Feuille d'exercices n° 12 : corrigé

MPSI Lycée Camille Jullian

20 janvier 2026

Exercice 1 (*)

Commençons par écrire la décomposition du nombre 150 en facteurs premiers : $150 = 2 \times 75 = 2 \times 3 \times 5^2$. Si on veut écrire 150 comme produit de deux entiers premiers entre eux, il faut donc séparer les facteurs 2, 3, 5 et 5 en deux ensembles, avec la condition que les deux facteurs 5 doivent être dans le même ensemble (pour avoir des nombres premiers entre eux). Quatre choix possibles : $5^2 = 25$ d'un côté, $2 \times 3 = 6$ de l'autre ; $5^2 \times 3 = 75$ d'un côté, 2 de l'autre ; $5^2 \times 2 = 50$ d'un côté et 3 de l'autre ; et enfin la solution triviale 150 et 1. Si on accepte les entiers relatifs, on a huit solutions au lieu de quatre : $\mathcal{S} = \{(150, 1), (75, 2), (50, 3), (25, 6), (-150, -1), (-75, -2), (-50, -3), (-25, -6)\}$.

Exercice 2 (*)

Il suffit d'écrire $n^4-20n^2+4 = (n^4-4n^2+4)-16n^2 = (n^2-2)^2-(4n)^2 = (n^2-4n+2)(n^2+4n+2)$. Les deux facteurs $n^2 - 4n + 2$ et $n^2 + 4n + 2$ sont évidemment entiers tous les deux, et ne peuvent pas être égaux tous les deux à ± 1 puisque leur écart est égal à $8n$. Le seul cas qui pourrait poser problème est $n = 0$ pour lequel $n^4 - 20n + 4 = 4$ n'est pas un nombre premier. On a donc bien prouvé que cette expression ne donnait jamais un nombre premier.

Exercice 3 (*)

Supposons donc $n = 3^p \times 5^q$, alors les diviseurs de n (on se restreint ici aux diviseurs positifs, les énoncés sont malheureusement souvent un peu ambigus à ce sujet) sont tous les entiers de la forme $3^i \times 5^j$, avec $0 \leqslant i \leqslant p$ et $0 \leqslant j \leqslant q$. Leur produit peut donc s'écrire sous la forme $z = \prod_{i=0}^{p} \prod_{j=0}^{q} 3^i 5^j = 3^{(q+1)\sum_{i=0}^{p} i} \times 5^{(p+1)\sum_{j=0}^{q} j} = 3^{\frac{(q+1)p(p+1)}{2}} \times 5^{(p+1)\frac{q(q+1)}{2}}$ (il ne faut pas oublier que quand on « sort » un terme constant d'un produit, il est élevé à une puissance égale au nombre de termes du produit). Or, $45^{42} = (3^2 \times 5)^{42} = 3^{84}5^{42}$, donc on doit avoir $(q + 1)p(p + 1) = 168 = 2 \times 84$ et $(p + 1)q(q + 1) = 84$, ce qui impose évidemment $p = 2q$, puis $q(q + 1)(2q + 1) = 84$. On n'a besoin que de trouver une solution évidente, $q = 3$ convient puisque $3 \times 4 \times 7 = 84$. Bien sûr, on aura alors $p = 6$, donc $n = 3^6 \times 5^3 = 729 \times 125 = 91\ 125$.

Exercice 4 (**)

Modulo 9, on calcule facilement $94 \equiv 4[9]$. Par ailleurs, les régles de calcul sur les congruences assurent qu'en posant a, b et c les restes modulo 9 des nombres entiers x, y et z, on aura toujours $x^3+y^3+z^3 \equiv a^3+b^3+c^3[9]$. Calculons donc tous les restes possibles de cubes modulo 9 : $0^3 \equiv 0[9]$, $1^3 \equiv 1[9]$, $2^3 \equiv -1[9]$, $3^3 \equiv 0[9]$, $4^3 \equiv 1[9]$, $5^3 \equiv -1[9]$, $6^3 \equiv 0[9]$, $7^3 \equiv 1[9]$ et $8^3 \equiv -1[9]$ (on peut éviter de faire certains calculs entièrement, par exemple $7^3 \equiv (-2)^3[9] \equiv -8[9] \equiv 1[9]$). En additionnant des 0, des 1 et des -1, on n'obtiendra jamais 4 (du moins pas avec trois nombres au départ), donc l'équation n'a pas de solution. En fait, on démontre de même que l'équation $x^3 + y^3 + z^3 = a$ ne peut pas avoir de solutions dans $\mathbb{Z}$ pour un gros paquet de valeurs possibles de a (toutes celles congrues à 4 ou 5 modulo 9.

Exercice 5 (*)

Rappelons que ce critère revient à dire qu'un nombre est divisible par 9 si et seulement si la somme de ses chiffres est elle-même divisible par 9. On peut en fait démontrer mieux : un nombre entier n a toujours le même reste modulo 9 que la somme de ses chiffres. En effet, si on note a_0, a_1, ..., a_k les chiffres de l'écriture décimale de n (en sens inverse : a_0 est le chiffre des unités, a_1 celui des dizaines etc), alors $n = \sum_{i=0}^{k} a_k 10^k$, donc $n \equiv \sum_{i=0}^{k} a_k 10^k [9]$. Or, $10 \equiv 1[9]$ donc $\forall k \in \mathbb{N}$, $10^k \equiv 1^k[9] \equiv 1[9]$. On en déduit immédiatement que $n \equiv \sum_{i=0}^{k} a_k[9]$, ce qui est exactement ce qu'on voulait démontrer. La même démonstration fonctionne bien entendu pour le critère de divisibilité par 3 puisque $10 \equiv 1[3]$.

Exercice 6 (*)

Le plus simple est de faire le raisonnement modulo 7 : on note a et b les restes modulo 7 des deux entiers n et p, et on suppose donc que $a^2 + b^2 \equiv 0[7]$ (ce qui revient exactement à dire que $n^2 + p^2$ est divisible par 7. Or, $a^2 \in 0, 1, 4, 9, 16, 25, 36$, donc $a^2 \equiv 0, 1, 2, 4[7]$ (notation pas vraiment autorisée mais vous aurez tous compris), et de même bien sûr pour b^2. Si on veut avoir $a^2 + b^2 \equiv 0[7]$, la seule possibilité est $a^2 = b^2 = 0[7]$, ce qui à son tour implique $a = b = 0$. Les deux entiers n et p sont donc bien divisibles tous les deux par 7.

Exercice 7 (**)

1. Allons-y pour une récurrence brutale : $u_0 = 3^2 + 5 = 14$ est divisible par 14. Supposons désormais u_n divisible par 14, alors $u_{n+1} = 3^{4n+6} + 5^{2n+3} = 3^4 \times (u_n - 5^{2n+1}) + 5^{2n+3} = 81u_n + 5^{2n+1} \times (25 - 81) = 81u_n - 56 \times 5^{2n+1}$. Comme u_n est divisible par 14 (hypothèse de récurrence) et 56 est lui-même un multiple de 14, on a manifestement u_{n+1} divisible par 14, ce qui achève la récurrence.
2. Puisque $u_n = 9 \times (3^4)^n + 5 \times (5^2)^n$, les racines de l'équation caractéristique correspondantes devraient être 3^4 et 5^2, et l'équation caractéristique elle-même est donc $x^2 - (81 + 25)x + 81 \times 25 = 0$, soit $x^2 - 106x + 2\ 025$. Les entiers a et b demandés par l'énoncé sont donc respectivement égaux à 106 et $-2\ 025$ (non, je ne ferai pas la vérification, c'est inutile).
3. Avec la relation de récurrence $u_{n+2} = 106u_{n+1} - 2\ 025$, l'hérédité de la récurrence double devient triviale : si u_n et u_{n+1} sont deux multiples de 14, u_{n+2} est la somme de deux multiples de 14, donc aussi un multiple de 14. Par contre, il nous faut une initialisation double, donc on doit calculer $u_1 = 3^6 - 5^3 = 729 + 125 = 854 = 14 \times 61$, qui est bien lui aussi un multiple de 14.

Exercice 8 (**)

1. En notant a le reste de la division de n par 8, on aura $n^2 \equiv a^2[8]$. On calcule donc simplement les restes modulo 8 de 0, 1, 4, 9, 16, 25, 36 et 49, qui donnent respectivement 0, 1, 4, 1, 4, 1, 4, 1.
2. Si n s'écrivait sous la forme $n = a^2 + b^2 + c^2$, on aurait enparticulier $a^2 + b^2 + c^2 \equiv 7[8]$. Or, il est impossible d'obtenir un reste égal à 7 en additionnant des 0, des 1 et des 4 (on peut obtenir 0, 1, 2, 3, 4, 5 et 6 assez facilement par contre).

Exercice 9 (**)

1. En écrivant $n^3 + 5 = n(n^2 + 7) + 5 - 7n$, on constate que, si $n^2 + 7 \mid n^3 + 5$, alors $n^2 + 7 \mid 7n - 5$. Cela suppose en particulier que $n^2 + 7 \leqslant |7n - 5| \leqslant 7|n| + 5$. En notant $x = |n|$, on doit

donc avoir $x^2 - 7x + 2 \leqslant 0$. Ce trinôme a pour discriminant $\Delta = 49 - 8 = 41$ et admet pour racines $x_1 = \dfrac{7 - \sqrt{41}}{2}$ et $x_2 = \dfrac{7 + \sqrt{41}}{2}$. Comme $6 < \sqrt{41} < 7$, on a $x_1 > 0$ et $x_2 < 7$. Le trinôme étudié est négatif entre ses racines, ce qui impose que $|n| \in \{1, 2, 3, 4, 5, 6\}$. Il ne reste plus qu'à tester brutalement les douze valeurs de n possibles (oui, parfois, l'arithmétique ce n'est pas très subtil). Pour $n = 1$, $n^2 + 7 = 8$ et $7n - 5 = 2$, ça ne marche pas. Pour $n = 2$, $n^2 + 7 = 11$ et $7n - 5 = 9$, toujours pas. Pour $n = 3$, $n^2 + 7 = 16$ et $7n - 5 = 16$, miracle, on a trouvé une solution. Pour $n = 4$, $n^2 + 7 = 23$ et $7n - 5 = 23$, une deuxième solution ! Pour $n = 5$, $n^2 + 7 = 32$ et $7n - 5 = 30$, ça ne marche pas. Et pour $n = 6$, $n^2 + 7 = 43$ et $7n - 5 = 37$, ça ne marche pas non plus (oui, la majoration de la valeur absolue par l'inégalité triangulaire en cours de calcul n'était pas optimale, on aurait pu éviter quelques vérifications ultérieures. Aucune valeur négative ne fonctionne (les valeurs de $n^2 + 7$ sont les mêmes que celles calculées pour les entiers positifs, et $7 \times (-1) - 5 = -12$ n'est pas multiple de 8 ; $-14 - 5 = -19$ n'est pas multiple de 11 ; $-21 - 5 = -26$ pas multiple de 16 ; $-28 - 5 = -33$ pas multiple de 23 ; $-35 - 5 = -40$ pas multiple de 30 et enfin $-42 - 5 = -47$ par multiple de 43). Finalement, $\mathcal{S} = \{3, 4\}$.

2. Si $\sqrt{\dfrac{11n - 5}{n + 4}}$ est un entier, son carré $\dfrac{11n - 5}{n + 4}$ aussi, ce qui implique que $n + 4$ divise $11n - 5$. Or, $11n - 5 = 11(n + 4) - 49$, donc on aura dans ca cas également 49 qui est un multiple de $n + 4$. Comme 49 n'a pas des tonnes de diviseurs, $n + 4$ doit donc appartenir à l'ensemble fini $\{-49, -7, -1, 1, 7, 49\}$, soit $n \in \{-53, -11, -5, -3, 3, 45\}$. Devinez quoi ? On va tester toutes ces possibilités une par une. Si $n = -53$, $\dfrac{11n - 5}{n + 4} = \dfrac{-588}{-49} = 12$, qui n'est pas vraiment un carré parfait. Si $n = -11$, $\dfrac{11n - 5}{n + 4} = \dfrac{-126}{-7} = 18$, toujours pas un carré parfait. Si $n = -5$, $\dfrac{11n - 5}{n + 4} = \dfrac{-60}{-1}$, toujours pas de carré parfait à l'horizon. Si $n = -3$, c'est encore pire puisque le quotien est alors négatif. Si $n = 3$, $\dfrac{11n - 5}{n + 4} = \dfrac{28}{7} = 4$, ça marche ! Et si $n = 45$, $\dfrac{11n - 5}{n + 4} = \dfrac{490}{49} = 10$ qui n'est pas un carré, donc $\mathcal{S} = \{3\}$.

Exercice 10 (**)

Comme n est supposé non premier, on peut écrire n sous la forme $a \times b$. Si $a \neq b$, les deux diviseurs sont certainement plus petits que $\dfrac{n}{2}$, donc que $n - 2$ (pour un entier plus grand que 4, $\dfrac{n}{2} < n - 2$), donc ils apparaissent tous les deux comme facteurs de $(n - 2)!$, qui par conséquent est divisible par n. C'est un peu plus dur dans le cas où n est un carré parfait, et donc $a = b = \sqrt{n}$. Dans ce cas, il faut faire apparaitre deux facteurs a dans $(n - 2)!$, ce qui sera le cas si $2a \leqslant n - 2$. Or $2a \leqslant n - 2 \Leftrightarrow a^2 - 2a - 2 \geqslant 0$ puisque par hypothèse $n = a^2$. Ce sera donc le cas si $(a - 1)^2 \geqslant 3$, donc si $(a - 1) \geqslant 2$ (tous ces nombres sont des entiers naturels), soit $a \geqslant 3$. Comme on a supposé $n \geqslant 6$, c'est bien le cas, ce qui prouve que a et $2a$ seront facteurs de $(n - 2)!$, et donc que cette dernière valeur est divisible par $a^2 = n$.

Exercice 11 (**)

Faisons tous les cas possibles un par un selon le nombre k d'entiers consécutifs à ajouter :

- pour $k = 1$ on est dans le cas trivial, on se contente de prendre 1 050.
- pour $k = 2$, on devrait avoir $1\,050 = p + (p + 1) = 2p + 1$, ce qui parait difficile dans le mesure où 1 050 est un entier pair.
- pour $k = 3$, on devrait avoir $1\,050 = p + (p + 1) + (p + 2) = 3p + 3$, donc en particulier $1\,050 \equiv 0[3]$, ce qui est le cas. Il ne reste qu'à calculer $\dfrac{1\,050 - 3}{3} = 349$ pour savoir où partir :

$1\,050 = 349 + 350 + 351$.

- de façon plus générale, si $1\,050 = p + (p+1) + (p+2) + \cdots + (p+k-1) = kp + \sum_{i=1}^{k-1} i = kp + \frac{k(k-1)}{2}$, alors 1 050 est nécessairement divisible par $\frac{k}{2}$. Écrivons alors la décomposition en facteurs premiers de 1 050 pour gagner un peu de temps et isoler les candidats potentiels : $1\,050 = 2 \times 525 = 2 \times 3 \times 175 = 2 \times 3 \times 5^2 \times 7$, donc les diviseurs naturels de 1 050 sont $1, 2, 3, 5, 6, 7, 10, 14, 15, 21, 25, 30, 35, 42, 50, 75, 105, 150, 175, 210, 350, 525$ et 1 050, auxquels il faudra rajouter les doubles $4, 12, 14, 20, 28, 60, 70, 84, 100, 150, 210, 300, 350, 420, 700$ et 2 100.
- pour $k = 4$, on devrait avoir $1\,050 = 4p + 6$, donc $p = \frac{1\,044}{4} = 261$. En effet, $1\,050 = 261 + 262 + 263 + 264$.
- pour $k = 5$, on devrait avoir $1\,050 = 5p + 10$, donc $p = \frac{1\,040}{5} = 208$. En effet, $1\,050 = 208 + 209 + 210 + 211 + 212$.
- pour $k = 6$, on devrait avoir $1\,050 = 6p + 15$, donc $p = \frac{1\,035}{6}$ qui n'est pas entier (c'est en fait normal, seuls les multiples de 4 pourront fonctionner parmi les doubles).
- pour $k = 7$, on devrait avoir $1\,050 = 7p + 21$, donc $p = \frac{1\,029}{7} = 147$. En effet, $1\,050 = 147 + 148 + 149 + 150 + 151 + 152 + 153$.
- pour $k = 10$, on devrait avoir $1\,050 = 10p + 45$, donc $p = \frac{1\,005}{10}$ qui n'est pas entier, comme prévu.
- pour $k = 12$, on devrait avoir $1\,050 = 12p + 78$, donc $p = \frac{978}{12}$, qui n'est pas non plus entier.
- pour $k = 14$, on devrait avoir $1\,050 = 14p + 91$, donc $p = \frac{959}{14}$ qui n'est pas entier.
- pour $k = 15$, on devrait avoir $1\,050 = 15p + 105$, donc $p = \frac{945}{15} = 63$. En effet, $1\,050 = 63 + 64 + 65 + 66 + 67 + 68 + 69 + 70 + 71 + 72 + 73 + 74 + 75 + 76 + 77$.
- pour $k = 20$, on devrait avoir $1\,050 = 20p + 190$, donc $p = \frac{860}{20} = 43$. En effet, $1\,050 = 43 + 44 + 45 + 46 + 47 + 48 + 49 + 50 + 51 + 52 + 53 + 54 + 55 + 56 + 57 + 58 + 59 + 60 + 61 + 62$.
- pour $k = 21$, on devrait avoir $1\,050 = 21p + 210$, donc $p = \frac{840}{21} = 40$. Bon, je ne vais pas écrire toutes les décompositions, car ça deviendrait lassant, mais ça fonctionne : $1\,050 = 40 + 41 + 42 + \cdots + 59 + 60$.
- pour $k = 25$, on devrait avoir $1\,050 = 25p + 300$, donc $p = \frac{750}{25} = 30$, donc $1\,050 = 30 + 31 + \cdots + 53 + 54$ (belle somme centrée sur la magnifique valeur 42).
- pour $k = 28$, on devrait avoir $1\,050 = 28p + 378$, donc $p = \frac{672}{28} = 24$, donc $1\,050 = 24 + 25 + \cdots + 50 + 51$.
- pour $k = 30$, on devrait avoir $1\,050 = 30p + 435$, donc $p = \frac{615}{30}$, qui n'est pas trop entier.
- pour $k = 35$, on devrait avoir $1\,050 = 35p + 595$, donc $p = \frac{455}{35} = 13$, donc $1\,050 = 13 + 14 + \cdots + 46 + 47$.
- pour $k = 42$, on devrait avoir $1\,050 = 42p + 861$, donc $p = \frac{189}{42}$, qui n'est hélas pas entier (ça ne marche pas pour 42, c'est scandaleux).
- pour $k = 50$, on devrait avoir $1\,050 = 50p + 1225$, donc $p = -\frac{175}{25}$, qui en plus de ne pas être entier est négatif, on oublie.
- pour $k = 60$, on devrait avoir $1\,050 = 60p + 1\,770$, donc $p = -\frac{720}{60} = -12$, donc $1\,050 = (-12) + (-11) + \cdots + (-1) + 0 + 1 + \cdots + 12 + 13 + 14 + \cdots + 46 + 47$, ce qui est en fait la même somme que pour $k = 35$ si on simplifie les valeurs négatives avec les premiers entiers positifs.

- pour $k = 75$, on devrait avoir $1\ 050 = 75p + 2\ 775$, donc $p = -\dfrac{-1\ 725}{75} = -23$. Cette solution n'est pas valable puisque l'énoncé parlait d'entiers naturels, mais on a bel et bien $1\ 050 = (-23)+(-22)+\cdots+(-1)+0+1+\cdots+50+51 = 24+25+\cdots+50+51$, c'est-à-dire une solution déjà obtenue pour $k = 28$.
- les valeurs suivantes donneront toujours des points de départ négatifs, et donc des cas déjà traités dans les cas où ça fonctionne.

On a obtenu au total pas moins de 10 décompositions différentes. Je vous laisse maintenant le soin de faire le même travail pour 105 050 (en fait, on peut arriver à compter les cas sans les écrire tous, mais ça nécessite un peu de soin).

Exercice 12 (**)

1. Puisque l'équation ne fait intervenir que les carrés des trois inconnues, si (x, y, z) est solution, alors $(|x|, |y|, |z|)$ sera un triplet de solutions dans $\mathbb{N}^3$. Réciproquement d'ailleurs, si (x, y, z) est une solution dans $\mathbb{N}^3$, alors tous les triplets de la forme $(\pm x, \pm y, \pm z)$ seront solutions du problème.
2. (a) Notons simplement d le pgcd des entiers x_0, y_0 et z_0. Par définition du pgcd, les nombres $x_1 = \dfrac{x_0}{d}$, $y_1 = \dfrac{y_0}{d}$ et $z_1 = \dfrac{z_0}{d}$ sont entiers, et ont un pgcd égal à 1. Or, le triplet (x_1, y_1, z_1) est clairement solution de l'équation de départ.

   (b) Faisons donc un petit tableau, toutes les valeurs étant donc des restes modulo 7 :

n	0	1	2	3	4	5	6
n^2	0	1	4	2	2	4	1
$-n^2$	0	6	3	5	5	3	6

   (c) Puisqu'on a bien entendu $7z_1^2 \equiv 0[7]$, l'équation initiale implique que $x_1^2 + y_1^2 \equiv 0[7]$, ou encore que $x_1^2 \equiv -y_1^2[7]$. D'après le tableau précédent, les seuls carrés pouvant être opposés modulo 7 sont ceux de nombres divisibles par 7 (on ne trouve aucun couple de valeurs identiques dans les deux dernières lignes du tableau ailleurs que dans la première colonne). Les nombres x_1^2 et y_1^2 doivent donc être tous les deux divisibles par 7 pour que le triplet (x_1, y_1, z_1) puisse être solution. Or, si 7 divise $x_1^2 = x_1 \times x_1$, alors 7 divise x_1 puisque 7 est un nombre premier. De même pour y_1.

   (d) Si x_1 et y_1 sont tous les deux divisibles par 7, alors $x_1^2+y_1^2$ est divisible par 7^2, donc $7z_1^2$ est un multiple de 49, ce qui implique que z_1^2 est un multiple de 7, et donc que z_1 également (même raisonnement qu'à la question précédente). Les trois nombres z_1, y_1 et x_1 sont donc des multiples de 7, ce qui contredit le fait que leur pgcd soit égal à 1. L'hypothèse qu'il existe une solution non triviale est donc absurde. NOtre équation a donc pour unique solution $(0, 0, 0)$.
3. Le triplet $(1, 2, 1)$ est solution de l'équation $x^2 + y^2 = 5z^2$ puisque $1^2 + 2^2 = 5 = 5 \times 1^2$. Or, multiplier une solution par un entier naturel quelconque produira toujours une nouvelle solution (si $x^2 + y^2 = 5z^2$, alors $(nx)^2 + (ny)^2 + 5(nz)^2$), ce qui produit directement une infinité de solutions distinctes de la forme $(n, 2n, n)$. Ce ne sont d'ailleurs pas du tout les seules : on peut changer les signes, permuter les valeurs de x et de y, et même trouver encore d'autres solutions comme $(2, 11, 5)$ (puisque $4 + 121 = 5 \times 25$) qui ne peut pas être obtenue à l'aide des manipulations précédentes. Il existe bien sûr des solutions pour lesquelles $x = 42$ (par exemple $(42, 84, 42)$ ou $(42, 21, 21)$), et aussi pour lesquelles $z = 42$ (encore une fois, $(42, 84, 42)$ convient !).

   L'équation $x^2+y^2 = 13z^2$ admet comme solution non triviale $(2, 3, 1)$, à partir de laquelle on construit aisément une infinité de solutions non triviales de la forme $(2n, 3n, n)$. Il suffit bien sûr de prendre $n = 42$ pour avoir comme solution $(84, 126, 42)$, pour laquelle $z = 42$. Mais en posant $n = 21$, on trouve aussi $(42, 63, 21)$ qui est une solution pour laquelle $x = 42$. En fait ce n'était pas vraiment plus dur avec 13 qu'avec 5.

Exercice 13 (**)

Supposons donc que $x = \frac{p}{q}$ soit solution de l'équation, avec tant qu'à faire $p \wedge q = 1$. On aurait donc $\frac{p^3}{q^3}+\frac{p^2}{q^2}+\frac{2p}{q}+1 = 0$, et a fortiori $p^3+qp^2+2pq^2+q^3 = 0$. Ceci implique que $q^3 = -p^3-qp^2-2pq^2$ divise p, ce qui n'est possible que si $q^3 = 1$ puisque p et q (et donc p et q^3) sont supposés premiers entre eux. On a donc $q = 1$, ce qui revient à dire que x est en fait un nombre entier. Or, x^3+x^2+2x+1 est toujours un entier impair lorsque x est entier, et ne peut donc jamais être égal à 0.

Exercice 14 (**)

1. Puisque $b = cq + r$, on peut écrire $a_b = a_{cq+r} = p^{cq+r} - 1 = p^r \times (p^{cq} - 1) + p^r - 1 = p^r(p^{cq} - 1) + a_r$. Or, on peut écrire $p^{cq} - 1 = (p^c)^q - 1 = (p^c - 1)\sum_{i=0}^{q-1}(p^c)^i$, qui est un multiple de a_c. On peut donc écrire a_b sous la forme $ka_c + a_r$. Un diviseur commun de a_b et de a_c divisera donc aussi $a_b - ka_c = a_r$, et réciproquement, tout diviseur commun de a_r et de a_c sera un diviseur de a_b. Le pgcd des deux couples (a_b, a_c) et (a_c, a_r) est donc également le même.
2. Il suffit d'appliquer l'algorithme d'Euclide à partir de b et de c. En notant r_i les restes succesifs, la question précédente assure que $a_b \wedge a_c = a_{r_i} \wedge a_{r_{i+1}}$ pour tout entier i. Au moment où l'agorithme s'achèvera, on aura $a_b \wedge a_c = a_{b\wedge c} \wedge a_0$, et comme $a_0 = 0$, ce dernier pgcd est simplement égal à $a_{b\wedge c}$, ce qui achève la preuve.

Exercice 15 (***)

1. On calcule donc $F_0 = 2^{2^0} + 1 = 2 + 1 = 3$ qui est premier, $F_1 = 2^2 + 1 = 5$ qui est aussi premier, $F_2 = 24 + 1 = 17$ qui est encore premier (ça vous rappelle des histoires de découpage de gâteau ? C'est tout à fait normal). C'est moins évident pour $F_3 = 2^8 + 1 = 257$, mais il est bien premier (pas divisible par 3 ni 5 par critères usuels, puis $257 = 7 \times 36 + 5$, $257 = 11 \times 23 + 4$ et $257 = 13 \times 19 + 10$, pas la peine d'aller plus loin puisque $17 > \sqrt{257}$). Enfin, $F_4 = 2^{16}+1 = 65\,537$. Pour vérifier la primalité, on écrit un programme Python bateau du genre :

```
def premier(n) :
    for i in range(2,int(n**0.5)+1) :
        if n%i==0 : return False
    return True
```

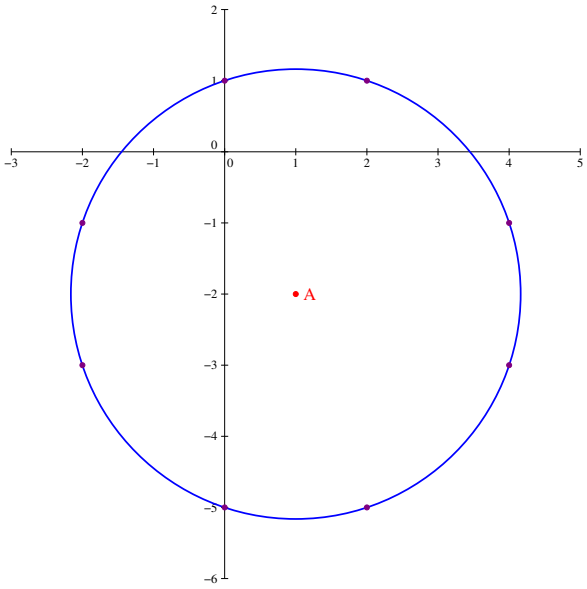
   Pas de mauvaise suprise, 65 537 est bien premier.
2. On écrit simplement $F_{n+1} - 2 = 2^{2^{n+1}} + 1 = (2^{2^n})^2 - 1 = (2^{2^n} - 1)(2^{2^n} + 1) = (F_n - 2)F_n$ via une classique identité remarquable.
3. On conjecture facilement à partir de la formule précédente que $F_n = 2 + \prod_{i=0}^{n-1} F_i$, ce qu'on prouve par une récurrence simple : au rang 1, $F_1 = 5 = 2 + F_0$, puis en supposant la formule vraie au rang n, on aura d'après la question précédente $F_{n+1} = 2 + \prod_{i=0}^{n-1} F_i(F_n) = 2 + \prod_{i=0}^{n} F_i$.
4. En effet un diviseur commun de F_n et de F_p (en supposant par exemple que n est le plus grand des deux entiers), diviserait F_n et $\prod_{i=0}^{n-1} F_i$, donc d'après la question précédente diviserait 2. C'est évidemment peu crédible (les nombres F_n sont tous impairs), la seule possibilité est que ce diviseur soit égal à 1, ce qui prouve que le pgcd recherché est lui-même égal à 1.

Exercice 16 (**)

Pour compter le nombre de diviseurs, le plus simple est de commencer par écrire la décomposition en facteurs premiers du nombre : $10! = 2\times3\times2^2\times5\times2\times3\times7\times2^3\times3^2\times2\times5 = 2^8\times3^4\times5^2\times7$. Un diviseur de 10! sera nécessairement de la forme $2^a\times3^b\times5^c\times7^d$, avec $a\in\{0,1,\dots,8\}$, $b\in\{0,1,2,3,4\}$, $c\in\{0,1,2\}$ et $d\in\{0,1\}$ (cela découle des propriétés de la valuation p-adique vues en cours). Chaque quadruplet d'entiers (a,b,c,d) donne un diviseur différent (par unicité de la décomposition en facteurs premiers), ce qui fait $9\times5\times3\times2 = 270$ diviseurs au total. Si on compte aussi les diviseurs négatifs, il y en a deux fois plus, soit 540. Par exemple, pour $a=5$, $b=1$, $c=2$ et $d=0$, on trouve le diviseur $32\times3\times25 = 2\,400$.

Exercice 17 (***)

1. Une astuce est d'écrire $xy-2x-3y=0$, soit $(x-3)(y-2)=6$. Comme il n'existe pas trente-six mille façons d'écrire 6 comme produit de deux entiers, on peut faire une liste des possibilités pour $x-3$ et $y-2$. Soit $x-3=6$ et $y-2=1$, ce qui donne la solution $(9,3)$; soit $x-3=3$ et $y-2=2$, ce qui donne $(6,4)$; soit $x-3=2$ et $y-2=3$, ce qui donne $(5,5)$; soit $x-3=1$ et $y-2=6$, ce qui donne $(4,8)$. Et n'oublions pas, bien entendu, les diviseurs négatifs : $x-3=-6$ et $y-2=-1$ donne $(-3,1)$; $x-3=-3$ et $y-2=-2$ donne $(0,0)$; $x-3=-2$ et $y-2=-3$ donne $(1,-1)$; et enfin $x-3=-1$ et $x-2=-6$ donne $(2,-4)$. Finalement, $\mathcal{S}=\{(-3,1),(0,0),(1,-1),(2,-4),(4,8),(5,5),(6,4),(9,3)\}$.
2. Il s'agit ici de mettre sous forme canonique : $(x-1)^2-1+(y+2)^2-4-5=0$, soit $(x-1)^2+(y+2)^2=10$. Pour écrire 10 comme somme de deux carrés, il faut nécessairement écrire $10=(\pm1)^2+(\pm3)^2$ (si on dépasse 3 on sera largement au-dessus de 10, et pour 2 rien ne marche). Cela laisse encore une fois huit possibilités : par exemple si $x-1=1$ et $y+2=3$, on trouve la solution $(2,1)$. Je vous passe les détails, on obtient $\mathcal{S}=\{(4,-1),(4,-3),(2,1),(2,-5),(0,1),(0,-5),(-2,-1),(-2,-3)\}$. Bien sûr, vous aurez reconnu dans le membre de gauche une équation de cercle : $(x-1)^2+(y+2)^2=10$, cercle de centre $A(1,-2)$ et de rayon $\sqrt{10}$. On a donc prouvé que ce cercle passait par exactement huit points du plan dont les deux coordonnées sont entières (voir illustration ci-dessous) :



3. Même technique que ci-dessus, $x^2-\left(3y-\dfrac{39}{6}\right)^2+\dfrac{169}{4}=40$, soit en factorisant $\left(x-3y+\dfrac{13}{2}\right)\left(x+3y-\dfrac{13}{2}\right)=-\dfrac{9}{4}$. Quitte à tout multiplier par 4, on trouve donc l'équation $(6y-2x-13)(2x+6y-13)=9$. Il y a six possibilités pour écrire 9 comme

un produit de deux entiers, qui vont donner à chaque fois un système à résoudre. D'abord $\begin{cases} 6y - 2x - 13 = 9 \\ 2x + 6y - 13 = 1 \end{cases}$. En additionnant les deux équations, $12y-26 = 10$, soit $12y = 36$ et $y = 3$, ce qui donne $2x = 14 - 6y = -4$, donc $x = -2$. Passons au deuxième système : $\begin{cases} 6y - 2x - 13 = 3 \\ 2x + 6y - 13 = 3 \end{cases}$. La somme des deux équations donne $12y - 26 = 6$, soit $y = \frac{32}{12} = \frac{8}{3}$, solution qui ne nous intéresse pas. Troisième système : $\begin{cases} 6y - 2x - 13 = 1 \\ 2x + 6y - 13 = 9 \end{cases}$. On somme comme d'habitude : $12y - 26 = 10$, on retrouve $y = 3$, mais cette fois-ci $2x = 22 - 6y = 4$, donc $x = 2$. Quatrième système : $\begin{cases} 6y - 2x - 13 = -9 \\ 2x + 6y - 13 = -1 \end{cases}$. On additionne : $12y - 26 = -10$, soit $y = \frac{4}{3}$, solution à éliminer ici. On trouvera la même valeur pour y avec -1 et -9 au lieu de -9 et -1. Reste donc le cinquième système : $\begin{cases} 6y - 2x - 13 = -3 \\ 2x + 6y - 13 = -3 \end{cases}$. On trouve $12y - 26 = -6$, soit $y = \frac{5}{3}$. Là encore, pas de solution entière en vue. Finalement, il n'y que deux couples solutions : $\mathcal{S} = \{(2,3),(-2,3)\}$ (notons que cette fois on a cherché les points à coordonnées entières sur une hyperbole).

4. Pas vraiment de méthode très subtile ici, il suffit de trouver toutes les possibilités en faisant augmenter la valeur de x puis celle de y. Si $x = 1$, on a déjà $\frac{1}{x} = 1$, donc on ne peut pas trouver de valeurs de y et de z convenables (en supposant les entiers naturels). Si $x = 2$, on doit avoir $\frac{1}{y} + \frac{1}{z} = \frac{1}{2}$. Il faut donc avoir au moins $y = 3$ pour que l'égalité puisse être vérifiée. Si $y = 3$, $z = 6$ convient puisque $\frac{1}{3} + \frac{1}{6} = \frac{1}{2}$. Si $y = 4$, on peut prendre $z = 4$. Si $y > 4$, on va trouver des valeurs éventuelles de z plus petites que y, donc des couples déjà obtenus (à l'ordre près). Passons donc à $x = 3$, si on ne veut pas retomber sur des solutions déjà trouvées, il faudra prendre $y \geqslant 3$ et $z \geqslant 3$, mais alors la seule possibilité est $x = y = z = 3$. Finalement, les seuls triplets possibles sont $(2,3,6)$, $(2,4,4)$ et $(3,3,3)$ ainsi que leurs permutations. Si on accepte les entiers relatifs dans les solutions, on trouve plus de possibilité puisque tous les triplets $(1,n,-n)$ seront solution (et leurs permutations, bien entendu). Par ailleurs, $\left|\frac{1}{n} + \frac{1}{p}\right| < \frac{1}{2}$ si n et p sont de signe opposés et (en valeur absolue) supérieurs ou égaux à 2. Il est donc impossible de trouver des solutions en entiers relatifs avec trois entiers tous différents de 1.

5. On a bien sûr très envie de factoriser cette équation sous la forme $(3x+y)(3x-y) = 32$. Comme $32 = 2^5$, cela ne laisse que cinq possibilités pour le décomposer comme produit de deux entiers : soit $3x+y = 1$ et $3x-y = 32$, ce qui en sommant implique $6x = 33$, on ne va pas obtenir une valeur très entière pour x, on oublie ; soit $3x+y = 2$ et $3x-y = 16$, ce qui donnera cette fois $6x = 18$, donc $x = 3$, puis $y = -7$; soit $3x+y = 4$ et $3x-y = 8$, ce qui implique $6x = 12$, donc $x = 2$, puis $y = -2$. Les autres possibilités changeront simplement le signe de y ou celui de x (si on considère les décompositions comme produit de facteurs négatifs), on a donc huit solutions au total : $\mathcal{S} = \{(3,-7),(3,7),(-3,-7),(-3,7),(2,-2),(2,2),(-2,-2),(-2,2)\}$.

6. J'ai une soudaine envie de regarder cette équation modulo 3 : les règles de calcul sur les congruences impliquent que $2y^2 \equiv 0[3]$, donc que $2y^2$ est divisible par 3. Comme 2 est premier avec 3, y^2 doit donc être divisible par 3, et y également. Autrement dit, $y = 3k$, avec $k \in \mathbb{Z}$. On peut alors réécrire l'équation sous la forme $15x^2 - 7 \times 9k^2 = 9$, soit $5x^2 - 21k^2 = 3$. Le même raisonnement modulo 3 que ci-dessus donne alors x^2 divisible par 3, donc $x = 3 \times j$, avec $j \in \mathbb{Z}$, puis on se ramène à $15j^2 - 7k^2 = 1$. Devinez quoi ? On va encore raisonner modulo 3. On doit désormais avoir $2k^2 \equiv 1[3]$. Ce ne sera pas le cas si k est un multiple de 3, ni si $k \equiv 1[3]$ (dans ce cas $2k^2 \equiv 2[3]$), ni si $k \equiv 2[3]$ puisque $2 \times 2^2 \equiv 2[3]$. Ce ne sera donc en fait jamais le cas, l'équation ne peut pas avoir de solution : $\mathcal{S} = \emptyset$.

7. On devrait donc avoir $y^3 = x(x+1)$. Or les entiers x et $x+1$ sont premiers entre eux (un

diviseur commun de x et de $x+1$ étant aussi diviseur de $x+1-x=1$). Tout facteur premier apparaissant avec une puissance non nulle dans la décomposition en facteurs premiers de x devra donc avoir une puissance multiple de 3 (il n'apparaitra pas dans celle de $x+1$, et toutes les valuations p-adiques de y^3 sont nécessairement multiples de 3). Cela revient exactement à dire que x est un cube parfait (cube d'un entier relatif). On peut faire exactement le même raisonnement pour $x+1$ qui doit lui aussi être un cube parfait. Or, deux cubes parfaits consécutifs dans $\mathbb{Z}$, c'est très rare : soit $x=0$ et $x+1=1$ (donc $y=0$), soit $x=-1$ et $x+1=0$ (et toujours $y=0$). Notre équation a donc exactement deux solutions : $\mathcal{S}=\{(0,0),(-1,0)\}$.

Exercice 18 (**)

1. Via la propriété d'additivité des valuations p-adiques, $v_p(n!)=\sum_{k=1}^{n} v_p(k)$. Or, le nombre d'entiers inférieurs ou égaux à n qui sont multiples de p^k (pour un certain entier k) est égal à $\left\lfloor \frac{n}{p^k} \right\rfloor$. Il y a donc entre 1 et n un nombre d'entiers dont la valuation p-adique vaut **exactement** k qui est égal à $\left\lfloor \frac{n}{p^k} \right\rfloor - \left\lfloor \frac{n}{p^{k+1}} \right\rfloor$. On en déduit que $v_p(n!)=\sum_{i=1}^{q} i\left(\left\lfloor \frac{n}{p^i} \right\rfloor - \left\lfloor \frac{n}{p^{i+1}} \right\rfloor\right)$, la somme allant jusqu'au premier entier q pour lequel $\left\lfloor \frac{n}{p^q} \right\rfloor = 0$ (cet entier existe, il vaut d'ailleurs $\lceil \log_p(n) \rceil$). Cette somme est « partiellement télescopique, il ne reste après simplification que $\sum_{i=1}^{q} \left\lfloor \frac{n}{p^i} \right\rfloor$, qui est bien la même expression que la somme infinie de l'énoncé, dont tous les termes deviennent nuls à partir de $k=q$.
2. Pour qu'un entier n ait une écriture décimale se terminant par au moins k zéros, il doit être divisible par 10^k, donc à la fois par 2^k et par 5^k. Plus précisément, le nombre de zéros terminant l'écriture décimale de n vaut exactement $\min(v_2(n), v_5(n))$. Il suffit donc de calculer $v_5(100!)=\sum_{k=1}^{+\infty} \left\lfloor \frac{100}{5^k} \right\rfloor = 20+4=24$, et $v_2(100!)=\sum_{k=1}^{+\infty} \left\lfloor \frac{100}{2^k} \right\rfloor = 50+25+12+6+3+1=97$. Notre nombre se finit donc par 24 zéros.

Exercice 19 (***)

1. Un récurrence simple suffit ici : $F_2F_0 - F_1^2 = 0-1=-1=(-1)^1$, donc P_1 est vraie. Supposons P_n vraie, alors $F_{n+2}F_n - F_{n+1}^2 = (F_{n+1}+F_n)F_n - F_{n+1}^2 = F_{n+1}F_n + F_n^2 - F_{n+1}^2 = F_{n+1}(F_n - F_{n+1}) + F_n^2$. Or, $F_{n+1}=F_n+F_{n-1}$, donc $F_n - F_{n+1} = -F_{n-1}$, donc l'expression devient $F_n^2 - F_{n+1} - F_{n-1} = -(-1)^n = (-1)^{n+1}$ en exploitant l'hypothèse de récurrence. On a bien prouvé la propriété au rang $n+1$.
2. Dans le cas où n est pair, l'égalité précédente est une identité de Bezout $aF_{n+1}+bF_n=1$, avec $a=F_{n-1}$ et $b=-F_n$ qui sont des coefficients entiers, donc F_n et F_{n+1} sont premiers entre eux. Si n est impair, il suffit de changer les signes pour aboutir à la même conclusion.
3. On va cette fois-ci effectuer une récurrence double sur l'entier p, n étant fixé. Pour $p=1$, $F_nF_0 + F_{n+1}F_1 = F_{n+1}$, donc la propriété est vraie au rang 1. Si $p=2$, $F_nF_1 + F_{n+1}F_2 = F_n + F_{n+1} = F_{n+2}$, donc la propriété est également vraie au rang 2. Supposons l'égalité valable aux rangs p et $p+1$, alors $F_{n+p+2} = F_{n+p+1} + F_{n+p} = F_nF_p + F_{n+1}F_{p+1} + F_nF_{p-1} + F_{n+1}F_p = F_n(F_p+F_{p-1}) + F_{n+1}(F_{p+1}+F_p) = F_nF_{p+1} + F_{n+1}F_{p+1}$, ce qui prouve la propriété au rang $p+2$ et achève la récurrence.

   Un diviseur commun à F_n et F_p sera donc diviseur de F_{n+p}, et par conséquent diviseur commun à F_n et F_{n+p}. De façon similaire, un diviseur commun à F_n et F_{n+p} sera diviseur de $F_{n+1}F_p$, et F_n et F_{n+1} étant premiers entre eux, le diviseur de F_n divisera nécessairement

F_p, et sera par conséquent diviseur commun de F_n et F_p. Les diviseurs communs des deux couples sont donc identiques.

4. D'après la question précédentes, $F_n \wedge F_m = F_n \wedge F_{n-m} = F_n \wedge F_{n-km}$ pour tout entier k (quitte à appliquer plusieurs fois de suite la relation). En appliquant successivement toutes les étapes de l'algorithme d'Euclide de recherche du pgcd aux entiers n et m, les couples (a, b) obtenus à toutes les étapes vérifieront donc $F_n \wedge F_m = F_a \wedge F_b$. Puisque le dernier couple obtenu sera $(n \wedge m, 1)$, on a donc $F_n \wedge F_m = F_{n\wedge m} \wedge F_1 = F_{n\wedge m}$.
5. En effet, par contraposée, si n n'est pas premier, on peut choisir un diviseur m de n non trivial, et on a alors $F_n \wedge F_m = F_{n\wedge m} = F_m$. En particulier, F_n est divisible par F_m et c'est certainement un diviseur distinct de 1 et de F_n. La réciproque est complètement fausse : $F_3 = 2$ est premier, $F_4 = 3$, $F_5 = 5$ est premier, $F_6 = 8$, $F_7 = 13$ est premier, $F_8 = 21$, $F_9 = 34$, $F_{10} = 55$, $F_{11} = 89$ est premier, $F_{12} = 144$, $F_{13} = 233$ est premier, $F_{14} = 377$, $F_{15} = 610$, $F_{16} = 987$, $F_{17} = 1\ 597$ qui est premier, $F_{18} = 2\ 584$, $F_{19} = 4181$. Et là, hop, au moment où plus personne n'y croit, $4\ 181 = 37 \times 113$ alors que 19 est premier !
6. On vient de calculer les premiers termes, la vérification est donc facile, et en effet $F_8 = 3 \times 7$ est le premier nombre de la suite divisible par 7. Si on calcule plus précisément les restes de la division par 7 des termes de la suite, on obtient pour les huit premiers termes 1, 1, 2, 3, 5, 1, 6, 0, puis on obtiendra ensuite (via la relation de récurrence définissant la suite) 6, 6, 5, 4, 2, 6, 1, 0, puis 1, 1, et on constate que la suite des restes est périodique de période 16, et donc qu'elle reprendra les valeurs 0 quand $n \equiv 0[16]$ ou $n \equiv 8[16]$, c'est-à-dire exactement quand n est divisible par 8.

Exercice 20 (**)

1. Les diviseurs de 32 sont 1, 2, 4, 8, 16 et 32 lui-même, donc $S(32) = 1+2+4+8+16+32 = 63$ (une belle somme de suite géométrique). Pour 28, on a comme diviseurs 1, 2, 4, 7, 14 et 28, donc $S(28) = 1+2+4+7+14+28 = 56$. Enfin, 60 admet beaucoup de diviseurs : 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30 et 60, ce qui donne $S(60) = 1+2+3+4+5+6+10+12+15+20+30+60 = 168$.
2. Un nombre premier n'admet comme diviseurs que 1 et lui-même. Dans ce cas, on a donc $S(n) = n + 1$.
3. Les seuls diviseurs de p^k sont les puissances inférieures de p : 1, p, p^2, …, p^k. On a donc une somme géométrique à calculer, comme pour $S(32)$ plus haut : $S(p^k) = \sum_{i=0}^{k} p^i = \frac{p^{k+1}-1}{p-1}$.
4. Le plus simple est de rédiger une récurrence sur l'entier k. Le cas où $k = 1$ est exactement celui traité à la question précédente, la formule obtenue correspond bien à celle de l'énoncé. Supposons donc, en posant $m = \prod_{i=1}^{k-1} p_i^{\alpha_i}$, que $S(m) = \prod_{i=1}^{k-1} \frac{p_i^{\alpha_i+1}-1}{p_i-1}$. Tout diviseur de n peut alors s'écrire sous la forme $d \times p_k^j$, avec d un diviseur quelconque de m (on notera D l'ensemble de ces diviseurs) et $j \in \{0, \ldots, \alpha_k\}$. On a donc $S(n) = \sum_{d\in D}\sum_{j=0}^{k} dp_k^j = \left(\sum_{d\in D} d\right) \times \frac{p_k^{k+1}-1}{p_k-1}$. Il ne reste plus qu'a appliquer l'hypothèse de récurrence pour conclure.
5. C'est assez évident : $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ et $m = \prod_{j=1}^{k'} q_j^{\beta_j}$, avec des p_i et q_j qui sont tous distincts deux à deux puisque les entiers n et m sont premiers entre eux. On a donc $nm = \prod_{i=1}^{k} p_i^{\alpha_i} \prod_{j=1}^{k'} q_j^{\beta_j}$ puis en appliquant la formule de la question précédente $S(nm) = \prod_{i=1}^{k} \frac{p_i^{\alpha_i+1}-1}{p_i-1} \times \prod_{j=1}^{k'} \frac{q_j^{\beta_j+1}-1}{q_j-1} =$

$S(n) \times S(m)$.

Exercice 21 (***)

1. Cela revient simplement à dire que 2 est le seul nombre premier pair, ce qui est effectivement vrai.
2. Faisons donc ce qu'on nous dit : notons p_1, p_2, …, p_k les seuls nombres premiers congrus à 3 modulo 4 (en supposant par l'absurde qu'il y en a un nombe fini) et posons $m = 4\prod_{i=1}^{k} p_i - 1$. L'entier m est évidemment impair, et ne peut avoir aucun des p_i comme facteur premier par construction (car cahque p_i est un diviseur de $m+1$). Tous ses facteurs premiers sont donc des entiers impairs congrus à 1 modulo 4. Or, le produit de deux tels entiers est lui-même congru à $1 \times 1 = 1$ modulo 4, donc m devrait être congru à 1 modulo 4. Mais la construction même de l'entier m montre que $m \equiv -1[4]$, ce qui est évidemment contradictoire. Conclusion : on a bien une infinité de nombres premiers de la forme $4k + 3$.
3. Commençons par constanter que, hormis 2 et 3, tous les nombres premiers sont nécessairement congrus à 1 ou 5 modulo 6 (si leur congruence était paire, ils seraient eux-mêmes pairs, et tout nombre congru à 3 modulo 6 est divisible par 3). On fait ensuite exactement le même raisonnement par l'absurde : supposons que la liste finie des entiers premiers congrus à 5 modulo 6 soit p_1, p_2, …, p_k, et posons $m = 6\prod_{i=1}^{k} p_i - 1$. Le nombre m est impair (pas de facteur 2 dans sa décomposition en facteurs premiers), pas divisible par 3 (puisque congru par construction à -1 modulo 3), et ne peut avoir aucun des p_i comme facteur premier. Tous ses facteurs premiers sont donc congrus à 1 modulo 6, ce qui implique que $m \equiv 1[6]$, ce qui est manifestement faux. On a donc une infinité de nombres premiers congrus à 5 modulo 6.

Si vous avez quelques heures (jours ?) devant vous, vous pouvez maintenant vous attaquer au très intéressant mais fort difficile **théorème de Dirichlet** : pour tout entier n non nul et tout entier k premier avec n, il existe une infinité de nombres premiers congrus à k modulo n (autrement dit, une suite arithmétique comporte toujours une infinité de nombres premiers si son premier terme est premier avec sa raison).

Exercice 22 (**)

1. En notant d et m le pgcd et le ppcm de a et de b, on a $a = da'$ et $b = db'$, avec $a' \wedge b' = 1$. On en déduit que $a + b = d(a' + b')$. De plus, $m = da'b'$ puisque $d \times m = ab$. Comme m et $a + b$ sont divisibles par d, il suffit donc de prouver que $a' + b'$ et $a'b'$ sont premiers entre eux pour prouver qu'il s'agit de leur pgcd. Or, si $a' + b'$ et $a'b'$ avaient un diviseur commun (autre que 1), on pourrait le choisir premier. Dans ce cas, il diviserait soit a', soit b' (puisqu'il divise leur produit). S'il divise par exemple a', il divisera aussi $(a' + b') - a' = b'$, et donc aussi $a'b'$, ce qui contredit notre définition. Les nombres $a' + b'$ et $a'b'$ sont donc bien premiers entre eux, et $(a + b) \wedge (a \vee b) = a \wedge b$.
2. En gardant les notations de la réponse précédente, on aurait $d = a \wedge b = (a+b) \wedge m = 144 \wedge 420$. Or, $144 = 12^2 = 2^4 \times 3^2$, et $420 = 4 \times 105 = 2^2 \times 3 \times 5 \times 7$, donc on obtient $d = 12$. Les entiers a' et b' ont donc une somme égale à 12 et un produit égal à $\frac{420}{12} = 35$. Ils sont alors solution de l'équation du second degré $x^2 - 12x + 35 = 0$, qui a pour discriminant $\Delta = 144 - 140 = 4$ et pour racines $x_1 = \frac{12-2}{2} = 5$ et $x_2 = \frac{12+2}{2} = 7$. On peut donc avoir $a' = 5$ et $b' = 7$, ce qui donne $a = 60$ et $b = 84$, ou le contraire. Il y a donc deux solutions : $\mathcal{S} = \{(60, 84), (84, 60)\}$.

Exercice 23 (***)

1. En effet, les diviseurs de 6 sont 1, 2, 3 et 6 dont la somme est bien égale à $12 = 2 \times 6$. De même, 28 a pour diviseurs 1, 2, 4, 7, 14 et 28 dont la somme vaut $56 = 2 \times 28$.
2. Raisonnons par contraposée. Si p n'est pas premier, alors on peut écrire $p = a \times b$, avec a, b tous les deux supérieurs ou égaux à 2. On peut alors écrire $2^p - 1 = (2^a)^b - 1 = (2^a - 1)\sum_{k=0}^{b-1}(2^a)^k$. On a écrit $2^n - 1$ comme produit de deux facteurs supérieurs ou égaux à 2, donc il n'est pas premier, ce qui prouve la propriété demandée.
3. Comme $2^p - 1$ est un entier premier, la décomposition en facteurs premiers de n est donnée par $n = 2^{p-1}(2^p - 1)$. Tous les diviseurs de n sont alors de la forme 2^k, avec $k \in \{0, 1, \ldots, p-1\}$, ou $2^k(2^p - 1)$, pour les mêmes valeurs de k. On calcule alors aisément $S(n) = (1 + 2^p - 1)\sum_{k=0}^{p-1} 2^k = 2^p \times \dfrac{2^p - 1}{2 - 1} = 2^p(2^p - 1) = 2n$, donc n est un nombre parfait.
4. La valeur $n = 6$ correspond à $p = 2$, $n = 28 = 4 \times (8 - 1)$ correspond à $n = 3$. On ne peut pas tester $p = 4$ qui n'est pas vraiment un nombre premier, passons donc à $p = 5$, qui donne $n = 16 \times 31 = 496$, qui est donc un entier parfait. Pour information, le suivant vaut 8 128 pour $p = 7$.
5. (a) Je vous laisse (re)lire la correction de l'exercice 19 qui prouve que, si n et m sont premier entre eux, alors $S(mn) = S(m)S(n)$. Ici, on obtient donc $S(n) = S(2^a)S(b)$ et il ne reste plus qu'à calculer $S(2^a) = 1 + 2 + \cdots + 2^a = \dfrac{2^{a+1} - 1}{2 - 1} = 2^a - 1$, ce qui donne bien la formule annoncée. Mais on doit aussi avoir, puisque n est un entier parfait, $S(n) = 2n$, donc $(2^a - 1)S(b) = 2n = 2^{a+1}b$, donc $2^{a+1}b = (2^{a+1} - 1)S(b)$. La décomposition en facteurs premiers de $S(b)$ contient donc le facteur 2^{a+1} (puisque $2^{a+1} - 1$ est impair, il ne peut contenir aucun facteur 2), ce qui revient bien à dire que $S(b) = 2^{a+1} \times c$.
   (b) D'après la question précédente, $S(b) = 2^{a+1}c$ et $2^{a+1}b = (2^{a+1} - 1)S(b)$, donc $b = (2^{a+1} - 1)c$, puis $S(b) = b + c$. Or, b et c sont des diviseurs distincts de b, il est donc indispensable d'avoir $c = 1$, ce qui implique que $S(b) = b + 1$, donc que b n'a pas d'autre diviseur que 1 et lui-même, et que b est donc un nombre premier.
   (c) Comme $b = 2^{a+1} - 1$, on a $n = 2^a \times (2^{a+1} - 1)$, avec $2^{a+1} - 1$ premier. C'est exactement ce qu'on voulait prouver.

Pour les curieux : on connait donc (au moins théoriquement, car déterminer si $2^p - 1$ est un nombre premier n'est pas évident, les nombres correspondants sont d'ailleurs appelés nombres de Mersenne) tous les nombres parfaits pairs. Qu'en est-il des nombres parfaits impairs ? On conjecture qu'il n'en existe aucun, mais personne n'a encore réussi à le prouver.

Problème (***)

1. Tout est assez évident, l'ensemble contient les deux éléments neutres 0 et 1, il est manifestement stable par somme et par produit (si a, b, c, d sont quatre entiers relatifs, $ad + bc$ et $ac - bd$ sont aussi entiers, donc $(a + bi)(c + di) \in G$), ainsi que par passage à l'opposé. C'est bien un sous-anneau de $\mathbb{C}$.
2. Si G admettait des diviseurs de 0, ils le seraient également dans $\mathbb{C}$ qui est intègre, donc G l'est aussi.
3. Pour x et y entiers de Gauss (avec y non nul), on note a et b les parties réelle et imaginaire de $\dfrac{x}{y}$.

(a) Calculons explicitement $\frac{c+id}{e+if} = \frac{(c+id)(e-if)}{e^2+f^2} = \frac{ce+df}{e^2+f^2} + \frac{de-cf}{e^2+f^2}i$. Les nombres $a = \frac{ce+df}{e^2+f^2}$ et $b = \frac{de-cf}{e^2+f^2}$ sont certainement rationnels.

(b) L'existence ne pose aucun problème (l'unicité par contre serait fausse pour cette « division euclidienne »), elle serait même vraie pour tout nombre réel. Si on pose $n = \lfloor a \rfloor$, on aura $n \leqslant a < n+1$, avec $(n+1-a)+(a-n) = 1$. On a donc une somme de deux nombres positifs qui est égale à 1, au moins l'un des deux est inférieur ou égal à $\frac{1}{2}$, ce qui prouve que $0 \leqslant a-n \leqslant \frac{1}{2}$ ou $0 \leqslant n+1-a \leqslant \frac{1}{2}$ et donne une valeur de p convenable. C'est exactement pareil pour q.

(c) Avec les notations de la question précédente, on peut écrire $|(a+ib)-(p+iq)| = \sqrt{(a-p)^2+(b-q)^2} \leqslant \sqrt{\frac{1}{4}+\frac{1}{4}} \leqslant \frac{1}{\sqrt{2}} < 1$. En notant $z = p+iq$, z est donc un entier de Gauss vérifiant $\left|\frac{x}{y} - z\right| < 1$. Il suffit de multiplier cette majoration par $|y|$ et d'appliquer les règles de calcul usuelles sur les modules pour en déduire $|x-yz| < |y|$.

(d) Prenons par exemple $x = 1$ et $y = 1-i$. On a donc $|y| = \sqrt{2}$. On peut poser $z = 0$: $|x-0y| = |x| = 1 < |y|$, mais on peut aussi poser $z = i$ par exemple : $|x-iy| = |1-i-1| = 1 < |y|$. Il y en fait ici quatre valeurs de z convenables : 0, 1, i et $i+1$.

4. (a) Les propriétés de multiplicativité des modules impliquent que, dans ce cas, $|y|^2 = |xz|^2 = |x|^2|z|^2$. Le module de z étant un entier naturel (comme pour tout entier de Gauss, il est de la forme a^2+b^2 avec $(a,b) \in \mathbb{Z}^2$, $|x|^2$ est bien un diviseur de $|y|^2$.

(b) D'après la question précédente, la norme des diviseurs potentiels de y sera majorée par $|y|$. en particulier, si $x = a+ib$ divise y, alors $|a| \leqslant |y|$ et $|b| \leqslant |y|$. On a donc un nombre fini de valeurs possibles pour a et b, et par conséquent un nombre fini de couples (a,b) pouvant correspondre à un entier de Gauss divisant y.

(c) Il suffit tout simplement d'appliquer tel quel l'algorithme d'Euclide (si on a des choix à faire lors de certaines divisions euclidiennes qui n'ont pas un couple quotient/reste unique, on choisit n'importe quel couple convenable). Par construction, si on part de deux entiers de Gauss x et y, et qu'on construit une suite r_n telle que $r_0 = x$, $r_1 = y$ et $r_{n-1} = qr_n + r_{n+1}$, les entiers de Gauss divisant r_n et r_{n+1} seront les mêmes que ceux divisant r_n et r_{n+1}(donc leur diviseur commun de plus grand module aura le même module), donc l'avant dernier reste obtenu avant d'avoir $r_n = 0$ sera un diviseur commun de plus grand module possible pour a et b. On est bien sûr certain d'avoir $r_n = 0$ au bout d'un nombre fini d'étapes, puisque la division euclidienne assure la stricte décroissance des carrés des modules des entiers de Gauss r_n, qui forment donc une suite strictement décroissante d'entiers positifs, qui finira par atteindre 0.

(d) On pose donc $r_0 = 7+11i$ et $r_1 = 1+8i$. Pour effectuer leur division euclidienne, on calcule tout simplement leur quotient puis on cherche l'entier de Gauss le plus proche du résultat, qui servira de quotient : $\frac{7+11i}{1+8i} = \frac{(7+11i)(1-8i)}{1+64} = \frac{95-45i}{65} = \frac{19}{13} - \frac{9}{13}i$. On va donc prendre comme quotient $q = 1-i$, et calculer $r_2 = r_0 - qr_1 = 7+11i-(1-i)(1+8i) = 7+11i-1-8i+i-8 = -2+4i$ (qui a bien un carré de module largement inférieur à 65). On continue : $\frac{1+8i}{-2+4i} = \frac{(1+8i)(-2-4i)}{4+16} = \frac{30-20i}{20} = \frac{3}{2} - i$. On peut par exemple prendre $q = 1-i$ (l'autre choix possible étant $q = 2-i$), ce qui donnera $r_3 = 1+8i-(1-i)(-2-4i) = 1+8i+2+4i-2i-4 = -1+2i$. Pas besoin de se fatiguer beaucoup pour se rendre compte que $r_2 = 2r_3$, donc le prochain reste sera nul, et notre diviseur de plus grand module est $r_3 = -1+2i$, qui a pour module $\sqrt{5}$. On peut vérifier que c'est bien un diviseur commun : $7+11i = (-1+2i)(3-5i)$ et $(1+8i) = (-1+2i)(3-2i)$.

5. Si un entier de Gauss divise 1, d'après la question 4.a, le carré de son module divise $|1|^2 = 1$,

donc son mudole est égal à 1. Il n'y a que quatre entiers de Gauss de module 1 : 1, -1, i et $-i$. Les quatre sont des diviseurs de 1 puisque $(-1)\times(-1) = i\times(-i) = 1$. Il y a donc quatre unités dans G.

6. C'est assez évident, il contient 1, est stable par produit (puisque le module du produit de deux entiers de Gauss de module 1 sera nécessairement un entier de Gauss de module 1) et par passage à l'inverse, c'est bien un sous-groupe multiplicatif de $\mathbb{C}^*$.

7. Soit donc d un diviseur de plus grand module de x et de y, alors les nombres $-d$, id et $-id$ sont aussi des entiers de Gauss divisant x et y et ont le même module que d, ce qui nous fait (au moins) quatre diviseurs de plus grand module possible pour x et y. Réciproquement, si d' est un diviseur de plus grand module de x et y autre que d, on a nécessairement d qui divise d' (et réciproquement), donc $d' = zd$, avec z un entier de Gauss qui par construction devra être de module 1 puisque $|d| = |d'|$. Il s'agit donc nécessairement d'une unité de G, ce qui prouve que d' est l'un des quatre nombres d, $-d$, id ou $-id$.

8. (a) Attention, un nombre premier au sens classique du terme ne sera pas toujours un entier de Gauss élémentaire. Par exemple, 2 est un nombre premier mais $2 = (1+i)(1-i)$ n'est pas un entier de Gauss élémentaire. Par contre, $1+i$ et $1-i$ sont élémentaires (ils ont un carré de module égal à 2, donc leurs diviseurs doident avoir un carré de module égal à 1 ou 2, autrement dit ce sont soit des unités, soit des multiples de $1+i$ ou $1-i$ par des unités).

   (b) On peut faire exactement la même démonstration que pour les nombres premiers : si la liste est finie, notons $p_1, p_2, \ldots, p_n$ tous les entiers de Gauss élémentaires, et posons $n = \prod_{i=1}^{n} p_i + i$ (histoire de faire intervenir un peu plus les complexes), alors n n'est divisible par aucun des nombres p_i (si p_i divisait n, comme il divise $n-i$, il diviserait également i et serait donc une unité de G). Soit n lui-même est un entier de Gauss élémentaire (et notre hypothèse était fausse), soit il admet des diviseurs élémentaires (tout entier de Gauss admet des diviseurs élémentaires, s'il n'est pas lui-même élémentaire, on l'écrit sous la forme yz, et si ni y ni z ne sont élémentaires, on recommence, le carré du module diminue strictement à chaque étape donc on tombera nécessairement sur un entier de Gauss élémentaire au bout d'un moment) qui n'appartiennent pas non plus à la liste des p_i, et on aboutit à la même contradiction.

9. (a) C'est exactement la même démonstration que pour le théorème de Bézout sur les entiers.

   (b) C'est exactement la même démonstration que pour le théorème de Gauss sur les entiers.