EXERCICES CORRIGÉS D'ARITHMÉTIQUE

BAKIR FARHI

1. Calculs et raisonnement par récurrence

Exercice 1 (encadrement et estimation de $n!$)**.**

(1) Montrer que pour tout $n \in \mathbb{N}^*$, on a :

$$2 \;\leq\; \left(1+\frac{1}{n}\right)^n \;\leq\; e. \tag{1}$$

(2) En déduire que pour tout $n \in \mathbb{N}^*$, on a les deux encadrements suivants pour le nombre $n!$:

$$e\left(\frac{n}{e}\right)^n \;\leq\; n! \;\leq\; 2\left(\frac{n}{2}\right)^n,$$

$$\left(\frac{n+1}{e}\right)^n \;\leq\; n! \;\leq\; \left(\frac{n+1}{2}\right)^n.$$

☞ Prendre les produits, depuis $n=1$ jusqu'à un certain entier $N \geq 1$, de chacun des membres de la double inégalité (1).

(3) En déduire l'estimation asymptotique :

$$\log(n!) \;=\; n\log n + \mathcal{O}(n),$$

où $\mathcal{O}$ est la notation « grand O » de Landau.

Exercice 2 (voir aussi l'exercice 25)**.** La suite harmonique $(H_n)_{n\geq 1}$ est définie par :

$$H_n \;:=\; \frac{1}{1}+\frac{1}{2}+\cdots+\frac{1}{n} \qquad (\forall n \in \mathbb{N}^*).$$

— Montrer que le nombre H_n n'est entier pour aucune valeur de $n \geq 2$.

☞ Montrer que pour tout entier $n \geq 2$, le nombre H_n s'écrit sous la forme $H_n = \dfrac{2p_n+1}{2q_n}$, avec p_n et q_n sont des entiers strictement positifs.

Date: **lundi, 3 mars 2014.**

2. Sur les diviseurs et les diviseurs premiers

Exercice 3. Montrer que pour tous $a, b \in \mathbb{N}^*$, on a :

$$\mathrm{pgcd}(a,b) \;=\; a+b-ab+2\sum_{k=1}^{b-1}\left\lfloor k\frac{a}{b}\right\rfloor,$$

où $\lfloor\cdot\rfloor$ est le symbole de la partie entière.

Exercice 4. Montrer que pour tous $a, b \in \mathbb{N}^*$, on a :

$$\mathrm{pgcd}(a,b) \;=\; \frac{1}{b}\sum_{n=0}^{b-1}\sum_{m=0}^{b-1} e^{2\pi i\frac{a}{b}nm}.$$

Exercice 5. Soient $n \geq 2$ un entier et $(d_i)_{1\leq i\leq k}$ la suite finie de tous les diviseurs de n, ordonnés par ordre croissant (i.e., $1 = d_1 < d_2 < \cdots < d_k = n$). Montrer que l'on a :

$$d_1d_2 + d_2d_3 + \cdots + d_{k-1}d_k \;\leq\; n^2 - n.$$

Exercice 6 (D'après E. Hlawka)**.** Montrer que le produit :

$$\prod_{\substack{p \text{ premier}\\ p\,|\,n\\ p>\log n}}\left(1-\frac{1}{p}\right) \qquad (n \in \mathbb{N}, n \geq 2)$$

tend vers 1 lorsque n tend vers $+\infty$.

3. Congruences

Exercice 7. Soit n un nombre naturel composé, différent de 4.
— Montrer qu'il existe un polynôme unitaire de second degré, à coefficients entiers, qui possède aux moins 3 racines modulo n.

Exercice 8.

(1) Soient p un nombre premier et n un entier positif. Montrer que :

$$1^n + 2^n + \cdots + (p-1)^n \;\equiv\; \begin{cases} -1[p] & \text{si } (p-1)\mid n \\ 0[p] & \text{sinon} \end{cases}.$$

☞ Pour démontrer la congruence du second cas, considérer un élément primitif modulo p.

(2) Soient n et m deux entiers naturels tels que $m \geq 3$. On suppose que l'on a :

$$1^n + 2^n + \cdots + (m-1)^n \;=\; m^n.$$

— Montrer que $(m-1)$ est nécessairement sans facteur carré et que le nombre rationnel

$$\sum_{\substack{p \text{ premier}\\ p|(m-1)}}\frac{1}{p}+\frac{1}{m-1}$$

est, en fait, entier.

4. Application sur le théorème des restes chinois

Exercice 9. On appelle « puissance parfaite » tout nombre naturel pouvant s'écrire sous la forme a^b avec a et b des entiers ≥ 2.

— Montrer que pour tout $N \in \mathbb{N}^*$, il existe N nombres naturels consécutifs tel qu'aucun ne soit une puissance parfaite.

☞ Commencer par montrer que si un nombre naturel n vérifie une congruence du type $n \equiv p \pmod{p^2}$ (où p est un nombre premier) alors n n'est pas une puissance parfaite. Ensuite, utiliser le théorème des restes chinois.

5. Equations diophantiennes

5.1. Equations diophantiennes linéaires.

Exercice 10. Un individu multiplie le jour de son anniversaire par 4 et le mois de son anniversaire par 17 et en additionnant les deux résultats, il trouve 124.

— Déterminer la date d'anniversaire de cet individu.

L'exercice qui suit est inspiré du livre du mathématicien arabe Abu Kamil [a], qui s'intitule "le livre des volatiles" (كِتَابُ الطَّير).

a. Abu Kamil (أَبُو كَامِل شُجَاعُ بنُ أَسلَم) : Mathématicien arabe du 9ème siècle. Il est né en Egypte vers 850 et mort vers 930. On lui doit en particulier l'algébrisation de l'arithmétique.

Exercice 11 (d'après Abu Kamil)**.** On veut acheter pour cent dirhams cent volatiles de trois espèces différentes : canards, poulets et pigeons. Sachant qu'un canard vaut six dirhams, deux poulets valent un dirham et cinq pigeons valent un dirham, combien achète-t-on de chaque espèce avec la somme donnée ? (en dépensant entièrement cette somme).

Exercice 12.

(1) Montrer que tout intervalle ouvert $]\alpha, \beta[$ de $\mathbb{R}$ (avec $\alpha, \beta \in \mathbb{R}$, $\alpha < \beta$), qui est de longueur > 1, contient au moins un entier.

(2) En déduire que pour tous $a, b, c \in \mathbb{N}^*$, avec $\text{pgcd}(a, b) = 1$ et $c \geq (a-1)(b-1)$, l'équation diophantienne :

$$a\,x + b\,y \;=\; c$$

possède au moins une solution dans $\mathbb{N}^2$.

5.2. Résolution par des méthodes élémentaires.

Exercice 13. Montrer que le nombre 7 ne peut pas s'écrire comme une somme de trois nombres rationnels.

Exercice 14 (du à l'auteur)**.** Montrer que les seules solutions à coordonnées entières de l'équation diophantienne :

$$x^3 - y^3 \;=\; 2xy$$

sont les couples $(0, 0)$ et $(-1, 1)$.

Exercice 15. Résoudre dans $\mathbb{Z}^2$ l'équation diophantienne :

$$y^2 \;=\; x^3 + 16.$$

Exercice 16. Montrer que pour tout $n \in \mathbb{N}^*$, l'équation :

$$x + \frac{1}{x} + y + \frac{1}{y} \ = \ 3n \tag{2}$$

n'a pas de solution $(x, y) \in \mathbb{Q}_+^{*2}$.

Exercice 17 (En liaison avec le théorème de Fermat-Wiles)**.**

(1) Montrer que l'équation :

$$xy(x+y) \ = \ 1$$

n'a pas de solution dans $\mathbb{Q}^2$.

(2) Plus généralement, soient $\alpha, \beta, \gamma \in \mathbb{N}^*$ tels que $\text{pgcd}(\alpha, \beta+\gamma) = \text{pgcd}(\beta, \alpha+\gamma) = \text{pgcd}(\gamma, \alpha+\beta) = 1$. Montrer que l'équation :

$$x^\alpha y^\beta (x+y)^\gamma \ = \ 1$$

n'a pas de solution dans $\mathbb{Q}^2$.

5.3. **Résolution par la méthode de la descente infinie.**

Dans l'exercice suivant, on montre qu'une certaine équation diophantienne ne possède pas de solution à coordonnées entières, et ceci en utilisant la méthode de la descente infinie.

Exercice 18. Soit n un entier strictement positif qui n'est pas un carré parfait.

— Montrer que l'équation diophantienne :

$$x^2 + y^2 \ = \ n(xy+1)$$

n'a pas de solution à coordonnées entières.

L'objectif de l'exercice qui suit est de montrer qu'il existe une infinité d'entiers naturels qu'on peut écrire comme une différence de deux cubes parfaits mais qu'on ne peut pas écrire comme somme de deux cubes parfaits.

Exercice 19.

(1) En utilisant la méthode de la descente infinie, montrer que l'équation :

$$x^3 + y^3 \ = \ 7 \cdot 8^n$$

n'a pas de solution $(x, y, n) \in \mathbb{N}^3$.

(2) En déduire qu'il existe une infinité d'entiers naturels qui peuvent s'écrire comme une différence de deux cubes parfaits mais qui ne peuvent pas s'écrire comme une somme de deux cubes parfaits.

Dans les exercices suivants, on montre qu'une certaine équation diophantienne possède une infinité de solutions entières et ceci en montrant qu'en partant d'une solution, on peut en trouver une autre qui soit de hauteur strictement plus grande. C'est cette idée même qui est utilisée dans la résolution de la célèbre équation de Markov : $x^2 + y^2 + z^2 = 3xyz$.

Exercice 20. Montrer que l'équation diophantienne

$$x^2 - 3xy + y^2 \;=\; 1 \tag{3}$$

possède une infinité de solutions dans $\mathbb{N}^{*2}$.

— Déterminer 5 de ces solutions.

Exercice 21. Montrer que l'équation diophantienne :

$$x^2 + y^2 + z^2 + t^2 \;=\; xyzt + 6 \tag{4}$$

possède une infinité de solutions dans $\mathbb{N}^{*4}$.

☞ Remarquer que le quadruplet $(1, 1, 2, 2)$ est une solution particulière de l'équation en question.

5.4. **Liens avec les résidus quadratiques.**

Les exercices qui suivent utilisent le théorème selon lequel « le nombre (-1) est un résidu quadratique modulo un nombre premier impair p si et seulement si p est de la forme $(4k+1)$ $(k \in \mathbb{N})$ ».

Exercice 22 (d'après Euler)**.** Montrer que l'équation diophantienne :

$$4xy - x - y \;=\; z^2$$

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

Exercice 23 (d'après V.A. Lebesgue)**.** Montrer que l'équation diophantienne :

$$y^2 \;=\; x^3 + 7$$

n'a pas de solution dans $\mathbb{Z}^2$.

L'exercice suivant utilise la loi de la réciprocité quadratique pour montrer qu'une certaine équation diophantienne n'a pas de solution à coordonnées entières.

Exercice 24.

(1) Montrer qu'étant donné $n \in \mathbb{Z}$, tout diviseur premier $p > 3$ du nombre $(n^2 + 3)$ est de la forme $(3k + 1)$ $(k \in \mathbb{N}^*)$.

(2) En déduire qu'étant donné $n \in \mathbb{Z}$, tout diviseur impair (positif) du nombre $(n^2 + 3)$ est congru à 0 ou à 1 modulo 3.

(3) En déduire que l'équation diophantienne :

$$(x - 1)(x^2 + 1) \;=\; y^2 + y + 1$$

n'a pas de solution à coordonnées entières.

6. Applications sur les valuations p-adiques

Exercice 25. Pour tout $n \in \mathbb{N}^*$, on note par a_n et b_n les entiers strictement positifs et premiers entre eux tels que :

$$H_n \;:=\; \frac{1}{1} + \frac{1}{2} + \cdots + \frac{1}{n} \;=\; \frac{a_n}{b_n}.$$

(1) Soit $n \in \mathbb{N}^*$. En désignant par 2^k ($k \in \mathbb{N}$) la plus grande puissance de 2 qui soit $\leq n$, montrer que le nombre b_n est un multiple de 2^k.
— En déduire que le nombre harmonique H_n n'est entier pour aucune valeur de $n \geq 2$.

(2) Montrer que pour tout $n \in \mathbb{N}^*$, le nombre b_n est multiple de tous les nombres premiers de l'intervalle $]\frac{n}{2}, n]$.

Exercice 26. Soient x, y et z trois entiers non nuls tels que :

$$\frac{x}{y} + \frac{y}{z} + \frac{z}{x} \in \mathbb{Z}.$$

— Montrer que le produit xyz est un cube parfait.

7. Sur les résidus quadratiques

Exercice 27. Soit p un nombre premier de la forme : $p = 8k + 5$ (avec $k \in \mathbb{N}$).
— Montrer que le nombre $N := (p-3)! + 1$ ne peut être un carré parfait.

8. Sur le ppcm

Exercice 28.

(1) Montrer que pour tout entier strictement positif n, on a :

$$\text{Card}\left\{(a,b) \in \mathbb{N}^{*2} : \text{ ppcm}(a,b) = n\right\} = \tau(n^2),$$

où τ désigne la fonction arithmétique qui compte le nombre de diviseurs d'un entier strictement positif donné.
☞ Considérer la décomposition de n en produit de facteurs premiers.

(2) En déduire l'identité :

$$\sum_{d|n} 2^{\omega(d)} = \tau(n^2) \qquad (\forall n \in \mathbb{N}^*),$$

où ω désigne la fonction arithmétique qui compte le nombre de facteurs premiers d'un entier strictement positif donné.
☞ Calculer autrement le cardinal en question en introduisant le p.g.c.d de a et b (pour tout couple $(a,b) \in \mathbb{N}^{*2}$ tel que $\text{ppcm}(a,b) = n$).

La résolution de cet exercice nécessite l'utilisation du résultat de la théorie analytique des nombres, selon lequel « la série numérique $\sum_{p \text{ premier}} \frac{1}{p \log p}$ converge ».

Exercice 29 (du à l'auteur)**.** Soit $(u_n)_{n\geq 1}$ une suite strictement croissante d'entiers strictement positifs tel que la série $\sum_{n=2}^{\infty} \frac{1}{u_n \log u_n}$ diverge.

(1) Montrer qu'il existe une infinité d'entier $n \geq 2$, satisfaisant :

$$\text{ppcm}(u_1, u_2, \ldots, u_n) = \text{ppcm}(u_1, u_2, \ldots, u_{n-1}).$$

(2) En déduire que pour toute suite arithmétique strictement croissante d'entiers strictement positifs $(a_n)_{n\geq 1}$, il existe une infinité d'entiers $n \geq 2$, satisfaisant :

$$\text{ppcm}(a_1, a_2, \ldots, a_n) \;=\; \text{ppcm}(a_1, a_2, \ldots, a_{n-1}).$$

Les solutions

Solution de l'exercice 1.

(1) Soit $n \in \mathbb{N}^*$. On a d'après la formule du binôme :

$$\begin{aligned}\left(1+\frac{1}{n}\right)^n &= 1+\binom{n}{1}\frac{1}{n}+\binom{n}{2}\frac{1}{n^2}+\cdots+\binom{n}{k}\frac{1}{n^k}+\cdots+\binom{n}{n}\frac{1}{n^n}\\ &= 1+n\cdot\frac{1}{n}+\frac{n(n-1)}{2!}\frac{1}{n^2}+\cdots+\frac{n(n-1)\cdots(n-k+1)}{k!}\frac{1}{n^k}+\cdots+\frac{n!}{n!}\frac{1}{n^n}.\end{aligned}$$

Ce qui montre d'une part que :

$$\left(1+\frac{1}{n}\right)^n \geq 1+n\cdot\frac{1}{n}=2$$

et d'autre part (en majorant trivialement $n(n-1)\cdots(n-k+1)$ par n^k pour $k=0,1,\ldots,n$) que :

$$\begin{aligned}\left(1+\frac{1}{n}\right)^n &\leq 1+\frac{1}{1!}+\frac{1}{2!}+\cdots+\frac{1}{n!}\\ &\leq \sum_{\ell=0}^{+\infty}\frac{1}{\ell!}=e.\end{aligned}$$

La double inégalité (1) est ainsi démontrée.

(2) Soit $n \in \mathbb{N}^*$. En prenant les produits depuis $k=1$ jusqu'à $(n-1)$ dans chacun des membres de la double inégalité $2 \leq \left(1+\frac{1}{k}\right)^k \leq e$ (démontrée à la question précédente), on obtient :

$$2^{n-1} \leq \prod_{k=1}^{n-1}\left(1+\frac{1}{k}\right)^k \leq e^{n-1}. \tag{5}$$

Maintenant, on a :

$$\prod_{k=1}^{n-1}\left(1+\frac{1}{k}\right)^k = \prod_{k=1}^{n-1}\frac{(k+1)^k}{k^k} = \prod_{k=1}^{n-1}\frac{(k+1)^{k+1}}{k^k}\cdot\prod_{k=1}^{n-1}\frac{1}{k+1} = \frac{1}{n!}\prod_{k=1}^{n-1}\frac{(k+1)^{k+1}}{k^k}.$$

Le produit $\prod_{k=1}^{n-1}\frac{(k+1)^{k+1}}{k^k}$ étant télescopique, il se simplifie en $\frac{n^n}{1^1}=n^n$. D'où l'on déduit que :

$$\prod_{k=1}^{n-1}\left(1+\frac{1}{k}\right)^k = \frac{n^n}{n!}.$$

En substituant ceci dans (5), on tire (après simplification) la 1ère double inégalité requise :

$$e\left(\frac{n}{e}\right)^n \leq n! \leq 2\left(\frac{n}{2}\right)^n.$$

— Pour démontrer la seconde double inégalité demandée, il suffit d'appliquer la première pour $(n+1)$ au lieu de n, puis diviser sur $(n+1)$.

(3) Etant donné $n \in \mathbb{N}^*$, en prenant les logarithmes des membres de la 1ère double inégalité obtenue en (2), on obtient que :

$$n\log n - n + 1 \leq \log(n!) \leq n\log n - n\log 2 + \log 2.$$

D'où :

$$-n+1 \leq \log(n!) - n\log n \leq -n\log 2 + \log 2.$$

Ce qui montre que :

$$\log(n!) - n\log n = \mathcal{O}(n)$$

et conclut à l'estimation asymptotique requise. ■

Solution de l'exercice 2. Nous allons montrer par une récurrence forte que tout nombre harmonique H_n $(n \geq 2)$ s'écrit sous la forme $H_n = \frac{a_n}{b_n}$, avec $a_n, b_n \in \mathbb{N}^*$, a_n est impair et b_n est pair.

• Pour $n = 2$, on a $H_2 = 1 + \frac{1}{2} = \frac{3}{2}$, qui est bien de la forme requise.

• Pour $n = 3$, on a $H_3 = H_2 + \frac{1}{3} = \frac{3}{2} + \frac{1}{3} = \frac{11}{6}$, qui est aussi de la forme requise.

• Soit $n \geq 4$ un entier. Supposons que pour tout entier m tel que $2 \leq m < n$, le nombre H_m s'écrit sous la forme $\frac{a_m}{b_m}$, avec $a_m, b_m \in \mathbb{N}^*$, a_m est impair et b_m est pair et montrons que H_n s'écrit également sous la même forme. Pour ce faire, considérons $k, \ell \in \mathbb{N}^*$ tels que $2k$ soit le plus grand entier pair $\leq n$ et $(2\ell + 1)$ soit le plus grand entier impair $\leq n$. Comme $n \geq 4$, on a $2k \geq 4$, i.e., $k \geq 2$. De plus, par définition même de k, on a : $2k \leq n$, d'où $k \leq \frac{n}{2} < n$. L'hypothèse de récurrence peut s'appliquer alors pour l'entier k. Maintenant, on a :

$$\begin{aligned} H_n &= \frac{1}{1} + \frac{1}{2} + \cdots + \frac{1}{n} \\ &= \left(\frac{1}{2} + \frac{1}{4} + \cdots + \frac{1}{2k}\right) + \left(\frac{1}{1} + \frac{1}{3} + \cdots + \frac{1}{2\ell+1}\right) \\ &= \frac{1}{2}\left(\frac{1}{1} + \frac{1}{2} + \cdots + \frac{1}{k}\right) + \left(\frac{1}{1} + \frac{1}{3} + \cdots + \frac{1}{2\ell+1}\right) \\ &= \frac{1}{2}H_k + \left(\frac{1}{1} + \frac{1}{3} + \cdots + \frac{1}{2\ell+1}\right). \end{aligned}$$

D'une part, comme $2 \leq k < n$ alors il existe (d'après l'hypothèse de récurrence) $a_k, b_k \in \mathbb{N}^*$, avec a_k est impair et b_k est pair, tels que $H_k = \frac{a_k}{b_k}$. D'autre part, le nombre rationnel $\left(\frac{1}{1} + \frac{1}{3} + \cdots + \frac{1}{2\ell+1}\right)$ est une somme de fractions rationnelles qui sont toutes de dénominateur impair ; ce nombre peut se représenter donc par une fraction rationnelle de dénominateur impair ; autrement dit, il existe $c_k, d_k \in \mathbb{N}^*$, avec d_k est impair, tels que : $\frac{1}{1} + \frac{1}{3} + \cdots + \frac{1}{2\ell+1} = \frac{c_k}{d_k}$. Il en résulte donc que :

$$H_n = \frac{1}{2}\frac{a_k}{b_k} + \frac{c_k}{d_k} = \frac{a_k d_k + 2c_k b_k}{2b_k d_k},$$

qui est bien de la forme requise, puisque a_k et d_k sont tous les deux impairs. Ce qui achève cette récurrence et confirme le fait énoncé.

Maintenant, comme un entier naturel impair ne peut être un multiple d'un entier naturel pair, aucun nombre harmonique H_n $(n \geq 2)$ ne peut être un entier, étant donné qu'il est le quotient d'un entier naturel impair sur un entier naturel pair. CQFD. ■

Solution de l'exercice 3. L'idée de preuve de la formule proposée est basée sur le lemme (facile) suivant :

LEMME. *Pour tout $x \in \mathbb{R}$ et tout $n \in \mathbb{Z}$, on a :*

$$\lfloor x \rfloor + \lfloor n - x \rfloor = \begin{cases} n & \text{si } x \in \mathbb{Z} \\ n-1 & \text{si } x \notin \mathbb{Z} \end{cases} = n - 1 + \mathbb{1}_{\mathbb{Z}}(x).$$

Soient $a, b \in \mathbb{N}^*$. On a par symétrie :

$$\sum_{k=1}^{b-1} \left\lfloor k\frac{a}{b} \right\rfloor \;=\; \sum_{k=1}^{b-1} \left\lfloor (b-k)\frac{a}{b} \right\rfloor .$$

D'où :

$$2\sum_{k=1}^{b-1} \left\lfloor k\frac{a}{b} \right\rfloor \;=\; \sum_{k=1}^{b-1} \left\lfloor k\frac{a}{b} \right\rfloor + \sum_{k=1}^{b-1} \left\lfloor (b-k)\frac{a}{b} \right\rfloor \;=\; \sum_{k=1}^{b-1} \left(\left\lfloor k\frac{a}{b} \right\rfloor + \left\lfloor a - k\frac{a}{b} \right\rfloor \right).$$

En se servant du lemme précédent, il vient que :

$$\begin{aligned} 2\sum_{k=1}^{b-1} \left\lfloor k\frac{a}{b} \right\rfloor &= \sum_{k=1}^{b-1} \left(a - 1 + \mathbb{1}_{\mathbb{Z}}\left(k\frac{a}{b}\right) \right) \\ &= (a-1)(b-1) + \sum_{k=1}^{b-1} \mathbb{1}_{\mathbb{Z}}\left(k\frac{a}{b}\right) \\ &= ab - a - b + 1 + \sum_{k=1}^{b-1} \mathbb{1}_{\mathbb{Z}}\left(k\frac{a}{b}\right). \end{aligned} \tag{6}$$

En posant maintenant $d := \mathrm{pgcd}(a,b)$, les deux entiers strictement positifs a et b s'écrivent $a = da'$ et $b = db'$, avec $a', b' \in \mathbb{N}^*$ et $\mathrm{pgcd}(a', b') = 1$. D'après le lemme de Gauss, pour tout $k \in \mathbb{N}$, le nombre rationnel $k\frac{a}{b} = k\frac{a'}{b'}$ est entier si et seulement si k est multiple de b'. D'où :

$$\begin{aligned} \sum_{k=1}^{b-1} \mathbb{1}_{\mathbb{Z}}\left(k\frac{a}{b}\right) &= \mathrm{Card}\left\{k \in [1, b[\cap\mathbb{N} :\ k \text{ est multiple de } b'\right\} \\ &= \mathrm{Card}\{b', 2b', \ldots, (d-1)b'\} \;=\; d-1. \end{aligned}$$

En substituant ceci dans (6), il vient que :

$$2\sum_{k=1}^{b-1} \left\lfloor k\frac{a}{b} \right\rfloor \;=\; ab - a - b + 1 + (d-1) \;=\; ab - a - b + d.$$

D'où l'on tire :

$$d \;=\; a + b - ab + 2\sum_{k=1}^{b-1} \left\lfloor k\frac{a}{b} \right\rfloor . \quad \text{CQFD.} \qquad \blacksquare$$

Solution de l'exercice 4. Soient $a, b \in \mathbb{N}^*$ et $d := \mathrm{pgcd}(a,b)$. On peut donc écrire $a = da'$ et $b = db'$, avec $a', b' \in \mathbb{N}^*$ et $\mathrm{pgcd}(a', b') = 1$. Etant donné $n \in \mathbb{Z}$, la suite de terme général $e^{2\pi i \frac{a}{b} nm}$ $(m \in \mathbb{N})$ est géométrique de raison $q = e^{2\pi i \frac{a}{b} n} = e^{2\pi i \frac{a'}{b'} n}$ et on a :

$$q = 1 \iff \frac{a'}{b'} n \in \mathbb{Z} \iff b' \mid a'n \iff b' \mid n$$

(en vertu du lemme de Gauss, puisque $\mathrm{pgcd}(a', b') = 1$). Il s'ensuit (d'après la formule sommatoire de termes consécutifs d'une suite géométrique de raison différente de 1) que l'on a pour tout $n \in \mathbb{Z}$:

$$\sum_{m=0}^{b-1} e^{2\pi i \frac{a}{b} nm} \;=\; \begin{cases} \displaystyle\sum_{m=0}^{b-1} 1 \;=\; b & \text{si } n \equiv 0[b'] \\[2ex] \dfrac{e^{2\pi i \frac{a}{b} nb} - 1}{e^{2\pi i \frac{a}{b} n} - 1} \;=\; 0 & \text{si } n \not\equiv 0[b'] \end{cases}.$$

D'où :

$$\sum_{n=0}^{b-1}\sum_{m=0}^{b-1} e^{2\pi i\frac{a}{b}nm} \;=\; \sum_{\substack{0\leq n\leq b-1\\ n\equiv 0[b']}} b.$$

Comme l'intervalle $[0, b-1] = [0, db'-1]$ contient exactement d multiples de b', il en découle que :

$$\sum_{n=0}^{b-1}\sum_{m=0}^{b-1} e^{2\pi i\frac{a}{b}nm} \;=\; bd;$$

ce qui donne :

$$d \;:=\; \frac{1}{b}\sum_{n=0}^{b-1}\sum_{m=0}^{b-1} e^{2\pi i\frac{a}{b}nm},$$

comme il fallait le prouver. ■

Solution de l'exercice 5. En posant $\mathscr{D} := \{d_1, d_2, \ldots, d_k\}$ l'ensemble des diviseurs de n, l'application $d \mapsto \frac{n}{d}$ de $\mathscr{D}$ dans $\mathscr{D}$ est clairement bijective et strictement décroissante. Ceci fait que l'image d'un diviseur d_i de n est le diviseur d_{k+1-i} de n et on a par conséquent $d_i d_{k+1-i} = n$ pour tout $i = 1, \ldots, n$. En se servant de cette importante propriété (d'ailleurs souvent exploitée pour traiter des problèmes sur les diviseurs d'un entier strictement positif), on a :

$$\begin{aligned}
\sum_{i=1}^{k-1} d_i d_{i+1} &= \sum_{i=1}^{k-1}\left(\frac{n}{d_{k+1-i}}\cdot\frac{n}{d_{k-i}}\right)\\
&= n^2\sum_{i=1}^{k-1}\frac{1}{d_{k-i}d_{k+1-i}}\\
&= n^2\sum_{j=1}^{k-1}\frac{1}{d_j d_{j+1}} \qquad \text{(en posant } j = k-i\text{)}\\
&\leq n^2\underbrace{\sum_{j=1}^{k-1}\left(\frac{1}{d_j}-\frac{1}{d_{j+1}}\right)}_{\text{somme télescopique}} \qquad \text{(car } d_{j+1}-d_j \geq 1\text{)}\\
&= n^2\left(\frac{1}{d_1}-\frac{1}{d_k}\right)\\
&= n^2\left(1-\frac{1}{n}\right)\\
&= n^2-n,
\end{aligned}$$

comme il fallait le prouver.

Remarque : Si l'on suppose de plus que l'entier positif n est impair, on peut montrer par la même méthode la majoration plus raffinée $\sum_{i=1}^{k-1} d_i d_{i+1} \leq \frac{n^2-n}{2}$. Remarquons enfin que cette dernière majoration caractérise même la propriété « n est impair ». En effet, pour n pair, on a $d_{k-1} = \frac{n}{2}$ et $d_k = n$; d'où $\sum_{i=1}^{k-1} d_i d_{i+1} \geq d_{k-1}d_k = \frac{n^2}{2} > \frac{n^2-n}{2}$. ■

Solution de l'exercice 6. Pour tout entier $n \geq 2$, posons :

$$f(n) \;:=\; \prod_{\substack{p \text{ premier}\\ p\,|\,n\\ p>\log n}}\left(1-\frac{1}{p}\right).$$

Il est immédiat que l'on a pour tout entier $n \geq 2$:

$$0 \ \leq \ f(n) \ \leq \ 1.$$

Pour démontrer le résultat requis, nous allons minorer $f(n)$ $(n \geq 3)$ par une fonction simple (en n) qui tend vers 1 lorsque n tend vers l'infini. Etant donné $n \geq 3$ un entier, désignons par $q_1, q_2, \ldots, q_k$ $(k \in \mathbb{N})$ les facteurs premiers (deux à deux distincts) de n qui sont $> \log n$. Comme n est multiple de chacun des nombres premiers $q_1, \ldots, q_k$, alors il est multiple du produit $q_1 q_2 \cdots q_k$. On a donc $q_1 q_2 \cdots q_k \leq n$. Mais d'autre part, puisque $q_i > \log n$ $(\forall i = 1, \ldots, k)$, on a : $q_1 q_2 \ldots q_k > (\log n)^k$. Il s'ensuit par comparaison que $(\log n)^k \leq n$. D'où :

$$k \ \leq \ \frac{\log n}{\log \log n}. \tag{7}$$

Maintenant, on a par définition :

$$\begin{aligned} f(n) \ &= \ \left(1 - \frac{1}{q_1}\right)\left(1 - \frac{1}{q_2}\right) \cdots \left(1 - \frac{1}{q_k}\right) \\ &> \ \left(1 - \frac{1}{\log n}\right)^k \qquad \text{(car } q_i > \log n \text{ pour tout } i = 1, \ldots, k\text{)} \\ &> \ \left(1 - \frac{1}{\log n}\right)^{\frac{\log n}{\log \log n}} \qquad \text{(en vertu de (7))}. \end{aligned}$$

On a donc pour tout entier $n \geq 3$:

$$\left(1 - \frac{1}{\log n}\right)^{\frac{\log n}{\log \log n}} \ < \ f(n) \ \leq \ 1.$$

Il ne reste qu'à montrer que $\lim_{n \to +\infty} \left(1 - \frac{1}{\log n}\right)^{\frac{\log n}{\log \log n}} = 1$ pour conclure (via le théorème des gendarmes) que $\lim_{n \to +\infty} f(n) = 1$. On a :

$$\log \left\{ \left(1 - \frac{1}{\log n}\right)^{\frac{\log n}{\log \log n}} \right\} \ = \ \frac{\log n}{\log \log n} \log \left(1 - \frac{1}{\log n}\right) \ = \ -\frac{1}{\log \log n} \cdot \frac{\log\left(1 - \frac{1}{\log n}\right)}{-\frac{1}{\log n}}$$

$$\underset{n \to +\infty}{\longrightarrow} 0$$

(car $\lim_{n \to +\infty} (-\frac{1}{\log \log n}) = 0$ et $\lim_{n \to +\infty} \frac{\log\left(1 - \frac{1}{\log n}\right)}{-\frac{1}{\log n}} = \lim_{x \to 0} \frac{\log(1+x)}{x} = 1$). D'où :

$$\lim_{n \to +\infty} \left(1 - \frac{1}{\log n}\right)^{\frac{\log n}{\log \log n}} \ = \ e^0 \ = \ 1.$$

Ce qui complète la preuve du résultat requis.

Remarque : On montre de la même façon que le produit :

$$\prod_{\substack{p \text{ premier} \\ p \,|\, n \\ p > \log n}} \left(1 + \frac{1}{p}\right) \qquad (n \in \mathbb{N}, n \geq 2)$$

tend vers 1 lorsque n tend vers $+\infty$. ■

Solution de l'exercice 7. On distingue les trois cas suivants :

1er cas : (Si n possède plus d'un facteur premier). Dans ce cas, on peut écrire : $n = ab$, avec $a, b \in \{2, 3, \ldots, n-1\}$. On considère alors le polynôme :

$$P(X) \ = \ (X - a)(X - b) \ = \ X^2 - (a + b)X + ab.$$

Il est bien clair que P est unitaire, de second degré et à coefficients dans $\mathbb{Z}$. De plus, on a :

$$\begin{aligned} P(a) &= 0 \equiv 0[n] \\ P(b) &= 0 \equiv 0[n] \\ P(0) &= ab = n \equiv 0[n]. \end{aligned}$$

Ainsi P possède aux moins 3 racines modulo n (à savoir $0, a$ et b).

2ème cas : (si n est une puissance d'un nombre premier impair). Disons $n = p^k$, avec p premier impair et k un entier ≥ 2. Considérons le polynôme :

$$P(X) = X(X - p^{k-1}).$$

Il est clair que P est unitaire, de second degré et à coefficients entiers. De plus, on a :

$$\begin{aligned} P(0) &= 0 \equiv 0[n] \\ P(p^{k-1}) &= 0 \equiv 0[n] \\ P(2p^{k-1}) &= 2p^{2k-2} = (2p^{k-2})n \equiv 0[n]. \end{aligned}$$

Ainsi P possède aux moins 3 racines modulo n (à savoir $0, p^{k-1}$ et $2p^{k-1}$).

3ème cas : (si n est une puissance de 2). Dans ce cas, n s'écrit : $n = 2^k$, avec $k \geq 3$ (puisque n est composé et différent de 4). Considérons le polynôme :

$$P(X) = X(X - 2^{k-2}).$$

Visiblement, P est unitaire, de second degré et à coefficients entiers. On a en outre :

$$\begin{aligned} P(0) &= 0 \equiv 0[n] \\ P(2^{k-2}) &= 0 \equiv 0[n] \\ P(2^{k-1}) &= 2^{k-1} \cdot 2^{k-2} = 2^{2k-3} = 2^{k-3} \cdot n \equiv 0[n]. \end{aligned}$$

Ce qui montre que P possède aux moins 3 racines modulo n (à savoir $0, 2^{k-2}$ et 2^{k-1}).
Pour tous les cas, il existe bien un polynôme unitaire de second degré, à coefficients entiers, qui possède aux moins 3 racines modulo n. CQFD. ■

Solution de l'exercice 8.

1)

1er cas : (si $(p-1) \mid n$).
Dans ce cas, on peut écrire $n = k(p-1)$ (pour un certain $k \in \mathbb{N}$). D'après le petit théorème de Fermat, on a pour tout $a \in \{1, 2, \ldots, p-1\}$: $a^{p-1} \equiv 1[p]$; ce qui fait que $(a^{p-1})^k \equiv 1^k[p] \equiv 1[p]$; c'est-à-dire $a^n \equiv 1[p]$. On a par conséquent :

$$1^n + 2^n + \cdots + (p-1)^n \equiv \underbrace{1 + 1 + \cdots + 1}_{(p-1) \text{ fois}}[p] \equiv p - 1[p] \equiv -1[p],$$

comme il fallait le prouver.

2nd cas : (si $(p-1) \nmid n$).
Pour ce cas, considérons $\xi \in \{1, 2, \ldots, p-1\}$ un élément primitif modulo p (c'est-à-dire tel que $\mathrm{Ord}_p(\xi) = p - 1$). Le fait que $\mathrm{Ord}_p(\xi) = (p-1) \nmid n$ entraîne que $\xi^n \not\equiv 1[p]$; soit $\xi^n - 1 \not\equiv 0[p]$. Par ailleurs, comme $\xi \wedge p = 1$, l'application $x \mapsto \xi x$ transforme tout système résiduel complet modulo p en un système résiduel complet modulo p. En appliquant cela au système résiduel complet $\{1, 2, \ldots, p-1\}$ modulo p, on obtient que

l'ensemble $\{\xi, 2\xi, \ldots, (p-1)\xi\}$ constitue un système résiduel complet modulo p. Par conséquent, on a :

$$\xi^n + (2\xi)^n + \cdots + ((p-1)\xi)^n \ \equiv\ 1^n + 2^n + \cdots + (p-1)^n [p].$$

Ce qui donne :

$$(\xi^n - 1)\,(1^n + 2^n + \cdots + (p-1)^n) \ \equiv\ 0[p].$$

Mais puisque $\xi^n - 1 \not\equiv 0[p]$ (d'après ce qui précède), on en conclut que :

$$1^n + 2^n + \cdots + (p-1)^n \ \equiv\ 0[p],$$

comme il fallait le prouver.

2) Montrer que $(m-1)$ est sans facteur carré revient à montrer que pour tout facteur premier p de $(m-1)$, on a $\vartheta_p(m-1) = 1$. Soit donc p un nombre premier tel que $p \mid (m-1)$ et montrons que $\vartheta_p(m-1) = 1$. Le fait $p \mid (m-1)$ permet d'écrire $m - 1 = kp$ (pour un certain $k \in \mathbb{N}^*$). On a alors d'une part :

$$\begin{aligned} 1^n + 2^n + \cdots + (m-1)^n &= 1^n + 2^n + \cdots + (kp)^n \\ &= \sum_{\ell=0}^{k-1} \sum_{r=1}^{p} (\ell p + r)^n \\ &\equiv \sum_{\ell=0}^{k-1} (1^n + 2^n + \cdots + (p-1)^n)\,[p] \\ &\equiv k\,(1^n + 2^n + \cdots + (p-1)^n)\,[p]. \end{aligned}$$

Et d'autre part :

$$\begin{aligned} 1^n + 2^n + \cdots + (m-1)^n \ =\ m^n \ &\equiv\ 1^m[p] \qquad\qquad (\text{puisque } m \equiv 1[p]) \\ &\equiv\ 1[p]. \end{aligned}$$

En confrontant les deux résultats, on tire que :

$$k\,(1^n + 2^n + \cdots + (p-1)^n) \ \equiv\ 1[p]. \tag{1}$$

Cette dernière congruence assure que $1^n + 2^n + \cdots + (p-1)^n \not\equiv 0[p]$; ce qui entraîne (d'après le résultat de la première question) que $(p-1) \mid n$ et $1^n + 2^n + \cdots + (p-1)^n \equiv -1[p]$. En substituant cette dernière congruence dans (1), on tire que $-k \equiv 1[p]$; d'où $k \equiv -1[p]$; autrement dit, k s'écrit $k = pu - 1$ (pour un certain $u \in \mathbb{N}^*$). On a par conséquent :

$$m - 1 \ =\ kp \ =\ (pu-1)p. \tag{2}$$

Ce qui entraîne que $\vartheta_p(m-1) = 1$. Comme p étant un facteur premier arbitraire de $(m-1)$, on en conclut que $(m-1)$ est sans facteur carré. CQFD.

Pour montrer la seconde propriété requise par la question, on a d'après (2) pour tout facteur premier p de $(m-1)$:

$$\frac{m-1}{p} + 1 \ \equiv\ 0[p].$$

Cela entraîne que :

$$\prod_{\substack{p \text{ premier} \\ p \mid (m-1)}} \left(\frac{m-1}{p} + 1\right) \ \text{ est multiple de } \prod_{\substack{p \text{ premier} \\ p \mid (m-1)}} p \ =\ m - 1.$$

Mais d'autre part, dans le développement du produit $P := \prod_{\substack{p \text{ premier} \\ p|(m-1)}} \left(1 + \frac{m-1}{p}\right)$, les produits deux à deux des nombres $\frac{m-1}{p}$ (p premier, $p \mid (m-1)$) sont des multiples de $(m-1)$, il en est de même des produits trois à trois, quatre à quatre, etc. Modulo $(m-1)$, ce produit P est donc congru à :

$$1 + (m-1) \sum_{\substack{p \text{ premier} \\ p|(m-1)}} \frac{1}{p}.$$

Par conséquent, on a :

$$1 + (m-1) \sum_{\substack{p \text{ premier} \\ p|(m-1)}} \frac{1}{p} \equiv 0[m-1].$$

D'où :

$$\frac{1}{m-1} + \sum_{\substack{p \text{ premier} \\ p|(m-1)}} \frac{1}{p} \equiv 0[1];$$

Ce qui revient au même de dire que le nombre rationnel $\frac{1}{m-1} + \sum_{\substack{p \text{ premier} \\ p|(m-1)}} \frac{1}{p}$ est entier. CQFD.

Remarque : P. Erdős avait conjecturé que la seule solution $(m,n) \in \mathbb{N}^{*2}$ de l'équation $1^n + 2^n + \cdots + (m-1)^n = m^n$ est sa solution triviale $(m,n) = (3,1)$ (qui provient de $1+2=3$). À ma connaissance, cette conjecture est toujours ouverte ! ■

Solution de l'exercice 9. Montrons d'abord le lemme suivant :

Lemme. *Soient p un nombre premier et n un entier naturel vérifiant la congruence $n \equiv p \pmod{p^2}$. Alors n n'est pas une puissance parfaite.*

Preuve du lemme. Par hypothèse, n s'écrit $n = kp^2 + p = p(kp+1)$ (avec $k \in \mathbb{N}$). D'où $v_p(n) = v_p(p) + v_p(kp+1) = 1 + 0 = 1$.
Procédons maintenant par l'absurde en supposant que n est une puissance parfaite, c'est-à-dire que n s'écrit $n = a^b$, avec a, b des entiers ≥ 2. On a ainsi $v_p(n) = v_p(a^b) = bv_p(a)$. En comparant les deux résultats, on obtient $bv_p(a) = 1$, ce qui est impossible puisque $b \geq 2$. D'où n ne peut être une puissance parfaite. Le lemme est démontré.

Retour à la solution de l'exercice. Soit $N \in \mathbb{N}^*$ fixé. Désignons par $(p_i)_{i \geq 1}$ la suite (strictement croissante) des nombres premiers et considérons le système des N congruences (à l'une inconnue $n \in \mathbb{Z}$) :

$$\begin{cases} n \equiv p_1 - 1 \pmod{p_1^2} \\ n \equiv p_2 - 2 \pmod{p_2^2} \\ \vdots \\ n \equiv P_N - N \pmod{P_N^2} \end{cases} . \qquad (S)$$

Comme les nombres $p_1^2, \ldots, p_N^2$ sont deux à deux premiers entre eux (car les nombres premiers $p_1, \ldots, p_N$ sont deux à deux distincts), le système (S) possède une unique solution modulo le produit $p_1^2 p_2^2 \cdots p_N^2$ (en vertu du théorème des restes chinois). En particulier, il

existe une infinité de $n \in \mathbb{N}$, vérifiant le système (S) ; c'est-à-dire vérifiant :

$$\left\{\begin{array}{rcl} n+1 & \equiv & p_1 \pmod{p_1^2} \\ n+2 & \equiv & p_2 \pmod{p_2^2} \\ \vdots & & \\ n+N & \equiv & P_N \pmod{P_N^2} \end{array}\right. .$$

Pour tout tel n, le dernier système entraîne (en vertu du lemme ci-dessus) qu'aucun des N nombres naturels consécutifs $n+1$, $n+2$, …, $n+N$ n'est une puissance parfaite. ■

Solution de l'exercice 10. Désignons respectivement par x et y le jour et le mois d'anniversaire de l'individu en question. On a donc $x, y \in \mathbb{Z}$, $1 \leq x \leq 31$ et $1 \leq y \leq 12$. De plus, d'après les données de l'exercice, on a : $4x + 17y = 124$. Ce qui équivaut à :

$$17y = 4(31 - x). \tag{8}$$

On a par suite : 17 divise $17y = 4(31-x)$. Mais puisque 17 est premier avec 4, alors (d'après le lemme de Gauss) : 17 divise $(31-x)$; autrement dit, il existe $k \in \mathbb{Z}$ tel que l'on ait $31 - x = 17k$; soit $\boxed{x = 31 - 17k}$. En substituant ceci dans (8), il vient que $\boxed{y = 4k}$. Les contraintes $1 \leq x \leq 31$ et $1 \leq y \leq 12$ vont pouvoir finalement limiter les valeurs (entières) de k. On a :

$$\left\{\begin{array}{l} 1 \leq x \leq 31 \\ \text{et} \\ 1 \leq y \leq 12 \end{array}\right. \iff \left\{\begin{array}{l} 1 \leq 31 - 17k \leq 31 \\ \text{et} \\ 1 \leq 4k \leq 12 \end{array}\right.$$

$$\iff \left\{\begin{array}{l} 0 \leq k \leq \frac{30}{17} = 1,7\ldots \\ \text{et} \\ \frac{1}{4} \leq k \leq 3 \end{array}\right.$$

$$\iff \left\{\begin{array}{ll} k \in \{0,1\} & \\ \text{et} & (\text{car } k \in \mathbb{Z}) \\ k \in \{1,2,3\} & \end{array}\right.$$

$$\iff \boxed{k = 1}\ .$$

L'unique valeur de k fournissant une solution admissible au problème est donc $k = 1$. Ce qui donne $\boxed{(x, y) = (14, 4)}$.

La date d'anniversaire de l'individu en question est le 14 avril. ■

Solution de l'exercice 11. Désignons respectivement par x, y et z les nombres de canards, de poulets et de pigeons que l'on peut acheter avec la somme d'argent dont nous disposons (en dépensant entièrement cette somme). Le problème s'interprète algébriquement par le système des deux équations :

$$\left\{\begin{array}{rcll} x + y + z & = & 100 & \ldots (I) \\ 6x + \frac{y}{2} + \frac{z}{5} & = & 100 & \ldots (II) \end{array}\right. .$$

L'équation (I) donne $z = 100 - x - y$. En substituant ceci dans (II), on obtient (après simplification) :

$$58x + 3y = 800. \tag{III}$$

Résolvons (III) dans $\mathbb{Z}^2$. En prenant les deux membres de (III) modulo 3, on obtient $x \equiv 2 \pmod 3$; autrement dit, il existe $k \in \mathbb{Z}$ tel que $\boxed{x = 3k + 2}$. En substituant ceci dans (III), on trouve (après résolution) : $\boxed{y = 228 - 58k}$. En substituant par suite ces

expressions de x et y en fonction de k dans (I), on trouve : $\boxed{z = 55k - 130}$. La solution générale du système des équations (I) et (II) dans $\mathbb{Z}^3$ est donc donnée par :

$$(x, y, z) \;=\; (3k + 2\ ,\ 228 - 58k\ ,\ 55k - 130) \qquad (k \in \mathbb{Z}).$$

Pour déterminer les solutions admissibles du problème, on doit tenir compte de la spécificité des entiers x, y et z. Comme chacun d'entre eux représente le nombre d'un certain type de volatiles, ils sont forcément tous positifs. On a :

$$\left\{\begin{array}{l} x \geq 0 \\ y \geq 0 \\ z \geq 0 \end{array}\right. \iff \left\{\begin{array}{l} 3k + 2 \geq 0 \\ 228 - 58k \geq 0 \\ 55k - 130 \geq 0 \end{array}\right. \iff \left\{\begin{array}{l} k \geq -\frac{2}{3} = -0,6\ldots \\ k \leq \frac{228}{58} = 3,9\ldots \\ k \geq \frac{130}{55} = 2,3\ldots \end{array}\right. \iff \boxed{k = 3}$$

(puisque $k \in \mathbb{Z}$). L'unique valeur de $k \in \mathbb{Z}$ fournissant une solution admissible du problème est donc $k = 3$. Ce qui donne $(x, y, z) = (11, 54, 35)$.
On achètera alors 11 canards, 54 poulets et 35 pigeons. ■

Solution de l'exercice 12.

(1) Soit $I =]\alpha, \beta[$ (avec $\alpha, \beta \in \mathbb{R}$, $\alpha < \beta$) un intervalle ouvert de $\mathbb{R}$, de longueur strictement plus grande que 1 (i.e., $\beta - \alpha > 1$), et montrons que I contient au moins un entier. Pour ce faire, considérons n_0 le plus grand entier qui soit $\leq \alpha$ et n_1 le plus petit entier qui soit $\geq \beta$. On a alors :

$$n_1 - n_0 \;\geq\; \beta - \alpha \;>\; 1.$$

En posant $n := n_0 + 1$, on a donc :

$$n_0 \;<\; n \;<\; n_1.$$

Ceci entraîne (en vertu de la définition de n_0) que $n > \alpha$ et entraîne aussi (en vertu de la définition de n_1) que $n < \beta$. D'où $n \in]\alpha, \beta[= I$. Ainsi I contient au moins un entier (qui est n). CQFD.

(2) Soient $a, b, c \in \mathbb{N}^*$ tels que $\text{pgcd}(a, b) = 1$ et $c \geq (a - 1)(b - 1)$. Montrons que l'équation diophantienne $ax + by = c$ possède au moins une solution dans $\mathbb{N}^2$. La condition $\text{pgcd}(a, b) = 1$ assure que l'équation en question possède au moins une solution $(x_0, y_0) \in \mathbb{Z}^2$. Par suite, une application "routinière" du lemme de Gauss montre que la solution générale de ladite équation dans $\mathbb{Z}^2$ est donnée par :

$$(x, y) \;=\; (bk + x_0, -ak + y_0) \qquad (k \in \mathbb{Z}).$$

Une telle solution est dans $\mathbb{N}^2$ si et seulement si[1] : $bk + x_0 > -1$ et $-ak + y_0 > -1$; c'est-à-dire, si et seulement si :

$$k \;\in\; \left]\frac{-x_0 - 1}{b}\ ,\ \frac{y_0 + 1}{a}\right[.$$

Ainsi, l'équation $ax + by = c$ possède au moins une solution dans $\mathbb{N}^2$ si et seulement si l'intervalle ouvert $]\frac{-x_0-1}{b}, \frac{y_0+1}{a}[$ contient au moins un entier. Comme cet intervalle est de

1. Naturellement, on devrait écrire $bk + x_0 \geq 0$ et $-ak + y_0 \geq 0$ mais de cette façon, il nous sera moins facile de conclure au résultat requis par le biais du résultat de la première question.

longueur

$$\frac{y_0+1}{a}-\frac{-x_0-1}{b} = \frac{y_0+1}{a}+\frac{x_0+1}{b} = \frac{ax_0+by_0+a+b}{ab}$$
$$= \frac{c+a+b}{ab} \quad \text{(puisque } (x_0,y_0) \text{ est une solution de l'equation en question)}$$
$$\geq \frac{(a-1)(b-1)+a+b}{ab} \quad \text{(car } c\geq(a-1)(b-1) \text{ par hypothèse)}$$
$$= \frac{ab+1}{ab} > 1,$$

alors (en vertu du résultat de la première question) il contient bien des entiers. Ce qui confirme que l'équation $ax+by=c$ possède au moins une solution dans $\mathbb{N}^2$. ■

Solution de l'exercice 13. Procédons par l'absurde en supposant qu'il existe $x,y,z\in\mathbb{Q}$ tels que :

$$x^2+y^2+z^2 = 7.$$

Ecrivons x, y et z sous forme de fractions rationnelles de même dénominateur ; soit

$$x=\frac{a}{d}\ ,\ y=\frac{b}{d} \quad \text{et} \quad z=\frac{c}{d},$$

avec $a,b,c,d\in\mathbb{Z}$ et $d\neq 0$. Quitte à simplifier ces fractions $\frac{a}{d}$, $\frac{b}{d}$ et $\frac{c}{d}$ par $\text{pgcd}(a,b,c,d)$ (c'est-à-dire diviser le numérateur et le dénominateur de chacune d'elles par $\text{pgcd}(a,b,c,d)$), on peut supposer que $\text{pgcd}(a,b,c,d)=1$. L'égalité $x^2+y^2+z^2=7$ devient :

$$\left(\frac{a}{d}\right)^2+\left(\frac{b}{d}\right)^2+\left(\frac{c}{d}\right)^2 = 7.$$

Ce qui équivaut à :

$$a^2+b^2+c^2 = 7\,d^2. \tag{9}$$

Maintenant, on distingue les deux cas suivants :

1er cas : (si d est pair)

Dans ce cas, on a : $d^2\equiv 0 \pmod 4$; d'où (d'après (9)) : $a^2+b^2+c^2\equiv 0 \pmod 4$. Mais comme on a : $n^2\equiv 0$ ou $1 \pmod 4$ pour tout entier n, la congruence $a^2+b^2+c^2\equiv 0 \pmod 4$ n'est possible que si $a^2\equiv 0 \pmod 4$, $b^2\equiv 0 \pmod 4$ et $c^2\equiv 0 \pmod 4$. Ce qui entraîne que les entiers a,b et c sont les trois pairs. On obtient alors que les entiers a,b,c et d sont tous pairs ; ce qui est bien en contradiction avec la supposition $\text{pgcd}(a,b,c,d)=1$. Ce 1er cas est donc impossible.

2nd cas : (si d est impair)

Dans ce cas, on a : $d^2\equiv 1 \pmod 8$; d'où (d'après (9)) : $a^2+b^2+c^2\equiv 7 \pmod 8$. Mais d'autre part on a : $n^2\equiv 0,1$ ou $4 \pmod 8$ pour tout entier n ; d'où l'on déduit que $a^2+b^2+c^2\equiv 0,1,2,3,4,5$ ou $6 \pmod 8$ (en combinant tous les cas possibles). Ce qui contredit la première congruence $a^2+b^2+c^2\equiv 7 \pmod 8$. Ce second cas est donc également impossible.

Conclusion : Le nombre 7 ne peut pas s'écrire comme une somme de trois nombres rationnels. ■

Solution de l'exercice 14. Nous donnons deux méthodes de résolution différentes.

1ÈRE MÉTHODE : Soit $(x,y)\in\mathbb{Z}^2$ une solution de l'équation proposée. Le nombre entier

$(x^3 - y^3)$ est alors pair, ce qui entraîne que l'entier $(x^3 + y^3)$ est aussi pair (puisque $(x^3 + y^3) = (x^3 - y^3) + 2y^3$). Posons :

$$u := \frac{x^3 - y^3}{2} \quad \text{et} \quad v := \frac{x^3 + y^3}{2}.$$

Ces nombres u et v sont donc des entiers. On a par suite :

$$\begin{aligned} x^3 - y^3 = 2xy &\iff u = xy \\ &\iff u^3 = x^3y^3 \\ &\iff u^3 = (v+u)(v-u) \\ &\iff u^3 = v^2 - u^2 \\ &\iff v^2 = u^2(u+1). \end{aligned} \tag{10}$$

Cette dernière égalité montre que v^2 est un multiple de u^2, ce qui entraîne que v est un multiple de u. On peut donc écrire :

$$v \;=\; ku \qquad (\text{avec } k \in \mathbb{Z}).$$

Par suite, on a :

$$\begin{aligned} (10) &\iff k^2u^2 = u^2(u+1) \\ &\iff u^2(u+1-k^2) = 0 \\ &\iff u = 0 \;\text{ ou }\; u = k^2 - 1. \end{aligned}$$

- Pour $u = 0$, on trouve $v = 0$, ce qui donne $(x, y) = (0, 0)$.
- Pour $u = k^2 - 1$, on trouve $v = ku = k(k^2 - 1) = k^3 - k$. D'où l'on tire :

$$\left\{ \begin{array}{lllll} x^3 & = & v + u & = & k^3 + k^2 - k - 1 \qquad \ldots (I) \\ y^3 & = & v - u & = & k^3 - k^2 - k + 1 \qquad \ldots (II) \end{array} \right.$$

On constate que lorsque $|k| \geq 2$, l'équation (I) entraîne $x^3 \in]k^3, (k+1)^3[$, ce qui est évidemment impossible ; d'où $|k| \leq 1$, autrement dit $k \in \{-1, 0, 1\}$.

- Pour $k = -1$, on trouve (d'après (I) et (II)) $(x, y) = (0, 0)$.
- Pour $k = 0$, on trouve $(x, y) = (-1, 1)$.
- Pour $k = 1$, on trouve de nouveau $(x, y) = (0, 0)$.

Conclusion : Les seules solutions de l'équation proposée dans $\mathbb{Z}^2$ sont les deux couples $(0, 0)$ et $(-1, 1)$. CQFD.

2NDE MÉTHODE : Soit $(x, y) \in \mathbb{Z}^2$ une solution de l'équation proposée. Lorsque $xy = 0$, on trouve immédiatement que $\boxed{(x, y) = (0, 0)}$ (la solution triviale). Supposons pour la suite que $(x, y) \neq (0, 0)$. On a donc $xy \neq 0$, c'est-à-dire $(x, y) \in \mathbb{Z}^{*2}$. Considérons $d := \text{pgcd}(x, y)$ $(d \in \mathbb{N}^*)$ et écrivons :

$$x = dx' \quad \text{et} \quad y = dy'.$$

Les nouveaux nombres x' et y' sont bien sûr des entiers relatifs vérifiant $\text{pgcd}(x', y') = 1$. L'équation proposée se transforme (après simplification) en :

$$d\left(x'^3 - y'^3\right) \;=\; 2x'y'. \tag{11}$$

En utilisant $\text{pgcd}(x', y') = 1$, on montre assez facilement que l'on a aussi $\text{pgcd}(x'y', x'^3 - y'^3) = 1$. On a donc (d'après (11)) : $x'y'$ divise $d(x'^3 - y'^3)$ et $x'y'$ est

premier avec $(x'^3 - y'^3)$. Ceci entraîne (en vertu du lemme de Gauss) que $x'y'$ divise d. Il existe donc $k \in \mathbb{Z}^*$ tel que :

$$d \;=\; kx'y'.$$

En remplaçant ceci dans (11), on obtient (après simplification) :

$$k\left(x'^3 - y'^3\right) \;=\; 2.$$

Cette dernière entraîne que $(x'^3 - y'^3)$ divise 2 ; d'où : $(x'^3 - y'^3) \in \{-2, -1, 1, 2\}$.
• Pour $x'^3 - y'^3 = -2$: l'unique possibilité est $(x', y') = (-1, 1)$, ce qui donne en remontant $k = -1$, puis $d = 1$ et enfin $\boxed{(x, y) = (-1, 1)}$.
• Pour $x'^3 - y'^3 = -1$: c'est impossible, puisque $x', y' \in \mathbb{Z}^*$.
• Pour $x'^3 - y'^3 = 1$: c'est également impossible puisque $x', y' \in \mathbb{Z}^*$.
• Pour $x'^3 - y'^3 = 2$: l'unique possibilité est $(x', y') = (1, -1)$, ce qui donne en remontant $k = 1$, puis $d = -1$; ce qui contredit le fait que $d \in \mathbb{N}^*$. Ce cas est donc également impossible.
Conclusion : Les seules solutions dans $\mathbb{Z}^2$ de l'équation diophantienne $x^3 - y^3 = 2xy$ sont les couples $(0, 0)$ et $(-1, 1)$. CQFD.

Remarque : La seconde méthode que nous avons utilisé s'applique plus généralement pour résoudre dans $\mathbb{Z}^2$ toute équation du type $x^3 - y^3 = nxy$ (avec $n \in \mathbb{Z}^*$, fixé). ■

Solution de l'exercice 15. Soit $(x, y) \in \mathbb{Z}^2$ une éventuelle solution de l'équation proposée. On a donc $y^2 = x^3 + 16$; ce qui équivaut à :

$$(y + 4)(y - 4) \;=\; x^3. \tag{12}$$

On distingue les deux cas suivants :

1er cas : (si y est impair)

Dans ce cas, tout diviseur commun d à $(y + 4)$ et $(y - 4)$ est d'une part impair (car $y - 4$ et $y + 4$ sont impairs, vu que y est impair) et d'autre part, il divise $(y + 4) - (y - 4) = 8$. Ce qui oblige d'avoir $d = 1$ et montre que $(y + 4)$ et $(y - 4)$ sont premiers entre eux. Par conséquent, l'égalité (12) entraîne que chacun des deux entiers $(y + 4)$ et $(y - 4)$ est un cube parfait. Autrement dit, il existe $u, v \in \mathbb{Z}$ (forcément impairs) tels que :

$$y + 4 \;=\; u^3 \quad \text{et} \quad y - 4 \;=\; v^3.$$

D'où l'on déduit que :

$$u^3 - v^3 \;=\; 8.$$

Ce qui est impossible car : comme l'ensemble des cubes parfaits impairs est constitué des nombres (donnés suivant l'ordre croissant) :

$$\ldots\ ,\ -27\ ,\ -1\ ,\ 1\ ,\ 27\ ,\ \ldots$$

alors l'ensemble des différences entre deux cubes parfaits impairs est constitué des nombres (donnés suivant l'ordre croissant) :

$$\ldots\ ,\ -26\ ,\ -2\ ,\ 0\ ,\ 2\ ,\ 26\ ,\ \ldots$$

et ne contient visiblement pas le nombre 8. Ce premier cas est donc impossible.

2nd cas : (si y est pair)

Dans ce cas, on peut écrire $y = 2y'$ ($y' \in \mathbb{Z}$). L'égalité (12) se transforme alors (après simplification) en :

$$4(y'+2)(y'-2) \;=\; x^3. \tag{13}$$

Cette dernière montre que x^3 est pair ; d'où x est pair. En écrivant alors $x = 2x'$ ($x' \in \mathbb{Z}$), on transforme (13) en :

$$(y'+2)(y'-2) \;=\; 2x'^3. \tag{14}$$

Par suite, comme $(y'+2)(y'-2) = y'^2 - 4$ est de même parité que y' alors (d'après (14)) y' est pair. En écrivant alors $y' = 2y''$ ($y'' \in \mathbb{Z}$), on transforme (14) en :

$$2(y''+1)(y''-1) \;=\; x'^3. \tag{15}$$

Mais cette dernière montre que x'^3 est pair ; d'où x' est pair. En écrivant alors $x' = 2x''$ ($x'' \in \mathbb{Z}$), on transforme (15) en :

$$(y''+1)(y''-1) \;=\; 4x''^3. \tag{16}$$

Par suite, comme $(y''+1)(y''-1) = y''^2 - 1$ est de parité différente de celle de y'' alors (d'après (16)) y'' est impair. En écrivant alors $y'' = 2k+1$ ($k \in \mathbb{Z}$), on transforme (16) en :

$$k(k+1) \;=\; x''^3.$$

Mais comme les entiers k et $(k+1)$ sont premiers entre eux (car ils sont consécutifs), la dernière égalité oblige k et $(k+1)$ d'être tous les deux des cubes parfaits. Ce qui n'est possible que si $k = 0$ ou $k = -1$. En remontant, $k = 0$ donne $(x'', y'') = (0, 1)$ puis $(x, y) = (0, 4)$ et $k = -1$ donne $(x'', y'') = (0, -1)$ puis $(x, y) = (0, -4)$. Enfin, on vérifie immédiatement que les deux couples $(0, 4)$ et $(0, -4)$ sont effectivement des solutions de l'équation en question.

Conclusion : Les seules solutions (dans $\mathbb{Z}^2$) de l'équation proposée sont les couples $(0, -4)$ et $(0, 4)$.

Remarque : Une équation diophantienne du type $y^2 = x^3 + k$ (où $k \in \mathbb{Z}^*$, fixé) aux inconnus $x, y \in \mathbb{Z}$ s'appelle « équation de Mordell ». On montre qu'une équation de Mordell possède toujours un nombre fini de solutions (ce résultat est du à Thue et Mordell). Un autre exemple d'équation de Mordell est proposé dans l'exercice 23. ■

Solution de l'exercice 16. Soit $n \in \mathbb{N}^*$ fixé. Procédons par l'absurde en supposant que (2) possède des solutions dans $\mathbb{Q}_+^{*2}$ et soit (x, y) une telle solution. Ecrivons $x = \frac{a}{b}$ et $y = \frac{c}{d}$, avec $a, b, c, d \in \mathbb{N}^*$ et $\text{pgcd}(a, b) = \text{pgcd}(c, d) = 1$. En substituant $x = \frac{a}{b}$ et $y = \frac{c}{d}$ dans (2), on obtient après simplification :

$$(a^2+b^2)cd + (c^2+d^2)ab \;=\; 3nabcd. \tag{17}$$

En prenant les deux membres de (17) modulo ab, on obtient :

$$(a^2+b^2)cd \equiv 0 \pmod{ab}.$$

Mais puisque $\text{pgcd}(a^2+b^2, ab) = 1$ (car $\text{pgcd}(a, b) = 1$), il s'ensuit que :

$$cd \equiv 0 \pmod{ab}. \tag{18}$$

De même, en prenant les deux membres de (17) modulo cd, on obtient :

$$(c^2+d^2)ab \equiv 0 \pmod{cd}.$$

Mais puisque $\text{pgcd}(c^2+d^2, cd) = 1$ (car $\text{pgcd}(c,d)=1$), il s'ensuit que :

$$ab \equiv 0 \pmod{cd}. \tag{19}$$

Les deux congruences (18) et (19) montrent que les deux entiers strictement positifs ab et cd sont multiples l'un de l'autre, ce qui équivaut à dire qu'il sont égaux ; soit

$$ab \;=\; cd. \tag{20}$$

Par suite, en substituant cd par ab dans (17), on obtient après simplification :

$$a^2+b^2+c^2+d^2 \;=\; 3nab.$$

Ce qui s'écrit aussi (puisque $ab = cd$) :

$$(a+b)^2+(c-d)^2 \;=\; 3nab, \tag{21}$$

$$(a-b)^2+(c+d)^2 \;=\; 3nab. \tag{22}$$

Mais puisque une somme de deux carrés d'entiers relatifs n'est multiple de 3 que si chacun de ces deux entiers est multiple de 3, les deux équations (21) et (22) entraînent que l'on a :

$$a+b \equiv 0 \pmod 3\ ,\ c-d \equiv 0 \pmod 3\ ,\ a-b \equiv 0 \pmod 3 \ \text{ et } \ c+d \equiv 0 \pmod 3.$$

Ce qui donne :

$$a \equiv b \equiv c \equiv d \equiv 0 \pmod 3.$$

Ce qui contredit visiblement les faits $\text{pgcd}(a,b) = \text{pgcd}(c,d) = 1$. Cette contradiction confirme que l'équation (2) proposée n'a pas de solution dans $\mathbb{Q}_+^{*2}$. ■

Solution de l'exercice 17.

1) Procédons par l'absurde en supposant qu'il existe $(x,y) \in \mathbb{Q}^2$ tel que $xy(x+y) = 1$. Il est clair qu'aucun des trois nombres x, y et $(x+y)$ n'est nul. Représentons x et y par deux fractions de même dénominateur ; soit

$$x \;=\; \frac{a}{c} \ \text{ et } \ y \;=\; \frac{b}{c},$$

avec $a, b, c \in \mathbb{Z}^*$. On a donc :

$$\frac{a}{c}\cdot\frac{b}{c}\left(\frac{a}{c}+\frac{b}{c}\right) \;=\; 1.$$

C'est à dire :

$$ab(a+b) \;=\; c^3.$$

Soit $d := \text{pgcd}(a,b)$. Puisque d divise a et divise b, il divise $(a+b)$ et donc d^3 divise $ab(a+b)$; c'est à dire d^3 divise c^3. Ce qui entraîne que d divise c. Posons par suite :

$$a' \;=\; \frac{a}{d}\ ,\ b' \;=\; \frac{b}{d} \ \text{ et } \ c' \;=\; \frac{c}{d}.$$

L'équation $ab(a+b) = c^3$ se transforme ainsi en :

$$a'b'(a'+b') \;=\; c'^3$$

et on a $a', b', c', a'+b' \in \mathbb{Z}^*$ et $\text{pgcd}(a',b') = 1$. On peut lire de la dernière équation que le produit des trois entiers non nuls et deux à deux premiers entre eux a', b' et $(a'+b')$ est un cube parfait. Mais ceci n'est possible que si chacun de ces trois entiers est un cube parfait. Autrement dit, il existe $u, v, w \in \mathbb{Z}^*$ tels que : $a' = u^3$, $b' = v^3$ et $a'+b' = w^3$. D'où :

$$u^3+v^3 \;=\; w^3.$$

Ce qui est impossible d'après le théorème de Fermat-Wiles [2].
L'équation $xy(x+y)=1$ n'a donc pas de solution dans $\mathbb{Q}^2$.

Remarque : On peut même montrer qu'on a équivalence entre :

(i) L'équation d'al-Khazin $x^3+y^3=z^3$ n'a pas de solution dans $\mathbb{Z}^{*3}$;

(ii) L'équation $xy(x+y)=1$ n'a pas de solution dans $\mathbb{Q}^2$.

2) Appliquer la même idée.
Comme application, on peut montrer par exemple que l'équation $x^2y^3(x+y)^6=1$ n'a pas de solution dans $\mathbb{Q}^2$.

Solution de l'exercice 18. Nous constatons d'abord que si $(x,y)\in\mathbb{Z}^2$ est une solution de l'équation proposée alors (y,x) et $(-x,-y)$ sont, eux aussi, des solutions pour la même équation. D'autre part, comme n n'est pas un carré parfait (par hypothèse) alors il ne peut y exister une solution $(x,y)\in\mathbb{Z}^2$ pour l'équation proposée tel que $x=0$ ou $y=0$. On constate enfin que si $(x,y)\in\mathbb{Z}^2$ est une solution de l'équation proposée alors x et y sont forcément de même signe. En effet, dans un tel cas, on a $xy+1=\frac{1}{n}(x^2+y^2)>0$ (puisqu'on a déjà vu que $x\neq 0$ et $y\neq 0$) ; ce qui entraîne (puisque le nombre $(xy+1)$ est entier) que $xy+1\geq 1$; d'où $xy\geq 0$, et comme $xy\neq 0$, il vient que $xy>0$, comme prétendu.
Utilisons la méthode de la descente infinie pour montrer que l'équation en question ne possède pas de solution dans $\mathbb{Z}^2$. Procédons par l'absurde en supposant qu'il existe $(x_0,y_0)\in\mathbb{Z}^2$ qui soit solution de ladite équation. Quitte à échanger (x_0,y_0) par $(-x_0,-y_0)$ si nécessaire, on peut supposer que $(x_0,y_0)\in\mathbb{N}^{*2}$. Par suite, quitte à permuter x_0 et y_0 si nécessaire, on peut supposer que $x_0\geq y_0$. Considérons maintenant l'équation de second degré (en t) :

$$t^2+y_0^2 \;=\; n(ty_0+1).$$

Par hypothèse, x_0 est une racine pour cette équation. La seconde racine de cette équation est donc :

$$x_1 \;=\; ny_0-x_0 \;=\; \frac{y_0^2-n}{x_0}.$$

La première expression de x_1 montre que $x_1\in\mathbb{Z}$. Le couple (x_1,y_0) constitue donc une autre solution (dans $\mathbb{Z}^2$) pour l'équation proposée. Il s'ensuit (d'après ce qui précède) que x_1 et y_0 sont de même signe ; d'où $x_1>0$. D'autre part, on a :

$$x_1 \;=\; \frac{y_0^2-n}{x_0} \;<\; \frac{y_0^2}{x_0} \;\leq\; y_0 \qquad (\text{car } y_0\leq x_0)\,;$$

d'où $\boxed{x_1<y_0}$. En considérant la hauteur de $\mathbb{Z}^2$ définie par :

$$\begin{array}{rccc} h: & \mathbb{Z}^2 & \longrightarrow & \mathbb{N} \\ & (x,y) & \longmapsto & \min(|x|,|y|) \end{array},$$

on a alors : $h(x_1,y_0)=x_1<y_0=h(x_0,y_0)$; ce qui montre que la nouvelle solution (x_1,y_0) de l'équation en question est de hauteur strictement plus petite que sa solution initiale (x_0,y_0). Le principe de la descente infinie conclut que cette équation n'a pas de solution dans $\mathbb{Z}^2$. ■

2. En fait d'après Euler, car le théorème de Fermat-Wiles pour l'exposant 3 a été démontré pour la première fois par Euler.

Solution de l'exercice 19. (**D'après A. Schinzel**).
(1) Procédons par l'absurde en supposant qu'il existe $(x, y, n) \in \mathbb{N}^3$ tel que :

$$x^3 + y^3 \;=\; 7 \cdot 8^n. \tag{23}$$

Comme le nombre 7 ne peut s'écrire comme une somme de deux cubes parfaits, on a forcément $n \neq 0$; i.e., $n \geq 1$. Cela entraîne que le nombre $x^3 + y^3 = 7 \cdot 8^n$ est pair. D'où l'on déduit que x et y sont de même parité. Montrons (par l'absurde) que x et y ne peuvent pas être tous les deux impairs. En supposant que x et y sont tous les deux impairs, la factorisation :

$$x^3 + y^3 \;=\; (x + y)(x^2 - xy + y^2) \tag{24}$$

montre que l'entier $(x^2 - xy + y^2)$ est un diviseur de $x^3 + y^3 = 7 \cdot 8^n$. Ce diviseur est, de plus, positif (car c'est un quotient de l'entier positif $(x^3 + y^3)$ sur l'entier positif $(x + y)$) et impair (car x et y sont supposés impairs). Comme les seuls diviseurs positifs impairs du nombre $7 \cdot 8^n$ sont 1 et 7, on a :
— Ou bien $x^2 - xy + y^2 = 1$. Ce qui entraîne (en vertu de (24)) que $x^3 + y^3 = x + y$; i.e., $(x^3 - x) + (y^3 - y) = 0$. Mais puisque $x^3 - x \geq 0$ et $y^3 - y \geq 0$, on a forcément $x^3 - x = 0$ et $y^3 - y = 0$. Ce qui entraîne (puisque les entiers naturels x et y sont supposés impairs) que $x = y = 1$. D'où $x^3 + y^3 = 2 \neq 7 \cdot 8^n$. Ce qui est bien absurde.
— Ou bien $x^2 - xy + y^2 = 7$. Ce qui équivaut à $(2x - y)^2 + 3y^2 = 28$. D'où l'on déduit que $3y^2 \leq 28$; i.e., $y^2 \leq \frac{28}{3} = 9,33\ldots$. Comme y est supposé impair, les seules possibilités sont $y = 1$ et $y = 3$. Pour $y = 1$, on obtient $x^2 - x = 6$, ce qui entraîne (puisque x est positif) que $x = 3$; et pour $y = 3$, on obtient $x^2 - 3x + 2 = 0$, ce qui entraîne (puisque x est supposé impair) que $x = 1$. On a donc $(x, y) \in \{(1, 3), (3, 1)\}$. Ce qui donne $x^3 + y^3 = 28$. D'où $7 \cdot 8^n = 28$; soit $8^n = 4$, ce qui est visiblement impossible.
Ces absurdités montrent que x et y ne peuvent pas être tous les deux impairs ; comme ils sont de même parité (d'après ce qui précède), ils sont par conséquent tous les deux pairs. On peut donc écrire : $x = 2x'$ et $y = 2y'$ (avec $x', y' \in \mathbb{N}$). En reportant ceci dans (23), on trouve (après simplification sur 8) :

$$x'^3 + y'^3 \;=\; 7 \cdot 8^{n-1}.$$

Ce qui montre que le triplet $(x', y', n - 1) \in \mathbb{N}^3$ est une autre solution de l'équation proposée. En considérant la hauteur h de $\mathbb{N}^3$, définie par :

$$\begin{array}{rccc} h : & \mathbb{N}^3 & \longrightarrow & \mathbb{N} \\ & (a, b, c) & \longmapsto & |c| \end{array},$$

on a :

$$h(x', y', n - 1) \;=\; n - 1 \;<\; n = h(x, y, n).$$

La nouvelle solution de l'équation proposée est ainsi de hauteur strictement plus petite que sa solution de départ. Le principe de la descente infinie conclut que l'équation en question n'a pas de solution dans $\mathbb{N}^3$. CQFD.
(2) Pour tout $n \in \mathbb{N}$, l'entier strictement positif $a_n := 7 \cdot 8^n$ s'écrit :

$$a_n \;=\; 7 \cdot 8^n \;=\; 8 \cdot 8^n - 8^n \;=\; 8^{n+1} - 8^n \;=\; (2^{n+1})^3 - (2^n)^3,$$

qui est une différence de deux cubes parfaits. En revanche, le résultat de la question précédente montre que a_n $(n \in \mathbb{N})$ ne peut s'écrire comme une somme de deux cubes parfaits. L'ensemble des entiers naturels qui peuvent se représenter comme une différence

de deux cubes parfaits mais qui ne peuvent pas se représenter comme une somme de deux cubes parfaits contient donc l'ensemble infini $\{a_n, n \in \mathbb{N}\}$, et il est par conséquent lui même infini. CQFD. ■

Solution de l'exercice 20. Comme l'équation en question est visiblement symétrique, on peut se focaliser sur ses solutions $(x, y) \in \mathbb{N}^{*2}$ telles que[3] $x < y$. On constate que $(x_0, y_0) = (1, 3)$ est l'une de telles solutions. A partir de celle-ci, nous allons construire par un procédé de récurrence, une suite $((x_n, y_n))_{n\in\mathbb{N}}$ de $\mathbb{N}^{*2}$ dont les termes sont tous des solutions de l'équation (3) et satisfont $x_n < y_n$ $(\forall n \in \mathbb{N})$. Supposons, pour un certain $n \in \mathbb{N}$, que (x_n, y_n) est déterminé comme on le voudrait ; c'est-à-dire que $x_n, y_n \in \mathbb{N}^*$, $x_n < y_n$ et $x_n^2 - 3x_n y_n + y_n^2 = 1$. Cette dernière égalité équivaut à dire que x_n est une solution de l'équation de second degré (en t) :

$$t^2 - 3y_n t + y_n^2 - 1 \;=\; 0.$$

La seconde solution (notée z_n) de cette équation en t est alors égale à :

$$z_n \;=\; 3y_n - x_n.$$

Comme $x_n, y_n \in \mathbb{N}^*$ et $x_n < y_n$ alors $z_n \in \mathbb{N}^*$ et $y_n < z_n$. De plus, on a (par définition de z_n) :

$$z_n^2 - 3y_n z_n + y_n^2 - 1 \;=\; 0;$$

ce qui montre que le couple (y_n, z_n) est une solution de (3). Il suffit alors de prendre

$$(x_{n+1}, y_{n+1}) \;:=\; (y_n, z_n) \;=\; (y_n, 3y_n - x_n)$$

comme étant le terme qui suit (x_n, y_n) dans la suite requise. Ceci termine notre construction de la suite $((x_n, y_n))_{n\in\mathbb{N}}$. Maintenant, on constate que l'on a pour tout $n \in \mathbb{N}$:

$$x_{n+1} \;=\; y_n \;>\; x_n.$$

Ce qui montre que notre suite $((x_n, y_n))_n$ est strictement croissante relativement à son abscisse. Par conséquent, ses termes (qui sont tous des solutions de l'équation (3)) sont forcément deux à deux distincts et constituent donc un ensemble infini. D'où l'on conclut que l'équation (3) possède une infinité de solutions dans $\mathbb{N}^{*2}$.

— Les calculs donnent :

$$(x_0, y_0) \;:=\; (1, 3) \;\;,\;\; (x_1, y_1) \;=\; (3, 8) \;\;,\;\; (x_2, y_2) \;=\; (8, 21) \;\;,\;\; (x_3, y_3) \;=\; (21, 55)$$
$$\text{et} \quad (x_4, y_4) \;=\; (55, 144),$$

qui sont tous des solutions de l'équation (3).

Remarque : On peut montrer (en suivant le procédé inverse du procédé de construction de la suite $((x_n, y_n))_n$) que toute solution de l'équation (3) dans $\mathbb{N}^{*2}$ est de l'une des deux formes (x_n, y_n) ou (y_n, x_n) $(n \in \mathbb{N})$. Par ailleurs, on peut montrer que l'on a : $(x_n, y_n) = (F_{2n+2}, F_{2n+4})$ $(\forall n \in \mathbb{N})$, où $(F_n)_{n\in\mathbb{N}}$ désigne la suite de Fibonacci usuelle (c'est-à-dire la suite réelle définie par : $F_0 = 0$, $F_1 = 1$ et $F_{n+2} = F_n + F_{n+1}$, $\forall n \in \mathbb{N}$). ■

Solution de l'exercice 21. Comme l'équation en question est visiblement symétrique, on peut se focaliser sur ses solutions $(x, y, z, t) \in \mathbb{N}^{*4}$ telles que $x \leq y \leq z \leq t$. Désignons par S l'ensemble de telles solutions. On vérifie immédiatement qu'il n'existe aucun quadruplet $(x, y, z, t) \in S$ tel que $x = y = z = 1$ ou tel que $x = y = z = t$. Pour tout

3. Remarquer que $x = y$ rend l'équation impossible.

$(x,y,z,t)\in S$, on a donc $yz\geq 2$ et $x<t$. Par ailleurs, les calculs montrent (comme on nous l'a fait remarquer dans l'exercice) que $(1,1,2,2)\in S$. À partir de ce quadruplet particulier $(x_0,y_0,z_0,t_0):=(1,1,2,2)$ de S, nous allons construire -par un procédé de récurrence- une suite judicieuse $((x_n,y_n,z_n,t_n))_{n\in\mathbb{N}}$ d'éléments de S. Supposons, pour un certain $n\in\mathbb{N}$, que (x_n,y_n,z_n,t_n) est déterminé dans S. On a donc : $x_n^2+y_n^2+z_n^2+t_n^2=x_ny_nz_nt_n+6$; ce qui équivaut à dire que x_n est une solution de l'équation de second degré (en U) :

$$U^2-y_nz_nt_n\,U+y_n^2+z_n^2+t_n^2-6\;=\;0.$$

La seconde solution (notée x_n') de cette équation en U est alors égale à :

$$x_n'\;=\;y_nz_nt_n-x_n.$$

Visiblement $x_n'\in\mathbb{Z}$. D'autre part, comme $(x_n,y_n,z_n,t_n)\in S$, on a : $y_nz_n\geq 2$; ce qui entraîne que $\boxed{t_n\leq x_n'}$ $\big($en effet : $x_n'-t_n=(y_nz_n-1)t_n-x_n\geq t_n-x_n\geq 0\big)$. De plus, par définition de x_n', on a :

$$x_n'^2-y_nz_nt_nx_n'+y_n^2+z_n^2+t_n^2-6\;=\;0;$$

ce qui montre que (y_n,z_n,t_n,x_n') est solution de (4). Par conséquent, on a $(y_n,z_n,t_n,x_n')\in S$. Il suffit alors de poser

$$(x_{n+1},y_{n+1},z_{n+1},t_{n+1})\;=\;(y_n,z_n,t_n,x_n')\;=\;(y_n,z_n,t_n,y_nz_nt_n-x_n)$$

comme étant le terme qui suit (x_n,y_n,z_n,t_n) dans la suite requise. Ceci termine la construction de notre suite $((x_n,y_n,z_n,t_n))_{n\in\mathbb{N}}$ d'éléments de S.
Considérons maintenant l'application (hauteur) de $\mathbb{N}^{*4}$ dans $\mathbb{N}$, qui associe à chaque quadruplet $(x,y,z,t)\in\mathbb{N}^{*4}$ l'entier positif $h(x,y,z,t):=x+y+z$. On constate que l'on a pour tout $n\in\mathbb{N}$:

$$\begin{aligned}h(x_{n+1},y_{n+1},z_{n+1},t_{n+1}) &= x_{n+1}+y_{n+1}+z_{n+1}\\ &= y_n+z_n+t_n\\ &> x_n+y_n+z_n\;=\;h(x_n,y_n,z_n,t_n)\end{aligned}$$

(car $x_n<t_n$, vu que $(x_n,y_n,z_n,t_n)\in S$). La suite d'entiers positifs $(h(x_n,y_n,z_n,t_n))_{n\in\mathbb{N}}$ est donc strictement croissante ; ce qui entraîne que les termes de la suite infinie $((x_n,y_n,z_n,t_n))_{n\in\mathbb{N}}$ (qui sont tous des solutions de (4)) sont deux à deux distincts et constituent donc un ensemble infini. D'où l'on conclut que l'équation (4) possède une infinité de solutions dans $\mathbb{N}^{*4}$.

Remarque : L'ensemble S $\big($i.e., l'ensemble des solutions (x,y,z,t) de l'équation (4) dans $\mathbb{N}^{*4}$ telles que $x\leq y\leq z\leq t\big)$ n'est pas constitué uniquement des termes de la suite $((x_n,y_n,z_n,t_n))_{n\in\mathbb{N}}$. Par exemple, le quadruplet $(1,2,3,4)$ appartient à S alors qu'il ne figure pas parmi les termes de ladite suite, qui commence par :

$$(1,1,2,2)\quad,\quad(1,2,2,3)\quad,\quad(2,2,3,11)\quad,\quad(2,3,11,64)\quad,\quad(3,11,64,2110)\quad,\text{etc.}\;\blacksquare$$

Solution de l'exercice 22. Nous procédons par l'absurde en supposant qu'il existe $(x,y,z)\in\mathbb{N}^{*3}$ tel que :

$$4xy-x-y\;=\;z^2.$$

En multipliant par 4 puis en ajoutant 1 aux deux membres de cette égalité, on obtient :

$$16xy - 4x - 4y + 1 \;=\; 4z^2 + 1;$$

c'est-à-dire :

$$(4x-1)(4y-1) \;=\; 4z^2+1. \tag{25}$$

Maintenant, l'entier positif impair $(4x-1)$ possède au moins un diviseur premier de la forme $(4k+3)$, $k \in \mathbb{N}$ $\big($car sinon, tous ses diviseurs premiers auraient la forme $(4k+1)$ et, par conséquent, lui même aurait cette même forme, ce qui n'est pas le cas$\big)$. Soit $p = 4k+3$ $(k \in \mathbb{N})$ un diviseur premier de $(4x-1)$. En vertu de (25), on a : $4z^2+1 \equiv 0 \pmod p$; d'où $(2z)^2 \equiv -1 \pmod p$, ce qui montre que (-1) est un résidu quadratique modulo p. Mais ceci ne peut être vrai puisque $p = 4k+3$. Cette absurdité montre que l'équation diophantienne proposée n'a pas de solution dans $\mathbb{N}^{*3}$. ■

Solution de l'exercice 23. Procédons par l'absurde en supposons qu'il existe $(x,y) \in \mathbb{Z}^2$ tel que $y^2 = x^3+7$. Si l'on suppose que x est pair, il en résulte que $y^2 \equiv 7 \pmod 8$, ce qui est impossible. Donc x est forcément impair. On peut alors écrire $x = 2z+1$ (pour un certain $z \in \mathbb{Z}$). Par suite, on a :

$$y^2+1 \;=\; x^3+8 \;=\; (x+2)(x^2-2x+4) \;=\; (x+2)\left((x-1)^2+3\right) \;=\; (x+2)(4z^2+3). \tag{26}$$

Maintenant, l'entier positif impair $(4z^2+3)$ possède au moins un diviseur premier de la forme $(4k+3)$, $k \in \mathbb{N}$ $\big($car sinon, tous ses diviseurs premiers auraient la forme $(4k+1)$ et, par conséquent, lui même aurait cette même forme, ce qui n'est pas le cas$\big)$. Soit p un diviseur premier de $(4z^2+3)$, ayant la forme $(4k+3)$ $(k \in \mathbb{N})$. D'après (26), on a : $y^2+1 \equiv 0 \pmod p$; d'où $y^2 \equiv -1 \pmod p$, ce qui montre que (-1) est un résidu quadratique modulo p. Mais ceci ne peut être vrai puisque p est de la forme $(4k+3)$ $(k \in \mathbb{N})$. Cette absurdité montre que l'équation proposée n'a pas de solution dans $\mathbb{Z}^2$. ■

Solution de l'exercice 24.

(1) Soient $n \in \mathbb{Z}$ et $p > 3$ un diviseur premier du nombre (n^2+3). Il s'agit de montrer que $p \equiv 1 \pmod 3$. On a par hypothèse $n^2+3 \equiv 0 \pmod p$; c'est-à-dire $n^2 \equiv -3 \pmod p$. Ceci montre que (-3) est un résidu quadratique modulo p ; soit $\left(\frac{-3}{p}\right) = 1$.
Par ailleurs, on a d'une part :

$$\left(\frac{-3}{p}\right) \;=\; \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) \;=\; (-1)^{\frac{p-1}{2}}\left(\frac{3}{p}\right) \tag{27}$$

et d'autre part (en vertu de la loi de la réciprocité quadratique) :

$$\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) \;=\; (-1)^{\frac{3-1}{2}\frac{p-1}{2}} \;=\; (-1)^{\frac{p-1}{2}}.$$

Ce qui donne :

$$\left(\frac{3}{p}\right) \;=\; (-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right)^{-1} \;=\; (-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right)$$

(puisque $\left(\frac{p}{3}\right) = \pm 1$).
En substituant ceci dans (27), on obtient :

$$\left(\frac{-3}{p}\right) \;=\; \left(\frac{p}{3}\right) \;=\; \begin{cases} 1 & \text{si } p \equiv 1 \pmod 3 \\ -1 & \text{si } p \equiv 2 \pmod 3 \end{cases}$$

(puisque 1 est l'unique résidu quadratique modulo 3).
Mais puisqu'on a $\left(\frac{-3}{p}\right) = 1$ alors forcément $p \equiv 1 \pmod 3$, comme il fallait le prouver.

(2) Soient $n \in \mathbb{Z}$ et d un diviseur impair positif du nombre (n^2+3). On a :
• Ou bien $d \equiv 0 \pmod 3$.
• Ou bien $d \not\equiv 0 \pmod 3$ et dans ce cas, la décomposition de d en produit de facteurs premiers s'écrit :

$$d \;=\; p_1^{\alpha_1} \cdots p_k^{\alpha_k},$$

avec $k \in \mathbb{N}$, $\alpha_1, \ldots, \alpha_k \in \mathbb{N}$ et $p_1, \ldots, p_k$ des nombres premiers qui sont tous strictement supérieurs à 3. Comme évidemment chacun de ces nombres premiers $p_1, \ldots, p_k$ est un diviseur de (n^2+3), il en résulte (en vertu du résultat de la 1ère question) que l'on a $p_i \equiv 1 \pmod 3$ pour tout $i = 1, \ldots, k$. D'où l'on déduit que $d \equiv 1^{\alpha_1} \cdots 1^{\alpha_k} \pmod 3 \equiv 1 \pmod 3$.
En conclusion, on a $d \equiv 0$ ou $1 \pmod 3$, comme il fallait le prouver.

(3) Procédons par l'absurde en supposant qu'il existe $(x, y) \in \mathbb{Z}^2$ satisfaisant :

$$(x-1)(x^2+1) \;=\; y^2+y+1.$$

Comme (x^2+1) et $(y^2+y+1) = (y+\frac{1}{2})^2 + \frac{3}{4}$ sont strictement positifs alors $(x-1)$ est, lui aussi, strictement positif. D'autre part, comme (y^2+y+1) est impair $\big($car $y^2+y = y(y+1)$ est pair, en tant que produit de deux entiers consécutifs$\big)$ alors $(x-1)$ et (x^2+1) sont, eux aussi, impairs (en tant que diviseurs d'un nombre impair). Ainsi, $(x-1)$ et (x^2+1) sont des diviseurs positifs impairs de (y^2+y+1). À fortiori, $(x-1)$ et (x^2+1) sont des diviseurs positifs impairs du nombre $4(y^2+y+1) = (2y+1)^2+3$. Il s'ensuit (en vertu du résultat de la 2ème question) que l'on a :

$$\left\{ \begin{array}{rcl} x-1 & \equiv & 0 \text{ ou } 1 \pmod 3 \\ \text{et} & & \\ x^2+1 & \equiv & 0 \text{ ou } 1 \pmod 3 \end{array} \right. . \tag{28}$$

Mais on a :

$$(28) \iff \left\{ \begin{array}{rcl} x & \equiv & 1 \text{ ou } 2 \pmod 3 \\ \text{et} & & \\ x^2 & \equiv & 0 \text{ ou } 2 \pmod 3 \end{array} \right. \iff \left\{ \begin{array}{rcl} x & \equiv & 1 \text{ ou } 2 \pmod 3 \\ \text{et} & & \\ x & \equiv & 0 \pmod 3 \end{array} \right. ,$$

ce qui est une absurdité apparente.
L'équation diophantienne $(x-1)(x^2+1) = y^2+y+1$ n'a donc aucune solution à coordonnées entières. ■

Solution de l'exercice 25. Pour les deux questions de cet exercice, on se sert de la propriété bien connue suivante des valuations p-adiques (p premier).

Propriété : *Soient p un nombre premier et $\alpha_1, \ldots, \alpha_n$ $(n \geq 2)$ des nombres rationnels non nuls. On suppose qu'il existe $k \in \{1, \ldots, n\}$ tel que l'on ait pour tout $i \in \{1, \ldots, n\}$, $i \neq k$: $\vartheta_p(\alpha_i) > \vartheta_p(\alpha_k)$. Alors, on a :*

$$\vartheta_p\left(\alpha_1 + \cdots + \alpha_n\right) \;=\; \vartheta_p(\alpha_k).$$

Retournons maintenant à l'exercice proprement dit.

(1) Soient $n \in \mathbb{N}^*$ et k le plus grand entier naturel tel que $2^k \leq n$. On doit montrer que b_n est un multiple de 2^k. On a d'une part $\vartheta_2(\frac{1}{2^k}) = -k$. D'autre part, on prétend que pour tout $i \in \{1, \ldots, n\}$, $i \neq 2^k$, on a $\vartheta_2(\frac{1}{i}) > -k$. En effet, s'il existe $i \in \{1, \ldots, n\}$, $i \neq 2^k$, vérifiant $\vartheta_2(\frac{1}{i}) \leq -k$, on obtient $\vartheta_2(i) \geq k$, ce qui entraîne que i s'écrit $i = 2^k\ell$, avec $\ell \in \mathbb{N}^*$. Mais le fait $i \neq 2^k$ entraîne $\ell \geq 2$, ce qui entraîne $i \geq 2^{k+1}$ et puis que $2^{k+1} \leq n$. Mais ceci est en contradiction avec le fait que 2^k est la plus grande puissance de 2 qui soit $\leq n$. D'où l'on a effectivement $\vartheta_2(\frac{1}{i}) > -k$ pour tout $i \in \{1, \ldots, n\}$, avec $i \neq 2^k$. La propriété énoncée ci-dessus s'applique donc pour le calcul de la valuation 2-adique du nombre $H_n := \frac{1}{1} + \frac{1}{2} + \cdots + \frac{1}{n}$ et l'on obtient : $\vartheta_2(H_n) = \vartheta_2(\frac{1}{2^k}) = -k$. D'où $\vartheta_2(\frac{a_n}{b_n}) = -k$; c'est-à-dire $\vartheta_p(a_n) - \vartheta_p(b_n) = -k$. Ce qui donne $\vartheta_p(b_n) = \vartheta_p(a_n) + k \geq k$. Ceci montre que b_n est bien un multiple de 2^k, comme il fallait le prouver.

— Pour $n \geq 2$, la plus grande puissance de 2 qui soit $\leq n$ est au moins égale à 2 et puisque b_n est un multiple de cette puissance (en vertu de ce qui précède) alors $b_n \neq 1$. Ce qui montre que H_n n'est pas entier, comme il fallait le prouver.

(2) Soient $n \geq 2$ un entier et p un nombre premier appartenant à l'intervalle $]\frac{n}{2}, n]$. Montrons que b_n est un multiple de p. On a $\vartheta_p(\frac{1}{p}) = -1$ et pour $i \in \{1, \ldots, n\}$, $i \neq p$, si l'on suppose $\vartheta_p(\frac{1}{i}) \leq -1$, il vient que $\vartheta_p(i) \geq 1$, ce qui entraîne que i est un multiple de p, et puisque $i \neq p$, il vient que $i \geq 2p > n$, ce qui contredit le fait $i \in \{1, \ldots, n\}$. Ce raisonnement d'absurde montre que $\vartheta_p(\frac{1}{i}) > -1$ pour tout $i \in \{1, \ldots, n\}$, avec $i \neq p$. La propriété énoncée ci-dessus s'applique donc pour le calcul de la valuation p-adique du nombre H_n et l'on obtient : $\vartheta_p(H_n) = \vartheta_p(\frac{1}{p}) = -1$. D'où $\vartheta_p(\frac{a_n}{b_n}) = -1$; c'est-à-dire $\vartheta_p(a_n) - \vartheta_p(b_n) = -1$. Ce qui donne $\vartheta_p(b_n) = \vartheta_p(a_n) + 1 \geq 1$ et montre que b_n est bien un multiple de p, comme il fallait le prouver. ■

Solution de l'exercice 26. Montrer que xyz est un cube parfait revient à montrer que pour tout nombre premier p, l'entier naturel $\vartheta_p(xyz)$ est un multiple de 3. Soit p un nombre premier arbitraire. En posant $\alpha := \vartheta_p(x)$, $\beta := \vartheta_p(y)$ et $\gamma := \vartheta_p(z)$, on a $\vartheta_p(xyz) = \vartheta_p(x) + \vartheta_p(y) + \vartheta_p(z) = \alpha + \beta + \gamma$. Il s'agit donc de prouver que l'on a : $\alpha + \beta + \gamma \equiv 0 \pmod 3$. Pour ce faire, on distingue les deux cas suivants :

1er cas : (si les entiers $\alpha - \beta$, $\beta - \gamma$ et $\gamma - \alpha$ sont deux à deux distincts)

Puisque

$$\begin{aligned} \vartheta_p\left(\tfrac{x}{y}\right) &= \vartheta_p(x) - \vartheta_p(y) = \alpha - \beta, \\ \vartheta_p\left(\tfrac{y}{z}\right) &= \vartheta_p(y) - \vartheta_p(z) = \beta - \gamma, \\ \vartheta_p\left(\tfrac{z}{x}\right) &= \vartheta_p(z) - \vartheta_p(x) = \gamma - \alpha, \end{aligned}$$

ce cas correspond au fait que les nombres rationnels $\frac{x}{y}$, $\frac{y}{z}$ et $\frac{z}{x}$ ont des valuations p-adiques deux à deux distinctes. Il s'ensuit (d'après les propriétés des valuations p-adiques) que :

$$\vartheta_p\left(\frac{x}{y} + \frac{y}{z} + \frac{z}{x}\right) = \min\left(\vartheta_p\left(\frac{x}{y}\right), \vartheta_p\left(\frac{y}{z}\right), \vartheta_p\left(\frac{z}{x}\right)\right) = \min(\alpha - \beta, \beta - \gamma, \gamma - \alpha).$$

Mais comme $\frac{x}{y} + \frac{y}{z} + \frac{z}{x} \in \mathbb{Z}$ (par hypothèse), on a $\vartheta_p\left(\frac{x}{y} + \frac{y}{z} + \frac{z}{x}\right) \geq 0$; soit $\min(\alpha - \beta, \beta - \gamma, \gamma - \alpha) \geq 0$. Ce qui équivaut à : $\alpha - \beta \geq 0$, $\beta - \gamma \geq 0$ et $\gamma - \alpha \geq 0$; c'est-à-dire : $\alpha \geq \beta \geq \gamma \geq \alpha$. D'où $\alpha = \beta = \gamma$. Ce qui donne $\alpha + \beta + \gamma = 3\alpha \equiv 0 \pmod 3$, comme il fallait le prouver.

2nd cas : (si les entiers $\alpha-\beta$, $\beta-\gamma$ et $\gamma-\alpha$ ne sont pas deux à deux distincts)
Quitte à permuter α, β et γ, on peut supposer que $\alpha-\beta=\beta-\gamma$. Ce qui donne $\gamma=2\beta-\alpha$. On a par conséquent :

$$\alpha+\beta+\gamma \;=\; \alpha+\beta+(2\beta-\alpha) \;=\; 3\beta \;\equiv\; 0 \pmod 3,$$

comme il fallait le prouver.

Conclusion : Pour tout nombre premier p, on a $\vartheta_p(xyz)\equiv 0 \pmod 3$. Ce qui prouve que l'entier xyz est un cube parfait. ■

Solution de l'exercice 27. Déterminons d'abord le reste de N (ou plutôt $2N$) modulo p. On a d'une part :

$$(p-1)! \;=\; (p-1)(p-2)\cdot(p-3)! \;=\; (p-1)(p-2)(N-1) \;\equiv\; (-1)(-2)(N-1)[p] \;\equiv\; 2N-2[p].$$

Et d'autre part (en vertu du théorème d'Ibn al-Haytham) :

$$(p-1)! \;\equiv\; -1[p].$$

En confrontant les deux résultats, il vient que : $2N-2\equiv -1[p]$; ce qui donne :

$$2N\equiv 1[p]. \tag{1}$$

Procédons maintenant par l'absurde en supposant que N est un carré parfait ; donc $4N$ aussi. Comme on a d'après (1) : $4N\equiv 2[p]$, il en résulte que 2 est un résidu quadratique modulo p ; c'est-à-dire que $\left(\frac{2}{p}\right)=1$. Mais, par ailleurs, on sait que :

$$\left(\frac{2}{p}\right) \;=\; (-1)^{\frac{p^2-1}{8}} \;=\; \begin{cases} 1 & \text{si } p\equiv 1,7[8] \\ -1 & \text{si } p\equiv 3,5[8] \end{cases}.$$

Comme dans notre cas, on a $p\equiv 5[8]$, on devrait avoir $\left(\frac{2}{p}\right)=-1$; ce qui est absurde. Cette absurdité assure que N n'est pas un carré parfait.

Remarque : La propriété « $(n!+1)$ est un carré parfait » est satisfaite par chacun des entiers $n=4$, $n=5$ et $n=7$ (en effet, on a : $4!+1=5^2$, $5!+1=11^2$ et $7!+1=41^2$). Il semble que ces nombres 4, 5 et 7 sont les seuls qui satisfont ladite propriété, bien que cela n'est, jusqu'à présent, ni confirmé ni infirmé ! ■

Solution de l'exercice 28.
(1) L'égalité requise est visiblement vraie pour $n=1$. Montrons la pour un entier $n\geq 2$ donné. Pour ce faire, considérons la décomposition de n en produit de facteurs premiers :

$$n \;=\; p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k},$$

avec $k,\alpha_1,\alpha_2,\ldots,\alpha_k\in\mathbb{N}^*$ et $p_1,p_2,\ldots,p_k$ des nombres premiers deux à deux distincts. Pour que deux entiers strictement positifs a et b satisfassent $\mathrm{ppcm}(a,b)=n$, il est nécessaire que a et b soient des diviseurs de n ; donc possèdent des décompositions en produit de facteurs premiers de la forme :

$$a \;=\; p_1^{\beta_1}p_2^{\beta_2}\cdots p_k^{\beta_k}$$
$$b \;=\; p_1^{\gamma_1}p_2^{\gamma_2}\cdots p_k^{\gamma_k},$$

avec $\beta_1, \beta_2, \ldots, \beta_k, \gamma_1, \gamma_2, \ldots, \gamma_k \in \mathbb{N}$ et pour tout $i \in \{1, 2, \ldots, k\}$: $\beta_i \leq \alpha_i$ et $\gamma_i \leq \alpha_i$. Dans cette situation, on a :

$$\operatorname{ppcm}(a,b) \;=\; p_1^{\max(\beta_1,\gamma_1)} p_2^{\max(\beta_2,\gamma_2)} \cdots p_k^{\max(\beta_k,\gamma_k)}.$$

D'où :

$$\begin{aligned} \operatorname{ppcm}(a,b) = n \iff & \max(\beta_i,\gamma_i) = \alpha_i \quad (\forall i = 1,\ldots,k) \\ \iff & \begin{cases} \beta_i = \alpha_i \text{ et } \gamma_i \in \{0,1,\ldots,\alpha_i\} \\ \text{ou} \\ \gamma_i = \alpha_i \text{ et } \beta_i \in \{0,1,\ldots,\alpha_i\} \end{cases} \qquad (\forall i = 1,\ldots,k). \end{aligned}$$

On voit alors que pour tout $i \in \{1, 2, \ldots, k\}$, le nombre de couples (β_i, γ_i) satisfaisant $\max(\beta_i, \gamma_i) = \alpha_i$ est égale à $(2\alpha_i + 1)$. Par conséquent, le nombre de couples (a, b) satisfaisant $\operatorname{ppcm}(a, b) = n$ est égale au produit $\prod_{i=1}^{k}(2\alpha_i + 1)$, qui n'est rien d'autre que $\tau(n^2)$, puisque $n^2 = \left(\prod_{i=1}^{k} p_i^{\alpha_i}\right)^2 = \prod_{i=1}^{k} p_i^{2\alpha_i}$. L'égalité requise est ainsi démontrée.

(2) Soit $n \in \mathbb{N}^*$ fixé. Pour tout couple $(a, b) \in \mathbb{N}^{*2}$, en posant $d := \operatorname{pgcd}(a, b)$, on peut écrire $a = da'$ et $b = db'$, avec $a', b' \in \mathbb{N}^*$ et $a' \wedge b' = 1$; ce qui fait que $\operatorname{ppcm}(da', db') = d \operatorname{ppcm}(a', b') = da'b'$ (puisque $a' \wedge b' = 1$). On a alors :

$$\operatorname{ppcm}(a,b) = n \iff da'b' = n.$$

Pour déterminer un couple $(a, b) \in \mathbb{N}^{*2}$ tel que $\operatorname{ppcm}(a, b) = n$, on peut alors procéder en choisissant d'abord d un diviseur de n, puis a' un diviseur de $\frac{n}{d}$ tel que $a' \wedge \frac{n/d}{a'} = 1$. Pour tout d ainsi choisi, si la décomposition de $\frac{n}{d}$ en produit de facteurs premiers est $\frac{n}{d} = q_1^{r_1} q_2^{r_2} \cdots q_\ell^{r_\ell}$ (avec $\ell \in \mathbb{N}$, $r_1, r_2, \ldots, r_\ell \in \mathbb{N}^*$ et $q_1, q_2, \ldots, q_\ell$ des nombres premiers deux à deux distincts) alors les diviseurs a' de $\frac{n}{d}$ tels que $a' \wedge \frac{n/d}{a'} = 1$ sont :

$$a' \;=\; q_1^{s_1} q_2^{s_2} \cdots q_\ell^{s_\ell},$$

avec $s_i \in \{0, r_i\}$ pour tout $i = 1, \ldots, \ell$ (car tout nombre premier q_i doit diviser exclusivement ou bien a' ou bien $\frac{n/d}{a'}$). Le nombres de tels a' est donc égale à $2^\ell = 2^{\omega(\frac{n}{d})}$. D'où la formule :

$$\begin{aligned} \operatorname{Card}\left\{(a,b) \in \mathbb{N}^{*2} :\ \operatorname{ppcm}(a,b) = n\right\} &= \sum_{d \mid n} 2^{\omega(\frac{n}{d})} \\ &= \sum_{d' \mid n} 2^{\omega(d')} \qquad \left(\text{en posant } d' = \frac{n}{d}\right). \end{aligned}$$

Il ne reste qu'à confronter ce résultat avec celui de la question précédente pour conclure à l'identité requise :

$$\sum_{d' \mid n} 2^{\omega(d')} \;=\; \tau(n^2).$$

Remarque : Dans nos exercices de Théorie Analytique des Nombres (niveau M2), on a proposé une généralisation de la dernière identité avec une nouvelle preuve. ■

Solution de l'exercice 29.

(1) Nous procédons par l'absurde en supposant qu'il n'existe qu'un nombre fini d'entiers $n \geq 2$ qui satisfont l'égalité $\operatorname{ppcm}(u_1, u_2, \ldots, u_n) = \operatorname{ppcm}(u_1, u_2, \ldots, u_{n-1})$. Il existe donc un entier $N \geq 2$ tel que l'on ait :

$$\text{ppcm}(u_1,u_2,\ldots,u_n) \;>\; \text{ppcm}(u_1,u_2,\ldots,u_{n-1}) \qquad (\forall n\geq N). \tag{29}$$

Comme pour tout $k\in\mathbb{N}^*$ et tout p premier, on a $\vartheta_p(\text{ppcm}(u_1,u_2,\ldots,u_k)) = \max(\vartheta_p(u_1),\vartheta_p(u_2),\ldots,\vartheta_p(u_k))$ alors (29) équivaut à l'existence (pour tout entier $n\geq N$) d'un diviseur premier p_n de u_n qui satisfait :

$$\vartheta_{p_n}(u_n) \;>\; \max_{1\leq k<n}\vartheta_{p_n}(u_k). \tag{30}$$

Désignons par $P(u_n)$ (pour un $n\geq N$ donné) le plus grand de tels diviseurs premiers p_n de u_n. On a :

$$\sum_{n\geq N}\frac{1}{u_n\log u_n} \;=\; \sum_{p\text{ premier}}\left(\sum_{n\geq N|P(u_n)=p}\frac{1}{u_n\log u_n}\right). \tag{31}$$

Maintenant, étant donné p un nombre premier, ou bien l'ensemble $\{n\geq N|P(u_n)=p\}$ est vide, et dans ce cas on a $\displaystyle\sum_{n\geq N|P(u_n)=p}\frac{1}{u_n\log u_n}=0$, ou bien il ne l'est pas, et dans ce cas, on convient de désigner par $e_1^{(p)},e_2^{(p)},e_3^{(p)},\ldots$ (avec $e_1^{(p)}<e_2^{(p)}<e_3^{(p)}<\ldots$) les termes de la suite $(u_n)_{n\geq1}$ tels que : $P(e_1^{(p)})=P(e_2^{(p)})=P(e_3^{(p)})=\cdots=p$. En vertu de (30), on a :

$$1 \;\leq\; \vartheta_p(e_1^{(p)}) \;<\; \vartheta_p(e_2^{(p)}) \;<\; \vartheta_p(e_3^{(p)}) \;<\; \ldots$$

Il s'ensuit par une simple récurrence que $\vartheta_p(e_i^{(p)})\geq i$ $(\forall i\geq1)$, ce qui montre que $e_i^{(p)}$ est un multiple de p^i. On a en particulier $e_i^{(p)}\geq p^i$ $(\forall i\geq1)$. Il résulte de cela que pour tout nombre premier p tel que $\{n\geq N|P(u_n)=p\}\neq\emptyset$, on a :

$$\sum_{n\geq N|P(u_n)=p}\frac{1}{u_n\log u_n} \;=\; \sum_i\frac{1}{e_i^{(p)}\log e_i^{(p)}} \;\leq\; \sum_{i=1}^{+\infty}\frac{1}{p^i\log(p^i)} \;\leq\; \left(\sum_{i=1}^{+\infty}\frac{1}{p^i}\right)\frac{1}{\log p}$$
$$= \;\frac{1}{(p-1)\log p}.$$

En reportant ceci dans (31), on obtient finalement :

$$\sum_{n\geq N}\frac{1}{u_n\log u_n} \;\leq\; \sum_{p\text{ premier}}\frac{1}{(p-1)\log p} \;\leq\; 2\sum_{p\text{ premier}}\frac{1}{p\log p} \;<\; +\infty,$$

$\left(\text{puisque la série } \displaystyle\sum_{p\text{ premier}}\frac{1}{p\log p} \text{ est convergente}\right)$.

Ceci contredit l'hypothèse de divergence de la série $\sum_{n=2}^{\infty}\frac{1}{u_n\log u_n}$ et conclut que l'égalité $\text{ppcm}(u_1,u_2,\ldots,u_n)=\text{ppcm}(u_1,u_2,\ldots,u_{n-1})$ a lieu pour une infinité d'entiers $n\geq2$, comme il fallait le prouver.

(2) Soit $(a_n)_{n\geq1}$ une suite arithmétique strictement croissante d'entiers strictement positifs et désignons par r sa raison qui est donc forcément un entier strictement positif. On a par conséquent $a_n=r(n-1)+a_1$ $(\forall n\geq1)$. Ce qui entraîne que l'on a $\frac{1}{a_n\log a_n}\sim_{+\infty}\frac{1}{rn\log n}$. Mais puisque la série $\sum_{n\geq2}\frac{1}{n\log n}$ est divergente, on en déduit que la série $\sum_{n\geq2}\frac{1}{a_n\log a_n}$ est également divergente. Il s'ensuit, en vertu de ce qui précède, qu'il existe une infinité d'entiers $n\geq2$ tels que $\text{ppcm}(a_1,a_2,\ldots,a_n)=\text{ppcm}(a_1,a_2,\ldots,a_{n-1})$. ■

B. Farhi

http://farhi.bakir.free.fr/