ et $y = n - m$, ou le contraire. On a alors $xy = (n + 1 + m)(n - m) = p + 5 = 2n + 6$, ce qui implique que $(n - m - 1)(n + m) = 6$. Comme le deuxième facteur est le plus grand, on a $n + m = 3$, $n - m - 1 = 2$, ou $n + m = 6$, $n - m - 1 = 1$. Dans le deuxième cas, $n = 4$, et $p = 2n + 1 = 9$, ce qui contredit la primalité de p. Donc on est dans le premier cas, $n = 3$, $m = 0$, $x = 4$, $y = 3$ (ou l'inverse) et $p = 7$.

En conclusion, les solutions (p, x, y) possibles sont $(2, 1, 4)$, $(2, 4, 1)$, $(3, 2, 3)$, $(3, 3, 2)$, $(7, 3, 4)$ et $(7, 4, 3)$, et donc les valeurs possibles de p sont $2, 3$ et 7.

Solution de l'exercice 31 (Résolu par Nathanaël Boutillon et Pablo Destic) Soit P_n : "Il est possible de relier $2n$ points avec $n^2 + 1$ segments sans former un seul trinagle, c'est-à-dire sans que 3 points puissent être reliés 2 à 2."
P_2 est clairement fausse, pour montrer que P_n est fausse pour tout $n \geq 2$, il suffit de montrer que P_{n+1} implique P_n.
Supposons P_{n+1}. Considérons 2 points reliés d'une configuration à $2n + 2$ points . Soit x le nombre de segments partant d'un des deux points. Si $x \geq 2n + 1$, alors il existe un sommet parmi les $2n$ restants qui soit relié aux deux points, et on a trouvé un triangle : contradiction avec notre hypothèse. Donc $x \leq 2n$, et parmi les $2n$ points restants, il reste $n^2+2n+2-1-x \geq n^2 + 1$ segments sans qu'on ait de triangle. Ainsi, P_{n+1} implique bien P_n, d'où la conclusion.

Solution de l'exercice 33 (Résolu par Antoine Stark) On se place dans le quart inférieur droit du rectangle, qui contient par symétrie le quart de l'octogone. La réponse correspond donc au rapport des aires de $BEGF$ et de $ABCD$ (voir figure).



G est à l'intersection des droites (AE) et (FC). Un calcul de coordonnées dans le repère $(A, \overrightarrow{AD}, \overrightarrow{AB})$ donne $HG = \frac{1}{3}AD$, (HG) étant parallèle à (AD). Comme $AF = \frac{1}{2}AB$ (appliquer Thalès dans le grand rectangle initial par exemple), on a $Aire(AFG) = \frac{1}{2}AF \times HG = \frac{AB \times AD}{12}$. On voit aisément que $Aire(AED) = \frac{AB \times AD}{2}$ et $Aire(ECD) = \frac{1}{4}AB \times AD$. Donc $Aire(BEGF) = Aire(ABCD) \times \left(1 - \frac{1}{2} - \frac{1}{4} - \frac{1}{12}\right)$, donc

$$Aire(BEGF) = \frac{1}{6}Aire(ABCD.$$

L'aire de l'octogone est donc $\frac{1}{6}$.

<u>*Solution de l'exercice 34*</u> (Résolu par Étienne Massart, Théodore Fougereux, Arthur Léonard et Julien Véron) • Si $x = 1$, les solutions sont celles telles que $2z = 3y$, donc les solutions sont les triplets $(1, 2k, 3k)$ avec $k \in \mathbb{N}^*$.
• Si $y = 2$, les solutions sont de même les triplets $(k, 2, 3k)$ avec $k \in \mathbb{N}^*$.
• Si $x = 2$, on a $\frac{1}{2} = \frac{2}{y} - \frac{3}{z}$ donc $\frac{6y}{4-y} = z$. Comme z est positif, $y \leq 3$. On vérifie que la seule solution est $(2, 3, 18)$.
• Si $y = 1$, de même $\frac{z}{3-z} = x$, donc $z \leq 2$, et $(2, 1, 2)$ est la seule solution.
• Si $x \geq 3$, $y \geq 3$, alors $\frac{1}{x} + \frac{2}{y} - \frac{3}{z} < \frac{1}{x} + \frac{2}{y} \leq 1$ donc l'équation n'a pas d'autre solution.

<u>*Solution de l'exercice 35*</u> (Résolu par Sylvain Procope-Mamert et Cyril Miras) Précisons que la fraction obtenue est irréductible (énoncé flou).
Notons $\frac{p_1}{q_1}$ et $\frac{p_2}{q_2}$ les deux fractions sous forme irréductible. L'égalité de l'énoncé donne $p_1p_2 = p_1q_2 + p_2q_1$. Posons $p_i = q_i + k_i$ pour $i = 1, 2$, on obtient $q_1q_2 = k_1k_2$. Or $pgcd(q_i, k_i) = 1$ donc $q_i = \pm k_{3-i}$. On peut supposer $p_i \geq 0$ donc $q_i = \pm k_{3-i}$. Donc $p_1 = p_2 = q_1 + q_2$. Et, $2007|q_1q_2$ et $q_1q_2|2007p_1p_2$ (puisqu'on divise p_1p_2/q_1q_2 en haut et en bas par $q_1q_2/2007$ pour obtenir la fraction de dénominateur 2007. Soit n un diviseur premier de $\frac{q_1q_2}{2007}$. Si n divise q_1, comme n divise $p_1p_2 = p_1^2$, n divise p_1 or p_1 et q_1 sont premiers entre eux, absurde. Donc $q_1q_2 = \pm 2007$. Comme $pgcd(q_1, q_2) = 1$ et $2007 = 9 \times 223$, on a sans restriction $q_1 = \pm 1$, $q_2 = \pm 2007$, ou $q_1 = 9, q_2 = \pm 223$. Soit N le numérateur cherché, on a donc $N = p_1p_2 = (q_1 + q_2)^2$.
Les valeurs possibles de $|q_1 + q_2|$ sont donc $2007 + 1, 2007 - 1, 223 + 9, 223 - 9$. On a donc 4 possibilités pour N, $214^2, 232^2, 2006^2$ et 2008^2. On vérifie aisément que $\frac{p_1}{q_1}$ et $\frac{p_2}{q_2}$ sont bien irréductibles dans ces cas-là.

Solution de l'exercice 36 (Résolu par Antoine Stark) Les 7 entiers sont $1, 2, 3, 4, 6, 8, 24$ et leur somme 48. En effet, ils sont distincts donc leur somme vaut au moins $1+2+3+4+5+6+7 = 28$. Seuls $30, 36, 40$ et 42 ont au moins 7 diviseurs. Et la somme des 7 plus petits est à chaque fois plus grande qu'eux.

Solution de l'exercice 40 (Résolu par Lucien Hua, Richard Pholvichitch et Théodore Fougereux) Il faut fusionner autant de fois qu'on sépare pour avoir le même nombre de piles à la fin. On rajoute donc un nombre pair de jetons durant le jeu. Or on en avait un nombre impair au départ (2 plus 2013 nombres impairs), donc on ne peut pas en avoir un nombre pair à l'arrivée, en particulier pas 2014×2014^{2014}.

Solution de l'exercice 41 (Résolu par Sébastien Zeitoun) Si a, b, c sont les longueurs des projections orthogonales de M sur $[BC]$, $[AC]$ et $[AB]$, et si S est l'aire du triangle, L la longueur d'un côté, on trouve : $a + b + c = \frac{2S}{L}$ donc cette quantité est bien constante.

Solution de l'exercice 42 (Résolu par Julien Vanel) Le jeu consiste en fait à rajouter tour à tour une dimension choisie du rectangle à l'autre. A joue et laisse un rectangle 2×1. Si B laisse un 3×2, A peut faire un 5×2, donc elle préfère laisser un 3×1. A est alors obligé de laisser un 4×3. On définit alors la suite (u_n) par $u_0 = 3, u_1 = 4$ puis $u_{n+1} = u_n + u_{n-1}$: les dimensions du rectangle après $n + 3$ tours sont (u_n, u_{n+1}) si on n'augmente jamais deux fois de suite le même côté. On vérifie que u_n est périodique modulo 5 (la période vaut 4, les résidus successifs étant $3, 4, 2, 1, 3, 4, 2, 1, 3, 4...$). On vérifie de même que $u_n + u_{n+2} \equiv 0 \pmod 5$, c'est-à-dire que si un des deux joueurs augmente le côté qui venait d'être augmenté (on obtient alors un rectangle de dimensions (u_n, u_{n+2}), son adversaire gagne en jouant bien. Ainsi, pour ne pas perdre, on est obligé de ne pas augmenter le côté qui venait d'être augmenter.
Conclusion : le jeu se poursuit indéfiniment.

Solution de l'exercice 55 (Résolu par François Sellier et Yakob Kahane) Montrons que P tel que $P(-2) = n$ existe et est unique. Unicité : Si $P(-2) = Q(-2), (P = \sum a_i X^i, Q = \sum b_i X^i)$, modulo 2 on voit que $a_0 = b_0$. Puis modulo 4, on voit $a_1 = b_1$. On continue ainsi et $P = Q$.
Existence : il y a 2^{2k+1} polynômes P de degré au plus $2k$. $P(-2)$ est entier, et sa valeur est comprise entre $m_k := -2 - 2^3 - \cdots - 2^{2k-1}$ et $M_k := 1 + 4 + \cdots + 2^{2k}$. Donc il peut prendre $M_k - m_k + 1$ valeurs. Or $M_k - m_k + 1 = 2^{2k+1}$ et on a vu que deux polynômes différents prenaient des valeurs différentes. Conclusion : $P \mapsto P(-2)$ qui à un polynôme de degré au plus $2k$ associe sa valeur en 2 est bijective vers $\{-m_k, 1 - m_k, \cdots, M_k - 1, M_k\}$. Donc chaque entier entre m_k et M_k est atteint par un polynôme convenable. Et m_k tend vers $-\infty$, M_k tend vers $+\infty$. Donc tout entier relatif est atteint.

Solution de l'exercice 56 (Résolu par Yakob Kahane et François Sellier) Montrons que $n \leq 5$. Soit $a_1, \cdots, a_k$ les éléments de A. On écrit $a_1 = pgcd(A) \times p_1^{\alpha_1} \times \cdots \times p_j^{\alpha_j}$ (décomposition en facteurs premiers de $\frac{a_1}{pgcd(A)}$). Pour tout $1 \leq i \leq j$, il existe a_i' dans A tel que p_i ne divise pas $\frac{a_i}{pgcd(A)}$. Si on prend $B = (a_1, a_1', a_2', \cdots, a_j')$, on voit ainsi que $pgcd(B) \leq pgcd(A)$. Et $pgcd(A) \leq pgcd(B)$ car $B \subset A$, donc il y a égalité. a_1 est clairement supérieur au produit des j plus petits nombres premiers, or $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 > 2013$, donc $j \leq 4$ et on peut prendre B de cardinal au plus $4 + 1 = 5$.
Et, si $A = (210, 330, 462, 770, 1175)$, on doit avoir $B = A$ (car chaque nombre de A est le produit de 4 éléments de $\{2, 3, 5, 7, 11\}$ de sorte que 4 éléments de A ont un pgcd > 1 et que $pgcd(A) = 1$). Conclusion : $n = 5$.

Solution de l'exercice 73 (Résolu par Yakob Kahane, Pablo Destic et Nathanaël Boutillon) Tout d'abord, il est clair que chaque ligne et chaque colonne doit avoir une ampoule éteinte. Notons P_n : "sur un échiquier de taille $n \times n+1$ avec $2n-1$ ampoules éteintes bien placées, on peut tout éteindre." On vérifie aisément que P_2 est fausse (sur 6 ampoules, 3 sont éteintes, il en faut une par colonne, et de là on ne peut rien faire). Montrons que P_n implique P_{n-1} pour $n > 2$.
Comme chacune des $n+1$ colonnes doit contenir une ampoule éteinte, il y en a une, C, qui contient au plus une ampoule éteinte. La suppression de cette colonne est possible. En effet, si cette ampoule A sert à éteindre une ampoule dans la colonne juste à gauche (mettons) de C, il faut déjà deux ampoules éteintes à côté de A dans la colonne à droite pour éteindre A', voisine de A dans C. Plus généralement, pour éteindre des ampoules à gauche de C grâce à des ampoules éteintes de C, il faut que les ampoules à la même hauteur dans la voisine à droite de C soient éteintes (sinon, les ampoules en question de C, allumées au départ, ne pourront être éteintes).
Il reste un tableau $n \times n$ avec $2n-2$ ampoules éteintes. On peut supprimer de même une colonne qui contient exactement une ampoule. On se retrouve avec $2n-3$ ampoules éteintes dans un tableau $n \times n-1$. Ainsi, P_{n+1} implique bien P_n. Par contraposée, comme P_2 est fausse, P_n est fausse pour tout $n \geq 2$. L'énoncé demandant si P_{2011} est vraie, la réponse est non.

Solution de l'exercice 75 (Résolu par Sylvain Procope-Mamert et Solal Gaudin) Par l'inégalité arithmético-géométrique, $\sqrt[m]{1^{m-1}(1+n)} \leq \frac{m-1+n+1}{m}$, donc

$$\frac{1}{\sqrt[m]{1+n}} \geq \frac{m}{m+n}.$$

En procédant de même avec l'autre membre, on obtient le résultat cherché.

Solution de l'exercice 78 (Résolu par Yakob Kahane)

— Pour tout $k \leq n$, $\lfloor \sqrt[k]{n} \rfloor$ correspond au nombre d'éléments $a \leq n$ tels que $a^k \leq n$. D'où

$$\begin{aligned} \sum_{k=2}^{n} \lfloor \sqrt[k]{n} \rfloor &= \sum_{k=2}^{n} |a \geq 1, a^k \leq n| \\ &= \sum_{k=2}^{n} |a \geq 2, a^k \leq n| + n \end{aligned}$$

— Pour tout $k \leq n$, $\lfloor log_k n \rfloor$ correspond au nombre d'éléments l tels que $k^l \leq n$. D'où

$$\begin{aligned} \sum_{k=2}^{n} \lfloor log_k n \rfloor &= \sum_{k=2}^{n} |l \geq 1, k^l \leq n| \\ &= \sum_{l=1}^{n} |k \geq 2, k^l \leq n| \\ &= \sum_{l=2}^{n} |k \geq 2, k^l \leq n| + n \end{aligned}$$

On obtient bien l'égalité demandée.

Solution de l'exercice 80 (Résolu par Antoine Stark) Par récurrence, $Q(u_n) = 0$ où $Q(X) = P(X) - X$ et $u_0 = 0$, $u_{n+1} = u_n^2 + 1$. Pour tout $n > 0$, $u_n^2 + 1 \geq_n +1 > u_n$ donc la suite

(u_n) est strictement croissante, ce qui nous assure que Q a une infinité de racines. C'est donc le polynôme nul. Conclusion : $P(X) = X$ est la seule solution.

Solution de l'exercice 87 (Résolu par Baptiste Serraille) On a $a-b|P(a)-P(b) = b-c$, de même, $b-c|c-a$ et $c-a|a-b$. On en déduit que $|a-b| = |b-c| = |c-a|$. Sans perte de généralité, a est le plus grand de ces entiers, donc $a-b = a-c$ et $b = c$, donc $a = b = c$. Ceci termine l'exercice.

Solution de l'exercice 88 (Résolu par Nathanaël Boutillon, Pablo Destic et indépendamment Julien Vanel.)

Soient J_1 le joueur qui commence et J_2 l'autre joueur.

• **si** mn **est pair :** on a donc un nombre pair de lignes ou de colonnes.

On peut alors associer deux à deux toutes les cases de telle sorte que deux cases associées soient dans la même rangée et aient un côté en commun.

Ainsi, à chaque tour, J_1 pourra jouer sur la case associée à celle sur laquelle se trouve la tour. J_2 devra alors jouer sur une case dont la case associée n'a jamais été occupée par la tour, jusqu'à ce qu'il n'y ait plus aucune case disponible et qu'il perde.

Donc J_1 **gagne.**

• **si** mn **est impair :** on a donc un nombre impair de lignes et de colonnes.

On peut alors associer deux à deux toutes les cases sauf c de telle sorte que deux cases associées soient sur la même ligne ou sur la même colonne et aient un côté en commun, de la façon suivante :

— Sur la colonne contenant c, on peut facilement associer chaque case à une autre ;
— Sur les autres colonnes, on associe chaque case à une autre sauf celle du bas ;
— Sur la ligne du haut, il reste un nombre impair de cases qu'on peut associer deux à deux.

J_2 peut alors appliquer la même stratégie que J_1 dans le cas précédent.

Donc J_2 **gagne.**

Solution de l'exercice 90 (Résolu par Yakob Kahane) On considère O de coordonnées $x_0 = \frac{1}{3}$ et $y_0 = \pi$. Montrons qu'il n'existe pas 2 points à coordonnées entières A et B tels que $OA = OB$. Si la médiatrice de $[AB]$ est la droite d'abscisse $\frac{1}{3}$, alors $\frac{x_A+x_B}{2} = \frac{1}{3}$, impossible car x_A, x_B entiers. Donc O est le seul point d'abscisse $1/3$ sur la médiatrice de $[AB]$, et $y_A \neq y_B$. Soit I le milieu de $[AB]$. En écrivant $\overrightarrow{IO} \cdot \overrightarrow{AB} = 0$, on exprime $y_O = \frac{y_A+y_B}{2} - \frac{(x_B-x_A)(\frac{1}{3}-\frac{x_A+x_B}{2})}{y_B-y_A}$, donc y_O serait rationnel, or π est irrationnel, absurde.
Ainsi, si on part d'un disque de rayon $0,0000001$ de centre O et qu'on le fait grandir continuement, le nombre de points à coordonnées entières à l'intérieur de celui-ci augmente de 1 en 1 et peut être arbitrairement grand, il finira donc bien par en contenir n exactement.

Solution de l'exercice 92 (Résolu par Julien Vanel) La réponse est $n = 8$. La configuration où les coordonnées des points sont $(0,0), (0.2,0.6), (0.4,0.4), (0.5,0.9), (0.6,0.2), (0.7,0.7), (0.9,0.5)$ et $(1,1)$ convient : on doit commencer par $(0.2,0.6)$ ou $(0.6,0.2)$ et après on est coincé. Pour $n \leq 7$ on vérifie que Arabelle s'en sort toujours.

Solution de l'exercice 96 (Résolu par Jean Zablocki et Arthur Léonard) Posons $Q(x) = P(x) - x$, Q a 2015 racines, les entiers de 0 à 2014, et est de degré 2015. Donc $Q(x) = cx(x-1)\cdots(x-2014)$. Et $Q(2015) = 1$. Donc $c = \frac{1}{2015!}$ et $Q(2016) = 2016$. Donc $P(2016) = 4032$.

Solution de l'exercice 100 (Résolu par Damien Galant, Savinien Kreczman, Corentin Simon et Henry Bambury) Appelons un nombre de la forme k^2+1 "suffisamment premier" lorsqu'il

n'est divisible par aucun nombre de la forme n^2+1 sauf 1 et lui-même. Supposons qu'il y en ait un nombre fini, soit N leur produit. N^2+1 n'est pas suffisamment premier. Il admet donc un diviseur de la forme a^2+1, qui n'est lui même pas suffisamment premier car premier avec N. On effectue une descente infinie qui atterrit sur une contradiction. Il y a donc une infinité de tels nombres.
PS : il reste à prouver qu'il existe un nombre suffisamment premier, c'est le cas de 5.

<u>Solution de l'exercice 110</u> (Résolu par Henry Bambury et Damien Galant) On supposera que P n'est pas l'un des points A, B, C (sinon l'énoncé n'a pas de sens). Comme K est l'intersection de deux tangentes extérieures en B et en C à Γ (le cercle circonscrit à ABC), (AK) est la symédiane issue de A dans ABC. L'équation barycentrique de (AK) est $c^2y - b^2z = 0$, a, b, c étant les longueurs des côtés $[BC], [CA], [AB]$ du triangle, et x, y, z les poids respectifs des points A, B, C dans le barycentre considéré. L'équation de Γ est $a^2yz + b^2xz + c^2xy$. Les coordonnées de A' vérfient donc ces deux équations, avec x, y, z non nuls car A' n'est sur aucun des côtés de ABC. La première équation donne $z = yb^2/c^2$. En remplaçant dans la deuxième, on trouve $a^2b^2y^2 + xy(b^4+c^4) = 0$. Comme $A' \notin [BC]$, on a $y \neq 0$, d'où $a^2b^2y + x(b^4+c^4) = 0$. Le point A' a donc comme coordonnées baycentriques $(-a^2b^2c^2, (b^4+c^4)c^2, (b^4+c^4)b^2)$.

Soient (α, β, γ) des coordonnées du point P. Si $\beta \neq 0$, un point de (AP) vérifie l'équation $z = \gamma y/\beta$ (on a $\beta \neq 0$). En injectant dans l'équation de Γ, on trouve pour le point A'' : $a^2\gamma y^2/\beta + xy(b^2\gamma/\beta + c^2) = 0$. On a $y \neq 0$ car sinon A'' serait égal à A. Donc $a^2\gamma y + x(b^2\gamma + c^2\beta) = 0$, ce qui permet d'en déduire que A'' a pour coordonnées $(-a^2\beta\gamma, \beta(b^2\gamma + c^2\beta), \gamma(b^2\gamma + c^2\beta))$. Ceci reste vrai si $\beta = 0$, car dans ce cas $P \in [AC]$ et donc $A'' = C$.

A partir des coordonnées barycentriques de A' et A'', on trouve l'équation de la droite joignant les deux points : $(b^6\gamma + b^4c^2\beta + b^2c^4\gamma + b^6\beta)x + a^2b^4\gamma y + a^2c^4\beta z = 0$. L'intersection X de $(A'A'')$ et de (BC) satisfait cette équation et $x = 0$ (ce qui élimine le coefficient compliqué de x dans l'équation de $(A'A'')$), et X a pour coordonnées $(0, c^4\beta, -b^4\gamma)$.

En permutant circulairement les points et les coefficients, on trouve que Y a pour coordonnées $(-c^4\alpha, 0, a^4\gamma)$, et que Z a pour coordonnées $(b^4\alpha, -a^4\beta, 0)$. Le déterminant formé par les trois triplets de coordonnées est alors nul, ce qui prouve que X, Y, Z sont alignés.

<u>Solution de l'exercice 112</u> (Résolu par Alexandre Thiault) Il est connu qu'on peut écrire $a = 2uv$, $b = u^2 - v^2$ et $c = u^2 + v^2$. Sachant que c est un carré, $u^2 + v^2 = d^2$ et on écrit de même $u = 2ij$, $v = i^2 + j^2$ et $d = i^2 + j^2$. L'aire du triangle, $ab/2$, se réécrit comme $2ij(j-i)(j+i)(j^4 + i^4 - 6i^2j^2)$. On vérifie par des petits calculs de congruence que c'est divisible par $4 \times 3 \times 7 = 84$.

<u>Solution de l'exercice 119</u> (Résolu par Paul Revenant) Comme ABC et $A'B'C'$ sont semblables, $\widehat{AB'C} = \widehat{CBA} = \pi - \widehat{CHA}$ Donc A, B', C, H sont cocycliques. De même, C, A', B, H sont cocycliques. Comme le reflété de H par rapport à (AC) appartient au cercle circonscrit $\mathcal{C}$ de ABC, $\mathcal{C}$ et le cercle passant par A, C, H ont même rayon r. On trouve donc que le cercle passant par C, B, H a le même rayon r. D'après la loi des sinus dans HCA' et HCB' on a

$$HA' = 2r\sin(\widehat{HCA'}) = 2r\sin(\widehat{HCB'}) = HB'$$

On trouve de la même façon $HB' = HC'$ donc H est le centre du cercle circonscrit à $A'B'C'$
Soit S la similitude envoyant ABC sur $A'B'C'$, de rapport k et d'angle α. Soit M le projeté de O sur (HH'). Alors $HM = HO\cos(\alpha)$ et $HH' = H'O' = k \cdot HO$, avec O' le centre du cercle circonscrit à $A'B'C'$. Pour finir l'exercice, il suffit de montrer que M est le milieu de $[HH']$, soit :

$$k = 2\cos(\alpha)$$

Soient A'' et B'' les projetés orthogonaux de A et B sur $[A'B']$ et $C'' = \mathcal{C} \cap [A'B'] \setminus \{C\}$. Grâce à la similitude S, on trouve que

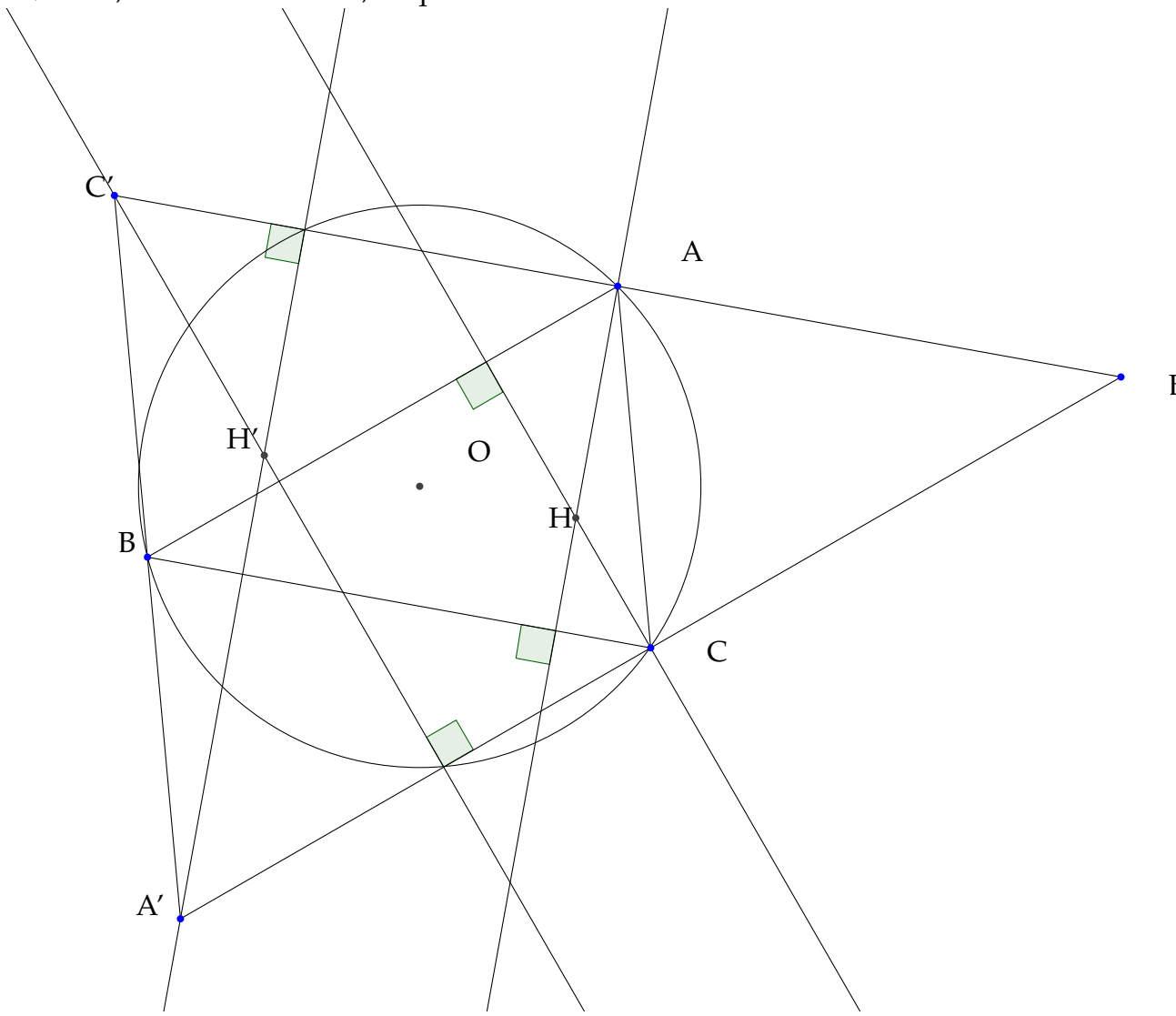
$$\begin{aligned} A''C'' &= AC\cos\alpha \\ A'C' &= AC \cdot k \end{aligned}$$

Ceci implique $k = 2\cos\alpha$, soit encore : $2A''C'' = A'C'$.

Les points A, B, C, B'' étant cocycliques,

$$\widehat{AB''C'} = \widehat{ACB} = \widehat{AC'B''}$$

et $AB''C'$ est isocèle en A donc $A''B'' = A''C'$. De même $C''B'' = C''A'$. Par somme, on obtient $A''C'' = A''C' + C''A'$, soit $2A''C'' = A'C'$, ce qu'il fallait démontrer.



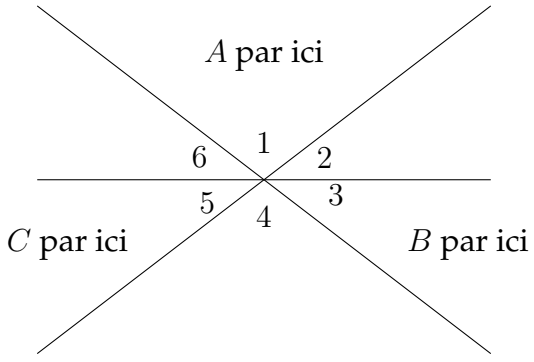
Solution de l'exercice 120 (Résolu par Paul Revenant) On peut supposer $z = a + b + c$ positif. On pose $x = a - b, y = b - c$. L'inégalité devient

$$xyz(x+y) \leq \frac{M}{9}(2x^2 + 2y^2 + 2xy + z^2)^2.$$

Or $xyz(x+y) \leq \frac{(x+y)^3}{4}$, avec égalité ssi $x = y$. $2x^2+2y^2+2xy \geq \frac{3}{2}(x+y)^2$, avec égalité ssi $x = y$. Donc il suffit de prouver $18zr^3 \leq M(6r^2+z^2)^2$ avec $r = \frac{x+y}{2}$. Par inégalité arithmético-géométrique, $6r^2+z^2)^2 = (2r^2+2r^2+2r^2+z^2)^2 \geq (4\sqrt[4]{8r^6z^2})^2$ Donc $M \leq \frac{9\sqrt{2}}{32}$.
Et, $(2, 2+3\sqrt{2}, 2-3\sqrt{2})$ est un cas d'égalité, donc on a trouvé la bonne valeur de M.

<u>Solution de l'exercice 126</u> (Résolu par Paul Revenant) Soit $T_n = \frac{n(n+1)}{2}$. Montrons par récurrence que les seuls n solution sont les entiers tels que T_n soit un carré parfait. Si ni T_n ni T_{n+1} ne sont des carrés, et que $\{a_1, \cdots, a_n\}$ est une permutation non sympathique, alors $\{a_1, \cdots, a_n, n+1\}$ est non sympathique.
Si T_n est un carré, et que $\{a_1, \cdots, a_{n-1}\}$ est non sympathique, alors $\{a_1, \cdots, a_{n-1}, n+1\}$ ne l'est pas non plus. Montrons que $\{a_1, \cdots, a_{n-1}, n+1, n\}$ est également antipathique : sinon, T_n et T_{n+1} sont des carrés, Posons $T_n = a^2$, un calcul immédiat donne $(a+1)^2 > T_{n+1}$ dès que $\sqrt{2n(n+1)} > n$, ce qui est vrai pour $n \geq 0$.
Il ne reste plus qu'à terminer par l'initialisation : la suite $2, 1, 3, 4, 5, 6, 7, 9, 8$ donne des permutations non sympathiques pour $n = 2, 3, 4, 5, 6, 7, 9$.

<u>Solution de l'exercice 130</u> (Résolu par Félix Breton) Soit M un point tel que $MA+MB+MC+MO < OA+OB+OC$. On trace les trois ellipses de foyers $(A, B); (B, C); (A, C)$ passant par O, et les trois tangentes en O à ces ellipses. Ces trois droites coupent le plan en 6 zones :



L'ellipse de foyers A et B est entièrement dans les zones $1, 2$ et 3, celle de foyers B et C dans les $3, 4$ et 5, celle de foyers C et A dans les $1, 5$ et 6. Aucune zone ne fait partie de ces 3 ensembles à la fois, donc M n'est pas dans l'ellipse de foyers A et B (mettons). Donc $MA+MB > OA+OB$ et $MC+MO \geq OC+OO$ par inégalité triangulaire, donc $MA+MB+MC+MO > OA+OB+OC+OO$ donc O est le point qui minimise $MA+MB+MC+MO$

<u>Solution de l'exercice 133</u> (Résolu par Félix Breton) On nomme Γ le plus petit cercle contenant tous les points et k son diamètre. Si aucun des points n'est sur Γ alors on peut diminuer son rayon, donc au moins un point est sur Γ. Si tous les points sur le cercle sont sur la même moitié, on peut déplacer le cercle "vers" cette moitié puis diminuer son rayon, donc soit on a deux points diamétralement opposés, soit au moins 3 points. Dans le premier cas, $k \leq D \leq \frac{2}{\sqrt{3}}D$. Dans le second cas, on peut prendre 3 points dont le triangle contient le centre de Γ (car ces points ne sont contenus dans aucune moitié de cercle). Il y a donc un angle $\alpha \geq 60$, donc l'angle au centre correspondant est ≥ 120. La distance entre les deux sommets correspondants vaut $k \times sin(\alpha) \geq \frac{\sqrt{3}}{2}k$ [car le sinus est croissant pour des angles aigus] donc dans tous les cas, $k \leq \frac{2}{\sqrt{3}}D$. On nomme Γ' le disque de même centre que Γ et de diamètre $k+d$, et S l'ensemble des disques de centres les n points et de diamètre d. Ces disques sont disjoints par définition

de d, et sont contenus dans Γ' par inégalité triangulaire. L'aire de Γ' est donc supérieure à celle de S et

$$(k+d)^2 \geq nd^2$$

En utilisant $k \leq \frac{2}{\sqrt{3}}D$, le résultat vient tout seul, comme un grand.

Solution de l'exercice 134 (Résolu par Félix Breton) On prend deux points A et B, on pose $D = AB$ et $(d) = (AB)$. Soit S l'ensemble des droites passant par B et un autre point. Les distances de A aux droites de S sont inférieures à D et entières. Or il y a au plus deux droites passant par B à même distance de A, donc S est fini. De même, S' l'ensemble des droites passant par A est fini. Les points hors de (d) sont sur des intersections de droites de S et S' donc il y a un nombre fini de points hors de (d). S'il existe C hors de (d), alors il y a un nombre fini de points hors de (AC) par le même raisonnement. Donc on n'a qu'on nombre fini de points, ce qui contredit l'énoncé. Conclusion : tous les points sont alignés.

XII. Citations mémorables

-"Le Flan" (plein de gens)
-Damien : "Apprenez le Brainfuck à quelqu'un, il codera mal un jour. Apprenez-lui le java, il codera mal toujours."
-Pierre : C'est du comique pas drôle de répétition.
Damien : C'est du comique pas drôle de répétition.
-Savinien : "VOUS N'ETES PAS PRÊTS !"
-Le conférencier : "On a 100 prisonniers..."
Arthur : "C'est le problème des prisonniers ?"
-Henry : "On s'est trompés dans l'endroit où on a mis l'erreur."
-Le conférencier : "Voici Animours, la mascotte française qui a tristement fini ses jours en Thaïlande, demandez à Vincent de vous raconter l'histoire..."
Les Belges : "Il faudra vraiment qu'on leur dise un jour."
-Timothée : "La salle de bain est si petite qu'on peut prendre une douche en pissant dans les toilettes."
-Yakob : "Dépêchez-vous, on perd la course au flan !"

(Durant la visite du musée)
-Corentin : "Ceci n'est pas de l'art, c'est un webdriver [marque quelconque] 2.0."
Félix : "la meilleure oeuvre d'art c'était le thermostat"
Antoine : "CodeGear et Deathnote c'est pareil, on a Coca-zero et coca-light" [tapé par un animatheur qui ne voit pas le lien avec le musée, mais bon...]

-Joon : "Mais ça se voit visuellement bien" [Note des élèves : ...sur la figure malfaite]
-Victor : "Soit P, A, B, C, D quatre points."
-Thomas : "Le point G, il est à peu près on ne sait pas où..."

(Au loup-garou)
-Rémi : "On est 7, il reste 3 frères, un chasseur, deux soeurs, une servante et 4 loups-garous. LE MJ NE SE FOUTRAIT PAS UN PEU DE NOTRE GUEULE ?"
Timothée : "Le boucher me désigne Pierre-alexandre... heu, la personne dont il veut couper la langue."
Timothée *(après que le village a voté la mort du montreur d'ours)* : "Suite à un souci de pilosité, les villageois ont pendu l'ours et empaillé le montreur."

(Au Mao) -Pierre (après 2h30 de jeu) : "Vous vous souvenez du début de la partie ?"
Corentin : "Je ne me souviens plus de mon nom !"

Savinien : "Le mao est un jeu qui se joue à six paquets de cartes, un échiquier, de cartes de tempêtes sur un échiquier, une table d'inversion modulo 13, de la musique..."
Timothée : "... et deux flans !"

Anonyme : "J'ai perdu." [NdLR : on a dû l'avoir chaque année, celle-là]
-Antoine (en test) : "26 est congru à 0 à modulo 4."
-Timothée : "J'ai eu un score parfait au test, j'ai eu 6, c'est un nombre parfait !"
Rémi : "Est-ce que 1 est un nombre parfait ?"
-Clara : "C'est quoi le CIV ?"
-Lucie : "Musée Fernand Léger, ça envoie du lourd !"
-Adrien : "C'est du beach-volley, mais sans *biatch*, quoi" [taper ceci fait pleurer un animatheur comme s'il pelait des oignons]