

Arithmétique dans $\mathbb{Z}$

Corrigé de l'exercice 1 : Division euclidienne et carrés modulo 8

1. D'abord, $37 \times 54 = 1998$ et $2026 - 1998 = 28$, avec $0 \leq 28 < 37$. Donc $2026 = 37 \times 54 + 28$: **quotient 54, reste 28**. Ensuite, $13 \times (-20) = -260$ et $-260 \leq -250 < -247$. Ainsi $-250 = 13 \times (-20) + 10$: **quotient -20, reste 10**. Le reste doit être positif : l'écriture $-250 = 13 \times (-19) - 3$ ne convient pas.
2. Écrivons $n = 8k + s$ avec $s \in \{0, \dots, 7\}$. Alors $n^2 = 8(8k^2 + 2ks) + s^2$, donc n^2 et s^2 ont le même reste modulo 8. Or les carrés 0, 1, 4, 9, 16, 25, 36, 49 ont pour restes 0, 1, 4, 1, 0, 1, 4, 1. Par conséquent, **les restes possibles de n^2 sont 0, 1 et 4**. De plus, si n est impair, alors $s \in \{1, 3, 5, 7\}$ et le reste vaut 1. On peut aussi le voir directement : $n = 2m + 1$ donne $n^2 = 4m(m+1) + 1$, et $m(m+1)$ est pair.
3. Soient $a, b, c \in \mathbb{Z}$. D'après la question 2, $a^2 + b^2 + c^2$ a le même reste modulo 8 qu'une somme de trois éléments de $\{0, 1, 4\}$. Ces sommes valent 0, 1, 2, 3, 4, 5, 6, 8, 9, 12. Leurs restes modulo 8 sont donc 0, 1, 2, 3, 4, 5, 6, 0, 1, 4. Le reste 7 n'apparaît jamais. Ainsi, **aucun entier de reste 7 modulo 8 n'est somme de trois carrés** ; c'est le cas par exemple de 7, 15 ou 23.

Point de méthode : pour étudier une expression polynomiale modulo n , il suffit de tester les n restes possibles de la variable.

Corrigé de l'exercice 2 : Divisibilité par récurrence

1. Posons $u_n = 3^{2n+1} + 2^{n+2}$. D'abord, $u_0 = 3 + 4 = 7$ est divisible par 7. Ensuite, supposons $7 \mid u_n$. On calcule

$$u_{n+1} = 9 \times 3^{2n+1} + 2 \times 2^{n+2} = 9u_n - 7 \times 2^{n+2}.$$

Les deux termes sont multiples de 7, donc $7 \mid u_{n+1}$. Par récurrence, 7 **divise** $3^{2n+1} + 2^{n+2}$ **pour tout** $n \in \mathbb{N}$.

2. Posons $w_n = 4^n + 6n - 1$. On a $w_0 = 0$, qui est divisible par 9. Supposons $9 \mid w_n$. Alors

$$w_{n+1} = 4 \times 4^n + 6n + 5 = 4w_n - 24n + 4 + 6n + 5 = 4w_n - 18n + 9.$$

Or $4w_n$, $18n$ et 9 sont multiples de 9. Donc 9 **divise** $4^n + 6n - 1$ **pour tout** $n \in \mathbb{N}$.

Point de méthode : exprimez u_{n+1} comme combinaison de u_n et d'un multiple évident du diviseur ; c'est la clé de toutes ces récurrences.

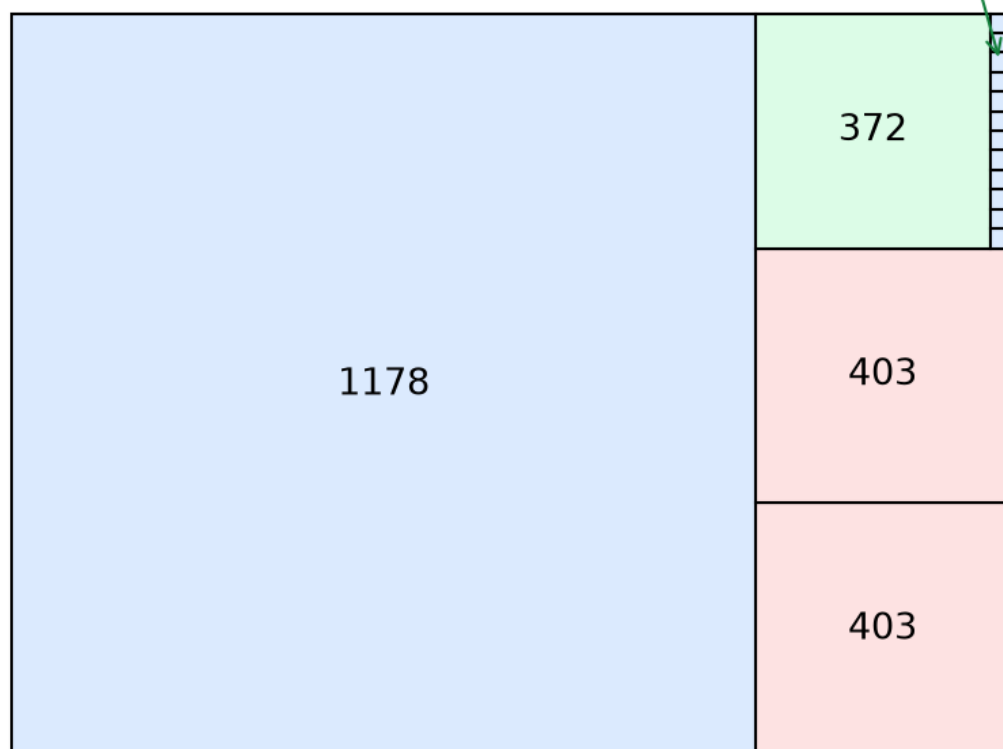
Corrigé de l'exercice 3 : PGCD par l'algorithme d'Euclide

- Soit δ un diviseur commun de a et b . Alors δ divise la combinaison $r = a - bq$. Réciproquement, un diviseur commun de b et r divise $a = bq + r$. Les couples (a, b) et (b, r) ont donc les mêmes diviseurs communs. Par conséquent, $a \wedge b = b \wedge r$, y compris lorsque certains de ces entiers sont nuls.
- On enchaîne les divisions euclidiennes :

$$\begin{aligned} 1581 &= 1 \times 1178 + 403, \\ 1178 &= 2 \times 403 + 372, \\ 403 &= 1 \times 372 + 31, \\ 372 &= 12 \times 31 + 0. \end{aligned}$$

Le dernier reste non nul est 31, donc $1581 \wedge 1178 = 31$. Chaque division correspond à une étape du découpage : on place un carré de côté 1178, puis deux de côté 403, un de côté 372 et enfin douze de côté 31. Ainsi, **le dernier carré a pour côté 31**, comme le montre la figure ci-dessous.

douze carrés de côté 31



$$1581 = 1178 + 403 ; 1178 = 2 \times 403 + 372 ; \\ 403 = 372 + 31 ; 372 = 12 \times 31$$

3. On a $1581 = 31 \times 51$ et $1178 = 31 \times 38$. D'après la relation $(a \wedge b)(a \vee b) = ab$, on obtient

$$1581 \vee 1178 = \frac{1581 \times 1178}{31} = 51 \times 1178 = 60078.$$

Donc $1581 \vee 1178 = 60078$. On vérifie que $60078 = 31 \times 51 \times 38$, et que $51 \wedge 38 = 1$.

Corrigé de l'exercice 4 : Algorithme d'Euclide étendu

1. On dresse le tableau de l'algorithme d'Euclide étendu. Chaque ligne vaut la ligne d'avant-hier moins

q_k fois la ligne d'hier :

$$\begin{array}{c|c|c|c}
 q_k & r_k & u_k & v_k \\
 \hline
 & 2026 & 1 & 0 \\
 & 311 & 0 & 1 \\
 6 & 160 & 1 & -6 \\
 1 & 151 & -1 & 7 \\
 1 & 9 & 2 & -13 \\
 16 & 7 & -33 & 215 \\
 1 & 2 & 35 & -228 \\
 3 & 1 & -138 & 899
 \end{array}$$

En effet, $2026 = 6 \times 311 + 160$, $311 = 160 + 151$, $160 = 151 + 9$,
 $151 = 16 \times 9 + 7$, $9 = 7 + 2$ et $7 = 3 \times 2 + 1$. Vérifions : $2026 \times 138 = 279588$
et $311 \times 899 = 279589$. Donc $2026 \times (-138) + 311 \times 899 = 1$, et $2026 \wedge 311 = 1$.

2. En lisant l'égalité modulo 2026 , on obtient $\frac{311 \times 899}{[2026]} \equiv 1$. Ainsi, **899 est un inverse de 311 modulo 2026**.

3. On multiplie la congruence par l'inverse : $311x \equiv 2$ équivaut à $\frac{x \equiv 2 \times 899 = 1798}{[2026]}$.
Réciproquement, ces entiers conviennent, puisque

$311 \times 1798 = 559178 = 276 \times 2026 + 2$. Donc **les solutions sont les** $\frac{x \equiv 1798}{[2026]}$.

Corrigé de l'exercice 5 : Existence de solutions de $ax + by = c$

1. D'abord, $12 \wedge 18 = 6$. Si (x, y) est solution, 6 divise $12x$ et $18y$, donc $6 \mid c$.
Réciproquement, supposons $c = 6c'$. Comme $12 \times (-1) + 18 \times 1 = 6$, le couple $(-c', c')$ est solution. Ainsi, **l'équation a une solution si et seulement si $6 \mid c$** .

2. L'équation $12x + 18y = 30$ équivaut à $2x + 3y = 5$, qui admet la solution particulière $(1, 1)$. Par soustraction, $2(x - 1) = -3(y - 1)$. Or $2 \wedge 3 = 1$ et 3 divise $2(x - 1)$, donc $3 \mid x - 1$ d'après le lemme de Gauss. Écrivons $x = 1 + 3k$; alors
 $2 \times 3k = -3(y - 1)$, soit $y = 1 - 2k$. Réciproquement, ces couples sont solutions. Donc
les solutions sont les $\begin{pmatrix} 1 + 3k \\ 1 - 2k \end{pmatrix}$, $k \in \mathbb{Z}$.

3. Comme 6 ne divise pas 25, **l'équation $12x + 18y = 25$ n'a aucune solution entière**.

D'ailleurs, le membre de gauche est pair et 25 est impair.

Corrigé de l'exercice 6 : Équation diophantienne $17x + 23y = c$

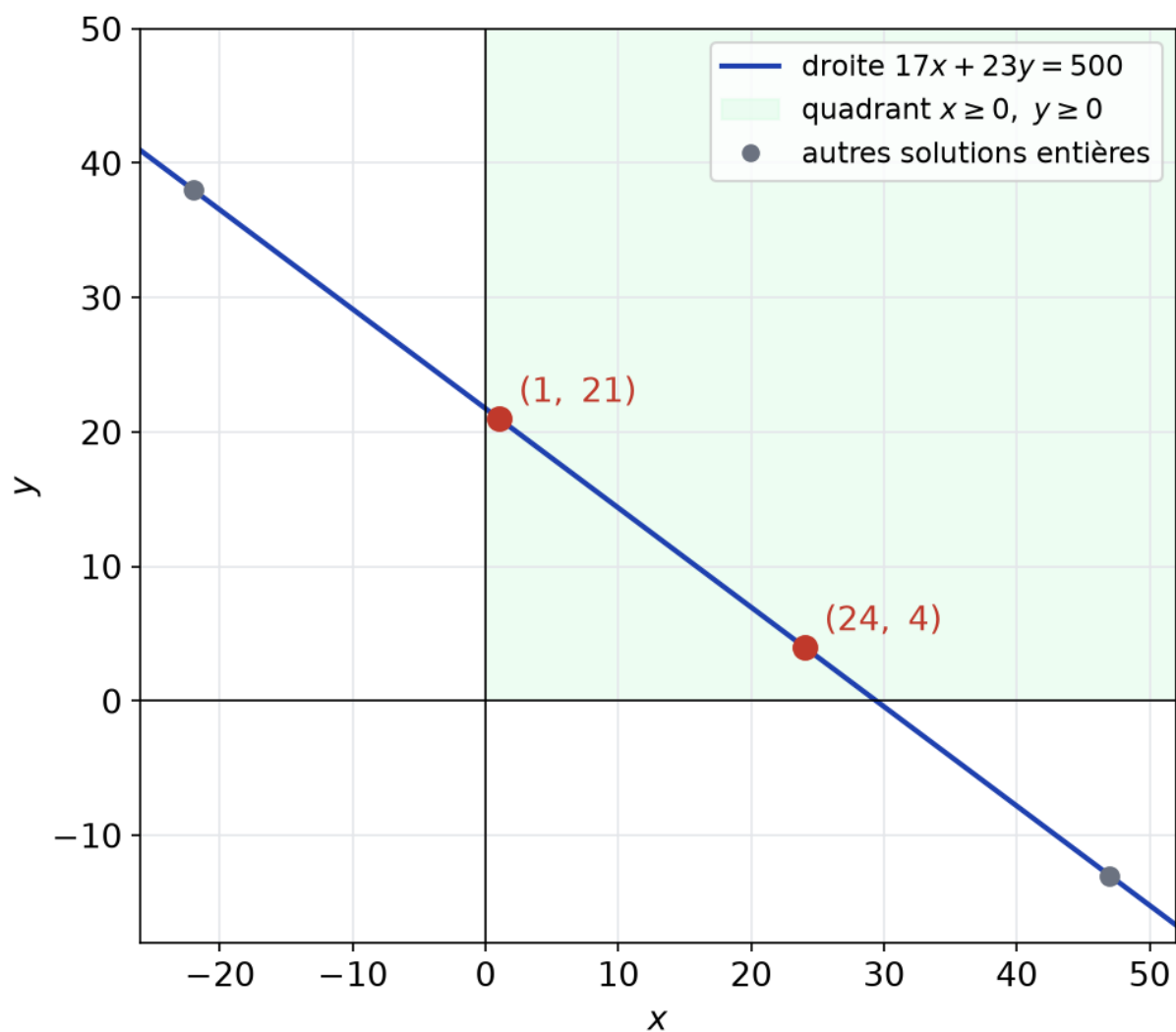
1. Les entiers 17 et 23 sont premiers distincts, donc $17 \wedge 23 = 1$. Ensuite, l'algorithme d'Euclide donne $23 = 17 + 6$, $17 = 2 \times 6 + 5$ et $6 = 5 + 1$. En remontant :

$$1 = 6 - 5 = 6 - (17 - 2 \times 6) = 3 \times 6 - 17 = 3(23 - 17) - 17 = 3 \times 23 - 4 \times 17.$$

Donc $(u, v) = (-4, 3)$ **convient** : $-68 + 69 = 1$.

2. En multipliant par 5, on obtient la solution particulière $(-20, 15)$. Si (x, y) est solution, alors $17(x + 20) = -23(y - 15)$. Ainsi, 23 divise $17(x + 20)$ et $23 \wedge 17 = 1$. Le lemme de Gauss donne $x = -20 + 23k$, puis $y = 15 - 17k$. Réciproquement, ces couples conviennent. Donc $\mathcal{S} = \left\{ \begin{pmatrix} -20 + 23k \\ 15 - 17k \end{pmatrix} \mid k \in \mathbb{Z} \right\}$. Ensuite, $x \geq 0$ impose $k \geq 1$, tandis que $y \geq 0$ impose $k \leq 0$. Par conséquent, **il n'existe aucune solution à coordonnées positives.**

3. De même, $(-2000, 1500)$ est solution de $17x + 23y = 500$, donc les solutions entières sont $\begin{pmatrix} -2000 + 23k \\ 1500 - 17k \end{pmatrix}$. D'une part, $x \geq 0$ équivaut à $23k \geq 2000$, soit $k \geq 87$, car $23 \times 86 = 1978$ et $23 \times 87 = 2001$. D'autre part, $y \geq 0$ équivaut à $17k \leq 1500$, soit $k \leq 88$, car $17 \times 88 = 1496$ et $17 \times 89 = 1513$. Ainsi $k \in \{87, 88\}$, ce qui donne $(x, y) = (1, 21)$ **ou** $(24, 4)$. On vérifie : $17 + 483 = 500$ et $408 + 92 = 500$. La figure ci-dessous montre ces deux points dans le quadrant positif.



4. Rendre 500 unités avec x pièces de 17 et y pièces de 23, c'est résoudre la question 3 dans $\mathbb{N}^2$. Il y a donc **exactement deux façons** : une pièce de 17 et vingt et une de 23, ou vingt-quatre pièces de 17 et quatre de 23.

Point de méthode : les contraintes de signe se traduisent par un encadrement du paramètre k ; calculez les bornes avec soin, en vérifiant les produits voisins.

Corrigé de l'exercice 7 : PGCD d'expressions polynomiales en n

1. On a $3(2n + 3) - 2(3n + 4) = 1$. D'après le théorème de Bézout, $2n + 3$ et $3n + 4$

sont premiers entre eux.

- On a $n^2 + 1 = (n + 1)(n - 1) + 2$. D'après le lemme de l'exercice 3, $(n^2 + 1) \wedge (n + 1) = (n + 1) \wedge 2$. Par conséquent, **le PGCD vaut 2 si n est impair et 1 si n est pair.**
- D'abord, $(2n + 1) - 2n = 1$, donc $n \wedge (2n + 1) = 1$. Notons ensuite $D = (n^3 + n) \wedge (2n + 1)$ et $D' = (n^2 + 1) \wedge (2n + 1)$. D'une part, D' divise $n^2 + 1$, donc $n(n^2 + 1) = n^3 + n$, ainsi que $2n + 1$: il divise D . D'autre part, D divise $2n + 1$, donc $D \wedge n$ divise $2n + 1$ et n , donc 1. Comme D divise $n(n^2 + 1)$ et $D \wedge n = 1$, le lemme de Gauss donne $D \mid n^2 + 1$, puis $D \mid D'$. Les deux entiers positifs se divisent mutuellement, donc $D = D'$.
- On calcule $4(n^2 + 1) - (2n + 1)(2n - 1) = 4n^2 + 4 - 4n^2 + 1 = 5$. Donc D' divise 5, et $D' \in \{1, 5\}$. Ensuite, $D' = 5$ exige $5 \mid 2n + 1$, c'est-à-dire $2n \equiv 4 \pmod{5}$. Comme 3 est l'inverse de 2 modulo 5, cela équivaut à $n \equiv 2 \pmod{5}$. Réciproquement, si $n \equiv 2 \pmod{5}$, alors $2n + 1 \equiv 0 \pmod{5}$ et $n^2 + 1 \equiv 5 \equiv 0 \pmod{5}$. Finalement, $(n^3 + n) \wedge (2n + 1) = 5$ **si et seulement si** $n \equiv 2 \pmod{5}$, et ce PGCD vaut 1 sinon. Par exemple, pour $n = 2$, on trouve $10 \wedge 5 = 5$.

Point de méthode : cherchez une combinaison à coefficients entiers qui élimine n ; elle fournit un multiple du PGCD.

Corrigé de l'exercice 8 : Couples d'entiers de PGCD et PPCM donnés

- Posons $m_0 = da'b'$. On a $m_0 = ab' = a'b$, donc m_0 est un multiple commun positif de a et b . Soit maintenant m un multiple commun de a et b . Écrivons $m = ak = da'k$. Comme $b = db'$ divise m , on obtient $b' \mid a'k$. Or $a' \wedge b' = 1$, donc le lemme de Gauss donne $b' \mid k$. Ainsi $m = da'b'j$ est un multiple de m_0 . Par conséquent, tout multiple commun strictement positif est supérieur ou égal à m_0 , et $a \vee b = da'b'$. Il vient $(a \wedge b)(a \vee b) = d \times da'b' = (da')(db')$, c'est-à-dire $(a \wedge b)(a \vee b) = ab$.

2. Écrivons $a = 18a'$ et $b = 18b'$ avec $a' \wedge b' = 1$. D'après la question 1, $a \vee b = 18a'b'$, donc la condition devient $a'b' = 30$. Or $30 = 2 \times 3 \times 5$. Les couples premiers entre eux avec $a' \leq b'$ sont $(1, 30)$, $(2, 15)$, $(3, 10)$ et $(5, 6)$. Réciproquement, ils conviennent tous. Donc $(a, b) \in \{(18, 540), (36, 70), (54, 180), (90, 1, 108)\}$.
3. Écrivons $a = 45a'$ et $b = 45b'$ avec $a' \wedge b' = 1$. La condition $a + b = 360$ devient $a' + b' = 8$. Les couples $(1, 7)$ et $(3, 5)$ conviennent. En revanche, $(2, 6)$ et $(4, 4)$ sont exclus, car leurs termes ne sont pas premiers entre eux. Donc $(a, b) \in \{(45, 315), (135, 225)\}$. On vérifie que $135 \wedge 225 = 45$.

Corrigé de l'exercice 9 : Racines rationnelles et lemme de Gauss

1. Supposons $P(p/q) = 0$ avec $p \wedge q = 1$. En multipliant par q^n , on obtient

$$a_n p^n + a_{n-1} p^{n-1} q + \dots + a_1 p q^{n-1} + a_0 q^n = 0.$$

Tous les termes sauf $a_0 q^n$ sont multiples de p , donc $p \mid a_0 q^n$. Or $p \wedge q = 1$ entraîne $p \wedge q^n = 1$. Le lemme de Gauss donne alors $p \mid a_0$. De même, tous les termes sauf $a_n p^n$ sont multiples de q , donc $q \mid a_n p^n$ et $q \mid a_n$.

2. Ici $a_0 = -1$ et $a_n = 6$. Les racines rationnelles possibles sont donc $\pm 1, \pm \frac{1}{2}, \pm \frac{1}{3}, \pm \frac{1}{6}$. On teste : $P(1) = 6 - 11 + 6 - 1 = 0$. Ensuite,

$$P\left(\frac{1}{2}\right) = \frac{3}{4} - \frac{11}{4} + 3 - 1 = 0, \quad P\left(\frac{1}{3}\right) = \frac{2}{9} - \frac{11}{9} + 2 - 1 = 0.$$

Un polynôme de degré 3 a au plus trois racines. Ainsi, **les racines rationnelles sont** $1, \frac{1}{2}$ et $\frac{1}{3}$, et $6X^3 - 11X^2 + 6X - 1 = (X - 1)(2X - 1)(3X - 1)$, en comparant les coefficients dominants.

3. Le réel $\sqrt[3]{2}$ est racine de $X^3 - 2$. Si ce polynôme avait une racine rationnelle p/q , alors $q \mid 1$ et $p \mid 2$, donc cette racine serait dans $\{-2, -1, 1, 2\}$. Or ces valeurs donnent respectivement $-10, -3, -1$ et 6 , qui sont non nuls. Par conséquent, $\sqrt[3]{2}$ **est irrationnel**.

Corrigé de l'exercice 10 : PGCD de trois entiers

1. D'abord, $462 = 330 + 132$, $330 = 2 \times 132 + 66$ et $132 = 2 \times 66$, donc $330 \wedge 462 = 66$. En remontant, $66 = 330 - 2 \times 132 = 3 \times 330 - 2 \times 462$. Ensuite, $770 = 11 \times 66 + 44$, $66 = 44 + 22$ et $44 = 2 \times 22$, donc $66 \wedge 770 = 22$. De plus, $22 = 66 - 44 = 12 \times 66 - 770$. En substituant,
$$22 = 12(3 \times 330 - 2 \times 462) - 770 = 36 \times 330 - 24 \times 462 - 770.$$

Donc $330 \wedge 462 \wedge 770 = 22$ avec $(u, v, w) = (36, -24, -1)$. On vérifie :
 $11880 - 11088 - 770 = 22$.
2. On a $6 \wedge 10 = 2$, donc ces entiers **ne sont pas premiers entre eux deux à deux**. En revanche, $6 + 10 - 15 = 1$, donc tout diviseur commun aux trois divise 1. Ainsi, 6, 10, 15 **sont premiers entre eux dans leur ensemble, avec** $(u, v, w) = (1, 1, -1)$.
3. Raisonnons par récurrence sur $k \leq n$. Pour $k = 1$, c'est l'hypothèse. Supposons que $A = a_1 \dots a_k$ divise N , avec $k < n$. L'entier a_{k+1} est premier avec chacun des a_i , donc avec leur produit A , d'après le corollaire du lemme de Gauss. Comme $A \mid N$, $a_{k+1} \mid N$ et $A \wedge a_{k+1} = 1$, on obtient $Aa_{k+1} \mid N$. Donc $a_1 a_2 \dots a_n$ **divise** N .
4. Les entiers $4 = 2^2$, $9 = 3^2$ et $25 = 5^2$ sont premiers entre eux deux à deux. D'après la question 3, tout multiple commun est multiple de 900. Comme 900 convient, **le plus petit est** 900. Avec 4, 6, 25, en revanche, l'hypothèse tombe : $4 \wedge 6 = 2$. Ainsi, **le produit** 600 **n'est pas le plus petit**, car 300 est déjà multiple de 4, 6 et 25.

Corrigé de l'exercice 11 : Crible d'Ératosthène jusqu'à 120

1. L'ensemble des diviseurs de n supérieurs ou égaux à 2 est non vide, car il contient n . Soit p son plus petit élément. Tout diviseur δ de p avec $1 < \delta < p$ diviserait n , ce qui contredit la minimalité. Donc p est premier. Ensuite, n n'est pas premier, donc $n = pm$ avec $m \geq 2$. Or m divise n , donc $m \geq p$. Ainsi $p^2 \leq pm = n$.
2. Comme $10^2 = 100 \leq 120 < 121 = 11^2$, un nombre composé $n \leq 120$ a un facteur premier au plus égal à 10. Par conséquent, **il suffit de barrer les multiples de 2, 3, 5 et 7**. On obtient la grille ci-dessous. Les nombres premiers sont

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113 . Il y en a donc 30 .

1	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~
101	~~102~~	103	~~104~~	~~105~~	~~106~~	107	~~108~~	109	~~110~~
~~111~~	~~112~~	113	~~114~~	~~115~~	~~116~~	~~117~~	~~118~~	~~119~~	~~120~~

30 nombres premiers inférieurs ou égaux à 120

3. On a $10^2 < 113 < 11^2$, donc il suffit de tester 2, 3, 5, 7 . Or 113 est impair, la somme de ses

chiffres vaut 5, il ne finit ni par 0 ni par 5, et $113 = 7 \times 16 + 1$. Ainsi, 113 **est premier**. En revanche, $119 = 7 \times 17$ **n'est pas premier**.

4. Soit $k \in \{2, \dots, n\}$. L'entier k divise $n!$ et k , donc il divise $n! + k$. De plus, $2 \leq k < n! + k$. Par conséquent, $n! + k$ **est composé**. On obtient ainsi $n - 1$ entiers consécutifs sans nombre premier. Autrement dit, **l'écart entre deux nombres premiers consécutifs peut être arbitrairement grand**.

Corrigé de l'exercice 12 : Infinité des premiers de la forme $6k + 5$

1. Soit $p \geq 5$ premier et r son reste modulo 6. Si $r \in \{0, 2, 4\}$, alors p est pair et supérieur à 2 : c'est impossible. Si $r = 3$, alors $p = 6k + 3 = 3(2k + 1)$ est multiple de 3 et différent de 3 : c'est impossible aussi. Donc $r \in \{1, 5\}$.
2. On a $(6a + 1)(6b + 1) = 6(6ab + a + b) + 1$. Ainsi, le produit de deux entiers de reste 1 a pour reste 1. Par récurrence sur le nombre de facteurs, **un produit d'entiers de reste 1 modulo 6 a pour reste 1**.
3. Écrivons $N = 6k + 5$. D'abord, N est impair. Ensuite, $N = 3(2k + 1) + 2$ n'est pas multiple de 3. Ainsi, les facteurs premiers de N sont au moins égaux à 5, et leur reste modulo 6 vaut 1 ou 5 d'après la question 1. S'ils avaient tous pour reste 1, leur produit N aurait pour reste 1 d'après la question 2. Or N a pour reste 5. Donc **N possède un diviseur premier de reste 5 modulo 6**.
4. Le nombre 5 est premier de reste 5, donc $r \geq 1$ et $N \geq 29$. De plus, $N = 6(p_1 \dots p_r - 1) + 5$ a pour reste 5 modulo 6. D'après la question 3, un premier q de reste 5 divise N . Par hypothèse, q est l'un des p_i , donc il divise $6p_1 \dots p_r$. Il divise alors la différence $6p_1 \dots p_r - N = 1$: c'est absurde. Par conséquent, **il existe une infinité de nombres premiers de la forme $6k + 5$** .

Point de méthode : dans ce type de preuve, on adapte l'argument d'Euclide en choisissant N dans la bonne classe de restes.

Corrigé de l'exercice 13 : Nombres de Fermat

1. Pour $n = 1$, on a $F_0 = 3 = 5 - 2 = F_1 - 2$. Supposons la formule vraie au rang n . Alors

$$F_0 \dots F_{n-1} F_n = (F_n - 2) F_n = (2^{2^n} - 1)(2^{2^n} + 1) = 2^{2^{n+1}} - 1 = F_{n+1} - 2.$$

Donc $F_0 F_1 \dots F_{n-1} = F_n - 2$ **pour tout** $n \geq 1$.

2. Soient $m < n$ et $\delta = F_m \wedge F_n$. D'abord, δ divise F_m , qui est un facteur du produit $F_0 \dots F_{n-1} = F_n - 2$. Ensuite, δ divise F_n , donc il divise la différence 2. Or F_n est impair, donc $\delta = 1$. Ainsi, **les nombres de Fermat sont premiers entre eux deux à deux**.
3. Pour tout n , $F_n \geq 3$ admet un diviseur premier p_n . Si $m \neq n$, alors $p_m \neq p_n$, sinon ce nombre premier diviserait $F_m \wedge F_n = 1$. L'application $n \rightarrow p_n$ est donc injective de $\mathbb{N}$ dans $\mathcal{P}$. Par conséquent, **l'ensemble des nombres premiers est infini**.

4. On a $5 \times 2^7 + 1 = 640 + 1 = 641$ et $5^4 + 2^4 = 625 + 16 = 641$. Ainsi $5 \times 2^7 \equiv -1$ _[641]. En élevant à la puissance 4, on obtient $5^4 \times 2^{28} \equiv 1$ _[641]. Or $5^4 = 641 - 2^4 \equiv -2^4$ _[641]. Donc

$$\begin{aligned} -2^4 \times 2^{28} &= -2^{32} \equiv 1 \\ \text{, [641], soit } 2^{32} + 1 &\equiv 0 \\ \text{, [641]}. \end{aligned}$$

Comme $F_5 = 2^{32} + 1$, 641 **divise** F_5 . Enfin, $641 < F_5$, donc F_5 **n'est pas premier** : précisément, $F_5 = 641 \times 6700417$.

Corrigé de l'exercice 14 : Décomposition de 4200 et 1764

1. On a $4200 = 42 \times 100 = (2 \times 3 \times 7)(2^2 \times 5^2)$. De plus, $1764 = 42^2$. Donc $4200 = 2^3 \times 3 \times 5^2 \times 7$ **et** $1764 = 2^2 \times 3^2 \times 7^2$.

2. On prend le minimum des valuations pour le PGCD et le maximum pour le PPCM :

$$4200 \wedge 1764 = 2^2 \times 3 \times 7 = 84, \quad 4200 \vee 1764 = 2^3 \times 3^2 \times 5^2 \times 7^2 = 88200.$$

Ainsi, **le PGCD vaut 84 et le PPCM 88200**. On vérifie que

$$84 \times 88200 = 7408800 = 4200 \times 1764.$$

3. Un diviseur positif s'écrit $2^a 3^b 5^c 7^d$ avec $0 \leq a \leq 3$, $0 \leq b \leq 1$, $0 \leq c \leq 2$ et $0 \leq d \leq 1$. Il y en a donc $4 \times 2 \times 3 \times 2$, soit **48 diviseurs**.

4. Un entier est un carré si et seulement si toutes ses valuations sont paires. Il faut donc $v_2(k)$, $v_3(k)$ et $v_7(k)$ impairs, donc au moins égaux à 1. Le plus petit choix est $k = 2 \times 3 \times 7 = 42$, et $4200 \times 42 = 176400 = 420^2$. De même, pour un cube, les valuations doivent être multiples de 3. Il faut donc $v_2(k) \geq 2$, $v_3(k) \geq 1$ et $v_7(k) \geq 2$. Ainsi $k = 3^2 \times 5 \times 7^2 = 2205$, et $4200 \times 2205 = 9261000 = 210^3$.

Corrigé de l'exercice 15 : Formule de Legendre et zéros de 1000!

1. Les multiples de p^k entre 1 et n sont les jp^k avec $1 \leq j \leq n/p^k$. Il y en a donc $\lfloor n/p^k \rfloor$. Ensuite, $v_p(n!) = \sum_{m=1}^n v_p(m)$ par additivité de la valuation. Or $v_p(m)$ est le nombre d'entiers $k \geq 1$ tels que $p^k \mid m$. En échangeant les deux sommes finies, on obtient

$$v_p(n!) = \sum_{k \geq 1} \text{card}\{m \leq n \mid p^k \mid m\} = \sum_{k \geq 1} \left\lfloor \frac{n}{p^k} \right\rfloor.$$

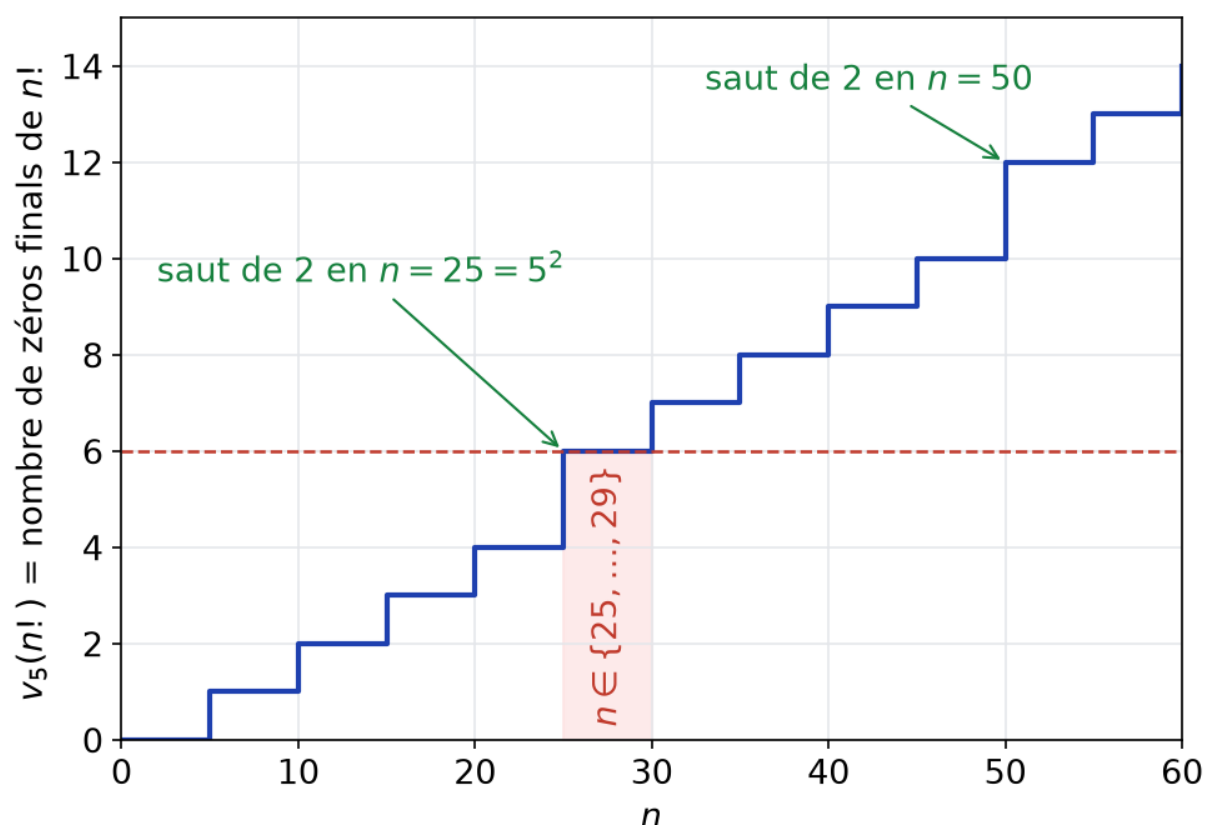
C'est **la formule de Legendre** ; la somme est finie, car les termes sont nuls dès que $p^k > n$.

2. Pour $p = 5$, on trouve $v_5(1000!) = 200 + 40 + 8 + 1 = 249$. Pour $p = 2$, on trouve $500 + 250 + 125 + 62 + 31 + 15 + 7 + 3 + 1 = 994$. Le nombre de zéros finals est le plus grand k tel que $10^k = 2^k 5^k$ divise $1000!$, soit $\min(v_2, v_5)$. Donc **1000! se termine par 249 zéros**.

3. On a $7^3 = 343 \leq 1000 < 2401 = 7^4$. Ainsi $v_7(1000!) = 142 + 20 + 2 = 164$.

4. Comme $v_2(n!) \geq v_5(n!)$, le nombre de zéros finals de $n!$ vaut $v_5(n!)$. Pour $n \leq 24$, on a $v_5(n!) = \lfloor n/5 \rfloor \leq 4$. Pour $25 \leq n \leq 29$, on a $v_5(n!) = 5 + 1 = 6$. Pour $n \geq 30$, on a $v_5(n!) \geq 6 + 1 = 7$. Donc **$n!$ se termine par exactement six zéros si**

et seulement si $25 \leq n \leq 29$. De plus, la valuation saute de 4 à 6 en $n = 25$. Ainsi, **aucune factorielle ne se termine par exactement cinq zéros.** La figure ci-dessous montre cet escalier.



Corrigé de l'exercice 16 : Nombre et somme des diviseurs

- Soit δ un diviseur positif de n . Pour tout premier p , on a $v_p(\delta) \leq v_p(n)$. Donc δ n'a pas d'autre facteur premier que les p_i , et $\delta = p_1^{\beta_1} \dots p_r^{\beta_r}$ avec $0 \leq \beta_i \leq \alpha_i$.
Réciproquement, ces entiers divisent n . De plus, l'unicité de la décomposition montre que des exposants différents donnent des diviseurs différents. Ainsi, $d(n) = (\alpha_1 + 1) \dots (\alpha_r + 1)$.
- En développant le produit, on obtient la somme de tous les $p_1^{\beta_1} \dots p_r^{\beta_r}$, chacun une seule fois :

$$\prod_{i=1}^r \left(1 + p_i + \dots + p_i^{\alpha_i} \right) = \sigma(n).$$

La somme géométrique donne alors $\sigma(n) = \prod_{i=1}^r \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}$. Pour $360 = 2^3 \times 3^2 \times 5$, on trouve $d(360) = 4 \times 3 \times 2 = 24$ et $\sigma(360) = 15 \times 13 \times 6 = 1170$.

- Le produit $(\alpha_1 + 1) \dots (\alpha_r + 1)$ est impair si et seulement si chaque facteur est impair. Cela équivaut à dire que tous les α_i sont pairs. Par conséquent, $d(n)$ **est impair si et seulement si n est un carré parfait**.
- Les écritures de 12 comme produit de facteurs au moins égaux à 2 sont 12 , 6×2 , 4×3 et $3 \times 2 \times 2$. Pour une liste d'exposants donnée, l'entier est minimal lorsque les plus grands exposants portent sur les plus petits premiers. On obtient ainsi $2^{11} = 2048$, $2^5 \times 3 = 96$, $2^3 \times 3^2 = 72$ et $2^2 \times 3 \times 5 = 60$. Donc **le plus petit entier ayant 12 diviseurs est 60**.

Corrigé de l'exercice 17 : Critères de divisibilité et derniers chiffres

- On a $10 \equiv 1 \pmod{9}$, donc $10^k \equiv 1 \pmod{9}$ par compatibilité avec les puissances. Ainsi, $N \equiv c_0 + \dots + c_m \pmod{9}$. De même, $10 \equiv -1 \pmod{11}$ donne $10^k \equiv (-1)^k \pmod{11}$. Donc $N \equiv c_0 - c_1 + c_2 - \dots + (-1)^m c_m \pmod{11}$.
- La somme des chiffres vaut $9 + 1 + 8 + 2 + 7 + 3 + 6 + 4 + 5 = 45$, qui est multiple de 9. Donc 918 273 645 **est divisible par 9**. Ensuite, la somme alternée à partir des unités vaut $5 - 4 + 6 - 3 + 7 - 2 + 8 - 1 + 9 = 25$. Or $25 = 2 \times 11 + 3$. Ainsi, **l'entier n'est pas divisible par 11 et son reste vaut 3**.
- On calcule $3^5 = 243 \equiv 43 \pmod{100}$, puis $3^{10} \equiv 43^2 = 1849 \equiv 49 \pmod{100}$. Ensuite, $3^{20} \equiv 49^2 = 2401 \equiv 1 \pmod{100}$. Comme $2026 = 20 \times 101 + 6$, il vient $3^{2026} \equiv 3^6 = 729 \equiv 29 \pmod{100}$. Donc **les deux derniers chiffres de 3^{2026} sont 2 et 9**.
- Le petit théorème de Fermat ne s'applique pas, car 9 n'est pas premier. Cependant, $5^3 = 125 = 13 \times 9 + 8$, donc $5^3 \equiv -1 \pmod{9}$ et $5^6 \equiv 1 \pmod{9}$. Comme $2026 = 6 \times 337 + 4$,

on obtient $5^{2026} \equiv 5^4 = 5^3 \times 5 \equiv -5 \equiv 4 \pmod{9}$. Ainsi, **le reste vaut 4**.

Point de méthode : cherchez d'abord une petite puissance congrue à 1 ou à -1, puis divisez l'exposant par sa période.

Corrigé de l'exercice 18 : Inverse modulo n et congruences linéaires

1. Dire que $au \equiv 1 \pmod{n}$, c'est dire qu'il existe $v \in \mathbb{Z}$ tel que $au + nv = 1$. D'après le théorème de Bézout, cela équivaut à $a \wedge n = 1$. Donc **a est inversible modulo n si et seulement si $a \wedge n = 1$** . Modulo 12, les entiers premiers avec 12 sont 1, 5, 7, 11. De plus, $5^2 = 25$, $7^2 = 49$ et $11^2 = 121$ sont congrus à 1. Ainsi, 1, 5, 7, 11 **sont inversibles et chacun est son propre inverse**.

2. L'algorithme d'Euclide donne $43 = 2 \times 17 + 9$, $17 = 9 + 8$ et $9 = 8 + 1$. En remontant :

$$1 = 9 - 8 = 2 \times 9 - 17 = 2(43 - 2 \times 17) - 17 = 2 \times 43 - 5 \times 17.$$

Donc $-5 \equiv 38$ est **un inverse de 17 modulo 43** : en effet,

$$17 \times 38 = 646 = 15 \times 43 + 1. \text{ Ensuite, } 17x \equiv 5 \text{ équivaut à }$$

$$x \equiv 38 \times 5 = 190 \equiv 18 \pmod{43}. \text{ On vérifie que } 17 \times 18 = 306 = 7 \times 43 + 5. \text{ Donc }$$

$$x \equiv 18 \pmod{43}.$$

3. Ici $6 \wedge 10 = 2$, donc 6 n'est pas inversible. Cependant, $10 \mid 6x - 4$ équivaut à $5 \mid 3x - 2$, c'est-à-dire $3x \equiv 2 \pmod{5}$. Or 2 est l'inverse de 3 modulo 5, donc $x \equiv 4 \pmod{5}$. Ainsi, $x \equiv 4 \pmod{10}$ **ou** $x \equiv 9 \pmod{10}$. On vérifie que $6 \times 4 = 24$ et $6 \times 9 = 54$ sont congrus à 4 modulo 10.

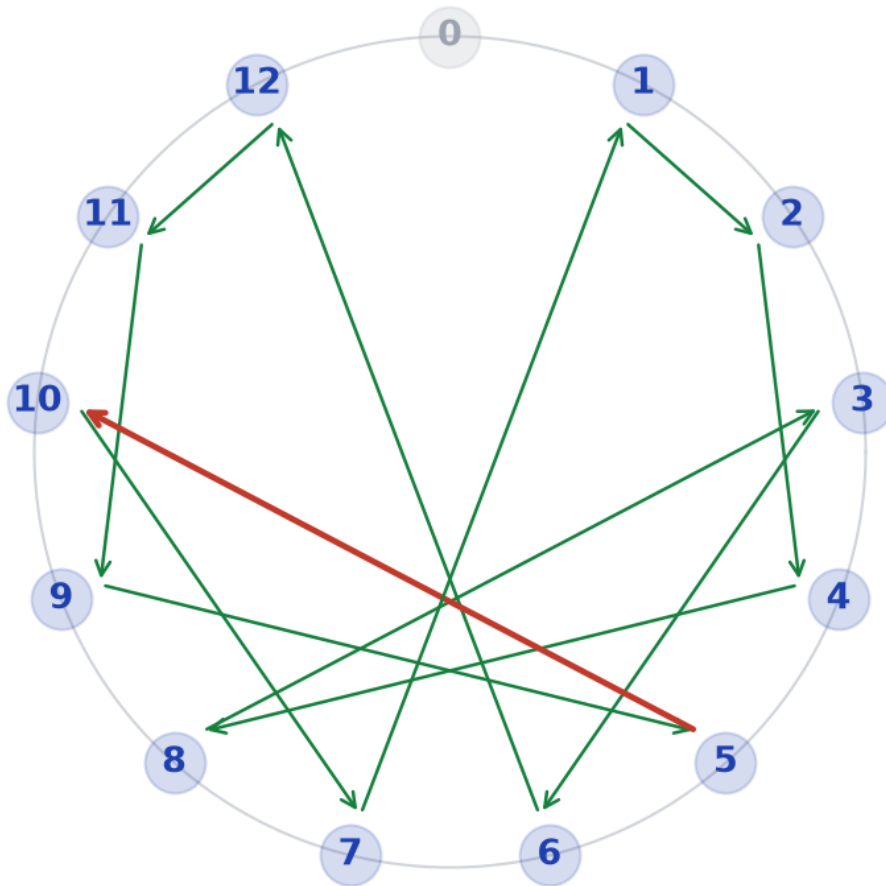
4. Pour tout entier x , $6x - 5$ est impair. Or un multiple de 10 est pair. Donc $6x \equiv 5 \pmod{10}$ **n'a aucune solution**. Plus généralement, $ax \equiv b \pmod{n}$ a une solution si et seulement si $a \wedge n$ divise b .

Corrigé de l'exercice 19 : Congruences simultanées

- La première condition s'écrit $x = 2 + 5k$ avec $k \in \mathbb{Z}$. La seconde devient $\begin{matrix} 5k \equiv 1 \\ , [7] \end{matrix}$. Or $5 \times 3 = 15 \equiv 1$, donc $\begin{matrix} k \equiv 3 \\ , [7] \end{matrix}$. En écrivant $k = 3 + 7j$, on obtient $x = 17 + 35j$.
Réciproquement, 17 a pour restes 2 et 3. Donc $\begin{matrix} x \equiv 17 \\ , [35] \end{matrix}$.
- On cherche $x = 17 + 35j$ avec $\begin{matrix} x \equiv 1 \\ , [3] \end{matrix}$. Comme $17 \equiv 2$ et $\begin{matrix} 35 \equiv 2 \\ , [3] \end{matrix}$, la condition devient $2 + 2j \equiv 1$, soit $\begin{matrix} 2j \equiv 2 \\ , [3] \end{matrix}$. Or 2 est inversible modulo 3, donc $\begin{matrix} j \equiv 1 \\ , [3] \end{matrix}$. Ainsi $x = 17 + 35(1 + 3i) = 52 + 105i$. Donc $\begin{matrix} x \equiv 52 \\ , [105] \end{matrix}$.
- Le nombre d'œufs vérifie les trois conditions, donc il s'écrit $52 + 105i$. La contrainte $100 \leq 52 + 105i \leq 200$ impose $i = 1$. Donc **la coopérative possède 157 œufs**. On vérifie : $157 = 3 \times 52 + 1 = 5 \times 31 + 2 = 7 \times 22 + 3$.
- Si $\begin{matrix} x \equiv 1 \\ , [4] \end{matrix}$, alors x est impair. Si $\begin{matrix} x \equiv 2 \\ , [6] \end{matrix}$, alors x est pair. Les deux conditions sont incompatibles, donc **le système n'a aucune solution**. Il manque l'hypothèse que **les modules soient premiers entre eux**, car $4 \wedge 6 = 2$.

Corrigé de l'exercice 20 : Petit théorème de Fermat et calculs de restes

- Le nombre 13 est premier et ne divise pas 2. D'après le petit théorème de Fermat, $\begin{matrix} 2^{12} \equiv 1 \\ , [13] \end{matrix}$.
Comme $2026 = 12 \times 168 + 10$, on a $\begin{matrix} 2^{2026} \equiv 2^{10} = 1024 \\ , [13] \end{matrix}$. Or $1024 = 13 \times 78 + 10$.
Donc **le reste vaut 10**. La figure ci-dessous montre les puissances successives de 2 modulo 13 : elles parcourent les douze restes non nuls avant de revenir à 1.



flèche : multiplication par 2 modulo 13 ; en rouge, le passage de 2^9 à $2^{10} \equiv 10$

2. De même, $7^{10} \equiv 1 \pmod{11}$. Comme $1003 = 10 \times 100 + 3$, on a $7^{1003} \equiv 7^3 = 343 \pmod{11}$. Or $343 = 11 \times 31 + 2$. Ainsi, **le reste vaut 2**.

3. On a $5^{12} \equiv 1 \pmod{13}$, donc $5 \times 5^{11} \equiv 1$: l'entier 5^{11} est un inverse de 5. Ensuite, $5^2 = 25 \equiv -1 \pmod{13}$, donc $5^8 \equiv 1$. Ainsi $5^{11} = 5^8 \times 5^2 \times 5 \equiv -5 \equiv 8 \pmod{13}$. **Un inverse de 5 modulo 13 est 8**, puisque $40 = 3 \times 13 + 1$. Enfin, $5x \equiv 3$ équivaut à $x \equiv 24 \equiv 11 \pmod{13}$. Donc $x \equiv 11 \pmod{13}$, et l'on vérifie que $55 = 4 \times 13 + 3$.

4. D'une part, $2^{70} = (2^{12})^5 \times 2^{10} \equiv 10 \pmod{13}$ d'après la question 1. D'autre part, $3^3 = 27 \equiv 1 \pmod{13}$,

donc $3^{70} = (3^3)^{23} \times 3 \equiv 3$. Ainsi $2^{70} + 3^{70} \equiv 13 \equiv 0$. Donc **13 divise**
 $2^{70} + 3^{70}$.

Corrigé de l'exercice 21 : Fermat et divisibilité par 2730

- Soit $n \in \mathbb{Z}$. Si $p \mid n$, alors n^{13} et n sont tous deux congrus à 0. Sinon, le petit théorème de Fermat donne $n^{p-1} \equiv 1$. Écrivons $12 = (p-1)s$. Alors $n^{12} = (n^{p-1})^s \equiv 1$, donc $n^{13} \equiv n$. Dans tous les cas, $n^{13} \equiv n$.
- Les diviseurs de 12 sont 1, 2, 3, 4, 6, 12. Les entiers p correspondants sont 2, 3, 4, 5, 7, 13, dont les premiers sont 2, 3, 5, 7, 13. Ces nombres premiers distincts sont premiers entre eux deux à deux, et chacun divise $n^{13} - n$. Leur produit divise donc $n^{13} - n$. Comme $2 \times 3 \times 5 \times 7 \times 13 = 2730$, **2730 divise $n^{13} - n$ pour tout n** .
- Modulo 3, on a $n^3 \equiv n$, donc $n^5 = n^3 n^2 \equiv n^3 \equiv n$. Ainsi $3n^5 + 5n^3 + 7n \equiv 0 + 5n + 7n = 12n \equiv 0$. Modulo 5, on a $n^5 \equiv n$, donc l'expression est congrue à $3n + 0 + 7n = 10n \equiv 0$. Comme $3 \wedge 5 = 1$, **15 divise $3n^5 + 5n^3 + 7n$** .
- Pour $1 \leq k \leq p-1$, p ne divise pas k , donc $k^{p-1} \equiv 1$. La somme contient $p-1$ termes, donc elle est congrue à $p-1$. Par conséquent, $1^{p-1} + \dots + (p-1)^{p-1} \equiv -1$.

Corrigé de l'exercice 22 : Nombres de Mersenne et leurs diviseurs

- On a $a^n - 1 = (a - 1)(a^{n-1} + \dots + a + 1)$. Le second facteur vaut au moins $a + 1 \geq 3$. Si $a^n - 1$ est premier, le premier facteur vaut donc 1, et $a = 2$. Supposons ensuite

$n = rs$ avec $1 < r < n$. Alors $2^n - 1 = (2^r)^s - 1$ est divisible par $2^r - 1$, qui vérifie $1 < 2^r - 1 < 2^n - 1$. C'est impossible si $2^n - 1$ est premier. Donc **$a = 2$ et n est premier.**

2. On a $2^a - 1 = 2^r(2^{bq} - 1) + (2^r - 1)$. Or $2^{bq} - 1 = (2^b - 1)(2^{b(q-1)} + \dots + 2^b + 1)$ est multiple de $2^b - 1$. Ainsi $2^a - 1 = K(2^b - 1) + (2^r - 1)$ avec $K \in \mathbb{N}$. Le lemme de l'exercice 3 donne $(2^a - 1) \wedge (2^b - 1) = (2^b - 1) \wedge (2^r - 1)$. Les exposants suivent donc exactement l'algorithme d'Euclide appliqué à (a, b) . Celui-ci s'arrête sur le couple $(a \wedge b, 0)$, et $2^0 - 1 = 0$. Par récurrence forte, $(2^a - 1) \wedge (2^b - 1) = 2^{a \wedge b} - 1$.
3. On calcule $23 \times 89 = 2047 = 2^{11} - 1$. Or 11 est premier, mais $2^{11} - 1$ ne l'est pas. Donc **la réciproque est fautive.**
4. L'entier $2^p - 1$ est impair, donc q est impair. D'après le petit théorème de Fermat, q divise $2^{q-1} - 1$. Il divise aussi $2^p - 1$, donc il divise leur PGCD, qui vaut $2^{p \wedge (q-1)} - 1$ d'après la question 2. Or p est premier, donc $p \wedge (q-1) \in \{1, p\}$. S'il valait 1, q diviserait $2^1 - 1 = 1$, ce qui est absurde. Donc $p \mid q-1$. Enfin, $q-1$ est pair et p est impair, donc $2p \mid q-1$. Ainsi, $\begin{matrix} q \equiv 1 \\ [2p] \end{matrix}$. On le vérifie sur $23 = 2 \times 11 + 1$ et $89 = 8 \times 11 + 1$.
5. Si 8191 n'était pas premier, il aurait un facteur premier q avec $q^2 \leq 8191 < 8281 = 91^2$. D'après la question 4, $\begin{matrix} q \equiv 1 \\ [26] \end{matrix}$ et $q \leq 90$. Les candidats sont 27, 53 et 79. Or 27 n'est pas premier. De plus, $8191 = 53 \times 154 + 29$ et $8191 = 79 \times 103 + 54$. Par conséquent, $2^{13} - 1 = 8191$ **est premier.**

Corrigé de l'exercice 23 : Problème : principe du chiffrement RSA

1. On a $n = 55$ **et** $(p-1)(q-1) = 4 \times 10 = 40$. Ensuite, $3 \wedge 40 = 1$, car $40 = 13 \times 3 + 1$, donc $e = 3$ convient. On cherche d tel que $\begin{matrix} 3d \equiv 1 \\ [40] \end{matrix}$. La relation $40 - 13 \times 3 = 1$ montre que $-13 \equiv 27$ est un inverse de 3. Donc $d = 27$, puisque $3 \times 27 = 81 = 2 \times 40 + 1$.
2. Par hypothèse, $(p-1)(q-1)$ divise $ed - 1$, donc $ed = 1 + k(p-1)(q-1)$ avec $k \in \mathbb{Z}$. Comme $ed \geq 1$, on a $k(p-1)(q-1) \geq 0$, donc $k \in \mathbb{N}$. Soit $m \in \mathbb{Z}$. Premier cas : si $p \mid m$, alors m^{ed} et m sont congrus à 0 modulo p , car $ed \geq 1$. Second cas : si

$m \not\equiv 0 \pmod{p}$, le petit théorème de Fermat donne $m^{p-1} \equiv 1 \pmod{p}$. Alors

$$m^{ed} \equiv m \pmod{p}.$$

Dans les deux cas, $m^{ed} \equiv m \pmod{p}$.

3. Par symétrie des rôles, $m^{ed} \equiv m \pmod{q}$. Ainsi, p et q divisent $m^{ed} - m$. Or p et q sont des nombres premiers distincts, donc premiers entre eux. Le corollaire du lemme de Gauss donne $pq \mid m^{ed} - m$, c'est-à-dire $m^{ed} \equiv m \pmod{n}$.

4. On calcule $8^3 = 512 = 9 \times 55 + 17$. Donc **le message chiffré est** $c = 17$.

5. Modulo 5, on a $17 \equiv 2$ et $2^4 \equiv 1$. Comme $27 = 4 \times 6 + 3$, on obtient $17^{27} \equiv 2^3 = 8 \equiv 3 \pmod{5}$. Modulo 11, on a $17 \equiv 6$ et $6^{10} \equiv 1$, donc $17^{27} \equiv 6^7 \pmod{11}$.

Ensuite, $6^2 = 36 \equiv 3$, $6^4 \equiv 9$, $6^6 \equiv 27 \equiv 5$, puis $6^7 \equiv 30 \equiv 8 \pmod{11}$. On cherche donc x avec $x \equiv 3 \pmod{5}$ et $x \equiv 8 \pmod{11}$. Écrivons $x = 8 + 11j$: comme $8 \equiv 3 \pmod{5}$ et $11 \equiv 1 \pmod{5}$, la condition devient $j \equiv 0 \pmod{5}$. Donc $x \equiv 8 \pmod{55}$, et **le message déchiffré est bien** $m = 8$, conformément à la question 3.

6. Connaissant p et q , on calcule $(p-1)(q-1)$. Ensuite, comme e est premier avec ce nombre, l'algorithme d'Euclide étendu fournit un couple de Bézout, donc l'inverse d de e . Ainsi, **factoriser n suffit pour trouver la clé secrète**. La sécurité repose donc sur la difficulté de factoriser n lorsque p et q sont très grands.

Point de méthode : pour calculer modulo pq , travaillez séparément modulo p et modulo q , puis recollez les résultats grâce au lemme de Gauss.

[Revenir aux énoncés des exercices](#)

Pour aller plus loin en maths sup

- Le cours : [arithmétique dans \$\mathbb{Z}\$, cours de maths sup](#)
- Les énoncés : [exercices de maths sup sur arithmétique dans \$\mathbb{Z}\$](#)
- À maîtriser avant : [Logique, ensembles, applications et relations](#)
- Chapitre précédent : [Dérivabilité et convexité](#)
- Chapitre suivant : [Structures algébriques usuelles : groupes, anneaux, corps](#)
- Le même thème en L1 : [arithmétique dans \$\mathbb{Z}\$, exercices de maths en L1](#)
- Tester vos connaissances : [QCM de maths sup par chapitre](#)
- Le sommaire : [tous les chapitres de maths sup](#) et les [chapitres de maths spé](#)