EXERCICES – CHAPITRE 12

ARITHMÉTIQUE DANS $\mathbb{Z}$

⋆ *application directe* ⋆⋆ *mise en œuvre* ⋆⋆⋆ *problème* ⋆⋆⋆⋆ *problème long, en autonomie*

Divisibilité et division euclidienne

EXERCICE 1 ⋆

Déterminer les couples $(a, b) \in \mathbb{N}^2$ tels que $a \leqslant 500$ et que la division euclidienne de a par b s'écrive $a = 24b + 17$.

EXERCICE 2 ⋆

Trouver tous les entiers $n \in \mathbb{N}$ vérifiant chacune des conditions suivantes.

(i) $n + 1 \mid n + 3$.

(ii) $n + 2 \mid n^2 + 3n + 5$.

(iii) $n + 1 \mid n^2 + 1$.

EXERCICE 3 ⋆

Soit $n \in \mathbb{N}^*$. Déterminer, selon la parité de n, le reste de la division euclidienne de $1 + 2 + \cdots + n$ par n.

EXERCICE 4 ⋆⋆

1. Soit $n \geqslant 2$ un entier. Montrer que la somme de n entiers naturels impairs consécutifs n'est jamais un nombre premier.
2. Montrer que la somme des cubes de trois entiers consécutifs est divisible par 9.

EXERCICE 5 ⋆⋆

Résoudre dans $\mathbb{Z}^2$ les équations suivantes, d'inconnue (n, p), en se ramenant à un produit de deux facteurs égal à une constante.

(i) $np = 3n + 2p$.

(ii) $\dfrac{1}{n} + \dfrac{1}{p} = \dfrac{1}{5}$.

(iii) $n^2 - p^2 - 4n - 2p = 5$.

EXERCICE 6 ⋆⋆

Montrer que, pour tout entier $n \geqslant 1$, n^2 divise $(n + 1)^n - 1$.

EXERCICE 7 ⋆⋆

Écriture en base b. Soit $b \geqslant 2$ un entier.

1. Montrer que tout entier $n \in \mathbb{N}^*$ s'écrit de façon unique sous la forme

$$n = \sum_{k=0}^{m} c_k b^k, \qquad \text{avec } m \in \mathbb{N},\ c_0, \dots, c_m \in [\![0\,;b-1]\!] \text{ et } c_m \neq 0.$$

   On pourra effectuer les divisions euclidiennes successives de n par b, puis du quotient par b, et ainsi de suite.

2. Écrire 2026 en base 7.

3. Montrer que $b-1$ divise $n - (c_0 + c_1 + \cdots + c_m)$. Quel critère de divisibilité retrouve-t-on pour $b = 10$?

PGCD, PPCM et relation de Bézout

EXERCICE 8 ⋆

Pour chacun des couples (a, b) suivants, calculer $a \wedge b$ par l'algorithme d'Euclide, puis obtenir une relation de Bézout en remontant l'algorithme.

(i) $(438, 51)$ (ii) $(1320, 720)$ (iii) $(120, 23)$ (iv) $(8136, 492)$

EXERCICE 9 ⋆

Soit $k \in \mathbb{N}$. Montrer que $2k+1$ et $9k+4$ sont premiers entre eux, et calculer $(2k-1) \wedge (9k+4)$.

EXERCICE 10 ⋆⋆

Pour $n \in \mathbb{N}$, on pose $u_n = n^2 + 1$. Déterminer, selon les valeurs de n, le PGCD de deux termes consécutifs $u_n \wedge u_{n+1}$.

EXERCICE 11 ⋆⋆

Déterminer l'ensemble $\{(2n+4) \wedge (3n+3) \mid n \in \mathbb{N}\}$.

EXERCICE 12 ⋆⋆⋆

Le théorème de Lamé. On note $(F_n)_{n\in\mathbb{N}}$ la suite de Fibonacci, définie par $F_0 = 0$, $F_1 = 1$ et $F_{n+2} = F_{n+1} + F_n$ pour tout $n \in \mathbb{N}$. Soit $a > b \geqslant 1$ deux entiers. On note $r_0 = a$, $r_1 = b$, et l'on suppose que l'algorithme d'Euclide comporte N divisions :

$$r_{k-1} = q_k r_k + r_{k+1} \quad \text{avec } 0 \leqslant r_{k+1} < r_k, \quad \text{pour } k \in [\![1\,;N]\!], \qquad r_N \neq 0, \quad r_{N+1} = 0.$$

1. Montrer que $r_N \geqslant 1$, que $r_{N-1} \geqslant 2$ et que $r_{k-1} \geqslant r_k + r_{k+1}$ pour tout $k \in [\![1\,;N-1]\!]$.

2. En déduire que $b \geqslant F_{N+1}$. Vérifier sur l'exemple $a = 21$, $b = 13$ de l'introduction du cours que cette inégalité peut être une égalité.

3. Montrer que $F_{n+5} > 10\,F_n$ pour tout $n \geqslant 2$.

4. En déduire que, si b s'écrit avec k chiffres en base 10, alors $N \leqslant 5k$.

Entiers premiers entre eux

EXERCICE 13 ⋆

Soit $n \in \mathbb{N}^*$.

1. Montrer que $n^2 + n$ et $2n + 1$ sont premiers entre eux.
2. Montrer que $3n^2 + 2n$ et $n + 1$ sont premiers entre eux.

EXERCICE 14 ⋆

Résoudre dans $\mathbb{Z}^2$ les équations suivantes, d'inconnue (x, y).

(i) $221x + 247y = 15$ (ii) $221x + 247y = 13$ (iii) $27x - 33y = 99$ (iv) $5x + 3y = 4$

EXERCICE 15 ⋆⋆

Montrer que, pour tout $n \in \mathbb{N}$, l'entier $n^4 - n^2$ est un multiple de 12.

EXERCICE 16 ⋆⋆

1. Soit $m, d \in \mathbb{N}^*$. À quelle condition le système

$$\begin{cases} x \wedge y = d \\ x \vee y = m \end{cases}$$

possède-t-il une solution $(x, y) \in (\mathbb{N}^*)^2$?

2. Déterminer les couples $(x, y) \in (\mathbb{N}^*)^2$ tels que $x \wedge y = 12$ et $x \vee y = 360$.
3. Déterminer les couples $(x, y) \in (\mathbb{N}^*)^2$ tels que $x \wedge y = 18$ et $x + y = 360$.

EXERCICE 17 ⋆⋆

Résoudre dans $(\mathbb{N}^*)^2$ les équations suivantes, d'inconnue (x, y).

(i) $x \wedge y + x \vee y = x + y$.

(ii) $x \wedge y + x \vee y = y + 9$.

EXERCICE 18 ⋆⋆

Soit a et b deux entiers naturels non nuls. Montrer que $(a + b) \wedge (a \vee b) = a \wedge b$.

EXERCICE 19 ⋆⋆

Montrer que tout entier $n > 6$ est la somme de deux entiers strictement supérieurs à 1 et premiers entre eux.

EXERCICE 20 ⋆⋆

Résoudre l'équation $3x + 4y + 5z = 6$, d'inconnue $(x, y, z) \in \mathbb{Z}^3$.

EXERCICE 21 ⋆⋆

1. Soit $a_0, \ldots, a_{n-1}$ des nombres entiers et $x \in \mathbb{Q}$ tel que $x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$. Montrer que $x \in \mathbb{Z}$, et que x divise a_0.
2. En déduire que l'équation $x^3 + x + 1 = 0$ n'a aucune solution rationnelle, puis que $\sqrt[3]{5}$ est irrationnel.

EXERCICE 22 ⋆⋆⋆

Soient p et q deux éléments de $\mathbb{N}^*$ avec $p > q$. On suppose que le quotient $\dfrac{p^2+q^2}{p^2-q^2}$ est un entier.

1. Montrer que l'on peut se ramener au cas où $p \wedge q = 1$. On le supposera par la suite.
2. Montrer que $(p^2-q^2) \wedge p^2 = 1$.
3. En déduire que $p^2 - q^2$ divise 2.
4. Aboutir à une contradiction. Qu'a-t-on montré ?

EXERCICE 23 ⋆⋆⋆

PGCD de nombres de Fibonacci. Soit $(F_n)_{n\in\mathbb{N}}$ la suite de Fibonacci de l'exercice 12, définie par

$$F_0 = 0, \qquad F_1 = 1 \qquad \text{et} \qquad \forall n \in \mathbb{N},\ F_{n+2} = F_{n+1} + F_n.$$

1. Montrer que $F_n \wedge F_{n+1} = 1$ pour tout $n \in \mathbb{N}$.
2. Montrer que, pour tout $n \in \mathbb{N}$ et tout $m \in \mathbb{N}^*$, $F_{n+m} = F_m F_{n+1} + F_{m-1} F_n$.
3. En déduire que, pour tous $n, m \in \mathbb{N}^*$, $F_n \wedge F_{n+m} = F_n \wedge F_m$.
4. En déduire que, si n et m sont deux entiers non nuls et si r est le reste de la division euclidienne de m par n, alors $F_n \wedge F_m = F_n \wedge F_r$.
5. Montrer que, pour tous $m, n \in \mathbb{N}^*$, $F_n \wedge F_m = F_{n\wedge m}$.

Nombres premiers

EXERCICE 24 ⋆

Décomposer 2024, 2025 et 2026 en produits de nombres premiers. En déduire le nombre de diviseurs positifs de chacun de ces entiers, puis calculer $2024 \wedge 2026$ et $2024 \vee 2026$ à l'aide des valuations p-adiques.

EXERCICE 25 ⋆⋆

Soit $n \geqslant 2$ un entier qui n'admet aucun diviseur premier p tel que $p^3 \leqslant n$. Montrer que n est premier ou produit de deux nombres premiers. En déduire, en ne testant que les diviseurs 2, 3, 5 et 7, que 391 est le produit de deux nombres premiers, puis les déterminer.

EXERCICE 26 ⋆⋆

Soit p un nombre premier supérieur ou égal à 5. Montrer que $p^2 - 1$ est divisible par 24.

EXERCICE 27 ⋆⋆

Soit $n \in \mathbb{N}^*$.

1. Montrer qu'il existe n entiers consécutifs dont aucun n'est premier.
2. Montrer qu'il existe un nombre premier compris entre $n+1$ et $n!+1$. En déduire une nouvelle preuve de l'existence d'une infinité de nombres premiers.

EXERCICE 28 ⋆⋆

Montrer que la somme de deux nombres premiers consécutifs n'est jamais le produit de deux nombres premiers.

EXERCICE 29 ⋆⋆

Déterminer les nombres premiers dont l'écriture en base 10 comporte en alternance des 0 et des 1, comme 101 ou 10 101.

EXERCICE 30 ⋆⋆

1. Montrer qu'il existe une infinité de nombres premiers congrus à 3 modulo 4. On pourra raisonner par l'absurde et considérer $4p_1p_2\cdots p_r - 1$.
2. Montrer qu'il existe une infinité de nombres premiers congrus à 5 modulo 6.

EXERCICE 31 ⋆⋆

1. Soit $n \in \mathbb{N}^*$. Montrer que $\sqrt{n}$ est soit un entier, soit un irrationnel.
2. Montrer que $\dfrac{\ln 2}{\ln 3}$ est irrationnel.

EXERCICE 32 ⋆⋆

Soit a et b deux entiers naturels non nuls premiers entre eux, tels que ab soit un carré parfait. Montrer que a et b sont deux carrés parfaits. Le résultat subsiste-t-il sans l'hypothèse $a \wedge b = 1$?

EXERCICE 33 ⋆⋆

Soit $n \in \mathbb{N}^*$. On note $\tau(n)$ le nombre de diviseurs positifs de n, et $\Pi(n)$ leur produit.

1. Montrer que $\tau(n)$ est impair si et seulement si n est un carré parfait.
2. Montrer que $\Pi(n)^2 = n^{\tau(n)}$. On pourra associer chaque diviseur d de n au diviseur $\dfrac{n}{d}$.
3. Déterminer les entiers $n \geqslant 2$ tels que $\Pi(n) = n^2$.

EXERCICE 34 ⋆⋆

Soit $n \in \mathbb{N}$. Calculer la valuation 2-adique de $5^{2^n} - 1$.

EXERCICE 35 ⋆⋆⋆

Formule de Legendre. Soient $n \in \mathbb{N}^*$ et p un nombre premier.

1. Soit $\alpha \in \mathbb{N}$. Combien y a-t-il d'entiers dans $[\![1\,;n]\!]$ multiples de p^α ? Combien y a-t-il d'entiers de p-valuation égale à α ?
2. En déduire que
$$v_p(n!) = \sum_{\alpha=1}^{+\infty} \left\lfloor \frac{n}{p^\alpha} \right\rfloor,$$
en expliquant pourquoi cette somme ne comporte qu'un nombre fini de termes non nuls.
3. Combien de zéros consécutifs, à partir de la droite, compte l'écriture décimale du nombre 1000! ?
4. Montrer que, pour tous r et s dans $\mathbb{N}$, le nombre $\dfrac{(2r)!\,(2s)!}{(r+s)!\,r!\,s!}$ est un entier.

Congruences

EXERCICE 36 ⋆

Rappeler et démontrer les critères de divisibilité par 2, 3, 4, 5, 6, 8, 9, 10 et 11. Les utiliser pour obtenir, à la main, la décomposition en facteurs premiers de 14 652.

EXERCICE 37 ⋆

1. Montrer que 13 divise $2^{70} + 3^{70}$.
2. Le nombre premier $2^{136\,279\,841} - 1$, découvert en octobre 2024, est le plus grand nombre premier connu au moment où cette feuille est écrite. Quel est son dernier chiffre ?
3. Montrer que 19 divise $2^{2^{6k+2}} + 3$ pour tout $k \in \mathbb{N}$.

EXERCICE 38 ⋆

Résoudre dans $\mathbb{Z}$ les congruences suivantes, d'inconnue x.

(i) $5x \equiv 1\ [7]$ (iii) $23x \equiv 0\ [97]$ (v) $4x \equiv 8\ [12]$
(ii) $3x \equiv 4\ [19]$ (iv) $8x \equiv 7\ [105]$ (vi) $4x \equiv 6\ [12]$

EXERCICE 39 ⋆

Montrer que, pour tous entiers a et b, 17 divise $2a + 3b$ si et seulement si 17 divise $9a + 5b$.

EXERCICE 40 ⋆⋆

Résoudre dans $\mathbb{Z}^2$ le système de congruences

$$\begin{cases} 4x + y \equiv 6\ [12] \\ x + 4y \equiv 3\ [12] \end{cases}$$

EXERCICE 41 ⋆⋆

Soit $n \in \mathbb{N}^*$ et $a, b \in \mathbb{Z}$ tels que $a \equiv b\ [n]$. Montrer que $a^n \equiv b^n\ [n^2]$.

EXERCICE 42 ⋆⋆

Déterminer les entiers $n \in \mathbb{N}$ tels que $n\,3^n \equiv 1\ [7]$.

EXERCICE 43 ⋆⋆

1. Montrer qu'il existe une infinité d'entiers $n > 0$ tels que $4n^2 + 1$ soit divisible à la fois par 5 et par 13.
2. Montrer que l'ensemble $\{2^n - 3 \mid n \geqslant 2\}$ contient une infinité de multiples de 5, une infinité de multiples de 13, mais aucun multiple de 65.

EXERCICE 44 ⋆⋆

À l'aide du petit théorème de Fermat, montrer que, pour tout $n \in \mathbb{N}$, $n^5 - n \equiv 0\ [30]$ et $n^7 - n \equiv 0\ [42]$.

EXERCICE 45 ⋆⋆

Montrer, en raisonnant modulo 5, que l'équation $15x^2 - 7y^2 = 9$, d'inconnue $(x, y) \in \mathbb{Z}^2$, n'admet aucune solution.

EXERCICE 46 ⋆⋆

1. Soit $n \in \mathbb{N}$. Déterminer à quelle condition « l'équation » $x^3 \equiv n\ [9]$ possède une solution dans $\mathbb{Z}$.
2. Montrer que, pour tous $a, b, c \in \mathbb{Z}$, $a^3 + b^3 + c^3 \neq 11\,111$.
3. En utilisant des propriétés fines du plus petit sous-corps de $\mathbb{R}$ contenant $\sqrt[3]{117}$, Finkelstein et London ont montré en 1971 que l'équation $x^3 + 117y^3 = 5$ n'avait pas de solution $(x, y) \in \mathbb{Z}^2$. Montrer leur résultat de façon plus élémentaire.

EXERCICE 47 ⋆⋆

Le nombre 2^{29} possède neuf chiffres, tous distincts. Quel est le chiffre manquant ? On ne demande pas de calculer 2^{29}.

EXERCICE 48 ⋆⋆

Montrer que $\min\left\{|36^n - 5^m| \;\middle|\; n, m \in \mathbb{N}^*\right\} = 11$.

EXERCICE 49 ⋆⋆

On appelle *repunit* un nombre entier dont l'écriture en base 10 ne contient que des 1. Caractériser les nombres premiers qui divisent au moins un repunit.

EXERCICE 50 ⋆⋆⋆

Théorème de Wilson. Soit $n \geqslant 2$. Montrer que n est premier si et seulement si $(n-1)! \equiv -1\ [n]$. On pourra, pour n premier, regrouper chaque entier de $[\![2\,;n-2]\!]$ avec son inverse modulo n.

EXERCICE 51 ⋆⋆⋆

Soit p un nombre premier impair.

1. On suppose que l'équation $x^2 \equiv -1\ [p]$ possède une solution dans $\mathbb{Z}$. Montrer que $p \equiv 1\ [4]$.
2. En déduire qu'il existe une infinité de nombres premiers congrus à 1 modulo 4.
3. Réciproquement, montrer que si $p \equiv 1\ [4]$, on a $\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv -1\ [p]$. On utilisera le théorème de Wilson de l'exercice 50.

Exercices de synthèse

EXERCICE 52 ⋆⋆

Vrai ou faux ? Justifier chaque réponse par une démonstration ou un contre-exemple.

1. Si a divise bc et ne divise pas b, alors a divise c.
2. Pour tous entiers a et b, $a \wedge b = (a+b) \wedge b$.
3. Si $a \wedge b = 1$ et $a \wedge c = 1$, alors $a \wedge (bc) = 1$.
4. Si un nombre premier p divise a^2, alors p^2 divise a^2.
5. Si $a \equiv b\ [n]$ et $c \equiv d\ [n]$, avec c et d dans $\mathbb{N}$, alors $a^c \equiv b^d\ [n]$.
6. Si n est premier, alors $2^n - 1$ est premier.
7. L'équation $6x + 10y = 7$ n'a aucune solution dans $\mathbb{Z}^2$.
8. Tout entier $n \geqslant 2$ qui n'est pas premier admet un diviseur premier p tel que $p^2 \leqslant n$.
9. Les entiers 72 et 108 ont le même nombre de diviseurs positifs.
10. Si $a^2 \equiv 1\ [n]$, alors $a \equiv 1\ [n]$ ou $a \equiv -1\ [n]$.

EXERCICE 53 ⋆⋆

PGCD et PPCM dans le cercle unité. Soit n et m deux entiers naturels non nuls. On rappelle que $\mathbb{U}_n = \{z \in \mathbb{C} \mid z^n = 1\}$ est l'ensemble des racines n-ièmes de l'unité (chapitre 4).

1. Montrer que $\mathbb{U}_n \cap \mathbb{U}_m = \mathbb{U}_{n \wedge m}$. On pourra utiliser une relation de Bézout.
2. On note $\mathbb{U}_n\mathbb{U}_m = \{zw \mid z \in \mathbb{U}_n,\ w \in \mathbb{U}_m\}$. Montrer que $\mathbb{U}_n\mathbb{U}_m = \mathbb{U}_{n \vee m}$.
3. On suppose $n \wedge m = 1$. Montrer que tout élément de $\mathbb{U}_{nm}$ s'écrit de façon unique sous la forme zw, avec $z \in \mathbb{U}_n$ et $w \in \mathbb{U}_m$.
4. On trace, inscrits dans le cercle unité, un dodécagone régulier et un polygone régulier à 18 côtés ayant tous deux le point d'affixe 1 pour sommet. Combien de sommets ont-ils en commun ? Quel ensemble obtient-on en multipliant l'affixe d'un sommet du premier par l'affixe d'un sommet du second, de toutes les façons possibles ?

EXERCICE 54 ⋆⋆⋆

Nombres parfaits. Pour tout $n \in \mathbb{N}^*$, on note $\sigma(n)$ la somme des diviseurs de n. On dit que n est *parfait* si $\sigma(n) = 2n$ (c'est-à-dire si n est égal à la somme de ses diviseurs différents de lui-même).

1. Montrer que 6 et 28 sont parfaits.
2. Soit $n \in \mathbb{N}^*$. En commençant par le cas où n est une puissance d'un nombre premier, établir une formule pour $\sigma(n)$ en fonction de la décomposition en facteurs premiers de n.
3. Montrer que si n et m sont des nombres premiers entre eux, alors $\sigma(mn) = \sigma(m)\sigma(n)$.
4. Soit p un nombre premier tel que $2^p - 1$ soit premier. Montrer que $2^{p-1}(2^p - 1)$ est parfait.
5. Soit n un entier pair parfait. Il existe $a \in \mathbb{N}^*$ et b entier impair tels que $n = 2^a b$.
   (a) Montrer : $\sigma(n) = (2^{a+1} - 1)\sigma(b)$.
   (b) En déduire qu'il existe un entier impair c tel que $b = (2^{a+1} - 1)c$ et $\sigma(b) = 2^{a+1}c$.
   (c) Montrer que $c = 1$ et que b est premier.
   (d) En déduire que n est de la forme $2^{k-1}(2^k - 1)$, avec $2^k - 1$ premier.

EXERCICE 55 ⋆⋆⋆

Nombres de Fermat.

1. Soit $m \in \mathbb{N}^*$ tel que $2^m + 1$ soit premier. Montrer qu'il existe $n \in \mathbb{N}$ tel que $m = 2^n$.
2. Pour $n \in \mathbb{N}$, on note $F_n = 2^{2^n} + 1$. Calculer F_0, F_1, F_2, F_3, F_4.
3. Montrer que $\forall n \in \mathbb{N}$, $F_{n+1} - 2 = (F_n - 2)F_n$.
4. En déduire, pour $n \in \mathbb{N}^*$, une expression de F_n en fonction des $(F_k)_{k=0}^{n-1}$.
5. Montrer que si $m \neq n$ alors F_n et F_m sont premiers entre eux.
6. En déduire une nouvelle preuve de l'existence d'une infinité de nombres premiers.

EXERCICE 56 ⋆⋆⋆

Nombres de Mersenne. Soit $a, b, n \geqslant 2$ trois entiers.

1. Montrer que $a^n - 1$ est divisible par $a - 1$.
2. En déduire que si $a^n - 1$ est un nombre premier, alors $a = 2$ et n est un nombre premier.
3. On note r le reste de la division euclidienne de a par b. Montrer que $2^r - 1$ est le reste de la division euclidienne de $2^a - 1$ par $2^b - 1$.
4. Montrer que $(2^a - 1) \wedge (2^b - 1) = 2^{a \wedge b} - 1$.

EXERCICE 57 ⋆⋆⋆

1. Soit p un nombre premier.
   (a) Prolonger la valuation p-adique en une fonction $v_p : \mathbb{Q} \to \mathbb{Z} \cup \{+\infty\}$ vérifiant la propriété
   $$\forall x, y \in \mathbb{Q}, \qquad v_p(xy) = v_p(x) + v_p(y).$$
   (b) Montrer que l'on conserve la propriété $\forall x, y \in \mathbb{Q}$, $v_p(x + y) \geqslant \min\left(v_p(x), v_p(y)\right)$.
2. Pour $n \geqslant 1$, on note $H_n = \displaystyle\sum_{k=1}^{n} \frac{1}{k}$. Calculer $v_2(H_n)$.
3. En déduire que pour tout $n > 1$, $H_n \notin \mathbb{Z}$ et que pour tous $m > n$, $H_m - H_n \notin \mathbb{Z}$.

EXERCICE 58 ⋆⋆⋆

Triplets pythagoriciens. On veut résoudre l'équation
$$x^2 + y^2 = z^2,$$
d'inconnue $(x, y, z) \in \mathbb{Z}^3$. De tels triplets sont appelés triplets pythagoriciens.

1. Montrer que l'on peut uniquement rechercher les triplets pythagoriciens dont les composantes sont positives et deux à deux premières entre elles. On les appelle triplets pythagoriciens primitifs.
2. Soit (x, y, z) un triplet pythagoricien primitif. Montrer que l'entier z est impair.

On supposera dans la suite que l'entier y est pair.

3. On pose $y = 2s$, $r = \dfrac{z + x}{2}$, et $t = \dfrac{z - x}{2}$. Montrer que $r \wedge t = 1$.
4. Montrer que r et t sont des carrés parfaits.
5. Montrer que l'ensemble des triplets pythagoriciens est :
$$\Big\{(d(u^2 - v^2), 2duv, d(u^2 + v^2)),\ (2duv, d(u^2 - v^2), d(u^2 + v^2))\ ;\ (d, u, v) \in \mathbb{Z}^3\Big\}.$$

EXERCICE 59 ⋆⋆⋆

Nombres premiers en progression arithmétique. Soit $r \in \mathbb{N}^*$ et $n \in \mathbb{N}^*$. On appelle *progression de nombres premiers* de raison r et de longueur n tout n-uplet $(p_1, \dots, p_n)$ de nombres premiers tel que $p_{i+1} = p_i + r$ pour tout $i \in [\![1\,;n-1]\!]$. Par exemple, $(5, 11, 17, 23, 29)$ est une progression de nombres premiers de raison 6 et de longueur 5.

1. Soit $(p_1, \dots, p_n)$ une progression de nombres premiers de raison r et de longueur $n \geqslant 3$. Montrer que $p_1 > 2$ et que r est pair.
2. Montrer que, pour toute progression de nombres premiers $(p_1, \dots, p_n)$, on a $n \leqslant p_1$. On pourra considérer le terme d'indice $p_1 + 1$.
3. Soit $(p_1, \dots, p_n)$ une progression de nombres premiers de raison r, et q un nombre premier strictement inférieur à n. On suppose, par l'absurde, que q ne divise pas r, et l'on note, pour $i \in [\![1\,;n]\!]$, ρ_i le reste de la division euclidienne de p_i par q.
   (a) Montrer que, pour tous $i, j \in [\![1\,;n]\!]$, on a $\rho_i = \rho_j$ si et seulement si q divise $i - j$.
   (b) En déduire que les restes $\rho_1, \dots, \rho_q$ sont deux à deux distincts.
   (c) Établir l'existence d'un indice $s \in [\![1\,;q]\!]$ tel que $p_s = q$, et aboutir à une contradiction.
4. En déduire que la raison d'une progression de nombres premiers de longueur n est divisible par le produit de tous les nombres premiers strictement inférieurs à n. Vérifier ce résultat sur la progression $(7, 37, 67, 97, 127, 157)$, et dire par quel entier est nécessairement divisible la raison d'une progression de nombres premiers de longueur 10.

EXERCICE 60 ⋆⋆⋆

Des ensembles emboîtés d'intersection vide. On note $F = \mathbb{Q} \setminus \{-1, 0, 1\}$ et f l'application définie sur $\mathbb{Q}^*$ par $f(x) = x - \dfrac{1}{x}$. On pose $f^{\circ 0} = \mathrm{id}_F$ et, pour $n \in \mathbb{N}$, $f^{\circ(n+1)} = f \circ f^{\circ n}$. Pour $x \in \mathbb{Q}^*$ de forme irréductible $\dfrac{p}{q}$, avec $p \in \mathbb{Z}^*$ et $q \in \mathbb{N}^*$, on appelle *hauteur* de x l'entier $H(x) = |p| + q$.

1. Montrer que $f(F) \subset F$. On pourra utiliser l'exercice 21.
2. Montrer que la suite d'ensembles $\left(f^{\circ n}(F)\right)_{n\in\mathbb{N}}$ est décroissante pour l'inclusion et qu'aucun de ses termes n'est vide. Calculer $f(2)$, $f^{\circ 2}(2)$ et $f^{\circ 3}(2)$, ainsi que leurs hauteurs.
3. Soit $x \in F$, de forme irréductible $\dfrac{p}{q}$. Montrer que $p^2 - q^2$ et pq sont premiers entre eux, et en déduire que
$$H\big(f(x)\big) = |p^2 - q^2| + |p|\, q.$$
4. En déduire que $H\big(f(x)\big) \geqslant H(x) + 1$ pour tout $x \in F$, puis que tout élément y de $f^{\circ n}(F)$ vérifie $H(y) \geqslant n + 3$.
5. Montrer que $\displaystyle\bigcap_{n\in\mathbb{N}} f^{\circ n}(F) = \varnothing$.

EXERCICE 61 ⋆⋆⋆

Les sous-anneaux de $\mathbb{Q}$. On note $\mathcal{P}$ l'ensemble des nombres premiers. Pour toute partie E de $\mathcal{P}$, on note A_E l'ensemble des rationnels qui peuvent s'écrire $\dfrac{a}{b}$, avec $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$ dont tous les diviseurs premiers appartiennent à E (l'entier $b = 1$, qui n'a aucun diviseur premier, est donc toujours permis).

1. Montrer que A_E est un sous-anneau de $\mathbb{Q}$. Déterminer $A_\varnothing$, $A_\mathcal{P}$ et $A_{\{2,5\}}$, et comparer $A_{\mathcal{P}\setminus\{2\}}$ avec l'anneau de l'exercice 35 de la feuille du chapitre 11.
2. Soit A un sous-anneau de $\mathbb{Q}$, et $x \in A$, de forme irréductible $\dfrac{a}{b}$. Montrer que $\dfrac{1}{b} \in A$, puis que $\dfrac{1}{p} \in A$ pour tout nombre premier p qui divise b.

3. Pour tout sous-anneau A de $\mathbb{Q}$, on note $E(A) = \left\{p \in \mathcal{P} \;\middle|\; \frac{1}{p} \in A\right\}$. Montrer que $A = A_{E(A)}$.
4. Montrer que l'application $E \longmapsto A_E$ est une bijection de l'ensemble des parties de $\mathcal{P}$ sur l'ensemble des sous-anneaux de $\mathbb{Q}$.
5. En déduire que $\mathbb{Q}$ est le seul sous-anneau de $\mathbb{Q}$ qui soit un corps, puis déterminer le plus petit sous-anneau de $\mathbb{Q}$ contenant $\frac{3}{10}$.

Les six derniers exercices sont des problèmes à traiter en autonomie : l'énoncé fixe le but, et c'est à vous de trouver le chemin.

EXERCICE 62 ⋆⋆⋆⋆

Un nombre $6666\ldots0000$ formé de six-cent-soixante-six « 6 » et éventuellement de quelques zéros à la fin peut-il être un carré parfait ?

EXERCICE 63 ⋆⋆⋆⋆

Résoudre dans $(\mathbb{N}^*)^2$ l'équation $x^y = y^x$.

EXERCICE 64 ⋆⋆⋆⋆

Soit $n \geqslant 2$. Montrer que le produit de trois entiers > 0 consécutifs n'est jamais une puissance n-ième.

EXERCICE 65 ⋆⋆⋆⋆

Déterminer tous les entiers $n \in \mathbb{N}^*$ tels que 2^n divise $3^n - 1$.

EXERCICE 66 ⋆⋆⋆⋆

Soit $n \in \mathbb{N}^*$. Montrer que n est impair si et seulement si n divise $\displaystyle\sum_{k=1}^{n} k^n$.

EXERCICE 67 ⋆⋆⋆⋆

Soit $a_0 \in \mathbb{N}^*$. On définit la suite $(a_n)_{n\in\mathbb{N}}$ par

$$\forall n \in \mathbb{N}, \qquad a_{n+1} = \begin{cases} \sqrt{a_n} & \text{si } \sqrt{a_n} \in \mathbb{N}^*, \\ a_n + 3 & \text{sinon.} \end{cases}$$

Déterminer les $a_0 \in \mathbb{N}^*$ tels que la suite $(a_n)_{n\in\mathbb{N}}$ prenne la même valeur une infinité de fois.