1. Rappels : multiples, diviseurs, parité, nombres premiers

Ex. 1 ★☆☆ Multiples et diviseurs

(a) On teste $d = 1, 2, 3, \ldots$: $156 = 1 \times 156 = 2 \times 78 = 3 \times 52 = 4 \times 39 = 6 \times 26 = 12 \times 13$, tandis que 5, 7, 8, 9, 10 et 11 ne divisent pas 156. On s'arrête à 12, car $13 \times 13 = 169 > 156$. Les 12 diviseurs positifs de 156 sont 1, 2, 3, 4, 6, 12, 13, 26, 39, 52, 78 et 156.

(b) Les diviseurs positifs de 15 sont 1, 3, 5 et 15. Dans $\mathbb{Z}$, on ajoute leurs opposés : $-15, -5, -3, -1$, 1, 3, 5, 15, soit 8 diviseurs.

(c) Oui : $0 = 23 \times 0$ et 0 est un entier, donc 0 est un multiple de 23
(et de tout entier).

(d) $391 = 17 \times 23$ avec 23 entier, donc $17 \mid 391$. En revanche, $391 \nmid 17$: un multiple non nul de 391 vaut au moins 391 en valeur absolue, et $0 < 17 < 391$. « a divise b » ne veut pas dire « b divise a ».

(e) Oui : $120 = (-8) \times (-15)$ et -15 est un entier, donc -8 divise 120. Dans $\mathbb{Z}$, un diviseur peut être négatif.

(f) Non : un nombre premier a exactement deux diviseurs positifs distincts, 1 et lui-même. Or 1 n'en a qu'un seul, lui-même : 1 n'est pas premier.

Ex. 2 ★☆☆ Critères de divisibilité sans confusion

(a) $16 = 4 \times 4$: le nombre formé par les deux derniers chiffres est un multiple de 4, donc $4 \mid 8\,316$. $8 + 3 + 1 + 6 = 18 = 9 \times 2$, donc $9 \mid 8\,316$.

(b) $4 + 1 + 2 + 5 = 12$ est un multiple de 3 mais pas de 9 : 4 125 n'est pas divisible par 9. Divisible par 3 n'entraîne pas divisible par 9.

(c) Non. Le critère par 4 porte sur les deux derniers chiffres : $18 = 4 \times 4 + 2$ n'est pas un multiple de 4, donc 3 718 n'est pas divisible par 4. Un nombre pair n'est pas forcément divisible par 4.

(d) Somme alternée : $3 - 9 + 2 - 7 = -11 = 11 \times (-1)$, multiple de 11.
Donc $11 \mid 7\,293$
(en effet $7\,293 = 11 \times 663$).

Ex. 2 (suite)

(e) Non. Malo applique le critère de la somme des chiffres, valable pour 3 et 9, pas pour 11. Somme alternée : $1 - 9 + 3 - 6 = -11$, multiple de 11 : 6 391 est divisible par 11
($6\,391 = 11 \times 581$).

Ex. 3 ★★☆ Vrai ou faux sur les entiers

(a) Faux. $n + (n + 1) = 2n + 1$ est impair pour tout entier n. Contre-exemple : pour $n = 0$, on obtient 1, qui est impair. L'affirmation est donc fausse.

(b) Vrai. $n^2 + n = n(n + 1)$ est le produit de deux entiers consécutifs. Si $n = 2k$, $n(n + 1) = 2\big(k(2k + 1)\big)$; si $n = 2k + 1$, $n(n + 1) = (2k + 1)(2k + 2) = 2\big((2k + 1)(k + 1)\big)$. Dans les deux cas, $n^2 + n$ s'écrit $2K$ avec K entier : il est pair.

(c) Faux. Avec deux lettres, $(2k + 1) + (2p + 1) = 2(k + p + 1)$: la somme est paire, mais pas forcément multiple de 4. Contre-exemple : $1 + 5 = 6 = 4 \times 1 + 2$ n'est pas un multiple de 4.

(d) Faux. Contre-exemple : $a = 6$, $b = 4$, $c = 9$. On a $bc = 36 = 6 \times 6$, donc $6 \mid 36$. Mais $4 = 6 \times 0 + 4$ et $9 = 6 \times 1 + 3$: $6 \nmid 4$ et $6 \nmid 9$. L'affirmation est donc fausse.

(e) Faux : quelques exemples ne prouvent pas une propriété vraie pour tout n. Contre-exemple : $n = 41$. Alors $41^2 + 41 + 41 = 41 \times (41 + 1 + 1) = 41 \times 43$. Ce nombre est divisible par 41 et différent de 1 et de 41 : il n'est pas premier.

Ex. 4 ★★☆ Parité et produit de trois consécutifs

(a) Si $n = 2k$: $n^2 = 4k^2 = 2(2k^2)$ est pair, comme n. Si $n = 2k + 1$: $n^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$ est impair, comme n. Dans les deux cas, n^2 et n ont la même parité.

(b) D'après la question précédente, n^2 et n ont la même parité, donc leur somme est paire : $n^2 + n = 2a$ avec a entier. Alors $n^2 + 3n + 5 = 2a + 2n + 4 + 1 = 2(a + n + 2) + 1$ avec $a + n + 2$ entier : $n^2 + 3n + 5$ est impair.

(c) n et $n + 1$ sont deux entiers consécutifs, donc l'un d'eux est pair : $n(n + 1) = 2b$ avec b entier. Alors $P = 2\big(b(n + 2)\big)$ avec $b(n + 2)$ entier : P est pair.

Ex. 4 **(suite)**

(d) Si $n = 3k$, $P = 3\big(k(n+1)(n+2)\big)$. Si $n = 3k+1$, $n+2 = 3(k+1)$, donc $P = 3\big(n(n+1)(k+1)\big)$. Si $n = 3k+2$, $n+1 = 3(k+1)$, donc $P = 3\big(n(k+1)(n+2)\big)$. Dans les trois cas, $P = 3K$ avec K entier : P est un multiple de 3.

(e) On a $P = 3K$ avec K entier. Si K était impair, $K = 2m+1$ et $P = 6m+3 = 2(3m+1)+1$ serait impair, ce qui contredit la question 3.
Donc K est pair : $K = 2K'$ et $P = 6K'$ avec K' entier.
Conclusion : P est un multiple de 6.

Ex. 5 ★★★ **Nombres premiers : corriger, puis démontrer**

(a) Lina n'a pas testé 7 : $91 = 7 \times 13$.
Donc 91 a au moins quatre diviseurs positifs (1, 7, 13, 91) : il n'est pas premier. Pour 223, si 223 avait un diviseur d tel que $1 < d < 223$, il en aurait un tel que $d \times d \leqslant 223$. Comme $14^2 = 196 \leqslant 223 < 225 = 15^2$, on teste de 2 à 14. 223 est impair, $2+2+3 = 7$ n'est pas multiple de 3 et 223 ne se termine ni par 0 ni par 5. Ensuite, $223 = 7 \times 31 + 6$, $223 = 11 \times 20 + 3$ et $223 = 13 \times 17 + 2$. Les autres entiers de 2 à 14 sont multiples de 2, 3 ou 5 : ils ne divisent pas 223 non plus. Donc 223 est premier.

(b) Tom a tort : 2 est pair et ses seuls diviseurs positifs sont 1 et 2, donc 2 est un nombre premier pair. Soit maintenant n un entier pair tel que $n > 2$. Alors $n = 2k$, et 1, 2 et n sont trois diviseurs positifs distincts de n : n n'est pas premier. Conclusion : 2 est le seul nombre premier pair.

(c) La division euclidienne donne $p = 6k + r$ avec $k \in \mathbb{N}$ et $0 \leqslant r \leqslant 5$. Si $r = 0$, 2 ou 4, alors $p = 2\left(3k + \frac{r}{2}\right)$ est pair. Or $p \geqslant 5$, donc $p \neq 2$, et p ne serait pas premier. Si $r = 3$, alors $p = 3(2k+1)$ est un multiple de 3, différent de 3, et p ne serait pas premier. Il reste $r = 1$ ou $r = 5$: $p = 6k+1$ ou $p = 6k+5$.

(d) Premier cas, $p = 6k+1$: $p^2 - 1 = 36k^2 + 12k = 12k(3k+1)$. Si $k = 2m$, alors $k(3k+1) = 2m(6m+1)$. Si $k = 2m+1$, alors $3k+1 = 6m+4 = 2(3m+2)$. Dans les deux cas, $k(3k+1) = 2K$ avec K entier, donc $p^2 - 1 = 24K$. Second cas, $p = 6k+5$: $p^2 - 1 = 36k^2 + 60k + 24 = 12(k+1)(3k+2)$. Si $k = 2m$, alors $3k+2 = 2(3m+1)$. Si $k = 2m+1$, alors $k+1 = 2(m+1)$. Là encore, $p^2 - 1 = 24K'$ avec K' entier. Conclusion : $24 \mid p^2 - 1$ pour tout nombre premier $p \geqslant 5$.

Ex. 5 **(suite)**

(e) Faux. Contre-exemple : $n = 25$. On a $25^2 - 1 = 624 = 24 \times 26$, donc $24 \mid 25^2 - 1$. Pourtant $25 = 5 \times 5$ n'est pas premier. La réciproque du résultat précédent est fausse.

Ex. 6 ★★★ **Quand n − 2 divise n + 7**

(a) Pour $n = 2$, on a $n - 2 = 0$ et $n + 7 = 9$. Pour tout entier k, $k \times 0 = 0 \neq 9$: 9 n'est pas un multiple de 0 (seul 0 est multiple de 0). La valeur $n = 2$ ne convient donc pas.

(b) Supposons $n - 2 \mid n + 7$: il existe $k \in \mathbb{Z}$ tel que $n + 7 = k(n-2)$. Alors $9 = (n+7) - (n-2) = k(n-2) - (n-2) = (k-1)(n-2)$, et $k - 1$ est un entier. Donc $n - 2 \mid 9$.

(c) Les diviseurs de 9 dans $\mathbb{Z}$ sont -9, -3, -1, 1, 3 et 9. D'après la question précédente, $n - 2$ est l'un d'eux, donc $n \in \{-7\,;-1\,;1\,;3\,;5\,;11\}$. Réciproquement, si $n - 2 \mid 9$, alors $n + 7 = (n-2) + 9$ est une somme de deux multiples de $n - 2$: c'en est un aussi. Les solutions sont donc -7, -1, 1, 3, 5 et 11. Par exemple, pour $n = -7$, on a $n + 7 = 0 = 0 \times (-9)$.

(d) Non, elle a tort. Contre-exemple : $n = 3$. On a $n - 2 = 1$, qui divise $n + 7 = 10$. Mais 10 ne divise pas 1, car pour tout entier k, $10k$ vaut 0 ou est de valeur absolue supérieure ou égale à 10, donc $10k \neq 1$. « a divise b » et « b divise a » sont deux affirmations différentes.

(e) Il existe des entiers k et k' tels que $b = ka$ et $a = k'b$. Alors $a = k'ka$, et comme $a \neq 0$, $kk' = 1$. Or a et b sont strictement positifs, donc k et k' sont des entiers naturels. Leur produit vaut 1, donc $k = k' = 1$ et $a = b$. Dans $\mathbb{Z}$, c'est faux : $3 \mid -3$ car $-3 = (-1) \times 3$, et $-3 \mid 3$ car $3 = (-1) \times (-3)$, mais $3 \neq -3$. On obtient seulement $a = b$ ou $a = -b$.

Ex. 7 ★★★ **Diviseurs en Python et nombres parfaits**

(a) Le programme affiche `[1, 45, 3, 15, 5, 9]`. On teste $d = 1$, puis $2, \ldots, 6$, et la boucle s'arrête à $d = 7$, car $7 \times 7 = 49 > 45$. Les diviseurs vont par paires d et $\frac{a}{d}$. Si $d \times d > a$, alors $\frac{a}{d} < d$: le diviseur associé à d est plus petit que d et a donc déjà été trouvé.

Ex. 7 **(suite)**

(b) Le programme affiche `[1, 49, 7, 7]` : comme $49 = 7 \times 7$, le diviseur 7 est ajouté deux fois.
Correction : on remplace la ligne `L.append(a // d)` par `if d != a // d:`, suivi de `L.append(a // d)` sur la ligne suivante, indenté une fois de plus. On n'ajoute ainsi le diviseur associé que s'il est différent de d. La fonction corrigée renvoie `[1, 49, 7]`.

(c) La fonction corrigée renvoie `[1, 496, 2, 248, 4, 124, 8, 62, 16, 31]`. Les diviseurs positifs de 496 autres que lui-même sont donc 1, 2, 4, 8, 16, 31, 62, 124 et 248. Leur somme vaut $31 + 465 = 496$.
Donc 496 est parfait.

(d) Si p est premier, ses seuls diviseurs positifs sont 1 et p. La somme de ses diviseurs autres que lui-même vaut donc 1. Or $p \geqslant 2$, donc $1 \neq p$: p n'est pas parfait. Le seul diviseur positif de 1 est 1 lui-même. La somme de ses autres diviseurs vaut donc $0 \neq 1$: 1 n'est pas parfait.

(e) Non, il a tort : un exemple ne prouve pas une propriété générale. Contre-exemple : 28. Ses diviseurs positifs autres que lui-même sont 1, 2, 4, 7 et 14, de somme 28 : 28 est parfait. Pourtant $28 = 6 \times 4 + 4$ n'est pas un multiple de 6.

2. *Divisibilité dans $\mathbb{Z}$ et division euclidienne*

Ex. 8 ★☆☆ **Divisions euclidiennes, dividendes négatifs compris**

(a) $37 \times 27 = 999 \leqslant 1\,000 < 37 \times 28 = 1\,036$.
Donc $1\,000 = 37 \times 27 + 1$ avec $0 \leqslant 1 < 37$: $q = 27$ et $r = 1$.

(b) $48 \times 42 = 2\,016 \leqslant 2\,026 < 48 \times 43 = 2\,064$.
Donc $2\,026 = 48 \times 42 + 10$ avec $0 \leqslant 10 < 48$: $q = 42$ et $r = 10$.

(c) Le plus grand multiple de 6 inférieur ou égal à -85 est $6 \times (-15) = -90$.
Donc $-85 = 6 \times (-15) + 5$ avec $0 \leqslant 5 < 6$: $q = -15$ et $r = 5$. Le reste n'est pas -1.

(d) Le plus grand multiple de 11 inférieur ou égal à -250 est $11 \times (-23) = -253$.
Donc $-250 = 11 \times (-23) + 3$ avec $0 \leqslant 3 < 11$: $q = -23$ et $r = 3$.

Ex. 8 **(suite)**

(e) Le plus grand multiple de 13 inférieur ou égal à -1 est $13 \times (-1) = -13$.
Donc $-1 = 13 \times (-1) + 12$ avec $0 \leqslant 12 < 13$: $q = -1$ et $r = 12$.

(f) Comme $0 \leqslant 7 < 15$, on a $7 = 15 \times 0 + 7$: $q = 0$ et $r = 7$.

Ex. 9 ★★☆ **Est-ce bien la division demandée ?**

(a) Non : on doit avoir $0 \leqslant r < 12$, or $22 \geqslant 12$. Comme $22 = 12 + 10$, on obtient $250 = 12 \times 20 + 10$ avec $0 \leqslant 10 < 12$: $q = 20$ et $r = 10$.

(b) Oui : $318 = 25 \times 12 + 18$ et $0 \leqslant 18 < 25$, donc par unicité de la division euclidienne $q = 12$ et $r = 18$.

(c) Non : en divisant par 12, il faut $0 \leqslant r < 12$, or $18 \geqslant 12$. On a $12 \times 26 = 312$, donc $318 = 12 \times 26 + 6$ avec $0 \leqslant 6 < 12$: $q = 26$ et $r = 6$.

(d) Non : -7 est négatif, ce n'est donc pas un reste. $-71 = 8 \times (-8) - 8 + 1 = 8 \times (-9) + 1$ avec $0 \leqslant 1 < 8$: $q = -9$ et $r = 1$.

(e) Oui : $9 \times (-7) + 3 = -63 + 3 = -60$ et $0 \leqslant 3 < 9$, donc $q = -7$ et $r = 3$.

Ex. 10 ★★☆ **Quand $n - 3$ divise $2n + 9$**

(a) Avec $u = 1$ et $v = -2$: $(2n + 9) - 2(n - 3) = 15$. Si $n - 3 \mid 2n + 9$, alors, puisque $n - 3 \mid n - 3$, $n - 3$ divise toute combinaison linéaire de ces deux nombres.
Donc $n - 3 \mid 15$.

(b) Dans $\mathbb{Z}$, les diviseurs de 15 sont ± 1, ± 3, ± 5 et ± 15. On a donc $n - 3 \in \{-15\,; -5\,; -3\,; -1\,; 1\,; 3\,; 5\,; 15\}$, d'où $n \in \{-12\,; -2\,; 0\,; 2\,; 4\,; 6\,; 8\,; 18\}$.

(c) Réciproquement, si $n - 3 \mid 15$, alors $n - 3$ divise $2(n - 3) + 15 = 2n + 9$. On contrôle aussi directement : $-15 = (-15) \times 1$, $5 = (-5) \times (-1)$, $9 = (-3) \times (-3)$, $13 = (-1) \times (-13)$, $17 = 1 \times 17$, $21 = 3 \times 7$, $25 = 5 \times 5$ et $45 = 15 \times 3$. Conclusion : $n \in \{-12\,; -2\,; 0\,; 2\,; 4\,; 6\,; 8\,; 18\}$.

(d) Parmi les entiers naturels trouvés, $n = 0$ donne -3 et $n = 2$ donne -13 : ces quotients sont négatifs. Pour $n = 4$, 6, 8 et 18, on obtient 17, 7, 5 et 3. Conclusion : $n \in \{4\,; 6\,; 8\,; 18\}$.

Ex. 11 ★★☆ **Restes d'une somme, d'un produit, changement de diviseur**

(a) On écrit $a = 14q + 9$ et $b = 14q' + 11$ avec q et q' entiers. Alors $a + b = 14(q + q') + 20 = 14(q + q' + 1) + 6$ avec $0 \leqslant 6 < 14$. Le reste est donc 6, et non 20.

(b) $ab = (14q + 9)(14q' + 11) = 14(14qq' + 11q + 9q') + 99$ et $99 = 14 \times 7 + 1$.
Donc $ab = 14(14qq' + 11q + 9q' + 7) + 1$ avec $0 \leqslant 1 < 14$: le reste est 1.

(c) $a = 14q + 9 = 7(2q + 1) + 2$, où $2q + 1$ est entier et $0 \leqslant 2 < 7$. Le reste de a dans la division par 7 est donc 2
(et non 9, car $9 \geqslant 7$).

(d) Non. Contre-exemple : $a = 23 = 14 \times 1 + 9$ a bien pour reste 9 dans la division par 14, mais $23 = 28 \times 0 + 23$, donc son reste par 28 vaut 23. En fait, si $q = 2k$, alors $a = 28k + 9$; si $q = 2k + 1$, alors $a = 28k + 23$. Le reste vaut donc 9 ou 23.

(e) Faux. Contre-exemple : $4 \times 21 = 84 = 14 \times 6$, donc $14 \mid 4 \times 21$, alors que $14 \nmid 4$ (car $0 < 4 < 14$) et $14 \nmid 21$ (car $21 = 14 \times 1 + 7$).

Ex. 12 ★★★ **Quand $n + 5$ divise $n^2 + 12$**

(a) Supposons que $n + 5 \mid n^2 + 12$. Comme $n + 5 \mid n + 5$, on a aussi $n + 5 \mid n(n + 5) = n^2 + 5n$. Par combinaison linéaire (avec $u = n$ et $v = -1$), $n + 5$ divise $n(n + 5) - (n^2 + 12) = 5n - 12$.

(b) $n + 5$ divise $n + 5$ et $5n - 12$, donc divise la combinaison $5(n + 5) - (5n - 12) = 37$. Or 37 est premier : ses diviseurs dans $\mathbb{Z}$ sont -37, -1, 1 et 37, sans oublier les négatifs.
Donc $n + 5 \in \{-37 ; -1 ; 1 ; 37\}$, c'est-à-dire $n \in \{-42 ; -6 ; -4 ; 32\}$.

(c) On a raisonné par implications seulement : rien ne garantit encore que ces valeurs conviennent. Contrôle : pour $n = -42$, $n^2 + 12 = 1\,776 = (-37) \times (-48)$; pour $n = -6$, $48 = (-1) \times (-48)$; pour $n = -4$, $28 = 1 \times 28$; pour $n = 32$, $1\,036 = 37 \times 28$. (On peut aussi écrire $n^2 + 12 = (n + 5)(n - 5) + 37$ pour obtenir la réciproque.) Conclusion : les solutions sont -42, -6, -4 et 32.

(d) Le quotient $\frac{n^2+12}{n+5}$ est un entier exactement quand $n + 5 \mid n^2 + 12$. Parmi les solutions, le seul entier naturel est $n = 32$. Pour cette valeur, $\frac{1\,036}{37} = 28$.

Ex. 13 ★★★ **Un reste égal au carré du quotient**

(a) Le reste vaut q^2, donc $a = 17q + q^2$. Un reste vérifie $0 \leqslant r < 17$, donc $q^2 < 17$. Comme $q \in \mathbb{N}$ et $5^2 = 25 > 17$, on a $q \leqslant 4$.

(b) $q \in \{0 ; 1 ; 2 ; 3 ; 4\}$ donne $a \in \{0 ; 18 ; 38 ; 60 ; 84\}$. Contrôle : $18 = 17 \times 1 + 1$, $38 = 17 \times 2 + 4$, $60 = 17 \times 3 + 9$, $84 = 17 \times 4 + 16$, avec des restes 1, 4, 9, 16 tous < 17 ; et $0 = 17 \times 0 + 0$. Conclusion : les solutions sont 0, 18, 38, 60 et 84.

(c) On écrit $a = 17q + q^2$ avec $0 \leqslant q^2 < 17$. Si $q \geqslant 0$, alors $a \geqslant 0$.
Donc $a < 0$ impose $q < 0$. De plus, $q^2 < 17$ donne $|q| \leqslant 4$. Ainsi $q \in \{-4 ; -3 ; -2 ; -1\}$, ce qui donne $a \in \{-52 ; -42 ; -30 ; -16\}$. Contrôle : $-16 = 17 \times (-1) + 1$, $-30 = 17 \times (-2) + 4$, $-42 = 17 \times (-3) + 9$ et $-52 = 17 \times (-4) + 16$. Les restes sont bien entre 0 et 16. Conclusion : les solutions négatives sont -52, -42, -30 et -16.

(d) Toute solution s'écrit $a = 17q + q^2 = q(q + 17)$ avec q entier. Si q est pair, alors $2 \mid q$, donc $2 \mid a$. Si q est impair, alors $q + 17$ est pair, donc $2 \mid a$. Conclusion : toutes les solutions sont paires.

(e) Il faut $0 \leqslant q^2 < 50$ avec $q \in \mathbb{N}$, soit $q \leqslant 7$, car $7^2 = 49 < 50 < 64 = 8^2$. Réciproquement, pour $q \in \{0 ; 1 ; \ldots ; 7\}$, l'entier $a = 50q + q^2$ vérifie $0 \leqslant q^2 < 50$. Par unicité de la division euclidienne, q et q^2 sont donc son quotient et son reste. Ces valeurs sont distinctes, car a croît avec q. Conclusion : il y a 8 entiers naturels, de 0 à $50 \times 7 + 49 = 399$.

Ex. 14 ★★★ **Carrés et division par 4**

(a) Si $n = 2k$ avec $k \in \mathbb{Z}$, alors $n^2 = 4k^2 + 0$: le reste vaut 0. Si $n = 2k + 1$, alors $n^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1$ avec $k^2 + k \in \mathbb{Z}$ et $0 \leqslant 1 < 4$: le reste vaut 1. Conclusion : le reste de n^2 par 4 vaut 0 ou 1.

(b) On écrit $a^2 = 4q_1 + r_1$ et $b^2 = 4q_2 + r_2$ avec $r_1, r_2 \in \{0 ; 1\}$. Alors $a^2 + b^2 = 4(q_1 + q_2) + (r_1 + r_2)$, avec $r_1 + r_2 \in \{0 ; 1 ; 2\}$, donc $0 \leqslant r_1 + r_2 < 4$: c'est le reste. Les trois cas sont atteints ($0^2 + 0^2 = 0$, $1^2 + 0^2 = 1$, $1^2 + 1^2 = 2$). Les restes possibles sont donc 0, 1 et 2.

(c) $2\,027 = 4 \times 506 + 3$ avec $0 \leqslant 3 < 4$: le reste de la division de 2 027 par 4 vaut 3. D'après la question précédente, une somme de deux carrés a pour reste 0, 1 ou 2.
Donc 2 027 n'est pas la somme des carrés de deux entiers.

Ex. 14 **(suite)**

(d) Vrai. Si $4 \mid a^2+b^2$, le reste vaut 0, donc $r_1+r_2=0$ et $r_1=r_2=0$. Or un entier impair a un carré de reste 1 : a et b ne sont donc pas impairs. Conclusion : a et b sont pairs.

(e) Si a et b sont impairs, alors d'après la question 1, a^2 et b^2 ont pour reste 1. On a donc $a^2+b^2=4(q_1+q_2)+2$ avec $0 \leqslant 2 < 4$: le reste vaut 2. Or le carré d'un entier a pour reste 0 ou 1. Conclusion : a^2+b^2 n'est le carré d'aucun entier.

3. *PGCD, algorithme d'Euclide et PGCD d'expressions en n*

Ex. 15 ★☆☆ **Euclide à la main**

(a) $2\,431 = 2 \times 1\,001 + 429$; $1\,001 = 2 \times 429 + 143$; $429 = 3 \times 143 + 0$. Le dernier reste non nul est 143 : $\text{PGCD}(2\,431\,;1\,001) = 143$. Contrôle : $2\,431 = 143 \times 17$ et $1\,001 = 143 \times 7$.

(b) Les diviseurs communs sont les diviseurs du PGCD $143 = 11 \times 13$: 1, 11, 13 et 143.

(c) $4\,199 - 2 \times 1\,547 = 1\,105$, et $\text{PGCD}(a\,;b) = \text{PGCD}(b\,;a-kb)$ avec $k=2$. Ensuite $1\,547 = 1 \times 1\,105 + 442$; $1\,105 = 2 \times 442 + 221$; $442 = 2 \times 221 + 0$. Donc $\text{PGCD}(4\,199\,;1\,547) = 221$.

(d) $\text{PGCD}((-126)\,;495) = \text{PGCD}(126\,;495)$. $495 = 3 \times 126 + 117$; $126 = 1 \times 117 + 9$; $117 = 13 \times 9 + 0$. Le PGCD vaut 9.

(e) Tout entier divise 0, donc les diviseurs communs de 637 et 0 sont les diviseurs de 637 : $\text{PGCD}(637\,;0) = 637$, et non 0.

(f) Un diviseur commun positif d divise $1\,848 - 1\,847 = 1$, donc $d=1$. Deux entiers consécutifs sont premiers entre eux : $\text{PGCD}(1\,847\,;1\,848) = 1$.

Ex. 16 ★☆☆ **Euclide en Python**

(a) Passage 2 : $a=147$, $b=21$, $r=21$. Passage 3 : $a=21$, $b=0$, $r=0$.

(b) Il affiche `(21, 3)` : $\text{PGCD}(1\,071\,;462) = 21$, obtenu en 3 divisions euclidiennes.

(c) Passage 1 : $r=147$, puis `b = r` donne $b=147$, et `a = b` donne $a=147$: l'ancienne valeur 462 de b est perdue. Passage 2 : $r = 147\,\%\,147 = 0$, puis $b=0$ et $a=0$. Affichage `(0, 2)`. Il faut ranger b dans a avant de remplacer b par r.

Ex. 16 **(suite)**

(d) Au premier passage, $462 = 0 \times 1\,071 + 462$, donc $r=462$, puis $a=1\,071$ et $b=462$: les nombres sont échangés. On retrouve ensuite les 3 passages : affichage `(21, 4)`.

(e) Comme $b=0$, on n'entre pas dans la boucle : affichage `(58, 0)`, ce qui est cohérent avec $\text{PGCD}(58\,;0) = 58$.

Ex. 17 ★★☆ **Un PGCD qui dépend de n**

(a) $a - 2b = 2n+7-2(n+2) = 3$. Comme $\text{PGCD}(a\,;b) = \text{PGCD}(b\,;a-2b)$, on a $\text{PGCD}(a\,;b) = \text{PGCD}(n+2\,;3)$. Ce PGCD divise 3 : il vaut donc 1 ou 3.

(b) Non. Pour $n=0$: $a=7$, $b=2$ et $\text{PGCD}(7\,;2)=1$. Le fait que « d divise 3 » ne donne que les valeurs possibles, pas la valeur du PGCD.

(c) $\text{PGCD}(n+2\,;3) = 3$ si et seulement si $3 \mid n+2$, c'est-à-dire $n \equiv 1\ [3]$. Réciproquement, si $n=3k+1$, alors $b=3(k+1)$ et $a=3(2k+3)$. Conclusion : le PGCD vaut 3 exactement pour les $n=3k+1$, $k \in \mathbb{N}$.

(d) $2\,026 = 3 \times 675 + 1$, donc le PGCD vaut 3 : la fraction $\frac{4\,059}{2\,028}$ n'est pas irréductible (elle vaut $\frac{1\,353}{676}$).
$2\,027 \equiv 2\ [3]$, donc le PGCD vaut 1 : la fraction $\frac{4\,061}{2\,029}$ est irréductible.

Ex. 18 ★★☆ **PGCD imposé, somme imposée**

(a) 24 divise a et b, donc $a=24a'$ et $b=24b'$ avec a', b' entiers naturels. Alors $24 = \text{PGCD}(24a'\,;24b') = 24 \times \text{PGCD}(a'\,;b')$, donc $\text{PGCD}(a'\,;b') = 1$.

(b) $24a' + 24b' = 288$, donc $24(a'+b') = 288$ et $a'+b' = 12$.

(c) Non. $48 + 240 = 288$, mais $\text{PGCD}(48\,;240) = 48$, car $240 = 5 \times 48$. Elle a oublié la condition $\text{PGCD}(a'\,;b') = 1$: ici, $\text{PGCD}(2\,;10) = 2$.

(d) On cherche $a' \leqslant b'$ avec $a'+b' = 12$ et a', b' premiers entre eux. Parmi $(0\,;12)$, $(1\,;11)$, $(2\,;10)$, $(3\,;9)$, $(4\,;8)$, $(5\,;7)$ et $(6\,;6)$, seuls $(1\,;11)$ et $(5\,;7)$ conviennent ($\text{PGCD}(0\,;12) = 12$). Les couples sont $(24\,;264)$ et $(120\,;168)$.

Ex. 19 ★★★ **Une fraction qui se simplifie parfois**

(a) $3a - 5b = 15n + 9 - 15n - 20 = -11$. Comme $d \mid a$ et $d \mid b$, d divise la combinaison linéaire $3a - 5b = -11$, donc $d \mid 11$. Or 11 est premier, donc $d=1$ ou $d=11$.

Ex. 19 **(suite)**

(b) On a $3a = 5b - 11$. Si $11 \mid b$, alors 11 divise $5b - 11 = 3a$. Comme 11 est premier et ne divise pas 3, $\text{PGCD}(11\,;3) = 1$ et, d'après le théorème de Gauss, $11 \mid a$. Réciproquement, si $11 \mid a$, alors 11 divise $3a + 11 = 5b$. Comme $\text{PGCD}(11\,;5) = 1$, le théorème de Gauss donne $11 \mid b$. Conclusion : $11 \mid b \iff 11 \mid a$.

(c) D'après la première question, $d = 1$ ou $d = 11$, et $d = 11$ si et seulement si 11 divise a et b, donc, d'après la question précédente, si et seulement si $11 \mid b$. Si $11 \mid 3n + 4$, alors 11 divise $4(3n + 4) = 11(n + 1) + (n + 5)$, donc $11 \mid n + 5$. Réciproquement, si $11 \mid n + 5$, alors 11 divise $3(n + 5) = (3n + 4) + 11$, donc $11 \mid 3n + 4$. Or $n + 5 = 11m$ avec $m \geqslant 1$ équivaut à $n = 11k + 6$ avec $k = m - 1 \in \mathbb{N}$. Conclusion : $d = 11$ si et seulement si $n = 11k + 6$, $k \in \mathbb{N}$, et $d = 1$ sinon.

(d) La fraction est irréductible si et seulement si $d = 1$, c'est-à-dire si n ne s'écrit pas $11k + 6$. Pour $n = 17 = 11 \times 1 + 6$, on a $d = 11$, avec $a = 88$ et $b = 55$.
Donc $\frac{88}{55} = \frac{8 \times 11}{5 \times 11} = \frac{8}{5}$, et cette fraction est irréductible.

Ex. 20 ★★★ **PGCD égal à 18 : produit ou écart imposé**

(a) 18 divise a et b, donc il existe des entiers naturels a' et b' tels que $a = 18a'$ et $b = 18b'$. D'après la propriété admise, $18 = \text{PGCD}(18a'\,;18b') = 18 \times \text{PGCD}(a'\,;b')$. Donc $\text{PGCD}(a'\,;b') = 1$: a' et b' sont premiers entre eux.

(b) Il ne convient pas. Comme $324 = 36 \times 9$, 36 divise 324, donc $\text{PGCD}(36\,;324) = 36 \neq 18$. Ici, $a' = 2$ et $b' = 18$ ne sont pas premiers entre eux : la condition sur le produit ne suffit pas.

(c) $ab = 324$ $a'b' = 11\,664$, donc $a'b' = 36$, avec $a' < b'$ et $\text{PGCD}(a'\,;b') = 1$. Les couples de produit 36 sont $(1\,;36)$, $(2\,;18)$, $(3\,;12)$ et $(4\,;9)$. On élimine $(2\,;18)$ (PGCD 2) et $(3\,;12)$ (PGCD 3). Réciproquement, $(1\,;36)$ et $(4\,;9)$ sont premiers entre eux, donc les couples obtenus conviennent. Les solutions sont $(18\,;648)$ et $(72\,;162)$.

(d) Soit d un diviseur commun de k et de $k + 1$. Il divise la combinaison linéaire $(k + 1) - k = 1$, donc $d = 1$. Conclusion : $\text{PGCD}(k\,;k + 1) = 1$, deux entiers consécutifs sont premiers entre eux.

Ex. 20 **(suite)**

(e) Si $b - a = 18$, alors $18(b' - a') = 18$, donc $b' = a' + 1$, avec $a' \geqslant 1$ puisque $a \geqslant 1$. Réciproquement, si $a = 18k$ et $b = 18(k + 1)$ avec $k \geqslant 1$, on a $b - a = 18$. De plus, $\text{PGCD}(a\,;b) = 18 \times \text{PGCD}(k\,;k + 1) = 18$ d'après la question précédente. Les solutions sont les couples $(18k\,;18k + 18)$ avec $k \in \mathbb{N}$ et $k \geqslant 1$.

Ex. 21 ★★★ **Un programme qui renvoie toujours 0**

(a) Les restes successifs sont 4, puis 2, puis 0. La boucle s'arrête quand $r = 0$ et la fonction renvoie ce reste nul : le programme affiche `0`. Or le PGCD est le dernier reste non nul, ici contenu dans `b`. On remplace la dernière ligne par `return b`. Alors `pgcd(28, 6)` renvoie 2. Ce résultat est aussi correct si le premier reste est nul, car on a alors $b \mid a$ et $\text{PGCD}(a\,;b) = b$.

(b) On écrit `for n in range(8):` puis, en retrait, `print(pgcd(n * n + 3, n + 1))`. La boucle affiche successivement 1, 2, 1, 4, 1, 2, 1, 4.

(c) $(n^2 + 3) - (n - 1)(n + 1) = n^2 + 3 - n^2 + 1 = 4$, donc $n^2 + 3 = (n + 1)(n - 1) + 4$. Or $\text{PGCD}(a\,;b) = \text{PGCD}(b\,;a - kb)$ pour tout entier k. Avec $k = n - 1$, on obtient $\text{PGCD}(n^2 + 3\,;n + 1) = \text{PGCD}(n + 1\,;4)$. Ce PGCD est donc un diviseur de 4 : il vaut 1, 2 ou 4.

(d) On pose $d = \text{PGCD}(n + 1\,;4)$ et on cherche le plus grand diviseur de 4 qui divise $n + 1$. Si $n + 1$ est multiple de 4, c'est-à-dire si $n = 4k + 3$, alors $d = 4$. Si $n + 1$ est pair sans être multiple de 4, c'est-à-dire si $n = 4k + 1$, alors $d = 2$. Si $n + 1$ est impair, c'est-à-dire si n est pair, alors $d = 1$. Conclusion : le PGCD vaut 4 si $n = 4k + 3$, 2 si $n = 4k + 1$ et 1 si n est pair, avec $k \in \mathbb{N}$. C'est cohérent avec l'affichage de la question précédente.

4. *Identité et théorème de Bézout*

Ex. 22 ★☆☆ **Remonter l'algorithme d'Euclide**

(a) $53 = 3 \times 17 + 2$, donc $2 = 53 - 3 \times 17$; $17 = 8 \times 2 + 1$, donc $1 = 17 - 8 \times 2$; $2 = 2 \times 1 + 0$. Le PGCD vaut 1. Remontée : $1 = 17 - 8(53 - 3 \times 17) = 25 \times 17 - 8 \times 53$. Couple : $(-8\,;25)$. Vérification : $-424 + 425 = 1$.

(b) $117 = 2 \times 45 + 27$; $45 = 1 \times 27 + 18$; $27 = 1 \times 18 + 9$; $18 = 2 \times 9 + 0$. Le PGCD vaut 9. Remontée : $9 = 27 - 18 = 27 - (45 - 27) = 2 \times 27 - 45 = 2(117 - 2 \times 45) - 45 = 2 \times 117 - 5 \times 45$. Couple : $(2\,;-5)$. Vérification : $234 - 225 = 9$.

Ex. 22 **(suite)**

(c) $100 = 2 \times 37 + 26$; $37 = 1 \times 26 + 11$; $26 = 2 \times 11 + 4$; $11 = 2 \times 4 + 3$; $4 = 1 \times 3 + 1$; $3 = 3 \times 1 + 0$. Le PGCD vaut 1. Remontée : $1 = 4 - 3 = 3 \times 4 - 11 = 3 \times 26 - 7 \times 11 = 10 \times 26 - 7 \times 37 = 10 \times 100 - 27 \times 37$. En multipliant par 3 : $100 \times 30 + 37 \times (-81) = 3$. Couple : $(30\,;-81)$. Vérification : $3\,000 - 2\,997 = 3$.

(d) $29 = 2 \times 12 + 5$; $12 = 2 \times 5 + 2$; $5 = 2 \times 2 + 1$. Remontée : $1 = 5 - 2 \times 2 = 5 - 2(12 - 2 \times 5) = 5 \times 5 - 2 \times 12 = 5(29 - 2 \times 12) - 2 \times 12 = 5 \times 29 - 12 \times 12$.
Donc $29u - 12v = 1$ avec $u = 5$ et $v = 12$ (et non $v = -12$). Vérification : $145 - 144 = 1$.

Ex. 23 ★☆☆ **Premiers entre eux pour tout entier n**

(a) $1 \times (2n+1) + (-2) \times n = 1$. Il existe donc des entiers $u = 1$ et $v = -2$ tels que $(2n+1)u + nv = 1$. D'après le théorème de Bézout, n et $2n+1$ sont premiers entre eux.

(b) $3(2n+1) - 2(3n+1) = 6n + 3 - 6n - 2 = 1$. D'après le théorème de Bézout, $2n+1$ et $3n+1$ sont premiers entre eux. Le numérateur et le dénominateur n'ont donc pas d'autre diviseur positif commun que 1 : la fraction est irréductible.

(c) $(n^2 + n + 1) - n(n+1) = 1$: c'est une combinaison à coefficients entiers 1 et $-n$ égale à 1. D'après le théorème de Bézout, $n+1$ et $n^2 + n + 1$ sont premiers entre eux.

(d) $2(2n+3) - (4n+1) = 4n + 6 - 4n - 1 = 5$. On sait seulement que $\text{PGCD}(2n+3\,;4n+1)$ divise 5. Pour $n = 1$: $2n+3 = 5$ et $4n+1 = 5$, de PGCD 5. On ne peut donc pas conclure : ils ne sont pas toujours premiers entre eux.

(e) Non. Pour $n = 4$: $2n+1 = 9$ et $3n+1 = 13$. Ils sont bien premiers entre eux (question b), mais $9 = 3 \times 3$ n'est pas premier. Être premiers entre eux est une propriété du couple, pas de chacun des deux nombres.

Ex. 24 ★★☆ **Bézout : vrai ou faux ?**

(a) Faux. L'égalité est juste ($24 - 20 = 4$), mais elle prouve seulement que $\text{PGCD}(6\,;10)$ divise 4. En fait $10 = 1 \times 6 + 4$, $6 = 1 \times 4 + 2$, $4 = 2 \times 2$, donc $\text{PGCD}(6\,;10) = 2 \neq 4$.

(b) Faux. Si $u \geqslant 1$ et $v \geqslant 1$, alors $14u + 9v \geqslant 14 + 9 = 23 > 1$. Un couple de Bézout existe pourtant, avec des coefficients de signes contraires : $14 \times 2 + 9 \times (-3) = 28 - 27 = 1$.

Ex. 24 **(suite)**

(c) Faux. $(3\,;-11)$ convient : $45 - 44 = 1$. Mais $(-1\,;4)$ convient aussi : $-15 + 16 = 1$. Plus généralement, les couples $(3 + 4k\,;-11 - 15k)$, avec k entier, conviennent : le couple de Bézout n'est pas unique.

(d) Vrai. En multipliant par -1 :
$13 \times (-3) + 20 \times 2 = -39 + 40 = 1$. Il existe donc des entiers $u = -3$ et $v = 2$ tels que $13u + 20v = 1$. D'après le théorème de Bézout, 13 et 20 sont premiers entre eux.

Ex. 25 ★★☆ **Euclide étendu en Python**

(a)

passage	a	b	u0	v0
départ	162	70	1	0
1	70	22	0	1
2	22	4	1	-2
3	4	2	-3	7
4	2	0	16	-37

Les quotients successifs sont 2, 3, 5, 2. Après le passage 4, $b = 0$: la boucle s'arrête.

(b) Le programme affiche `(2, 16, -37)`.
Donc $\text{PGCD}(162\,;70) = 2$ et $162 \times 16 + 70 \times (-37) = 2$. Vérification : $2\,592 - 2\,590 = 2$.

(c) On divise l'égalité par 2 : $81 \times 16 + 35 \times (-37) = 1$, soit $(x\,;y) = (16\,;-37)$. Vérification : $1\,296 - 1\,295 = 1$. D'après le théorème de Bézout, 81 et 35 sont premiers entre eux, alors qu'aucun des deux n'est premier.

(d) On multiplie l'égalité du b) par 7 :
$162 \times 112 + 70 \times (-259) = 14$, soit $(x\,;y) = (112\,;-259)$. Vérification : $18\,144 - 18\,130 = 14$. En revanche, 2 divise 162 et 70, donc 2 divise $162x + 70y$ pour tous entiers x, y. Comme $2 \nmid 15$, il n'existe pas d'entiers x, y tels que $162x + 70y = 15$.

Ex. 26 ★★★ **PGCD de deux expressions en n : un diviseur de 11**

(a) $5a - 2b = 10n + 15 - 10n - 4 = 11$. Tout diviseur commun de a et b divise la combinaison $5a - 2b$, donc $d \mid 11$: c'est tout ce que l'on peut affirmer. Contre-exemple : pour $n = 0$, $a = 3$ et $b = 2$, donc $d = 1 \neq 11$. Malik a tort : une combinaison égale à 11 ne prouve pas que le PGCD vaut 11.

(b) d est un diviseur positif de 11, et 11 est premier. Donc $d = 1$ ou $d = 11$.

Ex. 26 **(suite)**

(c) $6(2n+3)-11(n+2)=12n+18-11n-22=n-4$. Si $11 \mid 2n+3$, alors 11 divise $6(2n+3)$ et $11(n+2)$, donc leur différence : $11 \mid n-4$.

(d) Si $d=11$, alors $11 \mid a=2n+3$, donc $11 \mid n-4$ (question précédente) : il existe un entier k tel que $n=11k+4$. Réciproquement, si $n=11k+4$ avec $k \in \mathbb{N}$: $a=22k+11=11(2k+1)$ et $b=55k+22=11(5k+2)$, donc 11 est un diviseur commun et $d=11$ (car $d \in \{1;11\}$). Conclusion : $d=11$ si et seulement si $n=11k+4$ avec $k \in \mathbb{N}$; sinon $d=1$.

(e) $2\,026=11\times184+2$: n n'est pas de la forme $11k+4$, donc $d=1$ et la fraction est irréductible. $2\,028=11\times184+4$: $d=11$, donc la fraction n'est pas irréductible : $\frac{4\,059}{10\,142}=\frac{11\times369}{11\times922}=\frac{369}{922}$. On a divisé le numérateur et le dénominateur par leur PGCD : la fraction $\frac{369}{922}$ est irréductible.

Ex. 27 ★★★ **Euclide étendu, signes et couples de Bézout**

(a) $281=3\times76+53$; $76=1\times53+23$; $53=2\times23+7$; $23=3\times7+2$; $7=3\times2+1$; $2=2\times1+0$. Le dernier reste non nul est 1, donc $\text{PGCD}(281\,;76)=1$: 281 et 76 sont premiers entre eux.

(b) On isole les restes : $53=281-3\times76$, $23=76-53$, $7=53-2\times23$, $2=23-3\times7$, $1=7-3\times2$. Remontée : $1=7-3(23-3\times7)=10\times7-3\times23=10(53-2\times23)-3\times23=10\times53-23\times23=10\times53-23(76-53)=33\times53-23\times76=33(281-3\times76)-23\times76=33\times281-122\times76$. Vérification : $9\,273-9\,272=1$. Le couple $(33\,;-122)$ convient.

(c) Non. Pour tout entier k : $281(33+76k)+76(-122-281k)=281\times33-76\times122+281\times76k-76\times281k=1$. Il y a donc une infinité de couples. Pour $k=-1$: $(-43\,;159)$, et $281\times(-43)+76\times159=-12\,083+12\,084=1$.

(d) D'après la question précédente, $76\times159-281\times43=1$. Le couple $(x\,;y)=(159\,;43)$ est formé d'entiers naturels et convient (attention au signe : $y=43$ et non -43, car l'équation contient $-281y$).

Ex. 27 **(suite)**

(e) Le programme affiche les x de 0 à 280 tels que $281 \mid 76x-1$, suivis du quotient. Pour $x=159$: $76\times159-1=12\,083=281\times43$, il affiche `159 43`. Unicité : si x convient, 281 divise $(76x-1)-(76\times159-1)=76(x-159)$. En multipliant $33\times281-122\times76=1$ par $x-159$: $x-159=281\times33(x-159)-122\times76(x-159)$, somme de deux multiples de 281, donc $281 \mid x-159$. Comme $-159 \leqslant x-159 \leqslant 121$, on a $x-159=0$. Le programme affiche une seule ligne : `159 43`.

Ex. 28 ★★★ **Démontrer avec Bézout : ab et a + b**

(a) $\text{PGCD}(a\,;b)=1$, donc d'après le théorème de Bézout il existe u, v entiers tels que $au+bv=1$. Alors $a(u-v)+(a+b)v=au-av+av+bv=1$. Comme $u-v$ et v sont entiers, le théorème de Bézout donne : a et $a+b$ sont premiers entre eux.

(b) D'après le théorème de Bézout, il existe des entiers u_1, v_1, u_2, v_2 tels que $cu_1+av_1=1$ et $cu_2+bv_2=1$. En multipliant : $1=c(cu_1u_2+u_1bv_2+av_1u_2)+ab(v_1v_2)$. Les deux coefficients sont entiers, donc d'après le théorème de Bézout, c et ab sont premiers entre eux.

(c) D'après la question a), $a+b$ est premier avec a ; on admet qu'il est premier avec b. On applique la question b) avec $c=a+b$: $a+b$ et ab sont premiers entre eux.

(d) n et $n+1$ sont non nuls et $(n+1)\times1+n\times(-1)=1$: ils sont premiers entre eux d'après le théorème de Bézout. On applique la question c) avec $a=n$ et $b=n+1$: $ab=n^2+n$ et $a+b=2n+1$ sont premiers entre eux, donc la fraction est irréductible. (Autre combinaison possible : $(2n+1)^2-4(n^2+n)=1$.)

(e) Non. « Premiers entre eux » ne veut pas dire « premiers ». $14\times9+25\times(-5)=126-125=1$, donc 14 et 25 sont premiers entre eux (théorème de Bézout). D'après la question c), $14\times25=350$ et $14+25=39$ sont premiers entre eux. Zoé a tort.

5. *Théorème de Gauss et équations $ax+by=c$*

Ex. 29 ★☆☆ **Appliquer Gauss et son corollaire**

(a) $13\times5-8\times8=1$: d'après le théorème de Bézout, $\text{PGCD}(13\,;8)=1$. Comme $13 \mid 8n$ et que 13 est premier avec 8, le théorème de Gauss donne $13 \mid n$.

(b) $15\times3-4\times11=1$, donc $\text{PGCD}(15\,;4)=1$. Par Gauss, $15 \mid n-3$: $n=3+15k$ avec $k \in \mathbb{Z}$.

Ex. 29 (suite)

(c) Non : $\text{PGCD}(14\,;6) = 2 \neq 1$, donc on ne peut pas appliquer Gauss directement. Contre-exemple : $n = 7$, alors $6 \times 7 = 42 = 14 \times 3$, mais $14 \nmid 7$. On simplifie par 2 : $6n = 14k$ donne $3n = 7k$, donc $7 \mid 3n$. Comme $\text{PGCD}(7\,;3) = 1$, Gauss donne $7 \mid n$.

(d) $10 - 9 = 1$, donc 9 et 10 sont premiers entre eux. D'après le corollaire du théorème de Gauss, $9 \times 10 = 90$ divise n.

(e) Faux : $\text{PGCD}(8\,;12) = 4 \neq 1$, donc le corollaire ne s'applique pas. Contre-exemple : $n = 24$ est divisible par 8 et par 12, mais pas par 96. En revanche, $8 \mid n$ et $3 \mid n$ (car $3 \mid 12$), avec $\text{PGCD}(8\,;3) = 1$: par le corollaire, $24 \mid n$.

Ex. 30 ★☆☆ **Des solutions ou pas ?**

(a) $\text{PGCD}(21\,;35) = 7$ et $7 \mid 49$: il y a des solutions. Équation équivalente : $3x + 5y = 7$.

(b) $\text{PGCD}(18\,;42) = 6$ et $6 \nmid 15$ (reste 3) : comme 6 divise $18x + 42y$ pour tous entiers x, y, il n'y a aucune solution.

(c) $\text{PGCD}(26\,;39) = 13$ et $65 = 13 \times 5$: il y a des solutions. Équation équivalente : $2x - 3y = 5$.

(d) $\text{PGCD}(45\,;75) = 15$ et $15 \nmid 40$ (reste 10) : aucune solution.

(e) $\text{PGCD}(22\,;15) = 1$ et $1 \mid 7$: il y a des solutions et l'équation reste la même ($22 \times 1 + 15 \times (-1) = 7$, donc $(1\,;-1)$ est d'ailleurs une solution évidente).

Ex. 31 ★★☆ **Résolution complète avec Bézout**

(a) $\text{PGCD}(34\,;24) = 2$ et $2 \mid 6$: (E) admet des solutions. En divisant par 2, (E) équivaut à (E') : $17x + 12y = 3$.

(b) $17 = 12 \times 1 + 5$, $12 = 5 \times 2 + 2$, $5 = 2 \times 2 + 1$. En remontant : $1 = 5 - 2 \times 2 = 5 \times 5 - 2 \times 12 = 5 \times 17 - 7 \times 12$. En multipliant par 3 :
$17 \times 15 + 12 \times (-21) = 3$, donc $(15\,;-21)$ est une solution particulière de
(E').

(c) Si $(x\,;y)$ est solution, en soustrayant on obtient $17(x - 15) = 12(-21 - y)$.
Donc $12 \mid 17(x - 15)$ et $\text{PGCD}(12\,;17) = 1$: par le théorème de Gauss, $12 \mid x - 15$, soit $x = 15 + 12k$ avec $k \in \mathbb{Z}$. En remplaçant : $17 \times 12k = 12(-21 - y)$, d'où $y = -21 - 17k$. Réciproquement, $17(15 + 12k) + 12(-21 - 17k) = 255 - 252 = 3$. Les solutions sont donc les couples $(15 + 12k\,;-21 - 17k)$ avec $k \in \mathbb{Z}$.

Ex. 31 (suite)

(d) (E) et (E') ont les mêmes solutions. $0 \leqslant 15 + 12k < 12$ donne $k = -1$, donc $(x\,;y) = (3\,;-4)$. Vérification : $34 \times 3 + 24 \times (-4) = 102 - 96 = 6$.

(e) Pour $k = 1$: $(32\,;-33)$ et $17 \times 32 + 12 \times (-33) = 544 - 396 = 148 \neq 3$. Léo a inversé les coefficients : on ajoute à x un multiple du coefficient de y (12) et on retire à y un multiple du coefficient de x
(17).

Ex. 32 ★★☆ **Miel et confiture au marché**

(a) $9 - 7 = 2$ et $7 - 3 \times 2 = 1$, donc $\text{PGCD}(9\,;7) = 1$, qui divise 100 : il y a des solutions. En testant les valeurs de x : pour $x = 1$, $7y = 91$, donc $y = 13$. Le couple $(1\,;13)$ est une solution particulière.

(b) Si $9x + 7y = 100$, en soustrayant $9 \times 1 + 7 \times 13 = 100$ on obtient $9(x - 1) = 7(13 - y)$.
Donc $7 \mid 9(x - 1)$ et $\text{PGCD}(7\,;9) = 1$: par Gauss, $x = 1 + 7k$ avec $k \in \mathbb{Z}$, puis $y = 13 - 9k$. Réciproquement, $9(1 + 7k) + 7(13 - 9k) = 100$. Les solutions sont les couples $(1 + 7k\,;13 - 9k)$ avec $k \in \mathbb{Z}$.

(c) Il faut $x \geqslant 0$ et $y \geqslant 0$: $1 + 7k \geqslant 0$ donne $k \geqslant 0$, et $13 - 9k \geqslant 0$ donne $k \leqslant 1$ (car $k = 2$ donne $y = -5$).
Donc $k = 0$ ou $k = 1$: Inès a acheté 1 pot de miel et 13 de confiture, ou 8 pots de miel et 4 de confiture.

(d) Il faut $x \geqslant y$: seul $(8\,;4)$ convient. Vérification : $9 \times 8 + 7 \times 4 = 72 + 28 = 100$. Inès a acheté 8 pots de miel et 4 pots de confiture.

Ex. 33 ★★★ **Restes imposés (type bac)**

(a) Si N convient, on note x et y les quotients : $N = 19x + 4$ et $N = 12y + 7$.
Donc $19x + 4 = 12y + 7$, soit $19x - 12y = 3$.
Réciproquement, soit $(x\,;y)$ une solution de (E) et $N = 19x + 4 = 12y + 7$. On a $0 \leqslant 4 < 19$ et $0 \leqslant 7 < 12$.
Par unicité de la division euclidienne, les restes sont donc bien 4 et 7.

(b) On a $19 = 1 \times 12 + 7$, puis $12 = 1 \times 7 + 5$, puis $7 = 1 \times 5 + 2$, puis $5 = 2 \times 2 + 1$. On remonte : $1 = 5 - 2 \times 2 = 3 \times 5 - 2 \times 7 = 3 \times 12 - 5 \times 7 = 8 \times 12 - 5 \times 19$.
Donc $u = -5$ et $v = 8$ conviennent. En multipliant par 3 : $19 \times (-15) + 12 \times 24 = 3$, soit $19 \times (-15) - 12 \times (-24) = 3$. Le couple $(-15\,;-24)$ est une solution particulière de
(E).

Ex. 33 **(suite)**

(c) On soustrait $19 \times (-15) - 12 \times (-24) = 3$ à (E). On obtient $19(x+15) = 12(y+24)$.
Donc $12 \mid 19(x+15)$. De plus, $\text{PGCD}(12\,;19) = 1$ d'après la relation de Bézout de la question précédente. Par le théorème de Gauss, $12 \mid x+15$, donc $x = -15 + 12k$ avec $k \in \mathbb{Z}$. En reportant : $19 \times 12k = 12(y+24)$, donc $y = -24 + 19k$. Réciproquement, $19(-15+12k) - 12(-24+19k) = -285 + 288 = 3$. Conclusion : les solutions de (E) sont les couples $(-15+12k\,;-24+19k)$, avec $k \in \mathbb{Z}$.

(d) On a $N = 19x + 4 = 19(-15+12k) + 4 = -281 + 228k$, avec $k \in \mathbb{Z}$. On a bien aussi $12y + 7 = -288 + 228k + 7 = -281 + 228k$. Ensuite, $N \geqslant 0$ équivaut à $k \geqslant \frac{281}{228}$, soit $k \geqslant 2$ puisque k est entier. Le plus petit entier naturel qui convient est donc $N = -281 + 456 = 175$. Vérification : $175 = 19 \times 9 + 4 = 12 \times 14 + 7$.

(e) On résout $1\,000 \leqslant -281 + 228k \leqslant 2\,000$, soit $1\,281 \leqslant 228k \leqslant 2\,281$. Cela donne $5{,}6 < k \leqslant 10{,}004$ environ, donc $k \in \{6\,;7\,;8\,;9\,;10\}$. Les entiers cherchés sont 1 087, 1 315, 1 543, 1 771 et 1 999.

Ex. 34 ★★★ **Billetterie du musée de Nantes**

(a) On a $\text{PGCD}(14\,;8) = 2$. Pour tous entiers x et y, $14x + 8y = 2(7x+4y)$ est pair. Or 225 est impair : $\text{PGCD}(14\,;8)$ ne divise pas 225. L'équation $14x + 8y = 225$ n'a donc aucune solution entière : la caissière s'est trompée.

(b) (E) : $14x + 8y = 222$. On a $\text{PGCD}(14\,;8) = 2$, et 2 divise 222. On divise par 2 et on obtient l'équation équivalente (E') : $7x + 4y = 111$. On a $\text{PGCD}(7\,;4) = 1$ car $2 \times 4 - 7 = 1$.

(c) On a $7 \times 1 + 4 \times 26 = 111$: $(1\,;26)$ est une solution particulière. On soustrait : $7(x-1) = 4(26-y)$, donc $4 \mid 7(x-1)$. Comme $\text{PGCD}(4\,;7) = 1$, le théorème de Gauss donne $4 \mid x-1$, soit $x = 1 + 4k$ avec $k \in \mathbb{Z}$. Alors $7 \times 4k = 4(26-y)$, donc $y = 26 - 7k$. Réciproquement, $7(1+4k) + 4(26-7k) = 7 + 104 = 111$. Les solutions sont les couples $(1+4k\,;26-7k)$, avec $k \in \mathbb{Z}$.

(d) Ses couples sont bien des solutions : $7(9+8k) + 4(12-14k) = 63 + 48 = 111$. Mais il en oublie. Par exemple, $(5\,;19)$ est solution, car $35 + 76 = 111$. Or $9 + 8k = 5$ donne $k = -\frac{1}{2}$, qui n'est pas un entier. Hugo n'a donc pas raison : il a pris pour pas les coefficients 8 et 14 de (E). Il faut prendre ceux de (E'), soit 4 et 7.

Ex. 34 **(suite)**

(e) Les nombres x et y sont des entiers naturels. La condition $x = 1 + 4k \geqslant 0$ donne $k \geqslant 0$. La condition $y = 26 - 7k \geqslant 0$ donne $k \leqslant \frac{26}{7}$, donc $k \leqslant 3$. On obtient 4 compositions : $(1\,;26)$, $(5\,;19)$, $(9\,;12)$ et $(13\,;5)$. Une seule a plus d'adultes que d'enfants : le groupe compte 13 adultes et 5 enfants.

Ex. 35 ★★★ **Racines rationnelles d'un polynôme**

(a) On multiplie $3\left(\frac{p}{q}\right)^3 + \left(\frac{p}{q}\right)^2 + \frac{p}{q} - 2 = 0$ par $q^3 \neq 0$: on obtient $3p^3 + p^2q + pq^2 - 2q^3 = 0$, soit $3p^3 + p^2q + pq^2 = 2q^3$. Ainsi $2q^3 = p(3p^2 + pq + q^2)$, où $3p^2 + pq + q^2$ est un entier : $p \mid 2q^3$. De même, $3p^3 = q(2q^2 - p^2 - pq)$: $q \mid 3p^3$.

(b) On a $p \mid 2q^2 \times q$ et $\text{PGCD}(p\,;q) = 1$. Par le théorème de Gauss, $p \mid 2q^2 = 2q \times q$. On applique encore Gauss : $p \mid 2q$, puis $p \mid 2$. De même, $q \mid 3p^2 \times p$ et $\text{PGCD}(q\,;p) = 1$ donnent successivement $q \mid 3p^2$, puis $q \mid 3p$, puis $q \mid 3$. Conclusion : $p \mid 2$ et $q \mid 3$.

(c) On a $p \in \{-2\,;-1\,;1\,;2\}$ et $q \in \{1\,;3\}$ car $q > 0$. Les candidats sont donc ± 1, ± 2, $\pm\frac{1}{3}$ et $\pm\frac{2}{3}$. On pose $P(x) = 3x^3 + x^2 + x - 2$. On calcule $P(1) = 3$, $P(-1) = -5$, $P(2) = 28$, $P(-2) = -24$, $P\left(\frac{1}{3}\right) = -\frac{13}{9}$, $P\left(-\frac{1}{3}\right) = -\frac{7}{3}$ et $P\left(-\frac{2}{3}\right) = -\frac{28}{9}$. Enfin, $P\left(\frac{2}{3}\right) = \frac{8}{9} + \frac{4}{9} + \frac{6}{9} - 2 = 0$. La seule solution rationnelle de (E) est donc $\frac{2}{3}$.

(d) On a $\frac{2}{3} = \frac{4}{6}$. Avec $p = 4$ et $q = 6$, on a bien $p \mid 2q^3 = 432$, mais $4 \nmid 2$. Le théorème de Gauss exige que p soit premier avec q. Or ici $\text{PGCD}(4\,;6) = 2 \neq 1$: les déductions de la question précédente ne sont plus justifiées, et la conclusion $p \mid 2$ est fausse.

6. *Nombres premiers : test, infinité, décomposition, PGCD et PPCM*

Ex. 36 ★☆☆ **Tester la primalité, utiliser le crible**

(a) Non. Un nombre premier a exactement deux diviseurs positifs distincts, 1 et lui-même. Le nombre 1 n'a qu'un seul diviseur positif : 1 n'est pas premier.

(b) $16^2 = 256 < 263 < 289 = 17^2$, donc $\sqrt{263} < 17$: on teste 2, 3, 5, 7, 11 et 13. 263 est impair ; $2 + 6 + 3 = 11$, donc $3 \nmid 263$; 263 ne finit ni par 0 ni par 5 ; $263 = 7 \times 37 + 4 = 11 \times 23 + 10 = 13 \times 20 + 3$. Aucun ne divise 263 : 263 est premier.

Ex. 36 (suite)

(c) $391 = 400 - 9 = 20^2 - 3^2 = (20-3)(20+3) = 17 \times 23$.
Donc 17 est un diviseur de 391 tel que $1 < 17 < 391$.
Conclusion : 391 n'est pas premier.

(d) Non. $22^2 = 484 < 527 < 529 = 23^2$: il faut tester tous les nombres premiers jusqu'à 19, et pas seulement jusqu'à 13. Or $527 = 17 \times 31$: 527 est composé. Théo s'est arrêté trop tôt.

(e) Pas besoin d'aller jusqu'à 204 : si 409 était composé, il aurait un diviseur premier p tel que $p^2 \leqslant 409$. Comme $20^2 = 400 < 409 < 441 = 21^2$, on teste 2, 3, 5, 7, 11, 13, 17, 19. Les restes sont 1, 1, 4, 3, 2, 6, 1, 10. Aucun n'est nul : 409 est premier.

(f) À partir de $11^2 = 121$. Un multiple $11k$ avec $2 \leqslant k \leqslant 10$ a un facteur premier inférieur à 11 : il a déjà été barré.

(g) 13. En effet, $13^2 = 169 \leqslant 200$ mais $17^2 = 289 > 200$. Après les multiples de 13, tout entier non barré inférieur ou égal à 200 est premier.

Ex. 37 ★☆☆ Décomposer, compter les diviseurs, carrés parfaits

(a) $1\,008 = 2 \times 504 = 2^2 \times 252 = 2^3 \times 126 = 2^4 \times 63 = 2^4 \times 3^2 \times 7$.

(b) $(4+1)(2+1)(1+1) = 30$ diviseurs positifs.
L'exposant 1 de 7 compte : il donne le facteur 2.

(c) $2\,310 = 2 \times 1\,155 = 2 \times 3 \times 385 = 2 \times 3 \times 5 \times 7 \times 11$. Tous les exposants valent 1, donc on a $2^5 = 32$ diviseurs positifs.

(d) Un diviseur impair de $1\,008 = 2^4 \times 3^2 \times 7$ ne contient pas le facteur 2 : c'est un diviseur de $3^2 \times 7 = 63$. Il y en a $(2+1)(1+1) = 6$: 1, 3, 7, 9, 21 et 63.

(e) Non. Dans $1\,008 = 2^4 \times 3^2 \times 7$, l'exposant de 7 vaut 1, et il est impair.

(f) Il faut rendre pair l'exposant de 7 sans changer les autres : $k = 7$. On obtient $1\,008 \times 7 = 7\,056 = 2^4 \times 3^2 \times 7^2 = (2^2 \times 3 \times 7)^2 = 84^2$.

(g) $7\,056 = 2^4 \times 3^2 \times 7^2$ a $5 \times 3 \times 3 = 45$ diviseurs positifs. Tous les exposants sont pairs, donc chaque facteur $a+1$ est impair, et le produit est impair.

Ex. 38 ★★☆ PGCD et PPCM par les décompositions

(a) $a = 22 \times 100 = 2^3 \times 5^2 \times 11$ et $b = 2^5 \times 15 = 2^5 \times 3 \times 5$.

(b) Le facteur 3 est absent de a et le facteur 11 est absent de b : leur exposant y vaut 0, donc leur plus petit exposant est 0. Malik a oublié ces exposants nuls. D'ailleurs, 1 320 ne divise pas 480. Les seuls facteurs communs sont 2 (exposant $\min(3;5) = 3$) et 5 (exposant $\min(2;1) = 1$).
Donc $\mathrm{PGCD}(a;b) = 2^3 \times 5 = 40$.

(c) $\mathrm{PGCD}(a;b) \times \mathrm{PPCM}(a;b) = ab$, donc $\mathrm{PPCM}(a;b) = \frac{2\,200 \times 480}{40} = 26\,400$. Contrôle avec les plus grands exposants : $2^5 \times 3 \times 5^2 \times 11 = 26\,400$. Le résultat est confirmé.

(d) $2\,200m$ est un multiple de 2 200 et de 480, donc un multiple de leur PPCM $26\,400 = 2\,200 \times 12$. Ainsi, 12 divise m. Réciproquement, $2\,200 \times 12 = 26\,400 = 480 \times 55$. Le plus petit entier cherché est donc $m = 12$.

(e) Les diviseurs communs positifs de a et b sont les diviseurs positifs de $\mathrm{PGCD}(a;b) = 40 = 2^3 \times 5$. Il y en a $(3+1)(1+1) = 8$: 1, 2, 4, 5, 8, 10, 20 et 40.

Ex. 39 ★★☆ Une infinité de nombres premiers

(a) Le nombre 2 est premier, donc il fait partie de la liste. Le produit vaut donc au moins 2, et $N \geqslant 3 \geqslant 2$. Soit d le plus petit diviseur de N tel que $d \geqslant 2$. Si d n'était pas premier, il aurait un diviseur d' avec $1 < d' < d$, et d' diviserait N : c'est contraire au choix de d.
Donc $d = p$ est un diviseur premier de N.

(b) Posons $P = p_1 \times \cdots \times p_k$. Supposons que $p = p_i$. Alors $p \mid P$ et $p \mid N$, donc p divise la combinaison linéaire $N - P = 1$. C'est impossible, car $p \geqslant 2$.
Donc p n'est égal à aucun des p_i.

(c) p est un nombre premier qui ne figure pas dans la liste $p_1, \ldots, p_k$. Or cette liste devait contenir tous les nombres premiers : c'est une contradiction. Il existe donc une infinité de nombres premiers.

(d) $2 \times 3 \times 5 \times 7 \times 11 \times 13 + 1 = 30\,031 = 59 \times 509$. Lina a tort : ce nombre n'est pas premier. La preuve montre seulement que N a un diviseur premier hors de la liste. Ici, 59 et 509 sont bien premiers et plus grands que 13.

Ex. 39 **(suite)**

(e) Pour $n \geqslant 2$, $n! \geqslant 2$, donc $n! + 1 \geqslant 3$: comme à la question 1, $n! + 1$ admet un diviseur premier p. Si $p \leqslant n$, p est un des facteurs de $n! = 1 \times 2 \times \cdots \times n$, donc $p \mid n!$. Alors p divise $(n! + 1) - n! = 1$, ce qui est impossible.
Donc $p > n$. Pour $n = 5$: $5! + 1 = 121 = 11^2$ n'est pas premier, mais son diviseur premier 11 vérifie bien $11 > 5$.

Ex. 40 ★★★ **Expressions en n : premières ou non ?**

(a) $n^2 - 1 = (n-1)(n+1)$. Pour $n = 0$ on obtient -1 et pour $n = 1$ on obtient 0 : aucun des deux n'est premier. Pour $n = 2$, $n^2 - 1 = 1 \times 3 = 3$, qui est premier. Pour $n \geqslant 3$, on a $n - 1 \geqslant 2$ et $n + 1 \geqslant 4$, donc $n^2 - 1$ a un diviseur $n - 1$ tel que $1 < n - 1 < n^2 - 1$: il n'est pas premier. Conclusion : $n^2 - 1$ est premier seulement pour $n = 2$.

(b) $(n^2 + 2n + 2)(n^2 - 2n + 2) = (n^2 + 2)^2 - (2n)^2 = n^4 + 4n^2 + 4 - 4n^2 = n^4 + 4$. L'égalité est vraie pour tout entier naturel n.

(c) Pour $n = 0$, $n^4 + 4 = 4 = 2^2$ n'est pas premier. Pour $n = 1$, $n^4 + 4 = 5$ est premier : le facteur $n^2 - 2n + 2$ vaut 1, donc la factorisation ne fait pas apparaître de vrai diviseur. Pour $n \geqslant 2$, $n^2 - 2n + 2 = (n-1)^2 + 1 \geqslant 2$ et $n^2 + 2n + 2 > n^2 - 2n + 2$, donc les deux facteurs sont supérieurs ou égaux à 2 : $n^4 + 4$ est composé. Conclusion : $n^4 + 4$ est premier si et seulement si $n = 1$.

(d) $7^4 + 4 = 2\,401 + 4 = 2\,405$. D'après la question 2, $2\,405 = (49 + 14 + 2)(49 - 14 + 2) = 65 \times 37$, et $65 = 5 \times 13$. Comme $6^2 = 36 < 37 < 49 = 7^2$, il suffit de tester les nombres premiers 2, 3 et 5 : aucun ne divise 37 (restes 1, 1 et 2), donc 37 est premier. De même, $3^2 < 13 < 4^2$ et ni 2 ni 3 ne divise 13, donc 13 est premier ; 5 est premier. Conclusion : $2\,405 = 5 \times 13 \times 37$.

Ex. 40 **(suite)**

(e) Pour $n = 1$, la boucle ne s'exécute pas car $2 \times 2 > 1$: la fonction renvoie `True`, alors que 1 n'est pas premier.
Correction :

```
def premier(n):
    if n < 2:
        return False
    d = 2
    while d * d <= n:
        if n % d == 0:
            return False
        d = d + 1
    return True
```

Justification : si $n = ab$ avec $2 \leqslant a \leqslant b$, alors $a^2 \leqslant ab = n$. Un entier composé a donc un diviseur d tel que $d^2 \leqslant n$. Si aucun d de ce type ne divise n, alors n est premier : tester jusqu'à `n // 2` serait juste, mais inutilement long.

Ex. 41 ★★★ **Entiers à nombre de diviseurs imposé**

(a) Yanis a oublié que l'exposant 0 compte : chaque exposant doit être augmenté de 1. $56 = 2^3 \times 7^1$ a donc $(3+1)(1+1) = 8$ diviseurs positifs : ce sont les $2^b \times 7^c$ avec $0 \leqslant b \leqslant 3$ et $0 \leqslant c \leqslant 1$, soit 1, 2, 4, 8, 7, 14, 28 et 56.

(b) Il faut écrire 12 comme un produit de facteurs $a_i + 1 \geqslant 2$: 12, 6×2, 4×3 ou $3 \times 2 \times 2$. Avec p, q, r premiers distincts, les formes possibles sont donc : p^{11}, $p^5 q$, $p^3 q^2$ et $p^2 qr$.

(c) Dans chaque forme, on obtient le plus petit entier en mettant les plus petits nombres premiers sur les plus grands exposants : $2^{11} = 2\,048$; $2^5 \times 3 = 96$; $2^3 \times 3^2 = 72$; $2^2 \times 3 \times 5 = 60$. Conclusion : le plus petit entier naturel ayant exactement 12 diviseurs positifs est 60.

(d) n a $(a+1)(b+1)$ diviseurs, il faut donc $(a+1)(b+1) = 9$, d'où $(a+1\,;b+1) \in \{(1\,;9)\,;(3\,;3)\,;(9\,;1)\}$. Les solutions sont $(a\,;b) = (0\,;8)$, $(2\,;2)$ et $(8\,;0)$, soit $n = 3^8 = 6\,561$, $n = 2^2 \times 3^2 = 36$ et $n = 2^8 = 256$. Dans les trois cas, tous les exposants sont pairs, donc chaque n est un carré parfait : $6\,561 = 81^2$, $36 = 6^2$ et $256 = 16^2$.

Ex. 41 **(suite)**

(e) Soit $n = p_1^{a_1} \times \cdots \times p_r^{a_r}$ la décomposition de n (avec $a_i \geqslant 1$). Le nombre de diviseurs $(a_1+1) \times \cdots \times (a_r+1)$ est impair si et seulement si chaque $a_i + 1$ est impair, c'est-à-dire si chaque a_i est pair. Si tous les a_i sont pairs, $n = \left(p_1^{a_1/2} \times \cdots \times p_r^{a_r/2}\right)^2$ est un carré. Réciproquement, si $n = m^2$, les exposants de n sont le double de ceux de m, par unicité de la décomposition : ils sont pairs. Conclusion : n a un nombre impair de diviseurs si et seulement si n est un carré parfait.

Ex. 42 ★★★ **Retrouver deux entiers à partir de leur PGCD et de leur PPCM**

(a) On écrit $a = 2^4 \times 3^1 \times 5^0 \times 7^2$ et $b = 2^2 \times 3^3 \times 5^1 \times 7^0$. Le PGCD prend les plus petits exposants : $\text{PGCD}(a\,;b) = 2^2 \times 3 = 12$, car 5 et 7 ne sont pas communs (exposant 0). Le PPCM prend les plus grands : $\text{PPCM}(a\,;b) = 2^4 \times 3^3 \times 5 \times 7^2 = 105\,840$. Contrôle : $a = 2\,352$, $b = 540$ et $12 \times 105\,840 = 1\,270\,080 = 2\,352 \times 540$.

(b) On écrit $a = \prod p_i^{\alpha_i}$ et $b = \prod p_i^{\beta_i}$ avec les mêmes nombres premiers p_i (exposants éventuellement nuls). On a alors $\text{PGCD}(a\,;b) = \prod p_i^{\min(\alpha_i\,;\beta_i)}$ et $\text{PPCM}(a\,;b) = \prod p_i^{\max(\alpha_i\,;\beta_i)}$. Or pour tous réels α et β, on a $\min(\alpha\,;\beta) + \max(\alpha\,;\beta) = \alpha + \beta$. Donc $\text{PGCD}(a\,;b) \times \text{PPCM}(a\,;b) = \prod p_i^{\alpha_i+\beta_i} = ab$.

(c) Comme 18 divise a et b, on peut écrire $a = 18a'$ et $b = 18b'$. Alors $\text{PGCD}(a\,;b) = 18 \times \text{PGCD}(a'\,;b')$, donc $\text{PGCD}(a'\,;b') = 1$: a' et b' sont premiers entre eux. D'après la question 2, $ab = 18 \times 1\,260$, c'est-à-dire $18^2 a'b' = 18 \times 1\,260$. On en déduit $a'b' = \dfrac{1\,260}{18} = 70$.

(d) $70 = 2 \times 5 \times 7$. Les couples $(a'\,;b')$ tels que $a' \leqslant b'$, $a'b' = 70$ et a', b' premiers entre eux sont $(1\,;70)$, $(2\,;35)$, $(5\,;14)$ et $(7\,;10)$. Réciproquement, pour chacun d'eux, le PGCD vaut 18 et le PPCM vaut $18 \times 70 = 1\,260$. Les couples cherchés sont donc $(18\,;1\,260)$, $(36\,;630)$, $(90\,;252)$ et $(126\,;180)$.

(e) Nora a tort. Le PGCD divise a, qui divise le PPCM : le PGCD divise donc toujours le PPCM. Or $1\,000 = 18 \times 55 + 10$, donc $18 \nmid 1\,000$. Conclusion : deux tels entiers n'existent pas.

7. *Petit théorème de Fermat*

Ex. 43 ★☆☆ **Restes de grandes puissances**

(a) 13 est premier et $13 \nmid 2$, donc $2^{12} \equiv 1\ [13]$. On divise l'exposant par 12 et non par 13 : $150 = 12 \times 12 + 6$. Donc $2^{150} = (2^{12})^{12} \times 2^6 \equiv 2^6 = 64\ [13]$. Comme $64 = 4 \times 13 + 12$, le reste est 12.

(b) 11 est premier et $11 \nmid 5$, donc $5^{10} \equiv 1\ [11]$. $243 = 10 \times 24 + 3$, donc $5^{243} \equiv 5^3 = 125\ [11]$. Comme $125 = 11 \times 11 + 4$, le reste est 4.

(c) 17 est premier et $17 \nmid 2$, donc $2^{16} \equiv 1\ [17]$. $500 = 16 \times 31 + 4$, donc $2^{500} \equiv 2^4 = 16\ [17]$. Le reste est 16.

(d) 19 est premier et $19 \nmid 6$, donc $6^{18} \equiv 1\ [19]$. $2026 = 18 \times 112 + 10$, donc $6^{2026} \equiv 6^{10}\ [19]$. Or $6^2 = 36 \equiv -2\ [19]$, donc $6^8 \equiv (-2)^4 = 16\ [19]$ et $6^{10} \equiv 16 \times (-2) = -32 \equiv 6\ [19]$. Le reste est 6.

(e) 23 est premier et $23 \nmid 3$, donc $3^{22} \equiv 1\ [23]$. $1000 = 22 \times 45 + 10$, donc $3^{1000} \equiv 3^{10}\ [23]$. Or $3^5 = 243 = 10 \times 23 + 13$, donc $3^{10} \equiv 13^2 = 169\ [23]$. Comme $169 = 7 \times 23 + 8$, le reste est 8.

Ex. 44 ★☆☆ **Le théorème s'applique-t-il ?**

(a) 17 est premier et $17 \nmid 4$: la forme $a^{p-1} \equiv 1\ [p]$ s'applique, donc $4^{16} \equiv 1\ [17]$. Le reste est 1.

(b) $15 = 3 \times 5$ n'est pas premier : le théorème ne s'applique pas. On calcule directement : $10^2 = 100 = 6 \times 15 + 10$, donc $10^2 \equiv 10\ [15]$. De proche en proche, $10^k \equiv 10\ [15]$ pour tout $k \geqslant 1$. Le reste est 10, et non 1.

(c) 11 est premier, mais $11 \mid 22$: la forme $a^{p-1} \equiv 1\ [p]$ ne s'applique pas. Comme $22 \equiv 0\ [11]$, on a $22^{10} \equiv 0\ [11]$. Le reste est 0.

(d) 23 est premier : la forme $a^p \equiv a\ [p]$ s'applique pour tout entier a. Donc $5^{23} \equiv 5\ [23]$. Le reste est 5.

(e) $21 = 3 \times 7$ n'est pas premier : le théorème ne s'applique pas. $2^{10} = 1024 = 48 \times 21 + 16$, donc $2^{20} \equiv 16^2 = 256\ [21]$. Comme $256 = 12 \times 21 + 4$, le reste est 4, et non 1.

(f) 29 est premier et $29 \nmid 9$: la forme $a^{p-1} \equiv 1\ [p]$ s'applique, donc $9^{28} \equiv 1\ [29]$. Le reste est 1.

Ex. 45 ★★☆ **Trois élèves, trois affirmations**

(a) Léa a tort : elle a divisé l'exposant par $p = 11$ au lieu de $p - 1 = 10$. 11 est premier et $11 \nmid 3$, donc, d'après le petit théorème de Fermat, $3^{10} \equiv 1\ [11]$. Or $200 = 10 \times 20$, donc $3^{200} = (3^{10})^{20} \equiv 1\ [11]$. Le reste de 3^{200} modulo 11 est 1.

(b) Malik a tort : $561 = 3 \times 187 = 3 \times 11 \times 17$ n'est pas premier. Le petit théorème de Fermat dit « si p est premier, alors… » ; sa réciproque est fausse. Un entier composé peut vérifier $2^{n-1} \equiv 1\ [n]$. Conclusion : de $2^{560} \equiv 1\ [561]$ on ne peut pas déduire que 561 est premier, et 561 est composé.

(c) Nora a tort : pour $n = 11$, $11 \equiv 0\ [11]$, donc $11^{10} \equiv 0\ [11]$, et non 1. La forme $n^{10} \equiv 1\ [11]$ exige que $11 \nmid n$. Conclusion correcte : pour tout entier n non divisible par 11, $n^{10} \equiv 1\ [11]$; pour tout entier n, $n^{11} \equiv n\ [11]$.

Ex. 46 ★★☆ **Un diviseur commun à tous les $n^7 - n$**

(a) 7 est premier. D'après le petit théorème de Fermat, sous la forme valable pour tout entier, $n^7 \equiv n\ [7]$, même si $7 \mid n$.
Donc $n^7 - n \equiv 0\ [7]$. Conclusion : pour tout entier n, 7 divise $n^7 - n$.

(b) 3 est premier, donc pour tout entier n, $n^3 \equiv n\ [3]$ (Fermat). Alors $n^7 = n^3 \times n^3 \times n \equiv n \times n \times n = n^3 \equiv n\ [3]$. Conclusion : pour tout entier n, 3 divise $n^7 - n$.

(c) 2 est premier, donc pour tout entier n, $n^2 \equiv n\ [2]$ (Fermat). De proche en proche, $n^7 \equiv n\ [2]$: n^7 et n ont même parité. Conclusion : pour tout entier n, 2 divise $n^7 - n$.

(d) 2, 3 et 7 sont des nombres premiers distincts, donc premiers entre eux deux à deux. Ils divisent tous N, donc, par le corollaire du théorème de Gauss, $2 \times 3 \times 7 = 42$ divise N. On peut prendre $d = 42$. Vérification : $2^7 - 2 = 126 = 42 \times 3$ et $3^7 - 3 = 2184 = 42 \times 52$.

Ex. 47 ★★★ **Un faux premier : 341**

(a) 341 n'est divisible ni par 2, ni par 3, ni par 5, ni par 7. En revanche, $341 = 11 \times 31$, et 11 et 31 sont premiers. La décomposition est donc $341 = 11 \times 31$.

(b) $2^{10} = 1\,024$ et $1\,024 = 3 \times 341 + 1$ avec $0 \leqslant 1 < 341$. Le reste est donc 1, c'est-à-dire $2^{10} \equiv 1\ [341]$.

(c) $340 = 10 \times 34$, donc $2^{340} = (2^{10})^{34} \equiv 1^{34} = 1\ [341]$. Le reste de 2^{340} dans la division par 341 est 1.

Ex. 47 (suite)

(d) Non. Le petit théorème de Fermat dit : si p est premier et ne divise pas a, alors $a^{p-1} \equiv 1\ [p]$. La réciproque est fausse : on a $2^{340} \equiv 1\ [341]$, et pourtant $341 = 11 \times 31$ n'est pas premier. La conclusion de Hugo est fausse.

(e) 31 est premier et ne divise pas 3. D'après le petit théorème de Fermat, $3^{30} \equiv 1\ [31]$. On divise l'exposant par 30, et non par 31 : $340 = 30 \times 11 + 10$, donc $3^{340} = (3^{30})^{11} \times 3^{10} \equiv 3^{10}\ [31]$. Or $3^5 = 243 = 7 \times 31 + 26$, donc $3^5 \equiv -5\ [31]$ et $3^{10} \equiv 25\ [31]$. Le reste est 25.
Supposons que $3^{340} \equiv 1\ [341]$. Alors $341 \mid 3^{340} - 1$, donc $31 \mid 3^{340} - 1$, soit $3^{340} \equiv 1\ [31]$: c'est contradictoire.
Comme de plus $341 \nmid 3$, l'entier 3 est un témoin, et 341 n'est pas premier.

Ex. 48 ★★★ **Les diviseurs de $n^{17} - n$**

(a) 17 est premier. D'après le petit théorème de Fermat, sous la forme valable pour tout entier, $n^{17} \equiv n\ [17]$. Donc $17 \mid n^{17} - n$. Si $17 \mid n$, on a aussi directement $n^{17} \equiv 0 \equiv n\ [17]$. Conclusion : 17 divise N pour tout entier naturel n.

(b) Si $p \nmid n$: p est premier, donc $n^{p-1} \equiv 1\ [p]$ par le petit théorème de Fermat. Or $16 = 1 \times 16 = 2 \times 8 = 4 \times 4$ est un multiple de $p - 1$, donc $n^{16} \equiv 1\ [p]$, puis $n^{17} \equiv n\ [p]$. Si $p \mid n$: on ne peut pas écrire $n^{p-1} \equiv 1\ [p]$, mais $n^{17} \equiv 0 \equiv n\ [p]$. Dans les deux cas, $p \mid N$: 2, 3 et 5 divisent N.

(c) 2, 3, 5 et 17 divisent N. Ce sont des nombres premiers distincts, donc premiers entre eux deux à deux. Par le corollaire du théorème de Gauss, appliqué de proche en proche, leur produit divise N : $d = 2 \times 3 \times 5 \times 17 = 510$ divise N pour tout entier naturel n.

(d) Pour $n = 2$: $N = 2^{17} - 2 = 131\,072 - 2 = 131\,070$. Or $131\,070 = 4 \times 32\,767 + 2$, donc $4 \nmid 131\,070$. Conclusion : 4 ne divise pas N pour tout entier naturel n.

(e) Faux. 7 est premier, mais $7 - 1 = 6$ ne divise pas 16 : le raisonnement ne s'applique pas. Contre-exemple $n = 3$: $7 \nmid 3$, donc $3^6 \equiv 1\ [7]$; $16 = 6 \times 2 + 4$, donc $3^{16} \equiv 3^4 = 81 \equiv 4\ [7]$, puis $3^{17} \equiv 12 \equiv 5\ [7]$ et $3^{17} - 3 \equiv 2\ [7]$.
Donc 7 ne divise pas N pour $n = 3$: Ana a tort.

Ex. 49 ★★★ **Quels premiers divisent 2^p+1 ?**

(a) Si $n \geqslant 2$ n'est pas premier, alors $n = ab$ avec $2 \leqslant a \leqslant b$, donc $a^2 \leqslant ab = n$: n a un diviseur d tel que $2 \leqslant d$ et $d^2 \leqslant n$. Si aucun d vérifiant $d \times d \leqslant n$ ne divise n, alors n est premier. On peut donc arrêter la boucle dès que `d * d > n`.

(b) p est premier. D'après le petit théorème de Fermat, sous la forme valable pour tout entier (même $p = 2$), $2^p \equiv 2\ [p]$.
Donc $2^p + 1 \equiv 3\ [p]$, c'est-à-dire que $2^p + 1 - 3$ est un multiple de p. Ainsi $p \mid 2^p + 1$ si et seulement si $p \mid 3$.

(c) Le seul diviseur premier de 3 est 3. On vérifie : $2^3 + 1 = 9$, et $3 \mid 9$. Le seul nombre premier qui convient est donc $p = 3$, et le programme affiche uniquement 3.

(d) Non. Pour p premier, $3^p \equiv 3\ [p]$ par le petit théorème de Fermat, donc $3^p + 5 \equiv 8\ [p]$. Ainsi $p \mid 3^p + 5$ si et seulement si $p \mid 8$, c'est-à-dire $p = 2$. On vérifie : $3^2 + 5 = 14$, et $2 \mid 14$. Le programme affiche alors 2, et non 3 : Mila a tort.

(e) Faux. Pour $p = 2$, $2^{p-1} - 1 = 2^1 - 1 = 1$, et 2 ne divise pas 1. La forme $a^{p-1} \equiv 1\ [p]$ demande que p ne divise pas a. Ici $p = 2$ divise $a = 2$. L'affirmation est vraie seulement pour les nombres premiers $p \neq 2$.