CORRIGÉ – CHAPITRE 12

ARITHMÉTIQUE DANS $\mathbb{Z}$

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

Divisibilité et division euclidienne

EXERCICE 1 ⋆

L'égalité $a = 24b + 17$ est la division euclidienne de a par b si et seulement si le reste vérifie $0 \leqslant 17 < b$, c'est-à-dire $b \geqslant 18$ (théorème 1). La condition $a \leqslant 500$ s'écrit $24b \leqslant 483$, soit $b \leqslant 20$, puisque $\left\lfloor \frac{483}{24} \right\rfloor = 20$. Il reste donc $b \in \{18, 19, 20\}$.

$$\boxed{(a, b) \in \{(449, 18),\ (473, 19),\ (497, 20)\}}$$

Piège. L'erreur la plus répandue est d'oublier que le reste doit être strictement inférieur au diviseur. Avec $b = 10$, l'égalité $257 = 24 \times 10 + 17$ est vraie, mais ce n'est pas la division euclidienne de 257 par 10, dont le quotient est 25.

EXERCICE 2 ⋆

La méthode est la même dans les trois cas : on retranche au dividende un multiple du diviseur, ce qui ne change pas la divisibilité (proposition 1), jusqu'à obtenir une constante.

(i) Comme $n + 3 = (n + 1) + 2$, on a $n + 1 \mid n + 3$ si et seulement si $n + 1 \mid 2$, c'est-à-dire $n + 1 \in \{1, 2\}$.

$$\boxed{n \in \{0, 1\}}$$

(ii) On a $n^2 + 3n + 5 = (n + 2)(n + 1) + 3$, donc la condition équivaut à $n + 2 \mid 3$. Comme $n + 2 \geqslant 2$, il faut $n + 2 = 3$.

$$\boxed{n = 1}$$

Vérification : $3 \mid 9$. ✓

(iii) On a $n^2 + 1 = (n + 1)(n - 1) + 2$, donc la condition équivaut à $n + 1 \mid 2$.

$$\boxed{n \in \{0, 1\}}$$

EXERCICE 3 ⋆

On a $S = 1 + 2 + \cdots + n = \dfrac{n(n+1)}{2}$ (chapitre 3).

Si n est impair, $\dfrac{n+1}{2}$ est un entier, et $S = n \times \dfrac{n+1}{2}$ est un multiple de n.

Si n est pair, on écrit $n = 2m$: alors $S = m(2m + 1) = n \times m + m$, avec $0 \leqslant m < n$. Par unicité de la division euclidienne, le reste est m.

$$\boxed{\text{le reste vaut 0 si } n \text{ est impair, et } \frac{n}{2} \text{ si } n \text{ est pair}}$$

À retenir. Pour lire un reste sur une égalité $S = nq + r$, il faut vérifier $0 \leqslant r < n$; c'est l'unicité du théorème 1 qui permet alors de conclure.

EXERCICE 4 ⋆⋆

1. Soit $2k+1$, avec $k \in \mathbb{N}$, le plus petit des n entiers impairs consécutifs. Leur somme vaut

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

Les deux facteurs n et $2k+n$ sont supérieurs ou égaux à 2, donc la somme admet un diviseur n différent de 1 et d'elle-même : elle n'est pas première.

$$\boxed{\text{la somme vaut } n(2k+n),\ \text{produit de deux entiers } \geqslant 2}$$

2. Pour trois entiers consécutifs $n-1$, n, $n+1$, le développement donne

$$(n-1)^3+n^3+(n+1)^3 = 3n^3+6n = 3n(n^2+2).$$

Si $3 \mid n$, alors $9 \mid 3n$. Sinon $n \equiv \pm 1$ [3], donc $n^2 \equiv 1$ [3] et $3 \mid n^2+2$. Dans les deux cas, 9 divise $3n(n^2+2)$.

$$\boxed{(n-1)^3+n^3+(n+1)^3 = 3n(n^2+2) \equiv 0\ [9]}$$

EXERCICE 5 ⋆⋆

(i) L'équation s'écrit $np-3n-2p+6=6$, soit $(n-2)(p-3)=6$. Le facteur $n-2$ parcourt les diviseurs de 6, c'est-à-dire ± 1, ± 2, ± 3, ± 6, et $p-3$ vaut le quotient.

$$\boxed{(n,p) \in \{(3,9),(4,6),(5,5),(8,4),(1,-3),(0,0),(-1,1),(-4,2)\}}$$

(ii) L'équation impose $n \neq 0$ et $p \neq 0$, et s'écrit alors $5(n+p) = np$, soit $(n-5)(p-5) = 25$. Les diviseurs de 25 sont ± 1, ± 5, ± 25 ; le couple $n-5 = p-5 = -5$ donne $n = p = 0$, qu'il faut exclure.

$$\boxed{(n,p) \in \{(6,30),(10,10),(30,6),(4,-20),(-20,4)\}}$$

(iii) On complète les carrés : $(n-2)^2-(p+1)^2 = 5+4-1 = 8$, soit

$$(n-p-3)(n+p-1) = 8.$$

Les deux facteurs $A = n-p-3$ et $B = n+p-1$ ont pour somme $2n-4$, qui est paire : ils ont la même parité, donc sont tous deux pairs, puisque leur produit est pair. Il reste

$$(A,B) \in \{(2,4),(4,2),(-2,-4),(-4,-2)\}, \qquad \text{avec } n = \frac{A+B+4}{2} \text{ et } p = \frac{B-A-2}{2}.$$

$$\boxed{(n,p) \in \{(5,0),(5,-2),(-1,-2),(-1,0)\}}$$

Piège. Il ne faut pas oublier les diviseurs négatifs : dans $\mathbb{Z}$, l'équation $AB = 6$ a huit solutions, et non quatre. L'argument de parité de (iii) élimine d'emblée les couples $(1,8)$, $(8,1)$, etc.

EXERCICE 6 ⋆⋆

La formule du binôme (chapitre 3, théorème 2) donne

$$(n+1)^n - 1 = \sum_{k=1}^{n}\binom{n}{k}n^k = \binom{n}{1}n + \sum_{k=2}^{n}\binom{n}{k}n^k = n^2 + n^2\sum_{k=2}^{n}\binom{n}{k}n^{k-2}.$$

Les deux termes sont des multiples de n^2.

$$\boxed{n^2 \mid (n+1)^n - 1}$$

À retenir. Tout repose sur le terme $k=1$, qui vaut $n \times n$: c'est le coefficient binomial $\binom{n}{1} = n$ qui fournit le second facteur n.

EXERCICE 7 ⋆⋆

1. *Existence*, par récurrence forte sur n. Si $n < b$, l'écriture $n = c_0$ convient. Sinon, la division euclidienne donne $n = bq + c_0$ avec $0 \leqslant c_0 < b$ et $1 \leqslant q < n$; l'hypothèse de récurrence écrit $q = \sum_{k=0}^{m'} d_k b^k$, et l'on obtient $n = c_0 + \sum_{k=0}^{m'} d_k b^{k+1}$.

Unicité, encore par récurrence forte. Si $n = \sum_{k=0}^{m} c_k b^k$, alors $n = b\Big(\sum_{k=1}^{m} c_k b^{k-1}\Big) + c_0$ avec $0 \leqslant c_0 < b$: c'est la division euclidienne de n par b. Par unicité du théorème 1, c_0 est le reste et $\sum_{k\geqslant 1} c_k b^{k-1}$ le quotient, entier strictement plus petit que n dont l'écriture est unique par hypothèse de récurrence (s'il est nul, $m = 0$).

2. On divise successivement par 7 :

$$2026 = 7 \times 289 + 3, \qquad 289 = 7 \times 41 + 2, \qquad 41 = 7 \times 5 + 6, \qquad 5 = 7 \times 0 + 5.$$

Les restes, lus de bas en haut, donnent les chiffres.

$$\boxed{2026 = \overline{5623}^{\,7} = 5 \times 7^3 + 6 \times 7^2 + 2 \times 7 + 3}$$

Vérification : $1715 + 294 + 14 + 3 = 2026$. ✓

3. Comme $b \equiv 1\ [b-1]$, on a $b^k \equiv 1\ [b-1]$ pour tout k (chapitre 2, proposition 10), donc $n = \sum c_k b^k \equiv \sum c_k\ [b-1]$.

$$\boxed{b - 1 \mid n - (c_0 + c_1 + \cdots + c_m)}$$

Pour $b = 10$, on retrouve le critère de divisibilité par 9, et donc par 3 : un entier et la somme de ses chiffres ont le même reste modulo 9, comme l'exemple de la section 12.6 du cours l'a montré.

PGCD, PPCM et relation de Bézout

EXERCICE 8 ⋆

Dans chaque cas, on écrit l'algorithme d'Euclide en numérotant les lignes, puis on isole le dernier reste non nul et l'on remonte, en remplaçant à chaque étape le plus petit reste par son expression tirée de la ligne au-dessus.

(i) On a

$$438 = 8 \times 51 + 30, \quad 51 = 1 \times 30 + 21, \quad 30 = 1 \times 21 + 9, \quad 21 = 2 \times 9 + 3, \quad 9 = 3 \times 3.$$

Le dernier reste non nul est 3, et la remontée donne

$$3 = 21 - 2 \times 9 = 3 \times 21 - 2 \times 30 = 3 \times 51 - 5 \times 30 = 43 \times 51 - 5 \times 438.$$

$$\boxed{438 \wedge 51 = 3 = 438 \times (-5) + 51 \times 43}$$

(ii) On a $1320 = 1 \times 720 + 600$, $720 = 1 \times 600 + 120$ et $600 = 5 \times 120$, puis

$$120 = 720 - 600 = 720 - (1320 - 720) = 2 \times 720 - 1320.$$

$$\boxed{1320 \wedge 720 = 120 = 1320 \times (-1) + 720 \times 2}$$

(iii) On a

$$120 = 5 \times 23 + 5, \quad 23 = 4 \times 5 + 3, \quad 5 = 1 \times 3 + 2, \quad 3 = 1 \times 2 + 1, \quad 2 = 2 \times 1,$$

puis

$$1 = 3 - 2 = 2 \times 3 - 5 = 2 \times 23 - 9 \times 5 = 47 \times 23 - 9 \times 120.$$

$$\boxed{120 \wedge 23 = 1 = 120 \times (-9) + 23 \times 47}$$

(iv) On a

$$8136 = 16 \times 492 + 264, \quad 492 = 1 \times 264 + 228, \quad 264 = 1 \times 228 + 36, \quad 228 = 6 \times 36 + 12, \quad 36 = 3 \times 12,$$

puis

$$12 = 228 - 6 \times 36 = 7 \times 228 - 6 \times 264 = 7 \times 492 - 13 \times 264 = 215 \times 492 - 13 \times 8136.$$

$$\boxed{8136 \wedge 492 = 12 = 8136 \times (-13) + 492 \times 215}$$

Vérification : $105\,780 - 105\,768 = 12$. ✓
À retenir. Le couple de Bézout n'est pas unique : en (ii), $(-1 + 6k,\ 2 - 11k)$ convient aussi pour tout k, puisque $1320 \times 6 = 720 \times 11$. Ce qu'on obtient en remontant n'est qu'un couple parmi d'autres ; la section 12.4 décrit tous les autres.

EXERCICE 9 ⋆

On cherche une combinaison qui élimine k : $9(2k+1) - 2(9k+4) = 1$. Tout diviseur commun divise donc 1 (proposition 1), et

$$\boxed{(2k+1) \wedge (9k+4) = 1}$$

De même, $2(9k+4) - 9(2k-1) = 17$, donc $d = (2k-1) \wedge (9k+4)$ divise 17, qui est premier : $d \in \{1, 17\}$. Or $17 \mid 2k-1$ équivaut à $2k \equiv 1\ [17]$, soit, en multipliant par 9, inverse de 2 modulo 17, à $k \equiv 9\ [17]$. Dans ce cas, $9k + 4 \equiv 85 \equiv 0\ [17]$, donc 17 divise aussi $9k + 4$.

$$\boxed{(2k-1) \wedge (9k+4) = \begin{cases} 17 & \text{si } k \equiv 9\ [17], \\ 1 & \text{sinon.} \end{cases}}$$

Vérification : pour $k = 9$, $17 \wedge 85 = 17$. ✓

EXERCICE 10 ⋆⋆

Soit $d = u_n \wedge u_{n+1}$. Il divise $u_{n+1} - u_n = 2n + 1$, puis

$$4u_n - (2n+1)(2n-1) = 4n^2 + 4 - (4n^2 - 1) = 5.$$

Donc $d \in \{1, 5\}$. On cherche quand 5 divise les deux termes. Les carrés modulo 5 valent $0, 1, 4, 4, 1$ pour $n \equiv 0, 1, 2, 3, 4$, donc $5 \mid n^2 + 1$ si et seulement si $n \equiv 2$ ou $3\ [5]$, et $5 \mid (n+1)^2 + 1$ si et seulement si $n \equiv 1$ ou $2\ [5]$.

$$\boxed{u_n \wedge u_{n+1} = 5 \text{ si } n \equiv 2\ [5], \quad 1 \text{ sinon}}$$

Vérification : $u_2 \wedge u_3 = 5 \wedge 10 = 5$, et $u_7 \wedge u_8 = 50 \wedge 65 = 5$. ✓

EXERCICE 11 ⋆⋆

Soit $d_n = (2n+4) \wedge (3n+3)$. Il divise $3(2n+4) - 2(3n+3) = 6$, donc $d_n \in \{1, 2, 3, 6\}$. Les quatre valeurs sont atteintes : $d_0 = 4 \wedge 3 = 1$, $d_1 = 6 \wedge 6 = 6$, $d_3 = 10 \wedge 12 = 2$ et $d_4 = 12 \wedge 15 = 3$.

$$\boxed{\{(2n+4) \wedge (3n+3) \mid n \in \mathbb{N}\} = \{1, 2, 3, 6\}}$$

À retenir. La combinaison qui élimine n ne donne qu'un multiple du PGCD ; il faut ensuite vérifier quelles valeurs sont réellement atteintes. Ici, $2 \mid d_n$ si et seulement si n est impair, et $3 \mid d_n$ si et seulement si $n \equiv 1\ [3]$.

EXERCICE 12 ⋆⋆⋆

1. Le dernier reste non nul r_N est un entier naturel non nul, donc $r_N \geqslant 1$. La dernière division s'écrit $r_{N-1} = q_N r_N$, avec $r_{N-1} > r_N$: le quotient vérifie $q_N \geqslant 2$, d'où $r_{N-1} \geqslant 2r_N \geqslant 2$. Enfin, pour $k \leqslant N-1$, le quotient q_k est non nul puisque $r_{k-1} > r_k$, donc $r_{k-1} = q_k r_k + r_{k+1} \geqslant r_k + r_{k+1}$.

$$\boxed{r_N \geqslant 1 = F_2, \qquad r_{N-1} \geqslant 2 = F_3, \qquad r_{k-1} \geqslant r_k + r_{k+1}}$$

2. On montre par récurrence descendante sur k, de N à 1, que $r_k \geqslant F_{N-k+2}$. C'est vrai pour $k = N$ et $k = N-1$ d'après la question 1. Si c'est vrai aux rangs k et $k+1$, avec $k \geqslant 2$, alors

$$r_{k-1} \geqslant r_k + r_{k+1} \geqslant F_{N-k+2} + F_{N-k+1} = F_{N-k+3}.$$

Pour $k = 1$, on obtient $b = r_1 \geqslant F_{N+1}$.

$$\boxed{b \geqslant F_{N+1}}$$

Pour $a = 21$ et $b = 13$, l'algorithme comporte $N = 6$ divisions, de quotients $1, 1, 1, 1, 1, 2$, et $F_7 = 13 = b$: l'inégalité est une égalité. C'est pourquoi deux nombres de Fibonacci consécutifs sont le cas le plus lent de l'algorithme, comme l'annonçait l'introduction du cours.

3. En itérant la relation de récurrence, $F_{n+5} = 5F_{n+1} + 3F_n = 8F_n + 5F_{n-1}$. Pour $n \geqslant 2$, on a $F_{n-1} \geqslant 1$ et $F_n = F_{n-1} + F_{n-2} \leqslant 2F_{n-1}$, donc $5F_{n-1} > 4F_{n-1} \geqslant 2F_n$.

$$\boxed{F_{n+5} = 8F_n + 5F_{n-1} > 10\,F_n}$$

4. Par récurrence sur j, la question 3 donne $F_{5j+2} > 10^j F_2 = 10^j$ pour tout $j \geqslant 1$. Si b a k chiffres, alors $b < 10^k$. Si l'on avait $N \geqslant 5k+1$, la suite de Fibonacci étant croissante, on aurait

$$b \geqslant F_{N+1} \geqslant F_{5k+2} > 10^k,$$

ce qui est absurde.

$$\boxed{N \leqslant 5k}$$

À retenir. Le nombre d'étapes de l'algorithme d'Euclide croît comme le nombre de chiffres, c'est-à-dire comme le logarithme des entiers, et non comme les entiers eux-mêmes : c'est ce qui le rend utilisable sur des nombres de plusieurs centaines de chiffres, en cryptographie par exemple.

Entiers premiers entre eux

EXERCICE 13 ⋆

Dans les deux cas, on exhibe une relation de Bézout, et le théorème 4 conclut.

1. On a $(2n+1)^2 = 4(n^2+n) + 1$, d'où

$$\boxed{(2n+1) \times (2n+1) + (n^2+n) \times (-4) = 1}$$

2. La division de $3n^2 + 2n$ par $n+1$ donne $3n^2 + 2n = (n+1)(3n-1) + 1$, d'où

$$\boxed{(3n^2+2n) \times 1 + (n+1) \times (1-3n) = 1}$$

EXERCICE 14 ⋆

On applique la méthode du cours (section 12.4) : on calcule le PGCD, on cherche une solution particulière, puis on conclut par le lemme de Gauss.

(i) L'algorithme d'Euclide donne $247 = 221 + 26$, $221 = 8 \times 26 + 13$ et $26 = 2 \times 13$, donc $221 \wedge 247 = 13$. Comme 13 divise $221x + 247y$ pour tous entiers x et y, et ne divise pas 15 :

$$\boxed{\text{l'équation } 221x + 247y = 15 \text{ n'a aucune solution}}$$

(ii) On divise par 13 : l'équation équivaut à $17x + 19y = 1$. En remontant l'algorithme $19 = 17 + 2$, $17 = 8 \times 2 + 1$, on trouve

$$1 = 17 - 8 \times 2 = 17 - 8 \times (19 - 17) = 17 \times 9 + 19 \times (-8).$$

Si (x, y) est solution, $17(x - 9) = -19(y + 8)$; comme $17 \wedge 19 = 1$, le lemme de Gauss donne $19 \mid x - 9$, soit $x = 9 + 19k$, puis $y = -8 - 17k$. Réciproquement, ces couples conviennent.

$$\boxed{\mathcal{S} = \{(9 + 19k,\ -8 - 17k) \mid k \in \mathbb{Z}\}}$$

(iii) On divise par $3 = 27 \wedge 33$: l'équation équivaut à $9x - 11y = 33$, qui a la solution évidente $(0, -3)$. Si (x, y) est solution, $9x = 11(y + 3)$, donc $11 \mid x$ par le lemme de Gauss : $x = 11k$, puis $y = 9k - 3$.

$$\boxed{\mathcal{S} = \{(11k,\ 9k - 3) \mid k \in \mathbb{Z}\}}$$

(iv) Le couple $(2, -2)$ est solution. Si (x, y) en est une autre, $5(x - 2) = -3(y + 2)$, donc $3 \mid x - 2$.

$$\boxed{\mathcal{S} = \{(2 + 3k,\ -2 - 5k) \mid k \in \mathbb{Z}\}}$$

Piège. En (iii), l'erreur la plus répandue est de chercher un couple de Bézout de 27 et 33 avant de simplifier : on gagne du temps en divisant d'abord l'équation par le PGCD, qui divise bien 99.

EXERCICE 15 ⋆⋆

On factorise : $n^4 - n^2 = n^2(n - 1)(n + 1)$.

Divisibilité par 3. Parmi les trois entiers consécutifs $n - 1$, n, $n + 1$, l'un est multiple de 3.

Divisibilité par 4. Si n est pair, $4 \mid n^2$. Si n est impair, $n - 1$ et $n + 1$ sont pairs, et $4 \mid (n - 1)(n + 1)$.

Comme $3 \wedge 4 = 1$, la proposition 7 (i) conclut.

$$\boxed{12 \mid n^4 - n^2}$$

Piège. On ne peut pas remplacer 3 et 4 par 2 et 6 : un entier divisible par 2 et par 6 n'est pas nécessairement divisible par 12 (6 en est un exemple). L'hypothèse « premiers entre eux » est indispensable.

EXERCICE 16 ⋆⋆

1. Si (x, y) est solution, d divise x, qui divise m : il faut $d \mid m$. Réciproquement, si $d \mid m$, le couple (d, m) convient, puisque $d \wedge m = d$ et $d \vee m = m$.

$$\boxed{\text{le système a une solution si et seulement si } d \mid m}$$

2. On écrit $x = 12a$ et $y = 12b$ avec $a \wedge b = 1$ (proposition 5). Alors $x \vee y = 12ab$ d'après la proposition 7 (iii), et la condition devient $ab = 30$ avec $a \wedge b = 1$. Comme $30 = 2 \times 3 \times 5$, chaque facteur premier va entièrement dans a ou dans b : il y a $2^3 = 8$ couples (a, b).

$$\boxed{(x, y) \in \{(12, 360), (24, 180), (36, 120), (60, 72)\} \text{ et les quatre couples symétriques}}$$

3. De même $x = 18a$, $y = 18b$ avec $a \wedge b = 1$ et $a + b = 20$. Or $a \wedge b = a \wedge (a + b) = a \wedge 20$ (proposition 4) : il faut que a soit impair et non multiple de 5, avec $1 \leqslant a \leqslant 19$, soit $a \in \{1, 3, 7, 9, 11, 13, 17, 19\}$.

$$\boxed{(x, y) \in \{(18, 342), (54, 306), (126, 234), (162, 198), (198, 162), (234, 126), (306, 54), (342, 18)\}}$$

EXERCICE 17 ⋆⋆

On note $d = x \wedge y$, et l'on écrit $x = da$, $y = db$ avec $a \wedge b = 1$; alors $x \vee y = dab$.

(i) Comme $d \times (x \vee y) = xy$, l'équation, multipliée par d, devient $d^2 + xy = dx + dy$, c'est-à-dire $(x-d)(y-d) = 0$. Ainsi $x = d$ ou $y = d$, c'est-à-dire $x \mid y$ ou $y \mid x$.

$$\boxed{\mathcal{S} = \{(x,y) \in (\mathbb{N}^*)^2 \mid x \text{ divise } y \text{ ou } y \text{ divise } x\}}$$

(ii) L'équation s'écrit $d + dab = db + 9$, soit $d(1 + b(a-1)) = 9$. Le diviseur d de 9 vaut 1, 3 ou 9.

— Si $d = 9$: $b(a-1) = 0$, donc $a = 1$, et b est quelconque. On obtient $(9, 9b)$.

— Si $d = 3$: $b(a-1) = 2$, donc $(a,b) = (3,1)$ ou $(2,2)$; le second est exclu car $2 \wedge 2 \neq 1$. On obtient $(9,3)$.

— Si $d = 1$: $b(a-1) = 8$, donc $(a,b) \in \{(9,1),(5,2),(3,4),(2,8)\}$, et l'on exclut $(2,8)$. On obtient $(9,1)$, $(5,2)$ et $(3,4)$.

$$\boxed{\mathcal{S} = \{(9,9b) \mid b \in \mathbb{N}^*\} \cup \{(9,3),(9,1),(5,2),(3,4)\}}$$

Vérification : pour $(5,2)$, $1 + 10 = 2 + 9$; pour $(9,3)$, $3 + 9 = 3 + 9$. ✓

Piège. L'erreur la plus répandue est d'oublier la condition $a \wedge b = 1$ en fin de calcul : le couple $(a,b) = (2,8)$ donnerait $(x,y) = (2,8)$, pour lequel $2 + 8 \neq 8 + 9$.

EXERCICE 18 ⋆⋆

Soit $d = a \wedge b$, $a = da'$, $b = db'$ avec $a' \wedge b' = 1$. Alors $a + b = d(a' + b')$ et $a \vee b = da'b'$ (proposition 7 (iii)), donc, d'après la proposition 5,

$$(a+b) \wedge (a \vee b) = d \times \big((a' + b') \wedge a'b'\big).$$

Or $(a' + b') \wedge a' = b' \wedge a' = 1$ et de même $(a' + b') \wedge b' = 1$ (proposition 4), donc $(a' + b') \wedge a'b' = 1$ par la proposition 7 (ii).

$$\boxed{(a+b) \wedge (a \vee b) = a \wedge b}$$

À retenir. Le réflexe « on divise par le PGCD » ramène presque toujours une question sur a et b à une question sur deux entiers premiers entre eux, où le lemme de Gauss et la proposition 7 s'appliquent.

EXERCICE 19 ⋆⋆

On distingue selon le reste de n modulo 4. Dans chaque cas, les deux entiers proposés sont strictement supérieurs à 1 dès que $n > 6$, et leur PGCD divise leur différence.

— Si $n = 2k + 1$ est impair, $n = k + (k+1)$; deux entiers consécutifs sont premiers entre eux.

— Si $n = 4k$, $n = (2k-1) + (2k+1)$: le PGCD divise 2, et les deux entiers sont impairs, donc il vaut 1.

— Si $n = 4k + 2$, $n = (2k-1) + (2k+3)$: le PGCD divise 4, et les deux entiers sont impairs, donc il vaut 1. Pour $n \geqslant 10$, on a bien $2k - 1 \geqslant 3$.

$$\boxed{n = k + (k+1), \quad (2k-1) + (2k+1) \quad \text{ou} \quad (2k-1) + (2k+3)}$$

Piège. Pour $n = 6 = 4 + 2$, la troisième décomposition donnerait $1 + 5$, avec 1 exclu ; et 6 ne s'écrit ni $2 + 4$, ni $3 + 3$ avec des entiers premiers entre eux. C'est pourquoi l'énoncé impose $n > 6$.

EXERCICE 20 ⋆⋆

On fixe $z \in \mathbb{Z}$ et l'on résout $3x + 4y = 6 - 5z$. Le couple $(-1, 1)$ vérifie $3x + 4y = 1$, donc $(-(6-5z),\ 6-5z)$ est une solution particulière. Comme à l'exercice 14, le lemme de Gauss donne alors toutes les solutions : $x = 5z - 6 + 4k$, $y = 6 - 5z - 3k$, avec $k \in \mathbb{Z}$.

$$\boxed{\mathcal{S} = \{(5z - 6 + 4k,\ 6 - 5z - 3k,\ z) \mid (k, z) \in \mathbb{Z}^2\}}$$

Vérification : $3(5z - 6 + 4k) + 4(6 - 5z - 3k) + 5z = 6$. ✓
À retenir. Les solutions dépendent de deux paramètres entiers : c'est l'analogue, dans $\mathbb{Z}^3$, d'un plan, alors que les solutions de $ax + by = c$ forment une « droite » de points entiers à un paramètre.

EXERCICE 21 ⋆⋆

1. On écrit $x = \dfrac{p}{q}$ sous forme irréductible (proposition 6), avec $q \geqslant 1$. En multipliant l'équation par q^n :

$$p^n = -q(a_{n-1}p^{n-1} + a_{n-2}p^{n-2}q + \cdots + a_0 q^{n-1}).$$

Donc $q \mid p^n$. Comme $q \wedge p = 1$, on a $q \wedge p^n = 1$ (proposition 7 (ii)), et q, qui divise un entier avec lequel il est premier, vaut 1. Ainsi $x \in \mathbb{Z}$, et $a_0 = -x(x^{n-1} + a_{n-1}x^{n-2} + \cdots + a_1)$ est un multiple de x.

$$\boxed{x \in \mathbb{Z} \quad \text{et} \quad x \mid a_0}$$

2. Une solution rationnelle de $x^3 + x + 1 = 0$ serait un diviseur de 1, donc ± 1 ; or $1 + 1 + 1 = 3$ et $-1 - 1 + 1 = -1$ ne sont pas nuls. De même, $\sqrt[3]{5}$ est solution de $x^3 - 5 = 0$: s'il était rationnel, ce serait un entier, compris strictement entre 1 et 2 puisque $1 < 5 < 8$.

$$\boxed{x^3 + x + 1 = 0 \text{ n'a pas de solution rationnelle, et } \sqrt[3]{5} \notin \mathbb{Q}}$$

À retenir. Le résultat demande que le coefficient de x^n soit 1 : l'équation $2x - 1 = 0$ a la solution rationnelle $\dfrac{1}{2}$. Le chapitre 13, sur les polynômes, en donnera la forme générale.

EXERCICE 22 ⋆⋆⋆

1. Soit $d = p \wedge q$, et $p = dp'$, $q = dq'$ avec $p' \wedge q' = 1$ et $p' > q'$. Le quotient ne change pas :

$$\frac{p^2 + q^2}{p^2 - q^2} = \frac{d^2(p'^2 + q'^2)}{d^2(p'^2 - q'^2)} = \frac{p'^2 + q'^2}{p'^2 - q'^2}.$$

2. Soit $\delta = (p^2 - q^2) \wedge p^2$. Il divise p^2 et $p^2 - (p^2 - q^2) = q^2$. Or $p \wedge q = 1$ entraîne $p^2 \wedge q^2 = 1$, en appliquant deux fois la proposition 7 (ii). Donc $\delta = 1$.

$$\boxed{(p^2 - q^2) \wedge p^2 = 1}$$

3. Notons k l'entier $\dfrac{p^2 + q^2}{p^2 - q^2}$. Alors $2p^2 = (p^2 + q^2) + (p^2 - q^2) = (k + 1)(p^2 - q^2)$, donc $p^2 - q^2$ divise $2p^2$. Il est premier avec p^2 d'après la question 2, donc il divise 2 par le lemme de Gauss.

$$\boxed{p^2 - q^2 \mid 2}$$

4. Comme $p \geqslant q + 1$ et $q \geqslant 1$, on a $p^2 - q^2 \geqslant 2q + 1 \geqslant 3$, ce qui contredit la question 3.

$$\boxed{\text{pour tous } p > q \geqslant 1,\ \frac{p^2 + q^2}{p^2 - q^2} \text{ n'est jamais un entier}}$$

EXERCICE 23 ⋆⋆⋆

1. Par récurrence : $F_0 \wedge F_1 = 0 \wedge 1 = 1$, et si $F_n \wedge F_{n+1} = 1$, alors, d'après la proposition 4,

$$F_{n+1} \wedge F_{n+2} = F_{n+1} \wedge (F_{n+2} - F_{n+1}) = F_{n+1} \wedge F_n = 1.$$

2. On fixe n et l'on raisonne par récurrence double sur m. Pour $m = 1$, $F_1F_{n+1} + F_0F_n = F_{n+1}$; pour $m = 2$, $F_2F_{n+1} + F_1F_n = F_{n+1} + F_n = F_{n+2}$. Si la formule est vraie aux rangs m et $m+1$, on les additionne :

$$F_{n+m+2} = F_{n+m+1} + F_{n+m} = (F_{m+1} + F_m)F_{n+1} + (F_m + F_{m-1})F_n = F_{m+2}F_{n+1} + F_{m+1}F_n.$$

3. Par la question 2 et la proposition 4, $F_n \wedge F_{n+m} = F_n \wedge (F_mF_{n+1})$, puisque l'on retranche un multiple de F_n. Un diviseur commun à F_n et F_m divise évidemment F_mF_{n+1}. Réciproquement, un diviseur commun c à F_n et F_mF_{n+1} est premier avec F_{n+1}, puisqu'il divise F_n et que $F_n \wedge F_{n+1} = 1$; le lemme de Gauss donne $c \mid F_m$. Les deux couples ont donc les mêmes diviseurs communs.

$$\boxed{F_n \wedge F_{n+m} = F_n \wedge F_m}$$

4. Si $m = qn + r$, on applique q fois la question 3, en retranchant n à l'indice à chaque fois :

$$F_n \wedge F_m = F_n \wedge F_{m-n} = \cdots = F_n \wedge F_r.$$

Au dernier pas, si $r = 0$, on utilise directement $F_n \wedge F_n = F_n = F_n \wedge F_0$.

5. La question 4 dit que le couple (F_m, F_n) se transforme comme le couple (m, n) dans l'algorithme d'Euclide. On raisonne par récurrence forte sur n, pour tout m. Si $n \mid m$, alors $r = 0$ et $F_n \wedge F_m = F_n \wedge 0 = F_n = F_{n\wedge m}$. Sinon, $1 \leqslant r < n$, et l'hypothèse de récurrence appliquée au couple (n, r) donne

$$F_n \wedge F_m = F_r \wedge F_n = F_{r\wedge n} = F_{n\wedge m},$$

la dernière égalité venant de la proposition 4.

$$\boxed{F_n \wedge F_m = F_{n\wedge m}}$$

Par exemple, $F_{12} \wedge F_{18} = 144 \wedge 2584 = 8 = F_6$. ✓

À retenir. Le choix $F_0 = 0$, $F_1 = 1$ est essentiel. Avec la convention décalée $F_0 = F_1 = 1$, le résultat devient faux : on aurait $F_2 \wedge F_4 = 2 \wedge 5 = 1$, alors que $F_{2\wedge 4} = F_2 = 2$.

Nombres premiers

EXERCICE 24 ⋆

On divise par les nombres premiers successifs. On a $2024 = 8 \times 253$ et $253 = 11 \times 23$. Ensuite, $2025 = 81 \times 25$. Enfin, $2026 = 2 \times 1013$, et 1013 est premier : il n'est divisible par aucun des nombres premiers $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31$, qui sont tous ceux dont le carré ne dépasse pas 1013 (proposition 8).

$$\boxed{2024 = 2^3 \times 11 \times 23, \qquad 2025 = 3^4 \times 5^2, \qquad 2026 = 2 \times 1013}$$

Le théorème 6 donne le nombre de diviseurs positifs : $4 \times 2 \times 2 = 16$, puis $5 \times 3 = 15$, puis $2 \times 2 = 4$. Enfin, par la proposition 10 (iii), on prend le minimum ou le maximum des exposants.

$$\boxed{\tau(2024) = 16, \qquad \tau(2025) = 15, \qquad \tau(2026) = 4}$$

$$\boxed{2024 \wedge 2026 = 2, \qquad 2024 \vee 2026 = 2^3 \times 11 \times 23 \times 1013 = 2\,050\,312}$$

Seul $2025 = 45^2$ a un nombre impair de diviseurs : c'est un carré, ce que l'exercice 33 expliquera.

EXERCICE 25 ⋆⋆

Supposons que n soit le produit d'au moins trois nombres premiers, non nécessairement distincts : $n = p_1p_2p_3m$ avec $p_1 \leqslant p_2 \leqslant p_3$ et $m \geqslant 1$. Alors $p_1^3 \leqslant p_1p_2p_3 \leqslant n$, ce qui est exclu. Donc la décomposition de n (théorème 6) comporte un ou deux facteurs.

$$\boxed{n \text{ est premier ou produit de deux nombres premiers}}$$

Comme $7^3 = 343 \leqslant 391 < 512 = 8^3$, il suffit de vérifier que 2, 3, 5 et 7 ne divisent pas 391 : il est impair, la somme de ses chiffres vaut 13, il ne se termine ni par 0 ni par 5, et $391 = 7 \times 55 + 6$. Pour trouver les deux facteurs $p \leqslant q$, on cherche p parmi les nombres premiers de 11 à 19, puisque $p^2 \leqslant 391 < 400$: on trouve $391 = 17 \times 23$.

$$\boxed{391 = 17 \times 23}$$

EXERCICE 26 ⋆⋆

On a $p^2 - 1 = (p-1)(p+1)$, et $24 = 8 \times 3$ avec $8 \wedge 3 = 1$.

Divisibilité par 8. Comme p est impair, $p-1$ et $p+1$ sont deux entiers pairs consécutifs : l'un d'eux est multiple de 4, donc leur produit est multiple de 8.

Divisibilité par 3. Comme $p \geqslant 5$ est premier, $3 \nmid p$, donc $p \equiv \pm 1$ [3], et 3 divise $p-1$ ou $p+1$.

La proposition 7 (i) conclut.

$$\boxed{24 \mid p^2 - 1}$$

Par exemple $7^2 - 1 = 48$ et $11^2 - 1 = 120$; en revanche $3^2 - 1 = 8$, ce qui montre que l'hypothèse $p \geqslant 5$ est nécessaire.

EXERCICE 27 ⋆⋆

1. Les n entiers consécutifs $(n+1)! + 2$, $(n+1)! + 3$, …, $(n+1)! + (n+1)$ conviennent : pour $2 \leqslant k \leqslant n+1$, l'entier k divise $(n+1)!$, donc $(n+1)! + k$, qui est strictement plus grand que k.

$$\boxed{(n+1)! + k \text{ est divisible par } k, \text{ pour } k \in [\![2\,;n+1]\!]}$$

2. L'entier $N = n! + 1 \geqslant 2$ admet un diviseur premier $p \leqslant N$. Si l'on avait $p \leqslant n$, alors p diviserait $n!$, donc $N - n! = 1$, ce qui est absurde.

$$\boxed{n+1 \leqslant p \leqslant n! + 1}$$

Ainsi, pour tout n, il existe un nombre premier strictement plus grand que n : l'ensemble $\mathcal{P}$ n'est pas majoré, donc il est infini. C'est une variante de la preuve d'Euclide du chapitre 1.

EXERCICE 28 ⋆⋆

Soit $p < q$ deux nombres premiers consécutifs et $s = p + q$. Si $p = 2$, alors $q = 3$ et $s = 5$ est premier, donc n'est pas produit de deux nombres premiers.

Si $p \geqslant 3$, les entiers p et q sont impairs, donc s est pair, et $\dfrac{s}{2}$ est un entier strictement compris entre p et q. Il n'est pas premier, puisque p et q sont consécutifs. Supposons $s = ab$ avec a et b premiers. Comme $2 \mid ab$, le lemme d'Euclide donne $2 = a$ ou $2 = b$, et l'autre facteur vaut $\dfrac{s}{2}$, qui n'est pas premier : contradiction.

$$\boxed{p + q = ab \text{ avec } a, b \text{ premiers forcerait } \frac{p+q}{2} \text{ premier, entre } p \text{ et } q}$$

EXERCICE 29 ⋆⋆

Un tel nombre qui se termine par 0 est pair et supérieur à 10 : il n'est pas premier. Il reste les nombres $N_m = \sum_{k=0}^{m} 100^k$, qui comportent $m+1$ chiffres 1. Le nombre $N_0 = 1$ n'est pas premier, et $N_1 = 101$ l'est. Soit $m \geqslant 2$.

Si $m+1 = 2j$ est pair, avec $j \geqslant 2$, on regroupe les termes deux par deux :

$$N_m = (1+100)(1+10^4+\cdots+10^{4(j-1)}),$$

et les deux facteurs sont strictement supérieurs à 1.

Si $m+1$ est impair, avec $m+1 \geqslant 3$, on note R_{m+1} le nombre formé de $m+1$ chiffres 1. La formule $a^n - b^n$ (chapitre 3, proposition 5) donne

$$99\,N_m = 10^{2(m+1)} - 1 = (10^{m+1}-1)(10^{m+1}+1) = 9R_{m+1} \times (10^{m+1}+1).$$

Comme $m+1$ est impair, $10^{m+1} \equiv (-1)^{m+1} = -1$ [11], donc 11 divise $10^{m+1}+1$, et

$$N_m = R_{m+1} \times \frac{10^{m+1}+1}{11},$$

avec $R_{m+1} \geqslant 111$ et $\dfrac{10^{m+1}+1}{11} \geqslant 91$.

101 est le seul nombre premier de cette forme

Par exemple, $10\,101 = 3 \times 7 \times 13 \times 37 = 111 \times 91$, et $1\,010\,101 = 101 \times 10\,001$.

EXERCICE 30 ⋆⋆

1. Supposons qu'il n'y ait qu'un nombre fini de nombres premiers congrus à 3 modulo 4, que l'on note $p_1, \ldots, p_r$; on a $r \geqslant 1$, puisque 3 en fait partie. L'entier $N = 4p_1 \cdots p_r - 1$ est impair et congru à 3 modulo 4. Ses facteurs premiers sont impairs, donc congrus à 1 ou 3 modulo 4. S'ils étaient tous congrus à 1, leur produit N le serait aussi. L'un d'eux, q, est donc congru à 3 modulo 4 : c'est l'un des p_i, qui divise alors $4p_1 \cdots p_r - N = 1$. C'est absurde.

il y a une infinité de nombres premiers $p \equiv 3$ [4]

2. Même raisonnement avec $N = 6p_1 \cdots p_r - 1$, où $p_1 = 5$, …, p_r seraient tous les nombres premiers congrus à 5 modulo 6. Ni 2 ni 3 ne divisent N. Un nombre premier différent de 2 et 3 est congru à 1 ou 5 modulo 6, et un produit de nombres congrus à 1 l'est aussi ; comme $N \equiv 5$ [6], l'un de ses facteurs premiers est congru à 5, donc égal à un p_i, qui diviserait 1.

il y a une infinité de nombres premiers $p \equiv 5$ [6]

À retenir. Le même argument ne marche pas pour les nombres premiers congrus à 1 modulo 4 : un produit de facteurs congrus à 3 peut être congru à 1. L'exercice 51 traitera ce cas par une autre voie. Le résultat général, dû à Dirichlet (1837), affirme que toute progression $a+bn$ avec $a \wedge b = 1$ contient une infinité de nombres premiers.

EXERCICE 31 ⋆⋆

1. Supposons $\sqrt{n} = \dfrac{a}{b}$ avec $a \wedge b = 1$ et $b \geqslant 1$. Alors $nb^2 = a^2$, donc $b \mid a^2$. Or $b \wedge a^2 = 1$ (proposition 7 (ii)), donc $b = 1$, et $\sqrt{n} = a$ est un entier.

$$\boxed{\sqrt{n} \in \mathbb{N} \quad \text{ou} \quad \sqrt{n} \notin \mathbb{Q}}$$

2. Le quotient est strictement positif. S'il valait $\dfrac{p}{q}$ avec $p, q \in \mathbb{N}^*$, on aurait $q \ln 2 = p \ln 3$, soit $2^q = 3^p$. C'est impossible : le premier nombre est pair et le second impair, ou, ce qui revient au même, l'unicité de la décomposition (théorème 6) est contredite.

$$\boxed{\frac{\ln 2}{\ln 3} \notin \mathbb{Q}}$$

EXERCICE 32 ⋆⋆

Pour tout nombre premier p, la proposition 10 donne $v_p(a) + v_p(b) = v_p(ab)$, qui est pair puisque ab est un carré. Comme $a \wedge b = 1$, l'une des deux valuations est nulle (proposition 10 (iii)), donc l'autre est paire. Ainsi toutes les valuations de a et de b sont paires, et

$$\boxed{a = \prod_p p^{v_p(a)} = \Big(\prod_p p^{v_p(a)/2}\Big)^2 \quad \text{et de même pour } b}$$

Sans l'hypothèse, le résultat est faux : $2 \times 8 = 16$ est un carré, mais ni 2 ni 8 n'en est un. L'exercice 64 généralisera ce raisonnement aux puissances n-ièmes.

EXERCICE 33 ⋆⋆

1. Si $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, le théorème 6 donne $\tau(n) = (\alpha_1 + 1) \cdots (\alpha_r + 1)$. Ce produit est impair si et seulement si tous les α_i sont pairs, c'est-à-dire si n est un carré, comme à l'exercice 32.

$$\boxed{\tau(n) \text{ impair} \iff n \text{ carré parfait}}$$

2. L'application $d \mapsto \dfrac{n}{d}$ est une bijection de l'ensemble des diviseurs positifs de n sur lui-même, égale à sa propre réciproque. Donc $\Pi(n) = \displaystyle\prod_{d|n} \frac{n}{d}$, et

$$\Pi(n)^2 = \prod_{d|n} d \times \prod_{d|n} \frac{n}{d} = \prod_{d|n} n = n^{\tau(n)}.$$

$$\boxed{\Pi(n)^2 = n^{\tau(n)}}$$

3. Pour $n \geqslant 2$, l'égalité $\Pi(n) = n^2$ équivaut à $n^{\tau(n)} = n^4$, soit $\tau(n) = 4$. Comme $\tau(n) = \prod(\alpha_i + 1)$, il faut un seul facteur premier avec $\alpha_1 = 3$, ou deux facteurs premiers avec $\alpha_1 = \alpha_2 = 1$.

$$\boxed{n = p^3 \text{ ou } n = pq, \text{ avec } p \neq q \text{ premiers}}$$

Par exemple, les diviseurs de 15 sont $1, 3, 5, 15$, de produit $225 = 15^2$. ✓

EXERCICE 34 ⋆⋆

On note $u_n = 5^{2^n}$. Alors $u_{n+1} - 1 = u_n^2 - 1 = (u_n - 1)(u_n + 1)$. Comme $5 \equiv 1\ [4]$, on a $u_n \equiv 1\ [4]$, donc $u_n + 1 \equiv 2\ [4]$ et $v_2(u_n + 1) = 1$. La proposition 10 (i) donne $v_2(u_{n+1} - 1) = v_2(u_n - 1) + 1$, et $v_2(u_0 - 1) = v_2(4) = 2$.

$$\boxed{v_2(5^{2^n} - 1) = n + 2}$$

Vérification : $5^2 - 1 = 24 = 2^3 \times 3$ et $5^4 - 1 = 624 = 2^4 \times 39$. ✓

EXERCICE 35 ⋆⋆⋆

1. Les multiples de p^α dans $[\![1\,;n]\!]$ sont les kp^α avec $1 \leqslant k \leqslant \dfrac{n}{p^\alpha}$; il y en a $\left\lfloor \dfrac{n}{p^\alpha} \right\rfloor$. Un entier a une p-valuation égale à α s'il est multiple de p^α sans l'être de $p^{\alpha+1}$.

$$\boxed{\left\lfloor \frac{n}{p^\alpha} \right\rfloor \text{ multiples de } p^\alpha, \quad \left\lfloor \frac{n}{p^\alpha} \right\rfloor - \left\lfloor \frac{n}{p^{\alpha+1}} \right\rfloor \text{ entiers de valuation } \alpha}$$

2. Les termes sont nuls dès que $p^\alpha > n$. Par la proposition 10 (i), $v_p(n!) = \sum_{k=1}^{n} v_p(k)$. On écrit $v_p(k)$ comme le nombre d'entiers $\alpha \geqslant 1$ tels que $p^\alpha \mid k$, et l'on échange les deux sommes finies : $v_p(n!)$ est le nombre de couples (k, α) tels que $p^\alpha \mid k$, et, pour chaque α, il y a $\left\lfloor \dfrac{n}{p^\alpha} \right\rfloor$ entiers k qui conviennent, d'après la question 1.

$$\boxed{v_p(n!) = \sum_{\alpha \geqslant 1} \left\lfloor \frac{n}{p^\alpha} \right\rfloor}$$

3. Le nombre de zéros finaux est le plus grand entier k tel que $10^k = 2^k 5^k$ divise 1000!, c'est-à-dire $\min\big(v_2(1000!), v_5(1000!)\big)$. La formule donne

$$v_5(1000!) = 200 + 40 + 8 + 1 = 249, \qquad v_2(1000!) = 500 + 250 + 125 + 62 + 31 + 15 + 7 + 3 + 1 = 994.$$

$$\boxed{1000! \text{ se termine par } 249 \text{ zéros}}$$

4. On montre d'abord que, pour tous réels $x, y \geqslant 0$,

$$\lfloor 2x \rfloor + \lfloor 2y \rfloor \geqslant \lfloor x \rfloor + \lfloor y \rfloor + \lfloor x + y \rfloor.$$

En écrivant $x = \lfloor x \rfloor + a$ et $y = \lfloor y \rfloor + b$ avec $a, b \in [0, 1[$, les parties entières se simplifient, et l'inégalité équivaut à $\lfloor 2a \rfloor + \lfloor 2b \rfloor \geqslant \lfloor a + b \rfloor$. Si $a + b < 1$, le membre de droite est nul. Sinon, l'un des deux réels a ou b est supérieur à $\dfrac{1}{2}$, et le membre de gauche vaut au moins $1 = \lfloor a + b \rfloor$.

On applique cette inégalité avec $x = \dfrac{r}{p^\alpha}$ et $y = \dfrac{s}{p^\alpha}$, puis on somme sur α : la question 2 donne, pour tout nombre premier p,

$$v_p\big((2r)!\,(2s)!\big) \geqslant v_p\big((r+s)!\,r!\,s!\big).$$

D'après la proposition 10 (ii), le dénominateur divise le numérateur.

$$\boxed{\frac{(2r)!\,(2s)!}{(r+s)!\,r!\,s!} \in \mathbb{N}}$$

Pour $s = 0$, on retrouve que $\dbinom{2r}{r} = \dfrac{(2r)!}{r!\,r!}$ est un entier. Pour $r = s = 1$, le quotient vaut $\dfrac{2 \times 2}{2} = 2$. ✓

EXERCICE 36 ⋆

On écrit $n = \sum_{k=0}^{m} c_k 10^k$ en base 10 et l'on utilise la compatibilité des congruences avec les opérations (chapitre 2, proposition 10).

- Comme $10 \equiv 0$ [2], [5] et [10], on a $n \equiv c_0$ modulo 2, 5 et 10 : on regarde le dernier chiffre.
- Comme $100 \equiv 0$ [4] et $1000 \equiv 0$ [8], on a $n \equiv \overline{c_1 c_0}$ [4] et $n \equiv \overline{c_2 c_1 c_0}$ [8] : on regarde le nombre formé par les deux, ou les trois, derniers chiffres.
- Comme $10 \equiv 1$ [9], donc aussi modulo 3, on a $n \equiv \sum c_k$ modulo 3 et 9 : on regarde la somme des chiffres.
- Comme $10 \equiv -1$ [11], on a $n \equiv \sum (-1)^k c_k$ [11] : on regarde la somme alternée des chiffres, en partant des unités.
- Comme $2 \wedge 3 = 1$, un entier est divisible par 6 si et seulement s'il l'est par 2 et par 3 (proposition 7 (i)).

Pour 14 652 : le nombre 52 est divisible par 4, mais $652 = 8 \times 81 + 4$ ne l'est pas par 8, donc $v_2 = 2$ et $14\,652 = 4 \times 3663$. La somme des chiffres de 3663 vaut 18, donc $9 \mid 3663 = 9 \times 407$, et $4 + 0 + 7 = 11$ n'est pas multiple de 3. La somme alternée de 407 vaut $7 - 0 + 4 = 11$, donc $407 = 11 \times 37$, et 37 est premier.

$$\boxed{14\,652 = 2^2 \times 3^2 \times 11 \times 37}$$

EXERCICE 37 ⋆

1. Modulo 13, on a $2^6 = 64 \equiv -1$, donc $2^{12} \equiv 1$, et $3^3 = 27 \equiv 1$. Ainsi

$$2^{70} = (2^{12})^5 \times 2^{10} \equiv 1024 \equiv 10, \qquad 3^{70} = (3^3)^{23} \times 3 \equiv 3,$$

et $2^{70} + 3^{70} \equiv 13 \equiv 0$ [13].

$$\boxed{13 \mid 2^{70} + 3^{70}}$$

2. Les puissances de 2 modulo 10 valent $2, 4, 8, 6, 2, \ldots$: elles sont périodiques de période 4 à partir de l'exposant 1, puisque $2^5 = 32 \equiv 2$ [10]. Comme $136\,279\,841 = 4 \times 34\,069\,960 + 1$, on a $2^{136\,279\,841} \equiv 2$ [10].

$$\boxed{\text{le dernier chiffre est 1}}$$

3. D'après le petit théorème de Fermat, $2^{18} \equiv 1$ [19] : il suffit de connaître l'exposant 2^{6k+2} modulo 18. Or $2^{6k+2} = 4 \times 64^k \equiv 4$ [9], puisque $64 \equiv 1$ [9], et cet entier est pair ; l'entier $2^{6k+2} - 4$ est donc divisible par 9 et par 2, donc par 18. En écrivant $2^{6k+2} = 18j + 4$:

$$2^{2^{6k+2}} + 3 = (2^{18})^j \times 2^4 + 3 \equiv 16 + 3 = 19 \equiv 0 \text{ [19]}.$$

$$\boxed{19 \mid 2^{2^{6k+2}} + 3}$$

À retenir. Pour calculer a^N modulo un nombre premier p, on réduit d'abord l'exposant N modulo $p - 1$: c'est l'usage le plus fréquent du petit théorème de Fermat.

EXERCICE 38 ⋆

On suit la méthode de la section 12.6.2 : si $a \wedge n = 1$, on multiplie par un inverse de a modulo n.
(i) $5 \times 3 = 15 \equiv 1\ [7]$, donc $x \equiv 3\ [7]$.
(ii) $3 \times 13 = 39 \equiv 1\ [19]$, donc $x \equiv 13 \times 4 = 52 \equiv 14\ [19]$.
(iii) Comme 97 est premier et ne divise pas 23, le lemme d'Euclide donne $97 \mid x$, soit $x \equiv 0\ [97]$.
(iv) L'égalité $105 = 13 \times 8 + 1$ montre que $-13 \equiv 92$ est un inverse de 8 modulo 105, d'où

$$x \equiv 92 \times 7 = 644 \equiv 14\ [105].$$

(v) Ici $4 \wedge 12 = 4$: on ne peut pas inverser 4. On revient à la définition : $12 \mid 4x - 8$ si et seulement si $3 \mid x - 2$.
(vi) Si $12 \mid 4x - 6$, alors $4 \mid 6$, ce qui est faux.

$$\boxed{\text{(i) } x \equiv 3\ [7];\ \text{(ii) } x \equiv 14\ [19];\ \text{(iii) } x \equiv 0\ [97];\ \text{(iv) } x \equiv 14\ [105];\ \text{(v) } x \equiv 2\ [3];\ \text{(vi) aucune solution}}$$

Piège. En (v), l'erreur la plus répandue est de « diviser par 4 » en gardant le module 12, ce qui donne $x \equiv 2\ [12]$ et perd les solutions $x = 5$ et $x = 8$. Comme l'a montré la remarque de la section 12.6.1, on ne divise pas une congruence : on divise l'égalité $4x - 8 = 12k$, module compris.

EXERCICE 39 ⋆

On cherche une combinaison qui élimine a : $9(2a + 3b) - 2(9a + 5b) = 17b$. Si $17 \mid 2a + 3b$, alors $17 \mid 2(9a + 5b)$, et comme $17 \wedge 2 = 1$, le lemme de Gauss donne $17 \mid 9a + 5b$. Réciproquement, si $17 \mid 9a + 5b$, alors $17 \mid 9(2a + 3b)$, et $17 \wedge 9 = 1$ donne $17 \mid 2a + 3b$.

$$\boxed{17 \mid 2a + 3b \iff 17 \mid 9a + 5b}$$

EXERCICE 40 ⋆⋆

La première congruence équivaut à $y \equiv 6 - 4x\ [12]$. En reportant dans la seconde, le système équivaut à

$$\begin{cases} y \equiv 6 - 4x\ [12] \\ 24 - 15x \equiv 3\ [12] \end{cases}$$

La seconde ligne s'écrit $15x \equiv 21\ [12]$, soit $3x \equiv 9\ [12]$, c'est-à-dire $12 \mid 3(x - 3)$, ou encore $4 \mid x - 3$. On pose $x = 3 + 4k$; alors $6 - 4x = -6 - 16k \equiv 6 + 8k\ [12]$.

$$\boxed{\mathcal{S} = \{(3 + 4k,\ 6 + 8k + 12\ell) \mid (k, \ell) \in \mathbb{Z}^2\}}$$

Modulo 12, il y a trois solutions : $(3, 6)$, $(7, 2)$ et $(11, 10)$. Vérification pour $(7, 2)$: $30 \equiv 6$ et $15 \equiv 3\ [12]$. ✓

EXERCICE 41 ⋆⋆

On écrit $a = b + kn$. La formule du binôme donne

$$a^n = b^n + \binom{n}{1} b^{n-1} kn + \sum_{j=2}^{n} \binom{n}{j} b^{n-j} k^j n^j.$$

Le deuxième terme vaut $kn^2 b^{n-1}$, et les suivants contiennent n^j avec $j \geqslant 2$.

$$\boxed{a^n \equiv b^n\ [n^2]}$$

Comme à l'exercice 6, c'est le coefficient $\binom{n}{1} = n$ qui fournit le second facteur n.

EXERCICE 42 ⋆⋆

D'après le petit théorème de Fermat, $3^6 \equiv 1\ [7]$, donc 3^n ne dépend que du reste de n modulo 6 :

n mod 6	0	1	2	3	4	5
3^n mod 7	1	3	2	6	4	5
inverse modulo 7	1	5	4	6	2	3

La condition $n\,3^n \equiv 1\ [7]$ s'écrit $n \equiv (3^n)^{-1}\ [7]$. Pour chacun des six restes j de n modulo 6, on cherche parmi $j, j+6, \ldots, j+36$ l'entier congru à l'inverse modulo 7 : on trouve 36, 19, 32, 27, 16 et 17. Comme $6 \wedge 7 = 1$, la condition ne dépend que de n modulo 42.

$$\boxed{n \equiv 16,\ 17,\ 19,\ 27,\ 32 \text{ ou } 36\ [42]}$$

Vérification pour $n = 16$: $3^{16} \equiv 3^4 \equiv 4$ et $16 \times 4 = 64 \equiv 1\ [7]$. ✓

EXERCICE 43 ⋆⋆

1. Modulo 5 : $4n^2 + 1 \equiv 0$ équivaut à $4n^2 \equiv 4$, soit $n^2 \equiv 1$, c'est-à-dire $n \equiv \pm 1\ [5]$. Modulo 13, en multipliant par 10, inverse de 4 : $n^2 \equiv -10 \equiv 3$, ce qui équivaut à $n \equiv \pm 4\ [13]$, puisque la table des carrés modulo 13 montre que $4^2 = 16$ et $9^2 = 81$ sont les seuls carrés congrus à 3. L'entier $n = 56$ vérifie $56 \equiv 1\ [5]$ et $56 \equiv 4\ [13]$, et tous les $56 + 65k$ aussi.

$$\boxed{65 \mid 4n^2 + 1 \text{ pour tout } n = 56 + 65k,\ k \in \mathbb{N}}$$

Vérification : $4 \times 56^2 + 1 = 12\,545 = 65 \times 193$. ✓

2. Les puissances de 2 sont périodiques de période 4 modulo 5 $(2, 4, 3, 1)$ et de période 12 modulo 13 $(2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1)$. Ainsi $5 \mid 2^n - 3$ si et seulement si $n \equiv 3\ [4]$, et $13 \mid 2^n - 3$ si et seulement si $n \equiv 4\ [12]$: il y a une infinité de multiples de chaque sorte. Mais si 65 divisait $2^n - 3$, on aurait $n \equiv 4\ [12]$, donc $n \equiv 0\ [4]$, et $n \equiv 3\ [4]$: c'est impossible.

$$\boxed{\text{infinité de multiples de 5 } (n \equiv 3\ [4]),\ \text{de 13 } (n \equiv 4\ [12]),\ \text{aucun de 65}}$$

EXERCICE 44 ⋆⋆

Pour p premier, le petit théorème de Fermat donne $n^p \equiv n\ [p]$, et donc, en multipliant par une puissance de n, $n^{k(p-1)+1} \equiv n\ [p]$ pour tout $k \in \mathbb{N}$.

— Pour n^5 : $5 = 4 \times 1 + 1 = 2 \times 2 + 1 = 1 \times 4 + 1$, donc $n^5 \equiv n$ modulo 2, 3 et 5.

— Pour n^7 : $7 = 6 \times 1 + 1 = 3 \times 2 + 1 = 1 \times 6 + 1$, donc $n^7 \equiv n$ modulo 2, 3 et 7.

Les nombres 2, 3, 5, et de même 2, 3, 7, sont premiers entre eux deux à deux ; on applique deux fois la proposition 7 (i).

$$\boxed{30 \mid n^5 - n \qquad \text{et} \qquad 42 \mid n^7 - n}$$

EXERCICE 45 ⋆⋆

Modulo 5, on a $15 \equiv 0$, $-7 \equiv 3$ et $9 \equiv 4$: une solution vérifierait $3y^2 \equiv 4$, soit, en multipliant par 2, inverse de 3, $y^2 \equiv 8 \equiv 3\ [5]$. Or les carrés modulo 5 sont $0, 1, 4, 4, 1$.

$$\boxed{\text{aucune solution : 3 n'est pas un carré modulo 5}}$$

À retenir. Pour montrer qu'une équation n'a pas de solution entière, on cherche un module pour lequel elle n'en a pas ; le choix de 5 est dicté par le coefficient 15, qui disparaît.

EXERCICE 46 ⋆⋆

1. Si $x = 3k + r$, la formule du binôme donne $x^3 = 27k^3 + 27k^2r + 9kr^2 + r^3 \equiv r^3$ [9]. Les cubes modulo 9 sont donc $0^3 = 0$, $1^3 = 1$ et $2^3 = 8$.

$$\boxed{x^3 \equiv n \text{ [9] a une solution si et seulement si } n \equiv 0,\ 1 \text{ ou } 8 \text{ [9]}}$$

2. Chaque cube est congru à 0, 1 ou -1 modulo 9, donc une somme de trois cubes est congrue à un entier de $[\![-3\,;3]\!]$, c'est-à-dire à $0, 1, 2, 3, 6, 7$ ou 8. Or $11\,111 \equiv 5$ [9], par la somme de ses chiffres.

$$\boxed{a^3 + b^3 + c^3 \neq 11\,111}$$

3. Comme $117 = 9 \times 13$, une solution vérifierait $x^3 \equiv 5$ [9], ce qui est impossible d'après la question 1.

$$\boxed{x^3 + 117y^3 = 5 \text{ n'a pas de solution dans } \mathbb{Z}^2}$$

La démonstration élémentaire tient en une ligne ; elle ne dit rien, en revanche, des solutions rationnelles, que l'approche de Finkelstein et London permet d'étudier.

EXERCICE 47 ⋆⋆

On travaille modulo 9, où un entier est congru à la somme de ses chiffres. Comme $2^6 = 64 \equiv 1$ [9], on a $2^{29} = (2^6)^4 \times 2^5 \equiv 32 \equiv 5$ [9]. Si m est le chiffre manquant, la somme des neuf chiffres vaut $45 - m \equiv -m$ [9]. Donc $-m \equiv 5$, soit $m \equiv 4$ [9], et $m = 4$ puisque $0 \leqslant m \leqslant 9$.

$$\boxed{\text{le chiffre manquant est } 4}$$

Vérification : $2^{29} = 536\,870\,912$. ✓

EXERCICE 48 ⋆⋆

On a $36 - 25 = 11$, donc le minimum vaut au plus 11. Les puissances de 36 se terminent par 6 et celles de 5 par 5, donc $36^n - 5^m$ se termine par 1 s'il est positif, et $5^m - 36^n$ se termine par 9 s'il est positif. Les seules valeurs inférieures à 11 possibles pour $|36^n - 5^m|$ sont donc 1 et 9.

— $36^n - 5^m = 1$ est impossible : $36 \equiv 1$ [7], donc 7 divise $36^n - 1 = 5^m$, ce qui contredit le lemme d'Euclide.

— $5^m - 36^n = 9$ est impossible : 3 diviserait $5^m = 9 + 36^n$.

$$\boxed{\min\{|36^n - 5^m|\} = 11,\ \text{atteint pour } n = 1,\ m = 2}$$

EXERCICE 49 ⋆⋆

Le repunit à k chiffres vaut $R_k = \dfrac{10^k - 1}{9}$. Il est impair et se termine par 1, donc ni 2 ni 5 ne divisent un repunit. Le nombre 3 divise $R_3 = 111 = 3 \times 37$. Soit enfin p premier différent de 2, 3 et 5. Comme $p \nmid 10$, le petit théorème de Fermat donne $p \mid 10^{p-1} - 1 = 9R_{p-1}$, et comme $p \wedge 9 = 1$, le lemme de Gauss donne $p \mid R_{p-1}$.

$$\boxed{\text{les nombres premiers qui divisent un repunit sont tous les nombres premiers sauf 2 et 5}}$$

Par exemple, $7 \mid R_6 = 111\,111 = 3 \times 7 \times 11 \times 13 \times 37$.

EXERCICE 50 ⋆⋆⋆

Si n n'est pas premier, il s'écrit $n = ab$ avec $1 < a < n$. Alors a figure dans le produit $(n-1)!$, donc $a \mid (n-1)!$. Si l'on avait $(n-1)! \equiv -1\ [n]$, l'entier a, qui divise n, diviserait $(n-1)!+1$, donc 1 : c'est absurde.

Si $n = p$ est premier. Pour $p = 2$ et $p = 3$, on a $1! = 1 \equiv -1\ [2]$ et $2! = 2 \equiv -1\ [3]$. Soit $p \geqslant 5$. D'après la proposition 12, chaque $k \in [\![1\,;p-1]\!]$ admet un inverse modulo p, et un seul dans $[\![1\,;p-1]\!]$, que l'on note k'. On a $k' = k$ si et seulement si $k^2 \equiv 1$, c'est-à-dire $p \mid (k-1)(k+1)$, soit $k \in \{1, p-1\}$ par le lemme d'Euclide. Les entiers de $[\![2\,;p-2]\!]$ se regroupent donc en paires $\{k, k'\}$ de produit congru à 1, et

$$(p-1)! = 1 \times \Big(\prod_{k=2}^{p-2} k\Big) \times (p-1) \equiv 1 \times 1 \times (-1)\ [p].$$

$$\boxed{n \text{ premier} \iff (n-1)! \equiv -1\ [n]}$$

Pour $p = 7$, les paires sont $\{2,4\}$ et $\{3,5\}$, et $6! = 720 = 7 \times 103 - 1$. ✓

À retenir. Ce critère de primalité est exact mais inutilisable en pratique : calculer $(n-1)!$ modulo n demande $n-2$ multiplications, bien plus que les essais de divisions jusqu'à $\sqrt{n}$.

EXERCICE 51 ⋆⋆⋆

1. Soit x tel que $x^2 \equiv -1\ [p]$. Alors $p \nmid x$, et le petit théorème de Fermat donne, p étant impair,

$$1 \equiv x^{p-1} = (x^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}}\ [p].$$

Comme $p \geqslant 3$, on a $1 \not\equiv -1\ [p]$: l'exposant $\dfrac{p-1}{2}$ est pair, c'est-à-dire $p \equiv 1\ [4]$.

$$\boxed{p \equiv 1\ [4]}$$

2. Supposons qu'il n'y ait qu'un nombre fini de nombres premiers congrus à 1 modulo 4, notés $p_1 = 5, \ldots, p_r$, et posons $x = 2p_1 \cdots p_r$ et $N = x^2 + 1$. L'entier N est impair et supérieur à 2, donc admet un facteur premier impair q, qui vérifie $x^2 \equiv -1\ [q]$. D'après la question 1, $q \equiv 1\ [4]$, donc q est l'un des p_i ; il divise alors x et x^2+1, donc 1, ce qui est absurde.

$$\boxed{\text{il y a une infinité de nombres premiers } p \equiv 1\ [4]}$$

3. On pose $h = \dfrac{p-1}{2}$, qui est pair. On regroupe les facteurs de $(p-1)!$ en k et $p-k \equiv -k$, pour $1 \leqslant k \leqslant h$:

$$(p-1)! = \prod_{k=1}^{h} k \times \prod_{k=1}^{h} (p-k) \equiv \prod_{k=1}^{h} k \times \prod_{k=1}^{h} (-k) = (-1)^h (h!)^2 = (h!)^2\ [p].$$

Le théorème de Wilson de l'exercice 50 donne $(p-1)! \equiv -1$.

$$\boxed{\Big(\big(\frac{p-1}{2}\big)!\Big)^2 \equiv -1\ [p]}$$

Pour $p = 13$, $6! = 720 = 13 \times 55 + 5$ et $5^2 = 25 \equiv -1\ [13]$. ✓

À retenir. Les questions 1 et 3 forment une équivalence : pour p premier impair, -1 est un carré modulo p si et seulement si $p \equiv 1\ [4]$. C'est le point de départ du théorème de Fermat sur les sommes de deux carrés.

Exercices de synthèse

EXERCICE 52 ⋆⋆

1. Fausse. Avec $a = 4$, $b = c = 2$: 4 divise $bc = 4$, mais ne divise ni b ni c. Le lemme de Gauss demande $a \wedge b = 1$, et non $a \nmid b$.

2. Vraie. Par la proposition 4, $(a+b) \wedge b = b \wedge ((a+b) - b) = b \wedge a$.

3. Vraie. C'est la proposition 7 (ii).

4. Vraie. Par le lemme d'Euclide, $p \mid a$, donc $p^2 \mid a^2$. On peut aussi dire que $v_p(a^2) = 2v_p(a)$ est un entier pair non nul, donc au moins égal à 2.

5. Fausse. Avec $n = 3$: $2 \equiv 2$ et $1 \equiv 4$ [3], mais $2^1 = 2$ et $2^4 = 16 \equiv 1$ [3]. On peut remplacer la base par un entier congru, jamais l'exposant ; le petit théorème de Fermat dit seulement que, modulo p premier, on peut réduire l'exposant modulo $p - 1$.

6. Fausse. On a $2^{11} - 1 = 2047 = 23 \times 89$. La réciproque est vraie : si $2^n - 1$ est premier, alors n est premier (exercice 56).

7. Vraie. Le membre de gauche est pair. Plus généralement, $6 \wedge 10 = 2$ ne divise pas 7.

8. Vraie. C'est la proposition 8, qui fonde le crible d'Ératosthène.

9. Vraie. On a $72 = 2^3 \times 3^2$ et $108 = 2^2 \times 3^3$, et le théorème 6 donne $(3+1)(2+1) = 12 = (2+1)(3+1)$ diviseurs positifs.

10. Fausse. Avec $n = 8$ et $a = 3$: $9 \equiv 1$ [8], mais $3 \not\equiv \pm 1$ [8]. L'implication est vraie lorsque n est premier, par le lemme d'Euclide appliqué à $(a-1)(a+1)$, comme dans l'exercice 50.

$$\boxed{\text{vraies : 2, 3, 4, 7, 8, 9 ; \quad fausses : 1, 5, 6, 10}}$$

EXERCICE 53 ⋆⋆

1. On note $d = n \wedge m$, et l'on raisonne par double inclusion. Comme d divise n et m, la proposition 9 du chapitre 11 donne $\mathbb{U}_d \subset \mathbb{U}_n$ et $\mathbb{U}_d \subset \mathbb{U}_m$, donc $\mathbb{U}_d \subset \mathbb{U}_n \cap \mathbb{U}_m$. Réciproquement, soit $z \in \mathbb{U}_n \cap \mathbb{U}_m$; il est non nul. La relation de Bézout (théorème 3) fournit des entiers relatifs u et v tels que $nu + mv = d$, et les règles de calcul dans le groupe $(\mathbb{C}^*, \times)$ (chapitre 11, proposition 4) donnent

$$z^d = z^{nu+mv} = (z^n)^u \, (z^m)^v = 1.$$

$$\boxed{\mathbb{U}_n \cap \mathbb{U}_m = \mathbb{U}_{n \wedge m}}$$

Piège. L'erreur la plus répandue est de croire que deux ensembles $\mathbb{U}_n$ et $\mathbb{U}_m$ distincts n'ont que 1 en commun : -1 appartient à $\mathbb{U}_4$ et à $\mathbb{U}_6$, puisque $4 \wedge 6 = 2$. L'intersection se réduit à $\{1\}$ exactement lorsque n et m sont premiers entre eux.

2. On note $L = n \vee m$, et l'on raisonne encore par double inclusion. Si $z \in \mathbb{U}_n$ et $w \in \mathbb{U}_m$, l'entier L est un multiple de n et de m, donc $(zw)^L = (z^n)^{L/n} (w^m)^{L/m} = 1$, et $zw \in \mathbb{U}_L$. Réciproquement, avec $nu + mv = d$ comme à la question 1, et $L = \dfrac{nm}{d}$ (proposition 7 (iii)), on obtient

$$\mathrm{e}^{2\mathrm{i}\pi/L} = \mathrm{e}^{2\mathrm{i}\pi d/(nm)} = \mathrm{e}^{2\mathrm{i}\pi(nu+mv)/(nm)} = \mathrm{e}^{2\mathrm{i}\pi v/n} \, \mathrm{e}^{2\mathrm{i}\pi u/m}.$$

Pour tout $k \in \mathbb{Z}$, l'élément $\mathrm{e}^{2\mathrm{i}k\pi/L}$ de $\mathbb{U}_L$ s'écrit donc $\left(\mathrm{e}^{2\mathrm{i}\pi v/n}\right)^k \left(\mathrm{e}^{2\mathrm{i}\pi u/m}\right)^k$, produit d'un élément de $\mathbb{U}_n$ et d'un élément de $\mathbb{U}_m$. Comme tout élément de $\mathbb{U}_L$ est de cette forme (chapitre 4, proposition 21), on a l'inclusion réciproque.

$$\boxed{\mathbb{U}_n \mathbb{U}_m = \mathbb{U}_{n \vee m}}$$

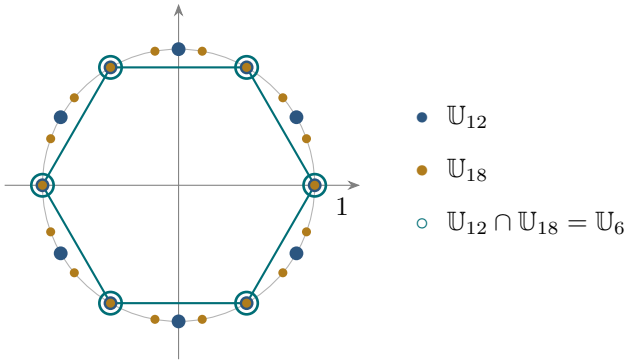
3. Lorsque $n \wedge m = 1$, la proposition 7 (iii) donne $n \vee m = nm$, et l'existence de l'écriture est la question 2. Pour l'unicité, supposons $zw = z'w'$ avec $z, z' \in \mathbb{U}_n$ et $w, w' \in \mathbb{U}_m$. Comme $\mathbb{U}_n$ et $\mathbb{U}_m$ sont des sous-groupes de $(\mathbb{C}^*, \times)$, le complexe $zz'^{-1} = w'w^{-1}$ appartient à $\mathbb{U}_n \cap \mathbb{U}_m = \mathbb{U}_1 = \{1\}$, d'après la question 1. Ainsi $z = z'$, puis $w = w'$.

$$\boxed{\text{si } n \wedge m = 1, \ (z, w) \longmapsto zw \text{ est une bijection de } \mathbb{U}_n \times \mathbb{U}_m \text{ sur } \mathbb{U}_{nm}}$$

L'hypothèse est indispensable : avec $n = m = 2$, on a $(-1) \times (-1) = 1 \times 1$, et l'application n'est pas injective.

4. Les sommets du dodécagone régulier inscrit dans le cercle unité et passant par le point d'affixe 1 ont pour affixes les $e^{2ik\pi/12}$, c'est-à-dire les éléments de $\mathbb{U}_{12}$ (chapitre 4, proposition 21) ; de même, ceux du second polygone forment $\mathbb{U}_{18}$. On a $12 = 2^2 \times 3$ et $18 = 2 \times 3^2$, donc $12 \wedge 18 = 6$ et $12 \vee 18 = 36$, et les questions 1 et 2 concluent.

$$\boxed{\text{6 sommets communs, ceux de l'hexagone régulier } \mathbb{U}_6 \ ; \quad \text{les produits forment } \mathbb{U}_{36}}$$



Les gros points sont les sommets du dodécagone, les petits ceux du polygone à 18 côtés ; ils ne coïncident qu'aux six sommets cerclés, tous les 60 degrés, car 60 est le plus petit multiple commun de 30 et de 20.

À retenir. Par la proposition 9 du chapitre 11, l'inclusion entre les $\mathbb{U}_n$ est la divisibilité entre les indices. L'exercice montre que l'intersection et le produit y jouent les rôles du PGCD et du PPCM, exactement comme $a\mathbb{Z} + b\mathbb{Z}$ et $a\mathbb{Z} \cap b\mathbb{Z}$ dans la définition du cours ; la question 3 annonce, sous forme multiplicative, le théorème chinois.

EXERCICE 54 ⋆⋆⋆

1. On a $\sigma(6) = 1 + 2 + 3 + 6 = 12$ et $\sigma(28) = 1 + 2 + 4 + 7 + 14 + 28 = 56$.

$$\boxed{\sigma(6) = 2 \times 6 \qquad \text{et} \qquad \sigma(28) = 2 \times 28}$$

2. Les diviseurs de p^α sont $1, p, \dots, p^\alpha$, donc $\sigma(p^\alpha) = \dfrac{p^{\alpha+1} - 1}{p - 1}$. Si $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, le théorème 6 dit que les diviseurs de n sont les $p_1^{\beta_1} \cdots p_r^{\beta_r}$, chacun obtenu une seule fois, avec $0 \leqslant \beta_i \leqslant \alpha_i$. En développant le produit des sommes (chapitre 3), on obtient chacun de ces termes exactement une fois.

$$\boxed{\sigma(n) = \prod_{i=1}^{r} \left(1 + p_i + \cdots + p_i^{\alpha_i}\right) = \prod_{i=1}^{r} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}}$$

3. Si $m \wedge n = 1$, aucun nombre premier ne divise à la fois m et n (proposition 10 (iii)). La décomposition de mn s'obtient en juxtaposant celles de m et de n, et le produit de la question 2 se scinde en deux.

$$\boxed{\sigma(mn) = \sigma(m)\sigma(n)}$$

4. On pose $q = 2^p - 1$, premier et impair, donc premier avec 2^{p-1}. Par les questions 2 et 3 :

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

$$\boxed{2^{p-1}(2^p - 1) \text{ est parfait}}$$

5. (a) Comme b est impair, $2^a \wedge b = 1$, et $\sigma(2^a) = 2^{a+1} - 1$.

$$\boxed{\sigma(n) = (2^{a+1} - 1)\sigma(b)}$$

(b) Comme n est parfait, $(2^{a+1}-1)\sigma(b) = 2n = 2^{a+1}b$. L'entier $2^{a+1}-1$ est impair, donc premier avec 2^{a+1}, et le lemme de Gauss donne $2^{a+1}-1 \mid b$. On écrit $b = (2^{a+1}-1)c$; en reportant et en simplifiant, $\sigma(b) = 2^{a+1}c$. L'entier c, qui divise b, est impair.

(c) Comme $a \geqslant 1$, on a $2^{a+1}-1 \geqslant 3$, donc $c < b$: les entiers b et c sont deux diviseurs distincts de b. Ainsi $\sigma(b) \geqslant b + c = 2^{a+1}c = \sigma(b)$. L'égalité impose que b et c soient les seuls diviseurs de b. Comme 1 en est un et que $b > 1$, on a $c = 1$, et b n'a que 1 et lui-même pour diviseurs positifs.

$$\boxed{c = 1 \text{ et } b = 2^{a+1}-1 \text{ est premier}}$$

(d) Avec $k = a+1$, on obtient $n = 2^{k-1}(2^k-1)$, avec 2^k-1 premier, ce qui impose aussi k premier d'après l'exercice 56.

$$\boxed{\text{les nombres parfaits pairs sont exactement les } 2^{k-1}(2^k-1), \text{ avec } 2^k-1 \text{ premier}}$$

À retenir. Ce résultat, énoncé par Euclide pour le sens direct et démontré par Euler pour la réciproque, ramène les nombres parfaits pairs aux nombres premiers de Mersenne. On ignore toujours s'il existe un nombre parfait impair.

EXERCICE 55 ⋆⋆⋆

1. Supposons que m admette un diviseur impair $d \geqslant 3$, et écrivons $m = de$. La formule $a^d - b^d$ du chapitre 3 (proposition 5), avec $a = 2^e$ et $b = -1$, donne, d étant impair,

$$2^m + 1 = (2^e)^d - (-1)^d = (2^e+1)\sum_{j=0}^{d-1}(2^e)^{d-1-j}(-1)^j.$$

Donc 2^e+1 divise 2^m+1, avec $1 < 2^e+1 < 2^m+1$, et 2^m+1 n'est pas premier. Ainsi m n'a pas de facteur premier impair : d'après le théorème 6, c'est une puissance de 2.

$$\boxed{m = 2^n}$$

2. On calcule directement.

$$\boxed{F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \quad F_4 = 65\,537}$$

3. On a $(F_n - 2)F_n = (2^{2^n}-1)(2^{2^n}+1) = 2^{2^{n+1}} - 1 = F_{n+1} - 2$.

4. Par récurrence : $F_1 - 2 = 3 = F_0$, et si $F_n - 2 = \prod_{k=0}^{n-1} F_k$, la question 3 donne $F_{n+1} - 2 = \prod_{k=0}^{n} F_k$.

$$\boxed{F_n = 2 + \prod_{k=0}^{n-1} F_k}$$

5. Soit $m < n$ et d un diviseur commun de F_m et F_n. Comme F_m figure dans le produit de la question 4, d divise $F_n - \prod_{k=0}^{n-1} F_k = 2$. Or F_n est impair, donc $d = \pm 1$.

$$\boxed{F_m \wedge F_n = 1}$$

6. Pour chaque n, on choisit un facteur premier q_n de $F_n \geqslant 3$. D'après la question 5, les q_n sont deux à deux distincts : on obtient une infinité de nombres premiers.
À retenir. Fermat pensait que tous les F_n étaient premiers, ce que confirment F_0 à F_4 ; Euler a montré en 1732 que $F_5 = 641 \times 6\,700\,417$. On ne connaît aujourd'hui aucun autre nombre de Fermat premier.

EXERCICE 56 ⋆⋆⋆

1. D'après le chapitre 3 (proposition 5), $a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + \cdots + 1)$.

2. Si $a^n - 1$ est premier, son diviseur $a - 1$ vaut 1 ou $a^n - 1$; le second cas est exclu car $n \geqslant 2$ et $a \geqslant 2$ donnent $a^n > a$. Donc $a = 2$. Si $n = kl$ avec $1 < k < n$, la question 1 appliquée à $(2^k)^l - 1$ montre que $2^k - 1$ divise $2^n - 1$, avec $1 < 2^k - 1 < 2^n - 1$: c'est exclu, donc n est premier.

$$\boxed{a = 2 \text{ et } n \text{ premier}}$$

3. On écrit $a = bq + r$ avec $0 \leqslant r < b$. Alors

$$2^a - 1 = 2^r\left(2^{bq} - 1\right) + 2^r - 1.$$

D'après la question 1, appliquée à $(2^b)^q - 1$, l'entier $2^b - 1$ divise $2^{bq} - 1$, et $0 \leqslant 2^r - 1 < 2^b - 1$. Par unicité de la division euclidienne, $2^r - 1$ en est le reste.

4. La question 3 et la proposition 4 donnent $(2^a - 1) \wedge (2^b - 1) = (2^b - 1) \wedge (2^r - 1)$: le couple $(2^a - 1, 2^b - 1)$ suit pas à pas l'algorithme d'Euclide appliqué à (a, b), comme les nombres de Fibonacci de l'exercice 23. Par récurrence forte sur b, en admettant $b \geqslant 1$ et $r \geqslant 0$, l'algorithme s'arrête sur le couple $(2^d - 1, 2^0 - 1) = (2^d - 1, 0)$, avec $d = a \wedge b$.

$$\boxed{(2^a - 1) \wedge (2^b - 1) = 2^{a \wedge b} - 1}$$

Par exemple, $(2^{12} - 1) \wedge (2^{18} - 1) = 4095 \wedge 262\,143 = 63 = 2^6 - 1$. ✓

EXERCICE 57 ⋆⋆⋆

1. (a) Pour $x = \dfrac{a}{b}$ non nul, avec $a, b \in \mathbb{Z}^*$, on pose $v_p(x) = v_p(a) - v_p(b)$, et $v_p(0) = +\infty$. Cette valeur ne dépend pas de l'écriture choisie : si $\dfrac{a}{b} = \dfrac{c}{d}$, alors $ad = bc$, et la proposition 10 (i) donne $v_p(a) + v_p(d) = v_p(b) + v_p(c)$. La multiplicativité découle alors de la proposition 10 (i), le cas d'un facteur nul étant immédiat avec la convention $+\infty$.

(b) On réduit x et y au même dénominateur : $x = \dfrac{a}{c}$ et $y = \dfrac{b}{c}$. Si $k = \min\left(v_p(a), v_p(b)\right)$, alors p^k divise a et b, donc $a + b$, et $v_p(a + b) \geqslant k$. On retranche $v_p(c)$. On en déduit aussi le cas d'égalité, essentiel pour la suite : si $v_p(x) < v_p(y)$, alors

$$v_p(x) = v_p\big((x + y) - y\big) \geqslant \min\left(v_p(x + y), v_p(y)\right),$$

ce qui impose $v_p(x + y) \leqslant v_p(x)$, donc $v_p(x + y) = v_p(x)$.

$$\boxed{v_p(x + y) \geqslant \min\left(v_p(x), v_p(y)\right), \text{ avec égalité si } v_p(x) \neq v_p(y)}$$

2. Soit k l'entier tel que $2^k \leqslant n < 2^{k+1}$. Dans $[\![1\,;n]\!]$, l'entier 2^k est le seul de valuation 2-adique k, puisque le multiple suivant de 2^k est $2^{k+1} > n$, et tous les autres ont une valuation strictement inférieure. Ainsi $v_2(\dfrac{1}{2^k}) = -k$, et la somme S des autres termes vérifie $v_2(S) > -k$ d'après la question 1 (b). Le cas d'égalité donne $v_2(H_n) = v_2(\dfrac{1}{2^k} + S) = -k$.

$$\boxed{v_2(H_n) = -k, \quad \text{où } 2^k \leqslant n < 2^{k+1}}$$

Par exemple, $H_4 = \dfrac{25}{12}$ et $v_2(H_4) = -2$. ✓

3. Pour $n > 1$, on a $k \geqslant 1$, donc $v_2(H_n) < 0$, alors qu'un entier a une valuation positive : $H_n \notin \mathbb{Z}$.

Pour $m > n \geqslant 1$, on a $H_m - H_n = \displaystyle\sum_{j=n+1}^{m} \frac{1}{j}$. Dans $[\![n + 1\,;m]\!]$, un seul entier a la plus grande valuation 2-adique k : si $2^k u < 2^k u'$ en avaient deux, avec u et u' impairs, l'entier $2^k(u + 1)$, compris

entre eux, aurait une valuation strictement plus grande. Le raisonnement de la question 2 donne $v_2(H_m - H_n) = -k$. Si $k \geqslant 1$, on conclut. Si $k = 0$, l'intervalle ne contient aucun entier pair, donc se réduit à $\{n+1\}$, et $H_m - H_n = \dfrac{1}{n+1}$ avec $n+1 \geqslant 2$.

$$\boxed{H_n \notin \mathbb{Z} \text{ pour } n > 1, \quad H_m - H_n \notin \mathbb{Z} \text{ pour } m > n \geqslant 1}$$

EXERCICE 58 ⋆⋆⋆

1. Changer le signe d'une composante conserve l'équation : on peut supposer $x, y, z \geqslant 0$. Écartons le triplet nul, et soit $d = x \wedge y$. Comme $d^2 \mid x^2 + y^2 = z^2$, on a $2v_p(d) \leqslant 2v_p(z)$ pour tout p, donc $d \mid z$ (proposition 10 (ii)). Le triplet $(\dfrac{x}{d}, \dfrac{y}{d}, \dfrac{z}{d})$ est encore solution, avec $\dfrac{x}{d} \wedge \dfrac{y}{d} = 1$. Ses composantes sont alors deux à deux premières entre elles : si un nombre premier p divisait $\dfrac{x}{d}$ et $\dfrac{z}{d}$, il diviserait $(\dfrac{y}{d})^2$, donc $\dfrac{y}{d}$, par le lemme d'Euclide. Réciproquement, multiplier un triplet primitif par d et changer des signes donne un triplet pythagoricien.

2. Les entiers x et y ne sont pas tous deux pairs. S'ils étaient tous deux impairs, on aurait $z^2 = x^2 + y^2 \equiv 2$ [4], alors qu'un carré est congru à 0 ou 1 modulo 4. Exactement l'un d'eux est donc pair, et z^2 est impair.

$$\boxed{z \text{ est impair}}$$

3. Comme x et z sont impairs, r et t sont des entiers naturels, avec $r + t = z$ et $r - t = x$. Un diviseur commun de r et t divise z et x, donc 1.

$$\boxed{r \wedge t = 1}$$

4. On a $y^2 = z^2 - x^2 = (z+x)(z-x) = 4rt$, donc $s^2 = rt$. Si $t = 0$, alors $r = z = x = 1$ et $y = 0$, et $r = 1^2$, $t = 0^2$. Sinon, r et t sont des entiers non nuls premiers entre eux dont le produit est un carré : ce sont des carrés d'après l'exercice 32.

$$\boxed{r = u^2 \quad \text{et} \quad t = v^2, \quad u, v \in \mathbb{N}}$$

5. On en tire $z = r + t = u^2 + v^2$, $x = r - t = u^2 - v^2$, et $s^2 = u^2 v^2$, donc $y = 2uv$. Si c'est x qui est pair, on échange les rôles de x et y. Par la question 1, un triplet quelconque s'obtient en multipliant par d et en changeant des signes. Or ces changements restent dans l'ensemble proposé : remplacer u par $-u$ change le signe de $2duv$ seul, échanger u et v celui de $d(u^2 - v^2)$ seul, et remplacer d par $-d$ change le signe des trois composantes. Réciproquement, l'identité $(u^2 - v^2)^2 + (2uv)^2 = (u^2 + v^2)^2$ montre que tous ces triplets sont pythagoriciens.

$$\boxed{\left\{(d(u^2 - v^2), 2duv, d(u^2 + v^2)),\ (2duv, d(u^2 - v^2), d(u^2 + v^2)) \ ;\ (d, u, v) \in \mathbb{Z}^3\right\}}$$

Pour $(d, u, v) = (1, 2, 1)$, on retrouve $(3, 4, 5)$; pour $(1, 3, 2)$, le triplet $(5, 12, 13)$.

EXERCICE 59 ⋆⋆⋆

1. Si l'on avait $p_1 = 2$, le terme $p_3 = 2 + 2r$ serait pair et strictement supérieur à 2, donc non premier. Ainsi $p_1 \geqslant 3$, et p_1 est impair. Le terme $p_2 > p_1 \geqslant 3$ est premier, donc impair lui aussi, et $r = p_2 - p_1$ est la différence de deux entiers impairs.

$$\boxed{p_1 > 2 \quad \text{et} \quad r \text{ est pair}}$$

2. Raisonnons par l'absurde en supposant $n > p_1$, c'est-à-dire $n \geqslant p_1 + 1$. Le terme d'indice $p_1 + 1$ existe alors, et il vaut

$$p_{p_1+1} = p_1 + p_1 r = p_1(1 + r).$$

Comme $p_1 \geqslant 2$ et $1 + r \geqslant 2$, c'est le produit de deux entiers supérieurs ou égaux à 2 : il n'est pas premier, ce qui est absurde.

$$\boxed{n \leqslant p_1}$$

La borne est atteinte : $(3, 5, 7)$, $(5, 11, 17, 23, 29)$ et $(7, 157, 307, 457, 607, 757, 907)$, de raisons 2, 6 et 150, sont des progressions de nombres premiers de longueur égale à leur premier terme.

3. (a) Par récurrence immédiate, $p_i = p_1 + (i - 1)r$, donc $p_i - p_j = (i - j)r$. Deux entiers ont le même reste dans la division par q si et seulement s'ils sont congrus modulo q (théorème 1). Ainsi $\rho_i = \rho_j$ si et seulement si q divise $(i - j)r$. Comme q est premier et ne divise pas r, le lemme d'Euclide (proposition 9 (ii)) montre que cela équivaut à $q \mid i - j$.

$$\boxed{\rho_i = \rho_j \iff q \mid i - j}$$

(b) Comme $q < n$, les indices $1, \ldots, q$ sont bien ceux de termes de la progression. Pour $i \neq j$ dans $[\![1\,;q]\!]$, on a $1 \leqslant |i - j| \leqslant q - 1$, donc q ne divise pas $i - j$, et $\rho_i \neq \rho_j$ d'après la question (a).

(c) Les q restes $\rho_1, \ldots, \rho_q$ sont deux à deux distincts et appartiennent à $[\![0\,;q-1]\!]$, qui a q éléments. L'ensemble qu'ils forment est une partie de $[\![0\,;q-1]\!]$ de même cardinal, donc égale à $[\![0\,;q-1]\!]$ tout entier (chapitre 2, lemme 3 (i)). En particulier, l'un d'eux est nul : il existe $s \in [\![1\,;q]\!]$ tel que q divise p_s. Comme p_s est premier et $q \geqslant 2$, on a $p_s = q$. Or la question 2 donne $p_s \geqslant p_1 \geqslant n > q$, ce qui est absurde.

$$\boxed{\text{tout nombre premier } q < n \text{ divise la raison } r}$$

4. Les nombres premiers strictement inférieurs à n sont deux à deux premiers entre eux et divisent tous r, d'après la question 3. La proposition 7 (i), appliquée de proche en proche, montre que leur produit divise r : à chaque étape, le produit des premiers déjà traités est premier avec le suivant, par la proposition 7 (ii).

$$\boxed{\prod_{q \in \mathcal{P},\ q<n} q \ \text{ divise } r}$$

La progression $(7, 37, 67, 97, 127, 157)$ a pour longueur 6 et pour raison $30 = 2 \times 3 \times 5$, qui est bien le produit des nombres premiers inférieurs à 6 ; son premier terme vérifie $7 \geqslant 6$, comme le veut la question 2. Pour une longueur 10, la raison est un multiple de

$$\boxed{2 \times 3 \times 5 \times 7 = 210}$$

et cette valeur est atteinte : les dix entiers $199 + 210k$, pour $k \in [\![0\,;9]\!]$, sont tous premiers, ce que l'on vérifie à l'ordinateur.

Piège. La condition n'est que nécessaire. Avec la raison 30, la progression issue de 13 donne 13, 43, 73, 103, puis $133 = 7 \times 19$: elle s'arrête à la longueur 4, alors que 30 est divisible par tous les premiers inférieurs à 6.

À retenir. L'exercice ne dit pas qu'il existe des progressions de nombres premiers de longueur arbitraire ; il dit seulement que, si elles existent, leur raison et leur premier terme doivent être très grands. Leur existence est un théorème difficile, démontré par Ben Green et Terence Tao en 2004.

EXERCICE 60 ⋆⋆⋆

1. Soit $x \in F$. Le nombre $f(x)$ est rationnel, et il reste à voir qu'il ne vaut ni 0, ni 1, ni -1. En multipliant par $x \neq 0$, on obtient les équivalences suivantes.

— $f(x) = 0$ équivaut à $x^2 = 1$, c'est-à-dire $x = \pm 1$, ce qui est exclu.

— $f(x) = 1$ équivaut à $x^2 - x - 1 = 0$. D'après l'exercice 21, une solution rationnelle de cette équation serait un entier divisant -1, donc ± 1 ; or $1 - 1 - 1 = -1$ et $1 + 1 - 1 = 1$ ne sont pas nuls.

— $f(x) = -1$ équivaut à $x^2 + x - 1 = 0$, et l'on conclut de même, puisque $1 + 1 - 1 = 1$ et $1 - 1 - 1 = -1$.

$$\boxed{f(F) \subset F}$$

2. Par associativité de la composition, $f^{\circ(n+1)}$ est aussi égale à $f^{\circ n} \circ f$. La question 1 donne alors

$$f^{\circ(n+1)}(F) = f^{\circ n}(f(F)) \subset f^{\circ n}(F).$$

Chaque $f^{\circ n}(F)$ est l'image de l'ensemble non vide F, donc n'est pas vide. Pour les calculs, on applique trois fois la définition de f.

$$\boxed{f(2) = \frac{3}{2}, \qquad f^{\circ 2}(2) = \frac{3}{2} - \frac{2}{3} = \frac{5}{6}, \qquad f^{\circ 3}(2) = \frac{5}{6} - \frac{6}{5} = -\frac{11}{30}}$$

Les hauteurs successives sont $H(2) = 3$, puis 5, 11 et 41 : elles augmentent, et c'est ce que la suite va exploiter. On peut d'ailleurs montrer que chaque $f^{\circ n}(F)$ est infini, puisque $f(x) = f(x')$ équivaut à $(x - x')(1 + \dfrac{1}{xx'}) = 0$, de sorte que f prend chaque valeur au plus deux fois.

3. Soit ℓ un nombre premier qui divise pq. Par le lemme d'Euclide, il divise p ou q ; s'il divise p et $p^2 - q^2$, il divise $q^2 = p^2 - (p^2 - q^2)$, donc q, ce qui contredit $p \wedge q = 1$. Le cas où ℓ divise q est symétrique. Ainsi $p^2 - q^2$ et pq n'ont aucun facteur premier commun, et leur PGCD, qui n'a aucun diviseur premier, vaut 1 (théorème 6). Par ailleurs, la réduction au même dénominateur donne

$$f(x) = \frac{p}{q} - \frac{q}{p} = \frac{p^2 - q^2}{pq}.$$

Si $p > 0$, c'est la forme irréductible de $f(x)$; si $p < 0$, c'est $\dfrac{q^2 - p^2}{|p|q}$. Dans les deux cas, l'unicité de la forme irréductible (proposition 6) donne la hauteur.

$$\boxed{(p^2 - q^2) \wedge pq = 1 \qquad \text{et} \qquad H(f(x)) = |p^2 - q^2| + |p|\, q}$$

4. On note $a = |p| \geqslant 1$. Si l'on avait $a = q$, l'égalité $p \wedge q = 1$ imposerait $a = q = 1$, donc $x = \pm 1$, ce qui est exclu. Ainsi $|a - q| \geqslant 1$, et

$$|p^2 - q^2| = |a - q|\,(a + q) \geqslant a + q = H(x), \qquad |p|\, q \geqslant 1.$$

En ajoutant ces deux inégalités, on obtient la première propriété.

$$\boxed{H(f(x)) \geqslant H(x) + 1}$$

Pour la seconde, on raisonne par récurrence sur n. Pour $n = 0$, tout $x \in F$ vérifie $H(x) \geqslant 3$, car $H(x) = 2$ impose $|p| = q = 1$. Si la propriété est vraie au rang n, tout $y \in f^{\circ(n+1)}(F)$ s'écrit $y = f(x)$ avec $x \in f^{\circ n}(F) \subset F$, et $H(y) \geqslant H(x) + 1 \geqslant n + 4$.

$$\boxed{\forall n \in \mathbb{N},\ \forall y \in f^{\circ n}(F), \quad H(y) \geqslant n + 3}$$

Piège. Le dénominateur seul ne croît pas : $f(\frac{1}{2}) = -\frac{3}{2}$ a le même dénominateur que $\frac{1}{2}$. C'est pourquoi on mesure la taille d'un rationnel par sa hauteur, qui fait intervenir le numérateur, et pourquoi il faut la forme irréductible : sans la question 3, rien n'empêcherait une simplification de faire baisser la hauteur.

5. Supposons qu'un rationnel y appartienne à tous les $f^{\circ n}(F)$. En particulier, $y \in f^{\circ H(y)}(F)$, et la question 4 donne $H(y) \geqslant H(y) + 3$, ce qui est absurde.

$$\boxed{\bigcap_{n\in\mathbb{N}} f^{\circ n}(F) = \varnothing}$$

À retenir. On a construit une suite décroissante d'ensembles non vides, et même infinis, dont l'intersection est vide. Cela heurte l'intuition, et cela ne peut pas arriver avec des segments de $\mathbb{R}$: si $[a_n, b_n]$ est une suite décroissante de segments non vides, la suite (a_n) est croissante et majorée par b_0, donc converge vers un réel ℓ (chapitre 7, théorème 8), qui appartient à tous les segments. L'arithmétique fournit ici l'invariant qui croît strictement, la hauteur, et c'est la forme irréductible qui la rend calculable.

EXERCICE 61 ⋆⋆⋆

1. On dira qu'un entier $b \in \mathbb{N}^*$ est *admissible* si tous ses diviseurs premiers appartiennent à E. L'entier $1 = \frac{1}{1}$ appartient à A_E. Si $x = \frac{a}{b}$ et $y = \frac{c}{d}$, avec b et d admissibles, alors

$$x - y = \frac{ad - bc}{bd} \qquad \text{et} \qquad xy = \frac{ac}{bd},$$

et bd est admissible, puisqu'un nombre premier qui divise bd divise b ou d (lemme d'Euclide). Ainsi A_E contient 1 et est stable par différence et par produit.

$$\boxed{A_E \text{ est un sous-anneau de } \mathbb{Q}}$$

Pour $E = \varnothing$, seul $b = 1$ est admissible, et $A_\varnothing = \mathbb{Z}$. Pour $E = \mathcal{P}$, tout b est admissible, et $A_\mathcal{P} = \mathbb{Q}$. Pour $E = \{2, 5\}$, un rationnel $\frac{a}{2^\alpha 5^\beta}$ s'écrit, avec $\gamma = \max(\alpha, \beta)$,

$$\frac{a}{2^\alpha 5^\beta} = \frac{a \times 2^{\gamma-\alpha} 5^{\gamma-\beta}}{10^\gamma},$$

qui est décimal ; réciproquement, $\frac{k}{10^n}$ a un dénominateur admissible. Enfin, pour $E = \mathcal{P} \setminus \{2\}$, les entiers admissibles sont les entiers impairs.

$$\boxed{A_\varnothing = \mathbb{Z}, \qquad A_\mathcal{P} = \mathbb{Q}, \qquad A_{\{2,5\}} = \mathbb{D}, \qquad A_{\mathcal{P}\setminus\{2\}} = \text{anneau de l'exercice 35 du chapitre 11}}$$

2. Comme $a \wedge b = 1$, le théorème de Bézout fournit des entiers u et v tels que $au + bv = 1$. En divisant par b, on obtient

$$\frac{1}{b} = u\,x + v.$$

Or A contient 1, donc $\mathbb{Z}$, puisqu'il est stable par somme et par opposé ; il est stable par somme et par produit, donc contient $ux + v$. Si p est un nombre premier qui divise b, on écrit $b = pc$, et $\frac{1}{p} = c \times \frac{1}{b}$ appartient à A.

$$\boxed{\frac{1}{b} \in A, \quad \text{et} \quad \frac{1}{p} \in A \text{ pour tout nombre premier } p \mid b}$$

Par exemple, si $\frac{3}{10} \in A$, la relation $3 \times 7 - 10 \times 2 = 1$ donne $\frac{1}{10} = 7 \times \frac{3}{10} - 2 \in A$, puis $\frac{1}{2} = 5 \times \frac{1}{10}$ et $\frac{1}{5} = 2 \times \frac{1}{10}$.

Piège. La forme irréductible est indispensable. L'anneau $A_{\{3\}}$ contient $\dfrac{2}{6} = \dfrac{1}{3}$, mais pas $\dfrac{1}{6}$: sinon il contiendrait $\dfrac{1}{2} = 3 \times \dfrac{1}{6}$, et l'on aurait $\dfrac{1}{2} = \dfrac{a}{3^k}$, soit $3^k = 2a$, ce qui est impossible puisque 3^k est impair.

3. On procède par double inclusion. Soit $x \in A$, de forme irréductible $\dfrac{a}{b}$. D'après la question 2, tous les diviseurs premiers de b appartiennent à $E(A)$, donc $x \in A_{E(A)}$. Réciproquement, soit $x = \dfrac{a}{b}$ avec b admissible pour $E(A)$. Par le théorème 6, b s'écrit $p_1 p_2 \cdots p_k$, avec des nombres premiers p_i non nécessairement distincts, tous dans $E(A)$ (et $k = 0$ si $b = 1$). Alors

$$x = a \times \frac{1}{p_1} \times \cdots \times \frac{1}{p_k}$$

est un produit d'éléments de A, donc appartient à A.

$$\boxed{A = A_{E(A)}}$$

4. On note Φ l'application $E \longmapsto A_E$, qui est bien à valeurs dans l'ensemble des sous-anneaux de $\mathbb{Q}$ d'après la question 1. Elle est surjective, puisque tout sous-anneau A s'écrit $\Phi\big(E(A)\big)$ par la question 3. Pour l'injectivité, on montre que $E(A_E) = E$. Si $p \in E$, alors $\dfrac{1}{p} \in A_E$, puisque p est admissible. Réciproquement, si $\dfrac{1}{p} \in A_E$, on écrit $\dfrac{1}{p} = \dfrac{a}{b}$ avec b admissible ; alors $b = pa$, donc p divise b, et $p \in E$. Ainsi, si $A_E = A_{E'}$, on a $E = E(A_E) = E(A_{E'}) = E'$.

$$\boxed{E \longmapsto A_E \text{ est bijective, de réciproque } A \longmapsto E(A)}$$

5. Soit A un sous-anneau de $\mathbb{Q}$ qui soit un corps, et p un nombre premier. L'élément p de A est non nul, donc admet un inverse dans A, qui est aussi un inverse de p dans $\mathbb{Q}$; par unicité de l'inverse (chapitre 11, proposition 2), c'est $\dfrac{1}{p}$. Ainsi $E(A) = \mathcal{P}$, et $A = A_{\mathcal{P}} = \mathbb{Q}$ par la question 3.

Soit maintenant A un sous-anneau de $\mathbb{Q}$ contenant $\dfrac{3}{10}$, qui est sous forme irréductible. La question 2 donne $\dfrac{1}{2} \in A$ et $\dfrac{1}{5} \in A$, donc $\{2, 5\} \subset E(A)$, et $A = A_{E(A)}$ contient $A_{\{2,5\}}$, puisqu'un entier admissible pour $\{2, 5\}$ l'est pour toute partie plus grande. Comme $A_{\{2,5\}} = \mathbb{D}$ contient $\dfrac{3}{10}$, c'est le plus petit sous-anneau cherché.

$$\boxed{\mathbb{Q} \text{ est le seul sous-anneau de } \mathbb{Q} \text{ qui soit un corps, et le plus petit sous-anneau contenant } \tfrac{3}{10} \text{ est } \mathbb{D}}$$

À retenir. Les sous-groupes de $\mathbb{Z}$ sont décrits par un seul entier (théorème 2) ; les sous-anneaux de $\mathbb{Q}$ le sont par une partie de $\mathcal{P}$, éventuellement infinie, et deux parties distinctes donnent deux sous-anneaux distincts. Il faut cependant prendre garde à ne pas confondre sous-anneau et sous-groupe : $\dfrac{1}{2}\mathbb{Z}$ est un sous-groupe de $(\mathbb{Q}, +)$ qui contient 1, mais ce n'est pas un sous-anneau, puisque $\dfrac{1}{2} \times \dfrac{1}{2} = \dfrac{1}{4}$ n'y appartient pas ; le plus petit sous-anneau qui le contient est $A_{\{2\}}$.

Les six derniers exercices sont des problèmes à traiter en autonomie ; le corrigé indique la démarche, puis la rédige.

EXERCICE 62 ⋆⋆⋆⋆

Idée. Un carré a toutes ses valuations paires : on compare celles de 2 et de 5.

Le nombre s'écrit $N = 6 \times R \times 10^k$, où R est le repunit à 666 chiffres et $k \in \mathbb{N}$ le nombre de zéros. Comme R est impair et se termine par 1, on a $v_2(R) = v_5(R) = 0$, donc

$$v_2(N) = 1 + k \qquad \text{et} \qquad v_5(N) = k.$$

Si N était un carré, ces deux entiers consécutifs seraient pairs, ce qui est impossible.

$$\boxed{\text{un tel nombre n'est jamais un carré parfait}}$$

Le nombre 666 de chiffres ne joue aucun rôle : le résultat vaut pour tout nombre de 6.

EXERCICE 63 ⋆⋆⋆⋆

Idée. Les valuations montrent que le plus petit divise le plus grand, et l'on se ramène à $x^{k-1} = k$.

Les couples (x, x) conviennent. Soit une solution avec $x < y$. Pour tout nombre premier p, on a $y\, v_p(x) = x\, v_p(y)$, donc $v_p(x) = \dfrac{x}{y} v_p(y) \leqslant v_p(y)$, et $x \mid y$ par la proposition 10 (ii). On écrit $y = kx$ avec $k \geqslant 2$. L'équation devient $x^{kx} = (kx)^x$, soit, en prenant la racine x-ième, $x^k = kx$, puis $x^{k-1} = k$. Comme $x = 1$ donnerait $k = 1$, on a $x \geqslant 2$, donc $k = x^{k-1} \geqslant 2^{k-1}$. Or $2^{k-1} > k$ pour $k \geqslant 3$, par récurrence ; il reste $k = 2$, puis $x = 2$ et $y = 4$.

$$\boxed{\mathcal{S} = \{(x, x) \mid x \in \mathbb{N}^*\} \cup \{(2, 4), (4, 2)\}}$$

EXERCICE 64 ⋆⋆⋆⋆

Idée. Le produit $(k-1)k(k+1) = k(k^2-1)$ est formé de deux facteurs premiers entre eux, qui doivent donc être eux-mêmes des puissances n-ièmes ; or deux puissances n-ièmes ne diffèrent pas de 1.

Soit $k \geqslant 2$ et supposons $k(k^2-1) = a^n$. Comme $k^2 - (k^2-1) = 1$, on a $k \wedge (k^2-1) = 1$. Pour tout nombre premier p, $v_p(k) + v_p(k^2-1) = n\, v_p(a)$, et l'une des deux valuations est nulle : n divise donc toutes les valuations de k et de k^2-1. Comme à l'exercice 32, on obtient $k = b^n$ et $k^2 - 1 = c^n$, avec $c \geqslant 1$ car $k^2 - 1 \geqslant 3$. Alors $(b^2)^n = c^n + 1$, donc $b^2 > c$, soit $b^2 \geqslant c + 1$. Mais la formule du binôme donne, puisque $n \geqslant 2$,

$$(b^2)^n \geqslant (c+1)^n \geqslant c^n + nc^{n-1} + 1 > c^n + 1,$$

ce qui est absurde.

$$\boxed{\text{le produit de trois entiers consécutifs strictement positifs n'est jamais une puissance } n\text{-ième}}$$

EXERCICE 65 ⋆⋆⋆⋆

Idée. On calcule $v_2(3^n - 1)$ en factorisant comme à l'exercice 34, puis on compare à n.

Si n est impair, $3^n \equiv 3\ [8]$, puisque $3^2 \equiv 1\ [8]$, donc $3^n - 1 \equiv 2\ [8]$ et $v_2(3^n - 1) = 1$.

Si $n = 2^a m$ avec $a \geqslant 1$ et m impair, on factorise a fois :

$$3^n - 1 = (3^m - 1)(3^m + 1)(3^{2m} + 1)(3^{4m} + 1) \cdots (3^{2^{a-1}m} + 1).$$

On a $v_2(3^m - 1) = 1$; comme $3^m \equiv 3\ [8]$, $v_2(3^m + 1) = 2$; enfin, pour $i \geqslant 1$, $3^{2^i m}$ est un carré impair, donc congru à 1 modulo 8, et $v_2(3^{2^i m} + 1) = 1$. Au total, $v_2(3^n - 1) = 1 + 2 + (a - 1) = a + 2$.

La condition $2^n \mid 3^n - 1$ s'écrit $n \leqslant v_2(3^n - 1)$. Pour n impair, il faut $n \leqslant 1$. Pour n pair, il faut $2^a m \leqslant a + 2$, ce qui impose $m = 1$, puis $2^a \leqslant a + 2$, soit $a \in \{1, 2\}$.

$$\boxed{n \in \{1, 2, 4\}}$$

Vérification : $3 - 1 = 2$, $9 - 1 = 8$ et $81 - 1 = 80 = 16 \times 5$. ✓

EXERCICE 66 ⋆⋆⋆⋆

Idée. Pour n impair, on associe k et $n-k$; pour n pair, on travaille modulo la plus grande puissance de 2 qui divise n.

On note $S = \sum_{k=1}^{n} k^n$.

Si n est impair, on a $(n-k)^n \equiv (-k)^n = -k^n\ [n]$, donc les termes d'indices k et $n-k$ se compensent, pour $1 \leqslant k \leqslant n-1$, et le terme n^n est nul modulo n. Ainsi $S \equiv 0\ [n]$.

Si $n = 2^a m$ est pair, avec $a \geqslant 1$ et m impair, on montre que 2^a ne divise pas S. Pour k pair, $v_2(k^n) \geqslant n \geqslant 2^a > a$, donc $k^n \equiv 0\ [2^a]$. Pour k impair, on montre par récurrence que $k^{2^j} \equiv 1\ [2^{j+1}]$: c'est vrai pour $j = 0$, et $k^{2^{j+1}} - 1 = \left(k^{2^j} - 1\right)\left(k^{2^j} + 1\right)$ est le produit d'un multiple de 2^{j+1} et d'un nombre pair. Ainsi $k^n = \left(k^{2^a}\right)^m \equiv 1\ [2^a]$. Comme $[\![1\,;n]\!]$ contient $\dfrac{n}{2} = 2^{a-1}m$ entiers impairs,

$$S \equiv 2^{a-1}m\ [2^a],$$

qui n'est pas nul puisque m est impair. Donc 2^a, et a fortiori n, ne divise pas S.

$$\boxed{n \mid \sum_{k=1}^{n} k^n \iff n \text{ est impair}}$$

Par exemple, pour $n = 2$, $S = 1 + 4 = 5$, et pour $n = 3$, $S = 1 + 8 + 27 = 36$. ✓

EXERCICE 67 ⋆⋆⋆⋆

Idée. On étudie la suite modulo 3, car l'opération $+3$ ne change pas le reste : un terme congru à 2 fait diverger la suite, un terme multiple de 3 la fait tourner dans $\{3, 6, 9\}$. La réponse est $a_0 = 1$ ou $3 \mid a_0$.

Le cas $a_0 = 1$. On a $\sqrt{1} = 1$, donc la suite est constante.

Un terme congru à 2 modulo 3. Un carré n'est jamais congru à 2 modulo 3. Si $a_n \equiv 2$, alors $a_{n+1} = a_n + 3 \equiv 2$, et ainsi de suite : la suite est strictement croissante à partir de ce rang, et elle ne prend chaque valeur qu'un nombre fini de fois.

Le cas $3 \mid a_0$. Tous les termes sont alors multiples de 3, car la racine d'un carré multiple de 3 est multiple de 3. Soit $a_n > 9$, et $j \geqslant 1$ tel que $(3j)^2 < a_n \leqslant (3j+3)^2$. En ajoutant 3, la suite ne rencontre aucun carré avant $(3j+3)^2$, puisqu'un carré multiple de 3 est celui d'un multiple de 3 ; elle atteint $(3j+3)^2$, puis passe à $3j+3$, qui est strictement inférieur à a_n car $3j + 3 < 9j^2$. Ainsi, tant qu'un terme dépasse 9, la suite redescend plus tard sous lui ; elle prend donc une infinité de fois une valeur de $\{3, 6, 9\}$, et l'une d'elles est prise une infinité de fois. De fait, $3 \to 6 \to 9 \to 3$ est un cycle.

Le cas $a_0 \equiv 1\ [3]$ et $a_0 > 1$. Tant que les termes sont congrus à 1, la suite avance de 3 en 3 jusqu'au premier carré c^2 congru à 1, puis passe à c. Si $(j-1)^2 < a_n \leqslant j^2$, ce carré est j^2 ou $(j+1)^2$, car l'un des deux entiers j et $j+1$ n'est pas multiple de 3, donc $c \leqslant j+1$. Si $a_n > 4$, on a $j \geqslant 3$, et $c \leqslant j+1 < (j-1)^2 < a_n$: la suite redescend strictement. Par descente, elle atteint donc un terme congru à 2, ou bien un terme congru à 1 compris entre 2 et 4, c'est-à-dire 4, dont la racine 2 est congrue à 2. Dans tous les cas, on est ramené au cas divergent, et aucune valeur n'est prise une infinité de fois.

$$\boxed{\text{la suite prend une valeur une infinité de fois si et seulement si } a_0 = 1 \text{ ou } 3 \mid a_0}$$

Remarque sur l'énoncé. Dans la version de l'Olympiade internationale de 2017, on impose $a_0 > 1$, et la réponse est « les multiples de 3 ». Avec $a_0 \in \mathbb{N}^*$, il faut ajouter le cas $a_0 = 1$, qui donne une suite constante.