Arithmétique

Marc SAGE

1er juillet 2008

Table des matières

Les pgcd et ppcm de deux entiers a et b seront notés

$$\begin{cases} a \wedge b := \text{pgcd}\,(a,b) \\ a \vee b := \text{ppcm}\,(a,b) \end{cases}.$$

Pour un entier $n \geq 2$ et p un nombre premier, on rappelle que la *valuation* p-adique, notée $v_p(n)$, est la puissance de p qui apparaît dans la décomposition de n en facteurs premiers, de sorte que chaque entier s'écrit

$$n = \prod_{p \text{ premier}} p^{v_p(n)}.$$

Pour p premier, le corps[1] à p éléments sera noté

$$\mathbb{F}_p := {}^{\mathbf{Z}}\!/_{p\mathbf{Z}}.$$

On rappelle également le principe de la *descente infinie*, dû à Fermat : pour montrer qu'une équation n'a pas de solutions, on associe à chaque solution s un certain entier $n(s) \in \mathbf{N}$, et on montre qu'à partir d'une solution s l'on peut construire une solution s' telle que $n(s') < n(s)$. On obtient ainsi par récurrence une suite strictement décroissante d'entiers naturels, ce qui est impossible. On peut aussi considérer par l'absurde une solution s minimisant $n(s)$ et contredire la minimalité de $n(s)$, ce qui revient exactement au même.

1 Mise en jambe

1. *Soit $n \geq 2$ un entier. Parmi n entiers, montrer que l'on peut toujours en choisir dont la somme est multiple de n.*
2. *Soit un nombre entier x de six chiffres divisible par 13, mettons $x = abcdef$ en base 10. Montrer que $bcdefa$ est aussi divisible par 13.*
3. *Montrer que la moyenne géométrique des diviseurs d'un entier $n \geq 1$ vaut la racine carrée de cet entier.*

Solution proposée.

1. Il s'agit là d'une application du principe des tiroirs. Nous pouvons former n tiroirs correspondant chacun à un reste possible modulo n. Identifions alors les sommes que l'on peut former à des chaussettes et rangeons chaque chaussette dans le tiroir correspondant. Comme il y a $2^n - 1 > n$ sommes possibles, un tiroir contient deux chaussettes, donc la différence des deux sommes correspondantes est multiple de n. Mais des coefficients négatifs peuvent apparaître. Pour pallier ce problème, on ne regarde que les sommes associées à des parties *croissantes* de notre ensemble $\{a_1, ..., a_n\}$ d'entiers. On peut en trouver n, par exemple les $a_1 + \cdots + a_k$ pour $1 \leq k \leq n$. Si deux chaussettes sont dans un même tiroir, c'est fini par ce qui précède. Sinon, chacun des n tiroirs contient au plus une chaussette, mais comme il y a n chaussettes, le tiroir numéro n en contient une, *CQFD.*
2. Notons $y = bcdefa$. Exprimons y en fonction de x modulo 13 (sachant que $x \equiv 0$ par hypothèse) :

$$y = 10x - 10^6 a + a \equiv \left(1 - 10^6\right) a.$$

Il suffit donc de montrer que $10^6 = 1$ modulo 13 :

$$10^6 \equiv (-3)^{3\times 2} = \left(3^3\right)^2 = 27^2 \equiv 1^2 = 1, \; CQFD.$$

[1] Le terme mathématique « corps » se dit "**f**ield" en anglais, d'où la lettre $\mathbb{F}$ choisie pour $\mathbb{F}_p$.

3. En notant $\tau(n)$ le nombre de diviseurs de n, on demande de montrer l'égalité

$$\prod_{d|n} d = \sqrt{n}^{\tau(n)}.$$

L'idée est de faire intervenir la bijection $d \mapsto \frac{n}{d}$ de l'ensemble des diviseurs de n. On obtient

$$\prod_{d|n} d = \prod_{d|n} \frac{n}{d} = \frac{n^{\tau(n)}}{\prod_{d|n} d}, \text{ d'où le résultat.}$$

2 De l'art d'utiliser les valuations

1. *Soit d et n deux entiers ≥ 1 tels que $d^2 \mid n^2$. Montrer que $d \mid n$.*
2. *Soit $a, b, c \geq 1$ trois entiers tels que*
$$\frac{1}{a} = \frac{1}{b} + \frac{1}{c}.$$
En notant d le pgcd des entiers a, b, c, montrer que les entiers $abcd$, $d(a-c)$ et $d(a-b)$ sont des carrés parfaits.
3. *Soient $a, b, c \geq 1$ trois naturels tels que la somme $\frac{a}{b} + \frac{b}{c} + \frac{c}{a}$ est entière. Montrer que le produit abc est un cube.*

Solution proposée.

1. Il s'agit de montrer que $v_p(d) \leq v_p(n)$ pour chaque premier p. Or, puisque $v_p\left(k^2\right) = 2v_p(k)$ pour entier k, l'hypothèse se réécrit $2v_p(d) \leq 2v_p(n)$, ce qui permet de conclure.
2. L'équation étant homogène en a, b, c et la conclusion cherchée invariante par multiplication de a, b, c par un même entier (non nul), on peut supposer a, b, c premiers entre eux. Par symétrie de b et c, il s'agit de montrer que abc et $a - c$ sont des carrés parfaits.

   L'équation régissant a, b, c se transforme en $bc = ac + ab$. Isoler $a - c$ donne

$$ac = b(c - a).$$

   On en déduit $abc = b^2(c - a)$, ce qui ramène le problème à montrer que $c - a$ est un carré parfait, *i. e.* que ses valuations p-adiques sont chacune paires.

   Soit p premier divisant $c - a$. Il divise $c(c - a) = ca$, donc divise a ou c, mais divisant la différence il les divise tous deux ; puisque a, b, c sont premiers entre eux, p ne peut pas diviser b. On en déduit la valuation de $c - a$:

$$v_p(c - a) = v_p(b(c - a)) = v_p(c) + v_p(a) = \gamma + \alpha$$

   avec les notations évidentes. En particulier, $v_p(c - a) \geq \alpha = v_p(a)$, donc la somme $c = (c - a) + a$ est de valuation $\geq \alpha$, ce qui s'écrit $\gamma \geq \alpha$. Par symétrie, on a l'égalité, d'où $v_p(c - a) = 2\alpha$ pair, *CQFD.*
3. hypothèse et conclusion invariant par division par ppcm –> OPS premiers entre eux.

   soit p diviseur a. Puisue $p \mid abc \mid a^2b + b^2c + c^2a$, on a $p \mid b^2c$, donc $p \mid b$ ou $p \mid c$, à l'exclusion car ppcm=1.

   Ainsi, les factuer premier de abc divisent exacmten deux facteurs parmi a, b, c.

   Soit $p \mid a, b$ et mq $v(b) = 2v(a)$ (chaque valuation est p adique) , ce quic conclura $v(abc) = 3v(a)$. Suppos abs $v(b) < 2v(a)$. Alors $v\left(a^2b + b^2c + c^2a\right) = v(b)$, absrde car $v\left(a^2b + b^2c + c^2a\right) \geq v(abc) > v(b)$. On a donc $v(b) \geq 2v(a)$. Si stricte, alors $3v(a) < v\left(a^2b + b^2c + c^2a\right) = 2v(a)$, absurde.

   Des exemples sont $a = b = c$ ou encore $(1, 2, 4)$,

3 Sur les nombres premiers

On se donne un partie P de l'ensemble $\mathbb{P}$ des nombres premiers ayant au moins trois éléments. On suppose que, pour chaque partie finie $\emptyset \subsetneq A \subsetneq P$, es facteurs premiers de $\left(\prod_{a\in A} a\right) - 1$ restent dans P.

1. *Montrer que* 2 *et* 3 *sont dans* P
2. *Montrer que* P *est infini*
3. *Conclure* $P = \mathbb{P}$.

Solution proposée.

1. Soit p impair dans P : le facteur premier 2 de l'entier pair $p-1 = \left(\prod_{a\in\{p\}} a\right) - 1$ doit rester dans P.

   Supposons par l'absurde que $3 \notin A$. Soit $p \in A$ autre que 2. Alors p vaut à ± 1 modulo 3. Si $p \equiv 1$, la même démonstration que celle pour 2 montre $3 \in A$, ce qui est exclu. Si $p \equiv -1$, l'entier $2p-1$ est multiple de trois et l'on conclut de même $3 \in A$.
2. On s'inspire de la démonstration d'Euclide : supposant P fini, fait alors sens l'entier $\pi := \prod_P p$. Puisque P contient au moins trois éléments, $\frac{\pi}{p}$ contient deux facteurs premiers, donc est $\geq 2\cdot 3 = 6$, donc $\frac{\pi}{p} - 1$ possède un facteur premier, lequel reste dans P par hypothèse et ne peut donc être que p.

   Appliquant à $p = 2$ et $p = 3$, il vient

$$\begin{cases} \frac{\pi}{2} = 2^\alpha + 1 \\ \frac{\pi}{3} = 3^\beta + 1 \end{cases} \quad \text{avec } \alpha, \beta \geq 1.$$

   Puisque $\pi \geq 2\cdot 3\cdot 5 = 30$, on a nécessairement $\alpha \geq 3$, d'où $\pi \equiv 2$ modulo 8. La seconde ligne donne $\pi - 3 = 3^{\beta+1}$, d'où $-1 \equiv 3^{\beta+1}$ modulo 8 ; or, les puissances de 3 valent 1 ou 3 modulo 8, d'où la contradiction.
3. Fixons un premier p. Le principe des tiroirs nous dit qu'il y a une infinité d'éléments $p_1, p_2, ...$ de P ayant même reste r modulo p. Un tel r est non nul, sinon on aurait dans A plusieurs nombres premiers divisibles par p. Pour $k \geq 1$, le produit $p_1 \cdots p_k$ vaut r^k modulo p et tous les facteurs premiers de $p_1 \cdots p_k - 1$ sont dans A. Pour conclure, il suffit de trouver un k tel que p divise $p_1 \cdots p_k - 1$, ce qui sera le cas si $r^k = 1$ modulo p ; puisque $r \neq 0$, il suffit de prendre pour k l'ordre de r dans $\mathbb{F}_p^*$.

4 Une identité à connaître sur l'indicatrice d'Euler

Pour n un entier ≥ 1, on note $\varphi(n)$ le nombre d'entiers parmi $\{1, ..., n\}$ qui sont premiers avec n. φ est appelée *indicatrice d'Euler*. On rappelle que φ peut être définie par[2]

$$\begin{cases} \varphi(1) = 1 \\ \varphi\left(p^\beta\right) = p^\beta - p^{\beta-1} \text{ si } p \text{ est premier et } \beta \geq 1 \\ \varphi(ab) = \varphi(a)\,\varphi(b) \text{ si } a \text{ et } b \text{ sont premiers entre eux} \end{cases}.$$

Montrer pour chaque entier $n \geq 1$ *l'égalité*

$$\sum_{d|n} \varphi(d) = n.$$

Solution proposée.

Première méthode (brutale).

[2] En fait, la bonne définition de $\varphi(n)$ est le cardinal $\left|\left(\mathbb{Z}/n\mathbb{Z}\right)^\times\right|$ des inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$. Sa multiplicativité résulte alors immédiatement du théorème chinois.

Cassons $n=\prod_{i=1}^{r} p_i^{\alpha_i}$ en produit de facteurs premiers (avec $r=0$ si $n=1$). On calcule comme une brute en utilisant les propriétés de φ rappelées plus haut :

$$\begin{aligned}\sum_{d|n}\varphi(d) &= \sum_{\substack{d=\prod_{i=1}^{r} p_i^{\beta_i}\\ 0\le\beta_1\le\alpha_1\\ \dots\\ 0\le\beta_r\le\alpha_r}}\varphi(d)=\sum_{\substack{0\le\beta_1\le\alpha_1\\ \dots\\ 0\le\beta_r\le\alpha_r}}\varphi\left(\prod_{i=1}^{r}p_i^{\beta_i}\right)=\sum_{\substack{0\le\beta_1\le\alpha_1\\ \dots\\ 0\le\beta_r\le\alpha_r}}\prod_{i=1}^{r}\varphi\left(p_i^{\beta_i}\right)=\prod_{i=1}^{r}\sum_{0\le\beta\le\alpha_i}\varphi\left(p_i^{\beta}\right)\\ &= \prod_{i=1}^{r}\left(\sum_{\beta=1}^{\alpha_i}\left(p_i^{\beta}-p_i^{\beta-1}\right)+1\right)=\prod_{i=1}^{r}\left((p_i^{\alpha_i}-1)+1\right)=\prod_{i=1}^{r}p_i^{\alpha_i}=n.\end{aligned}$$

Deuxième méthode (moins brutale).

Raisonnons par récurrence sur le nombre r de facteurs premiers de n.
Pour $r=1$, on $n=p^{\alpha}$, donc

$$\sum_{d|n}\varphi(d)=\sum_{\beta=0}^{\alpha}\varphi\left(p^{\beta}\right)=\sum_{\beta=1}^{\alpha}\left(p^{\beta}-p^{\beta-1}\right)+1=(p^{\alpha}-1)+1=n.$$

Pour la suite, soit $n=p^a m$ où $p\wedge m=1$. Alors

$$\sum_{d|n}\varphi(d)=\sum_{\substack{d|m\\ d'|p^{\alpha}}}\varphi(dd')=\sum_{\substack{d|m\\ d'|p^{\alpha}}}\varphi(d)\varphi(d')=\sum_{d|m}\varphi(d)\sum_{d|p^{\alpha}}\varphi(d')=mp^{\alpha}=n$$

en appliquant les cas 1 et $r-1$.

En fait, on a fait le même calcul que lors de la méthode brutale, sauf que la récurrence nous a épargné les signes et conditions multiples peu agréables à se coltiner.

Troisième méthode (dénombrement).

On observe qu'une fraction $\frac{a}{n}$ où $1\le a\le n$ se met sous forme irréductible $\frac{e}{d}$ ssi e est premier avec d (et bien sûr $1\le e\le d$). À d fixé, il y a donc exactement $\varphi(d)$ fractions $\frac{a}{n}$ dont la réduite a pour dénominateur d. Comme il y a n telles fractions en tout, on en déduit le résultat. Ploum.

Remarque (màj 27 08 19). Démystifions cette dernière solution pour qui la verrait un peu trop "ploumesque". Regroupons les éléments du groupe additif $\mathbf{Z}/n$ selon leur ordre, lequel doit diviser l'ordre n du groupe. Pour chaque diviseur $d\mid n$, est d'ordre d l'élément $\frac{n}{d}$, mais aussi l'élément $e\frac{n}{d}$ pour chaque entier $e\in[1,d]$ étranger à d (et il y a justement $\varphi(d)$ tels entiers e) ; or chaque élément $\overline{a}\in\mathbf{Z}/n$ peut s'écrire sous cette forme (cela revient à disposer d'une égalité $\frac{a}{n}=\frac{e}{d}$ où $\begin{cases}e\wedge d=1\\ 1\le e\le d\end{cases}$ et on retrouve nos fractions ci-dessus), donc il n'y a pas d'autre élément d'ordre d : il y en a exactement $\varphi(d)$.

En effaçant toutes les traces ci-dessus, on obtient une preuve condensée en une seule phrase : fait sens et est bijective l'application $\begin{cases}\mathbf{Z}/n & \xrightarrow{\sim} & \coprod_{d|n}\{(d,e)\}_{1\le e\le d}^{e\wedge d=1}\\ a & \longmapsto & \left(\frac{n}{a\wedge n},\frac{a}{a\wedge n}\right)\\ e\frac{n}{d} & \longleftarrow\mid & (d,e)\end{cases}$, d'où l'égalité cardinale recherchée.

5 Nombres pairs parfaits

Rappell sur σ (somme des diviseurs)
montrer que multiplicative (expliciter)
montrer $\sigma(ab)\ge a\sigma(b)$ avec $=$ ssi $a=1$.
(dem : $\sigma(ab)=\sum_{d|ab}d\ge\sum_{d'|b}ad'=a\sigma(b)$ avec $=$ ssi a a un seul divusuer, ie si $a=1$)
Un nombre entier est *parfait* s'il vaut la somme de ses diviseurs stricts, ie si $\sigma(n)=2n$.

Montrer q'un pair est parfait ssi il est de la forme $2^a p$ où p estun premier valant $2^{a+1}-1$.

vérif :

$$\sigma\left(2^{\alpha}p\right)=\left(2^{\alpha+1}-1\right)(p+1)=p2^{\alpha+1}=2\left(2^{\alpha}p\right).$$

Soit $n=2^{\alpha}m$ parfait où m impair :

$$2^{\alpha+1}m=2n=\sigma(n)=\left(2^{\alpha+1}-1\right)\sigma(m).$$

En particulieu, $p:=2^{\alpha+1}-1$ divise m, mettons $m=kp$. En réinjectant, on trouve

$$2^{\alpha+1}k=\sigma(kp)\geq k\sigma(p)\geq k(p+1)=k2^{\alpha+1},$$

donc égal partout, donc$k=1$ et $\sigma(p)=p+1$ donc $p=m$ premier

6 Formule de Legendre et deux applications

1. *Démontrer la* formule de Legendre[3]*, qui donne la valuation p-adique d'une factorielle :*

$$v_p(n!)=\sum_{v\geq 1}\left\lfloor\frac{n}{p^v}\right\rfloor.$$

2. *Montrer, en notant $S_p(n)$ la somme des chiffres de n en base p, que cette quantité vaut également*

$$v_p(n!)=\frac{n-S_p(n)}{p-1}.$$

3. *Par combien de zéros se termine* $100!$ *?*
4. *Pour des entiers $a,b\geq 1$, montrer que $\binom{a+b}{a}$ divise $\binom{2a}{a}\binom{2b}{b}$. ? ? ? ? genéralistion dans ENgel ?*

Solution proposée.

1. On regarde à p fixé la contribution en p de chaque entier compris entre 2 et n. Pour un entier $v\geq 1$, notons $\mathcal{M}_v$ les multiples de p^v dans $\{1,...,n\}$ et $m_v=\#\mathcal{M}_v$ le nombre de tels multiples.

   Il y a déjà les multiples de p qui apportent chacun une contribution de 1. Puis les multiples de p^2 apportent chacun un facteur 2 dans le calcul de $v_p(n!)$, mais on a déjà compté en partie leur contribution dans les multiples de p, de sorte que la contribution supplémentaire de $\mathcal{M}_2$ est en fait de 1 pour chacun de ces multiples. Ainsi de suite, chaque multiple de p^{v+1} contribue de $v+1$, mais la partie v a déjà été comptée dans la contribution de $\mathcal{M}_v$, ce qui donne au final une contribution de 1 pour tous les multiples. Ainsi :

$$v_p(n!)=\sum_{v\geq 1}m_v.$$

   Si l'on n'est pas convaincu, en notant a_v le nombre d'entiers de $\{1,...,n\}$ de valuation v, il est clair que $v_p(n!)=\sum_{v\geq 1}va_v$, ce que l'on peut réécrire sous la forme

$$\begin{aligned}a_1+2a_2+3a_3+4a_4+\cdots &= (a_1+a_2+a_3+a_4+\cdots)+\\ &\quad (a_2+a_3+a_4+\cdots)+\\ &\quad (a_3+a_4+\cdots)+\\ &\quad (a_4+\cdots)+\cdots.\end{aligned}$$

   Maintenant, $\sum_{i\geq v}a_i$ compte les entiers de $\{1,...,n\}$ dont la valuation est $\geq v$, *i. e.* les multiples de p^v, d'où $\sum_{i\geq v}a_i=m_v$.

   Il reste à calculer m_v. Or, ce dernier vérifie

$$m_vp^v\leq n<(m_v+1)p^v \iff m_v\leq\frac{n}{p^v}<m_v+1 \iff m_v=\left\lfloor\frac{n}{p^v}\right\rfloor.$$

[3] On a noté $\lfloor x\rfloor$ la *partie entière* d'un réel x, qui rappelons-le est caractérisée par l'encadrement

$$\lfloor x\rfloor\leq x<\lfloor x\rfloor+1.$$

2. Quant à la seconde formule, plus anecdotique (il faut le dire), écrivons $n = a_N a_{N-1} ... a_1 a_0$ en base p, de sorte que $\left\lfloor \frac{n}{p^v} \right\rfloor = a_N a_{N-1} ... a_{v+1} a_v$ (raisonner comme en base dix où diviser par 10^v revient à déplacer la virgule de v places vers la gauche). Il en résulte

$$\begin{aligned} v_p(n!) = \sum_{v \geq 1} \left\lfloor \frac{n}{p^v} \right\rfloor &= \left(a_1 + a_2 p + a_3 p^2 + a_4 p^3 + \cdots\right) + \\ &\quad \left(a_2 + a_3 p + a_4 p^2 + \cdots\right) + \\ &\quad (a_3 + a_4 p + \cdots) + \\ &\quad (a_4 + \cdots) + \cdots \\ &= a_1 + a_2(p+1) + a_3\left(p^2 + p + 1\right) + a_4\left(p^3 + p^2 + p + 1\right) + \cdots \\ &= a_1 \frac{p-1}{p-1} + a_2 \frac{p^2-1}{p-1} + a_3 \frac{p^3-1}{p-1} + a_4 \frac{p^4-1}{p-1} + \cdots \\ &= \frac{a_1 p + a_2 p^2 + a_3 p^3 + \cdots - (a_1 + a_2 + a_3 + \cdots)}{p-1} \\ &= \frac{(n - a_0) - (S_p(n) - a_0)}{p-1}, \ CQFD. \end{aligned}$$

3. Le nombre de zéros est la puissance maximale de 10 qui apparaît dans le produit 100!. Puisque les 2 apparaissent plus souvent que les 5, on recherche la puissance maximale de 5 dans 100!, *i. e.* la valuation 5-adique de 100!. On applique Legendre :

$$v_5(100!) = \left\lfloor \frac{100}{5} \right\rfloor + \left\lfloor \frac{100}{25} \right\rfloor + 0 = 20 + 4 = 24.$$

4. Il s'agit de montrer l'intégralité du quotient

$$\frac{\binom{2a}{a}\binom{2b}{b}}{\binom{a+b}{a}} = \frac{(2a)!\,(2b)!}{a!b!\,(a+b)!},$$

donc de montrer que la valuation p-adique du numérateur est plus grande que celle du dénominateur pour chaque p premier, *i. e.* (en utilisant Legendre)

$$\begin{aligned} & v_p((2a)!) + v_p((2b)!) \overset{?}{\geq} v_p(a!) + v_p(b!) + v_p((a+b)!) \\ \iff & \sum_{v \geq 1} \left\lfloor \frac{2a}{p^v} \right\rfloor + \sum_{v \geq 1} \left\lfloor \frac{2a}{p^v} \right\rfloor \overset{?}{\geq} \sum_{v \geq 1} \left\lfloor \frac{a}{p^v} \right\rfloor + \sum_{v \geq 1} \left\lfloor \frac{b}{p^v} \right\rfloor + \sum_{v \geq 1} \left\lfloor \frac{a+b}{p^v} \right\rfloor \\ \iff & \sum_{v \geq 1} \left\lfloor \frac{2a}{p^v} \right\rfloor + \left\lfloor \frac{2a}{p^v} \right\rfloor \overset{?}{\geq} \sum_{v \geq 1} \left\lfloor \frac{a}{p^v} \right\rfloor + \left\lfloor \frac{b}{p^v} \right\rfloor + \left\lfloor \frac{a+b}{p^v} \right\rfloor. \end{aligned}$$

Il suffit donc de montrer que

$$\left\lfloor \frac{2a}{p^v} \right\rfloor + \left\lfloor \frac{2a}{p^v} \right\rfloor \overset{?}{\geq} \left\lfloor \frac{a}{p^v} \right\rfloor + \left\lfloor \frac{b}{p^v} \right\rfloor + \left\lfloor \frac{a+b}{p^v} \right\rfloor.$$

Simplifions déjà en effectuant une division euclidienne de a et b par p^v : $\begin{cases} a = a' p^v + \alpha \\ b = b' p^v + \beta \end{cases}$. On veut donc

$$\begin{aligned} & 2a' + \left\lfloor \frac{2\alpha}{p^v} \right\rfloor + 2b' + \left\lfloor \frac{2\beta}{p^v} \right\rfloor \overset{?}{\geq} a' + b' + (a' + b') + \left\lfloor \frac{\alpha + \beta}{p^v} \right\rfloor \\ \iff & \left\lfloor \frac{2\alpha}{p^v} \right\rfloor + \left\lfloor \frac{2\beta}{p^v} \right\rfloor \overset{?}{\geq} \left\lfloor \frac{\alpha + \beta}{p^v} \right\rfloor. \end{aligned}$$

Si l'on montre que, pour tous réels positifs x, y,

$$\lfloor 2x \rfloor + \lfloor 2y \rfloor \geq \lfloor x + y \rfloor ,$$

on aura gagné. Or, si par exemple $x \geq y$, on a $2x \geq x + y$, d'où $\lfloor 2x \rfloor \geq \lfloor x + y \rfloor$ et le résultat vu que $\lfloor 2y \rfloor \geq 0$.

7 Une équation diophantienne

Résoudre pour des entiers $a, b \geq 1$ l'équation $a^b = b^a$.

Solution proposée.

Première méthode (arithmétique).
On peut supposer $a \leq b$ par symétrie, et même $a \geq 2$ vu que

$$a = 1 \implies 1^b = b^1 \implies (a, b) = (1, 1)$$

qui est clairement solution. On se ramène à des entiers premiers entre eux en posant $\begin{cases} a = \delta\alpha \\ b = \delta\beta \end{cases}$ avec $\begin{cases} \alpha \wedge \beta = 1 \\ \delta = a \wedge b \end{cases}$ et $\alpha \leq \beta$. On obtient $\delta^b \alpha^b = \delta^a \beta^a$, ou encore $\beta^a = \delta^{b-a} \alpha^b$. Mais la condition $\alpha \wedge \beta = 1$ impose $\alpha = 1$ car chaque facteur premier de α divise les deux membres et doit donc apparaître dans β, ce qui est impossible. On a donc $a \mid b$ et on peut écrire $b = ka$ avec $k \in \mathbf{N}^*$. L'équation se réécrit

$$b^a = a^b = a^{ka} = \left(a^k\right)^a \iff b = a^k \iff ka = a^k \iff k = a^{k-1}.$$

On voit que, pour k grand, la puissance à droite écrase le terme de gauche. Précisément, dès que $k \geq 2$ on a $2^k \geq 2k$, donc

$$k = a^{k-1} \geq 2^{k-1} \geq k \implies a = 2 \text{ et } k = 2.$$

Les solutions sont donc les couples (a, a) pour $a \geq 1$ (correspondant à $k = 1$), $(2, 4)$ et $(4, 2)$.

Seconde méthode (analytique).
En passant au logarithme, l'équation se réécrit

$$\frac{\ln a}{a} = \frac{\ln b}{b}.$$

Il est donc judicieux d'étudier la fonction $f : \begin{cases} [1, \infty[& \longrightarrow & \mathbf{R} \\ x & \longmapsto & \frac{\ln x}{x} \end{cases}$. On cherche les droites horizontales coupant le graphe de f en au moins deux points d'abscisses entières (les couples $a = b$ étant trivialement solutions du problème).

Une dérivation donne $f'(x) = \frac{\frac{1}{x} x - \ln x}{x^2}$ qui est du signe de $1 - \ln x$, *i. e.* de $e - x$. On en déduit que f est strictement croissante sur $[1, e]$ et strictement décroissante sur $[e, \infty[$.

Ainsi, si une droite horizontale coupe le graphe de f en $\begin{pmatrix} u \\ f(u) \end{pmatrix}$ et $\begin{pmatrix} v \\ f(v) \end{pmatrix}$ avec $u < v$ entiers, alors u est nécessairement plus petit que e, ce qui impose $u = 1$ ou 2 :

- $u = 1 \implies 0 = \dfrac{\ln u}{u} = \dfrac{\ln v}{v} \implies v = 1$;
- $u = 2 \implies \dfrac{\ln 2}{2} = \dfrac{\ln v}{v} \implies 2^v = v^2 \implies v = 2$ ou 4.

Finalement, les solutions sont les (a, a) pour $a \geq 1$, $(2, 4)$ et $(4, 2)$.

8 Équation de Pythagore

On demande de résoudre l'équation en les entiers $x, y, z \geq 1$:

$$x^2 + y^2 = z^2.$$

Même question pour $x, y > 0$ rationnels et $z = 1$.

Solution proposée.
Observer avant toute chose qu'on peut passer d'une équation à l'autre en divisant par l'entier z^2 ou en multipliant par le ppcm de x et y.

Première méthode (arithmétique).
Commençons par quelques simplifications préliminaires.
Quitte à diviser par le pgcd $x \wedge y$, dont le carré doit diviser la somme $x^2 + y^2$ qui vaut z^2 par hypothèse, on peut supposer que x et y sont premiers entre eux.
Ceci implique la primalité relative de x et z (ainsi que de y et z) : en effet, si d divise x et z, d divise z^2 et x^2, donc la différence $z^2 - x^2 = y^2$, d'où $d \mid x^2 \wedge y^2 \wedge z^2 = 1$. On montrerait de même que $y \wedge z = 1$.
On réécrit alors l'équation sous la forme

$$x^2 = (z - y)(z + y).$$

Si les deux termes de droite était premiers entre eux, on pourrait dire qu'ils sont tous deux des carrés et en déduire la forme de y et z puis de x. Mais cela est faux en général (prendre z et y pairs).
On se souvient alors qu'un carré vaut toujours 1 ou 0 modulo 4, ce qui impose à x ou y d'être pair (sinon $z^2 = 2$ modulo 4), disons $x = 2t$. On a donc

$$t^2 = \frac{z - y}{2} \frac{z + y}{2}.$$

Maintenant, les termes de droites $\frac{z-y}{2}$ et $\frac{z+y}{2}$ sont premiers entre eux : si d est un diviseur commun, d doit diviser la somme z et la différence y, donc vaudra 1, y et z étant premiers entre eux. On peut donc écrire

$$\begin{cases} \frac{z+y}{2} = u^2 \\ \frac{z-y}{2} = v^2 \end{cases} \quad \text{où } u > v > 0 \text{ sont deux entiers premiers entre eux,}$$

d'où $\begin{cases} z = u^2 + v^2 \\ y = u^2 - v^2 \end{cases}$ et $x = 2t = 2uv$. En remultipliant par le pgcd n de x et y, on trouve les solutions générales :

$$\text{si } \frac{x}{x \wedge y} \text{ est pair, } \begin{cases} x = n2uv \\ y = n\left(u^2 - v^2\right) \\ z = n\left(u^2 + v^2\right) \end{cases} \quad \text{où } \begin{cases} n > 0 \\ u > v > 0 \\ u \wedge v = 1 \end{cases}.$$

Réciproquement, on vérifie que

$$(2uv)^2 + \left(u^2 - v^2\right)^2 = 4u^2v^2 + \left(u^4 - 2u^2v^2 + v^4\right) = u^4 + 2u^2v^2 + v^4 = \left(u^2 + v^2\right)^2.$$

Quant à l'équation à inconnues rationnelles, quitte à la multiplier par un dénominateur commun, on peut reprendre les solutions de la question précédentes et conclure : les solutions rationnelles de $x^2 + y^2 = 1$ sont de la forme ? ? ?

Seconde méthode (analytique).
Nous proposons une méthode indépendante qui aurait pu s'utiliser pour le cas entier : il s'agit d'un reparamétrage judicieux de nos inconnues qui fait se simplifier l'équation de départ.
Posant pour $x \neq 0$ un rationnel λ tel que $y = \lambda x - 1$, notre équation se réécrit

$$\begin{aligned} 1 &= x^2 + (\lambda x - 1)^2 = x^2\left(1 + \lambda^2\right) - 2\lambda x + 1, \\ \text{d'où } x &= \frac{2\lambda}{1 + \lambda^2} \text{ et } y = \lambda x - 1 = \frac{1 - \lambda^2}{1 + \lambda^2}. \end{aligned}$$

Le cas $x = 0$ (forçant $y = \pm 1$) étant obtenu pour $\lambda = 0$, le paramétrage ci-dessus recouvre bien chaque solution de notre équation à l'exception du point $(0, -1)$, lequel peut être vu comme le cas limite où $|\lambda| \longrightarrow \infty$

1. Le lecteur vérifiera de lui-même que les valeurs ci-dessus donnent bien des points du cercle unité. C'est le *paramétrage rationnel* du cercle unité :

$$\begin{cases} x = \frac{2t}{1+t^2} \\ y = \frac{1-t^2}{1+t^2} \end{cases} \quad \text{où } t \text{ décrit } \mathbf{Q} \cup \{\infty\}.$$

Remarque. En autorisant des égalités larges dans les conditions sur n, u, v, on rajoute les solutions « évidentes » $(0, n, n)$ et $(n, 0, n)$ pour n décrivant $\mathbf{N}$: faire $v = 0$ ou $u = v$. On obtient ainsi les solutions à l'équation de Pythagore dans $\mathbf{N}^3$.

Pour obtenir les solutions dans $\mathbf{Z}^3$, il suffit de remarquer qu'en prenant les valeurs absolues on tombe dans $\mathbf{N}^3$ et par là même dans ce qui précède : on rajoutera donc des signes $\pm$ devant chaque coordonnée pour couvrir toutes les solutions.

Rq : on retrouve l'irrationalité de $\sqrt{2}$: $x = y$ impose $2uv = u^2 - v^2$ et pb mod 4 ? ? ?

9 Illustrer la descente infinie

Résoudre l'équation suivante en les entiers $a, b, c \geq 1$:

$$a^4 + b^4 = c^2.$$

Solution proposée.

Nous allons faire une descente infinie en utilisant les résulats connus sur les solutions de l'équation de Pythagore.

Soit (a, b, c) une solution minimisant c. Les entiers a, b, c sont donc deux à deux premiers entre eux (diviser par leur pgcd abaisse c) et l'exercice précédent permet d'écrire (en supposant a pair)

$$\begin{cases} a^2 = 2uv \\ b^2 = u^2 - v^2 \\ c = u^2 + v^2 \end{cases} \quad \text{avec } u \wedge v = 1.$$

La deuxième ligne est encore une équation de Pythagore :

$$u^2 = v^2 + b^2 \text{ avec } u \wedge v = 1.$$

b étant impair (il est premier avec a), v doit être pair et l'on a alors

$$\begin{cases} v = 2UV \\ b = U^2 - V^2 \\ u = U^2 + V^2 \end{cases} \quad \text{avec } U \wedge V = 1.$$

On en déduit les trois inconnues à l'aide des paramètres U et V :

$$\begin{cases} a^2 = 4\left(U^2 + V^2\right)UV \\ b = U^2 - V^2 \\ c = \left(U^2 + V^2\right)^2 + 4U^2V^2 \end{cases}.$$

La première ligne exprimant la factorisation d'un carré, on a de bonnes chances d'en tirer de l'information.

Il est facile de voir que U est premier avec $U^2 + V^2$: si p était un diviseur premier commun aux deux, p diviserait $\left(U^2 + V^2\right) - UU = V^2$, donc p diviserait V, et comme $U \wedge V = 1$, p vaudrait 1, ce qui n'est pas possible pour un premier. On montrerait de même que $V \wedge \left(U^2 + V^2\right) = 1$. Les trois nombres U, V et $U^2 + V^2$ sont par conséquent premiers entre eux et leur produit est un carré $\left(\frac{a}{2}\right)^2$, donc sont tous les trois des carrés :

$$\begin{cases} U = \alpha^2 \\ V = \beta^2 \\ U^2 + V^2 = \gamma^2 \end{cases}.$$

On en tire une nouvelle solution (α, β, γ) à notre équation de départ. En remarquant que

$$\gamma \leq \gamma^2 = U^2 + V^2 = u < u^2 + v^2 = c,$$

on peut appliquer le principe de descente infinie sur la troisième coordonnée et conclure à la contradiction.

Remarque. On déduit de cet exercice le théorème de Fermat pour $n = 4$: l'équation

$$a^4 + b^4 = c^4$$

n'a pas de solution dans $\mathbf{N}^{*3}$.

10 Une autre équation diophantienne

Résoudre en les entiers $a, b \geq 1$ l'équation

$$3^a - 2^b = 1.$$

Solution proposée.
Laissons déjà de côté la solution évidente $(a, b) = (1, 1)$. On suppose donc $a, b \geq 2$.

L'idée est de factoriser $2^b = 3^a - 1$ ou $3^a = 2^b + 1$; en effet, le terme de gauche est à chaque fois la puissance d'un nombe premier, ce qui forcera les termes factorisés à droite à être aussi des puissances de ce même nombre premier.

Avant cela, réduisons modulo des petits nombres premiers pour avoir de l'information sur a et b. Modulo 3, b doit être impair, donc, modulo 4, a doit aussi être pair (car $b \geq 2$), mettons $a = 2c$. On a donc

$$2^b = 3^{2c} - 1 = (3^c - 1)(3^c + 1)$$

Les deux termes de droite sont des puissances de 2 distantes de 2, donc valent 2 et 4, d'où $3^c - 1 = 2$, $c = 1$ et $a = 2$, puis $2^b = 3^2 - 1 = 8$ et $b = 3$.

Remarque. Ce résultat est un cas particulier de feu la *conjecture de Catalan* (prouvée par Preda Mihăilescu en avril 2002) qui affirme que les seules puissances entières consécutives (non triviales) sont 8 et 9.

11 Fibonacci

mq $F_a \wedge F_b = F_{a \wedge b}$.
voir soulami et Engel pour plein d'identités analogues

montrre que chaque eniter est somme de fibo non consécutif (de manière unique)
trouver des f stt croissant de $\mathbf{N}^*$ dans $\mathbf{N}^* tq$ $f(1) = 2$, $f(f(n)) = f(n) + n$

? ? ? ?
$ff^2 = f + id$ <=>$F_{n+2} = F_{n+1} + F_n$. COmment formaliser ?
On écrit un nombre comme somme de fibo, et on décale les indices.
unicité ? ? ?

12 Suites d'entiers spéciaux

Montrer qu'il y a des suites arbitrairement longues d'entiers qui chacun n'est ni une puissance parfaite (un n^k avec $n, k \geq 2$) ni un premier.

contredire pusisance -> imposer une valuation 1, eg $\equiv p \left[p^2\right]$
contredire premier-> imposer une divisibilité en plus, eg $\equiv 0 \left[q\right]$
Synthèse
soit $\binom{p_1 \ \cdots \ p_n}{q_1 \ \cdots \ q_n}$ $2n$ premiers distaincts. Soit $x \begin{array}{l} \equiv p_k - k \ \left[p_k^2\right] \\ \equiv -k \left[q_k\right] \end{array}$ pour chq k.
Alors $x + k = p_k \left[p_k^2\right]$ donc n'est pas une puissane parfaite.
De plus $x + k = 0 \left[q_k\right]$, donc $x + k$ multiples de p_k et q_k, donc pas premier

Les deux exercices qui suivent mettent en valeur l'utilisation des trinômes de second degré pour la résolution d'équation diophantiennes.

13 Intégralité de $\frac{a^3+b^3-a^2b^2}{(a+b)^2}$

Trouver tous les entiers $a, b \geq 1$ tels que

$$\frac{a^3 + b^3 - a^2b^2}{(a+b)^2}$$

soit un entier relatif, puis naturel.

Solution proposée.
On commencer par simplifier la fraction en faisant apparaître le dénominateur $a + b$ au numérateur :

$$\frac{a^3 + b^3 - a^2b^2}{(a+b)^2} = \frac{(a+b)^3 - 3ab^2 - 3a^2b - a^2b^2}{(a+b)^2} = a + b - \frac{ab}{(a+b)^2}\left(3\left(a+b\right) + ab\right).$$

En notant $\left\{ \begin{array}{c} s := a + b \\ p := ab \end{array} \right.$, pour $\left\{ \begin{array}{c} \text{« somme »} \\ \text{« produit »} \end{array} \right.$, il faut que $\frac{p}{s}\left(3 + \frac{p}{s}\right)$ soit entier, ce qui force $\frac{p}{s}$ à être entier : en effet, si $\frac{p}{s} = \frac{u}{v}$ avec $u \wedge v = 1$, on dispose de l'entier

$$\frac{p}{s}\left(3 + \frac{p}{s}\right) = \frac{u}{v}\left(3 + \frac{u}{v}\right) = \frac{3uv + u^2}{v^2},$$

donc

$$v \mid v^2 \mid 3uv + u^2 \implies v \mid u^2 \implies v = 1.$$

Notons k l'entier $\frac{p}{s}$. On sait que a et b sont les racines du trinôme $X^2 - sX + p$. Le discriminant de ce dernier doit donc être un carré δ^2, ce qui s'écrit

$$\delta^2 = s^2 - 4p = s^2 - 4ks.$$

De même, s est racine de $X^2 - 4kX - \delta^2$, donc son discriminant réduit doit être un carré c^2 :

$$c^2 = (2k)^2 + \delta^2.$$

On reconnait là une équation de Pythagore, avec $2k$ pair. On en déduit $\left\{ \begin{array}{l} \delta = n\left(u^2 - v^2\right) \\ 2k = n\left(2uv\right) \\ c = n\left(u^2 + v^2\right) \end{array} \right.$ où n et $u \geq v$ sont des entiers positifs, d'où

$$s = 2k + c = n\left(2uv + \left(u^2 + v^2\right)\right) = n\left(u + v\right)^2$$

(la solution négative est à rejeter car $s = a + b > 0$). Il en résulte, en supposant $a \leq b$ par symétrie

$$\begin{cases} a = \frac{s-\delta}{2} = \frac{n(u+v)^2 - n\left(u^2-v^2\right)}{2} = \frac{n2uv+2nv^2}{2} = nv\,(u+v) \\ b = \frac{s+\delta}{2} = \frac{n(u+v)^2 + n\left(u^2-v^2\right)}{2} = \frac{n2u^2+2nuv}{2} = nu\,(u+v) \end{cases}.$$

On vérifie réciproquement que

$$\frac{ab}{a+b} = \frac{nv\,(u+v)\,nu\,(u+v)}{nv\,(u+v) + nu\,(u+v)} = \frac{n^2uv\,(u+v)^2}{n\,(u+v)\,(u+v)} = nuv \in \mathbf{N}.$$

Passons à la deuxième question : on veut à présent que $s - \frac{p}{s}\left(3 + \frac{p}{s}\right)$ soit un entier *positif*. Remarquer que $nuv = \frac{p}{s} > 0$, donc $n, u, v \geq 1$. Ceci implique

$$\begin{aligned} 0 \leq \frac{s - \frac{p}{s}\left(3 + \frac{p}{s}\right)}{nuv} &= \frac{n\,(u+v)^2 - nuv\,(3 + nuv)}{nuv} \\ \implies 0 \leq \frac{u}{v} + 2 + \frac{v}{u} - 3 - nuv \leq u + v - 1 - uv &= \underbrace{(u-1)}_{\geq 0}\underbrace{(1-v)}_{\leq 0} \leq 0. \end{aligned}$$

On en déduit $u = v = 1$, et de plus le cas d'égalité dans l'inégalité utilisée $-nuv \leq -uv$ impose $n = 1$. Les valeurs de a et b tombent alors d'elles-mêmes :

$$\begin{cases} a = nv\,(u+v) = 2 \\ b = nu\,(u+v) = 2 \end{cases}.$$

Réciproquement, pour ces valeurs, on trouve

$$\frac{a^3 + b^3 - a^2b^2}{(a+b)^2} = \frac{8 + 8 - 4 \times 4}{4^2} = 0 \in \mathbf{N}.$$

Remarque. Pour expliciter deux entiers ≥ 1 dont la somme divise le produit, on peut également procéder de la manière suivante. Notons a et b nos deux entiers et k l'entier $\frac{ab}{a+b}$. Cela se réécrit $ak + bk = ab$, d'où (en rajoutant ce qu'il faut pour factoriser)

$$(a-k)\,(b-k) = ab - ak - bk + k^2 = k^2.$$

En notant $\begin{cases} \alpha := a - k \\ \beta := b - k \end{cases}$, on obtient $k^2 = \alpha\beta$. Devant une telle égalité, on **doit** avoir envie de montrer que α et β sont premiers entre eux. Or,

$$\operatorname{pgcd}(a, b, k) = \operatorname{pgcd}(k + \alpha, k + \beta, k) = \operatorname{pgcd}(\alpha, \beta, k),$$

et on peut toujours supposer ces derniers égaux à 1 (quitte à diviser a, b, k par $a \wedge b \wedge k$), donc il n'y a pas de diviseur premier commun à α et β (un tel diviseur devrait diviser $\alpha\beta = k^2$, donc k). On en déduit que α et β sont des carrés, mettons $(\alpha, \beta) = \left(u^2, v^2\right)$, d'où $k = uv$ et

$$(a, b) = (k + \alpha, k + \beta) = (u\,(u+v)\,, v\,(u+v))\,.$$

On retrouve la forme trouvée plus haut.

14 Le carré parfait $\frac{a^2+b^2}{1+ab}$ (IMO 1988)

Soient a et b des entiers ≥ 1. Montrer par une descente infinie que, si $\frac{a^2+b^2}{1+ab}$ est entier, alors c'est un carré parfait.

Solution proposée.

On raisonne comme le suggère l'énoncé : considérons par l'absurde un couple $(a,b) \in \mathbf{N}^{*2}$ tel que $\frac{a^2+b^2}{1+ab}$ soit un entier k non carré, et cherchons à construire une solution plus « petite ». C'est la présence de carrés, donc d'équation du second, qui permettra de descendre les marches vers l'enfer.

Il est déjà clair que $k \neq 0$, et si de plus $a = b$, alors $k = \frac{2a^2}{1+a^2} = 2 - \frac{2}{a^2+1}$ n'est entier que pour $a = \pm 1$, auquel cas $k = 1$ qui est un carré parfait, ce qui est exclu. Par symétrie, on peut imposer $a > b$.

L'équation $k = \frac{a^2+b^2}{1+ab}$ se réécrit sous la forme d'un trinôme en a :

$$a^2 - (kb)\, a + \left(b^2 - k\right) = 0.$$

Elle admet une autre solution en a, mettons a', qui est entière car $a' = kb - a$, et qui est positive : en effet, on a clairement $k = \frac{a'^2+b^2}{1+a'b}$ par définition de a', donc $k\,(1 + ba') = a'^2 + b^2 > 0$, d'où $1 + ba' > 0$, $ba' \geq 0$ et $a' \geq 0$. Si a' était nul, on trouverait $k = \frac{a^2+0^2}{1+0} = a^2$, cas que l'on a exclu. On peut donc supposer que (a', b) est une nouvelle solution dans $\mathbf{N}^{*2}$.

Il reste à trouver la quantité qui décroît lorsque l'on passe de (a,b) à (a',b). C'est là que l'on va utiliser l'hypothèse $a > b$. Cette dernière permet en effet d'écrire

$$a' = \frac{b^2 - k}{a} < \frac{b^2 - k}{b} < b,$$

d'où $\max\{a', b\} = b < a = \max\{a, b\}$. La quantité recherchée est donc $\max\{a, b\}$.

Remarque. Cet exercice est ****difficile**** , malgré la simplicité de la solution ci-dessus (dénomée parfois "saut de Viète"). La lectrice intéresse pourra à ce sujet consulter la video https ://www.sciencealert.com/the-legend-of-question-six-one-of-the-hardest-maths-problems-ever