

Arithmétique dans $\mathbb{Z}$

Corrigé de l'exercice 1 : Divisibilité et combinaisons linéaires

- Supposons $a \mid b$ et $b \mid a$. Si $a = 0$, alors b est un multiple de 0 , donc $b = 0$ et $|a| = |b|$. Sinon, $a = kb$ avec $a \neq 0$, donc $b \neq 0$. Or un diviseur d'un entier non nul lui est inférieur en valeur absolue. Ainsi $|b| \leq |a|$ et, de même, $|a| \leq |b|$. **Par conséquent** $|a| = |b|$.
- On remarque que $2n + 13 = 2(n + 3) + 7$. Si $n + 3$ divise $2n + 13$, alors il divise la combinaison $(2n + 13) - 2(n + 3) = 7$. Réciproquement, si $n + 3$ divise 7 , il divise $2(n + 3) + 7 = 2n + 13$. La condition équivaut donc à $n + 3 \in \{-7, -1, 1, 7\}$. **Les solutions sont** $n \in \{-10, -4, -2, 4\}$. Par exemple, pour $n = 4$, on trouve bien $7 \mid 21$.
- On écrit $n^2 + n = n(n + 1)$ et l'on distingue selon le reste de n modulo 2 . Si $n = 2k$, alors $n(n + 1) = 2k(2k + 1)$. Si $n = 2k + 1$, alors $n(n + 1) = 2(2k + 1)(k + 1)$. **Dans les deux cas, $n^2 + n$ est pair.**

Point de méthode : pour une condition du type « $n + 3$ divise une expression », on retranche un multiple adapté de $n + 3$ afin d'obtenir une constante.

Corrigé de l'exercice 2 : Division euclidienne et carrés modulo 4

- On a $17 \times 119 = 2023$, donc $2024 = 17 \times 119 + 1$, avec $0 \leq 1 < 17$. Ensuite, on en déduit $-2024 = 17 \times (-119) - 1 = 17 \times (-120) + 16$. **Le quotient de 2024 par 17 vaut 119 et le reste 1 ; pour -2024, le quotient vaut -120 et le reste 16.**
- Le plus grand multiple de 6 inférieur ou égal à -47 est -48 . Ainsi $-47 = 6 \times (-8) + 1$

. Le quotient vaut -8 et le reste 1 .

3. D'après la division euclidienne par 2 , tout entier n s'écrit $2k$ ou $2k + 1$. Dans le premier cas, $n^2 = 4k^2$, de reste 0 modulo 4 . Dans le second cas, $n^2 = 4(k^2 + k) + 1$, de reste 1 . **Un carré est donc congru à 0 ou à 1 modulo 4 .**
4. Soient x et y deux entiers. D'après la question précédente, $x^2 + y^2$ est congru à $0 + 0$, $0 + 1$ ou $1 + 1$ modulo 4 . Ainsi $x^2 + y^2$ est congru à 0 , 1 ou 2 modulo 4 , jamais à 3 . **Un entier de la forme $4k + 3$ n'est donc jamais somme de deux carrés.** Par exemple, 7 , 11 et 15 ne le sont pas.

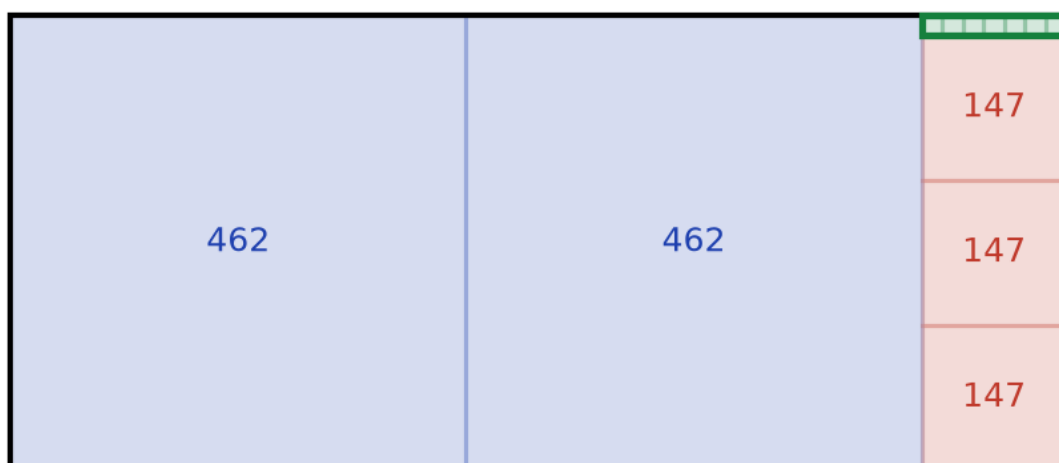
Corrigé de l'exercice 3 : PGCD par l'algorithme d'Euclide

1. On effectue les divisions successives :

$$\begin{aligned} 1071 &= 2 \times 462 + 147 \\ 462 &= 3 \times 147 + 21 \\ 147 &= 7 \times 21 + 0. \end{aligned}$$

Le dernier reste non nul vaut 21 . **Ainsi** $1071 \wedge 462 = 21$.

2. Un carré de côté c pave le rectangle si et seulement si c divise la longueur 1071 et la largeur 462 . Le côté cherché est donc le plus grand diviseur commun, c'est-à-dire 21 . On place alors $1071 / 21 = 51$ carrés en longueur et $462 / 21 = 22$ carrés en largeur. **Il faut** $51 \times 22 = 1122$ **carrés de côté** 21 . La figure ci-dessous illustre l'algorithme : chaque division correspond à une série de carrés, et le dernier carré a pour côté le PGCD.



$$1071 = 2 \times 462 + 147 \quad \text{puis} \quad 462 = 3 \times 147 + 21$$



agrandissement de la bande verte $147 \times 21 : 147 = 7 \times 21$

3. On a $4620 = 3 \times 1386 + 462$, car $3 \times 1386 = 4158$. Ensuite $1386 = 3 \times 462 + 0$.
Le dernier reste non nul donne $4620 \wedge 1386 = 462$.

Corrigé de l'exercice 4 : Coefficients de Bézout

1. On remonte l'algorithme de l'exercice 3. La deuxième division donne $21 = 462 - 3 \times 147$. La première donne $147 = 1071 - 2 \times 462$. En substituant, on obtient

$$21 = 462 - 3(1071 - 2 \times 462) = 7 \times 462 - 3 \times 1071.$$

On vérifie : $7 \times 462 = 3234$ et $3 \times 1071 = 3213$, dont la différence vaut 21. **On peut prendre** $u = -3$ **et** $v = 7$.

2. On a $51 = 2 \times 22 + 7$, puis $22 = 3 \times 7 + 1$. Le dernier reste non nul vaut 1. D'ailleurs, $51 = 3 \times 17$ et $22 = 2 \times 11$ n'ont aucun facteur premier commun. **Donc** $51 \wedge 22 = 1$.

3. Comme $1071 = 21 \times 51$ et $462 = 21 \times 22$, l'équation équivaut à $51u + 22v = 1$. Le couple $(-3, 7)$ en est solution. Par différence, $51(u + 3) = -22(v - 7)$. Ainsi 22 divise $51(u + 3)$, et $22 \wedge 51 = 1$. Le lemme de Gauss donne $u + 3 = 22k$ avec $k \in \mathbb{Z}$. En reportant, $51 \times 22k = -22(v - 7)$, donc $v - 7 = -51k$. Réciproquement, ces couples conviennent. **Les solutions sont les couples** $(u, v) = (-3 + 22k, 7 - 51k)$, $k \in \mathbb{Z}$.

Corrigé de l'exercice 5 : Inverse modulaire par l'algorithme d'Euclide étendu

1. On écrit les divisions successives :

$$\begin{aligned} 97 &= 2 \times 35 + 27, & 35 &= 1 \times 27 + 8, \\ 27 &= 3 \times 8 + 3, & 8 &= 2 \times 3 + 2, \\ 3 &= 1 \times 2 + 1, & 2 &= 2 \times 1 + 0. \end{aligned}$$

Le dernier reste non nul vaut 1, donc $97 \wedge 35 = 1$.

2. On remonte les divisions, du bas vers le haut. D'abord $1 = 3 - 2$. Ensuite, $2 = 8 - 2 \times 3$ donne $1 = 3 \times 3 - 8$. Puis $3 = 27 - 3 \times 8$ donne $1 = 3 \times 27 - 10 \times 8$. De plus, $8 = 35 - 27$ donne $1 = 13 \times 27 - 10 \times 35$. Enfin, $27 = 97 - 2 \times 35$ donne

$$1 = 13 \times 97 - 36 \times 35.$$

On vérifie : $13 \times 97 = 1261$ et $36 \times 35 = 1260$. **On peut prendre $u = 13$ et $v = -36$.**

3. La relation précédente s'écrit $35 \times (-36) \equiv 1_{[97]}$. Or $-36 \equiv 61_{[97]}$. On vérifie : $35 \times 61 = 2135 = 22 \times 97 + 1$. **L'inverse de 35 modulo 97 est 61.**

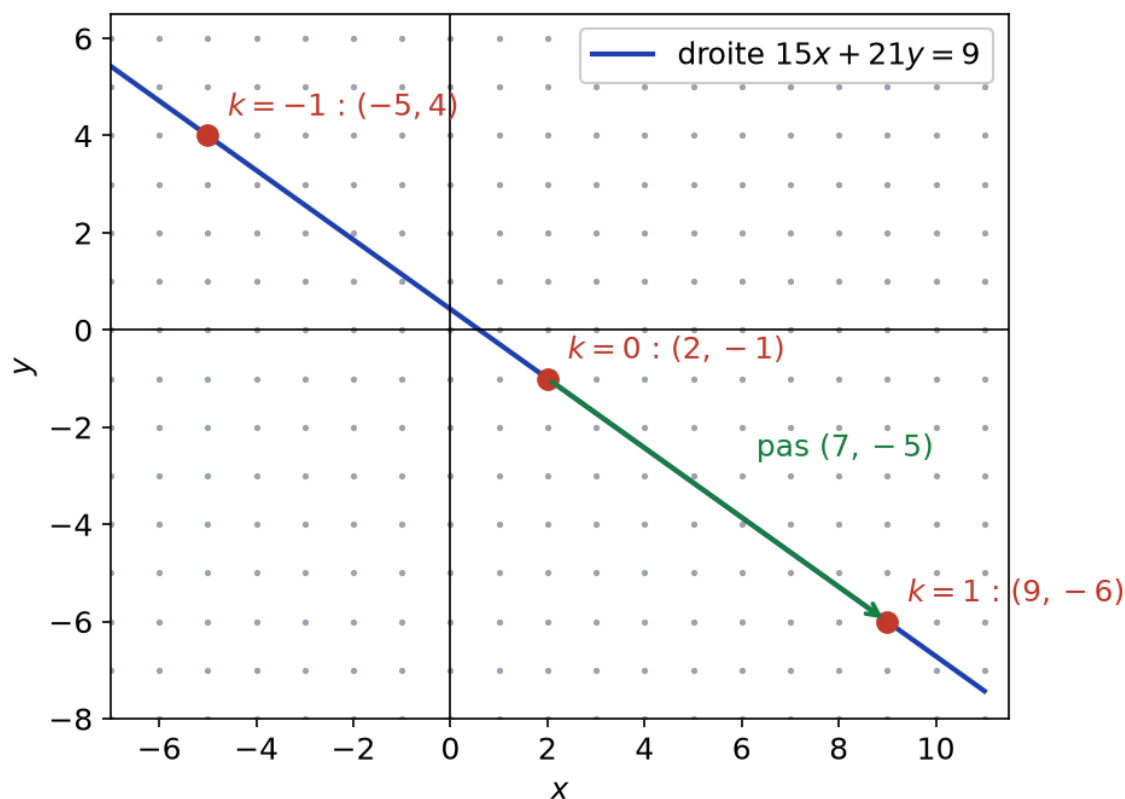
4. Comme 35 est inversible modulo 97, on multiplie la congruence par 61. Ainsi $35x \equiv 4_{[97]}$ équivaut à $x \equiv 244_{[97]}$. Or $244 = 2 \times 97 + 50$. Réciproquement, $35 \times 50 = 1750 = 18 \times 97 + 4$. **Les solutions sont les entiers $x = 50 + 97k$, $k \in \mathbb{Z}$.**

Point de méthode : vérifiez toujours la relation de Bézout par un calcul direct, car une erreur de signe en remontant l'algorithme est fréquente.

Corrigé de l'exercice 6 : Équation diophantienne $15x + 21y = c$

- On a $15 = 3 \times 5$ et $21 = 3 \times 7$, donc 3 divise $15x + 21y$ pour tous entiers x, y . Or 3 ne divise pas 10 . **L'équation $15x + 21y = 10$ n'a donc aucune solution entière.**
- On a $15 \wedge 21 = 3$. D'après le théorème sur les équations diophantiennes, l'équation a des solutions si et seulement si 3 divise c . **Les entiers c cherchés sont les multiples de 3 .**
- On divise par 3 : l'équation équivaut à $5x + 7y = 3$. Le couple $(2, -1)$ est solution, car $10 - 7 = 3$. Soit (x, y) une solution. Par différence, $5(x - 2) = -7(y + 1)$. Ainsi 7 divise $5(x - 2)$, avec $7 \wedge 5 = 1$. D'après le lemme de Gauss, $x - 2 = 7k$ avec $k \in \mathbb{Z}$. On en déduit $35k = -7(y + 1)$, soit $y = -1 - 5k$. Réciproquement,
 $5(2 + 7k) + 7(-1 - 5k) = 3$. **Les solutions sont les couples $(2 + 7k, -1 - 5k)$, $k \in \mathbb{Z}$.**

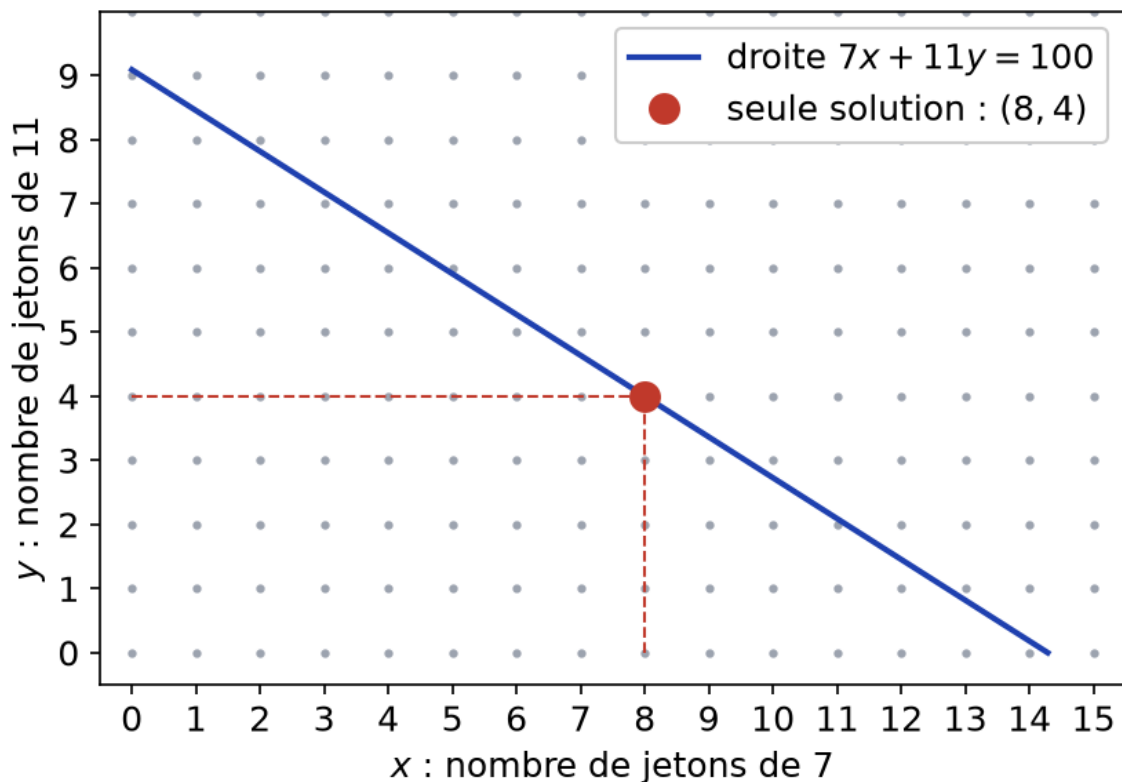
Comme le montre la figure ci-dessous, ces points sont alignés sur la droite $15x + 21y = 9$, espacés par le vecteur $(7, -5)$.



4. La condition $0 \leq 2 + 7k < 7$ équivaut à $-2 \leq 7k < 5$, donc à $k = 0$. **La solution cherchée est $(2, -1)$.**

Corrigé de l'exercice 7 : Atteindre 100 avec des jetons de 7 et de 11

1. On applique l'algorithme d'Euclide : $11 = 1 \times 7 + 4$, $7 = 1 \times 4 + 3$, $4 = 1 \times 3 + 1$. On remonte ensuite : $1 = 4 - 3 = 4 - (7 - 4) = 2 \times 4 - 7$. Or $4 = 11 - 7$, donc $1 = 2 \times 11 - 3 \times 7$. **On peut prendre $u = -3$ et $v = 2$: $7 \times (-3) + 11 \times 2 = 1$.**
2. En multipliant par 100, le couple $(-300, 200)$ est solution de $7x + 11y = 100$. Soit (x, y) une solution. Par différence, $7(x + 300) = -11(y - 200)$. Comme 11 divise $7(x + 300)$ et $11 \wedge 7 = 1$, le lemme de Gauss donne $x = -300 + 11k$. On en déduit $y = 200 - 7k$. Réciproquement, $7(-300 + 11k) + 11(200 - 7k) = -2100 + 2200 = 100$. **Les solutions sont les couples $(-300 + 11k, 200 - 7k)$, $k \in \mathbb{Z}$.**
3. La condition $x \geq 0$ s'écrit $11k \geq 300$, soit $k \geq 28$, car $11 \times 27 = 297 < 300$. La condition $y \geq 0$ s'écrit $7k \leq 200$, soit $k \leq 28$, car $7 \times 29 = 203 > 200$. Donc $k = 28$, puis $x = -300 + 308 = 8$ et $y = 200 - 196 = 4$. On vérifie : $56 + 44 = 100$. **Il existe une seule façon : huit jetons de 7 et quatre jetons de 11.** La figure ci-dessous montre que la droite ne passe que par un seul point du quadrillage dans le quart de plan positif.



Corrigé de l'exercice 8 : PGCD d'expressions dépendant de n

- On calcule la combinaison $3(2n + 1) - 2(3n + 2) = -1$. Tout diviseur commun positif de $2n + 1$ et $3n + 2$ divise donc 1. Autrement dit, on dispose d'une relation de Bézout. **Ainsi** $(2n + 1) \wedge (3n + 2) = 1$.
- On a $n^2 + n + 1 = n(n + 1) + 1$. D'après le lemme clé de l'algorithme d'Euclide, $(n^2 + n + 1) \wedge (n + 1) = (n + 1) \wedge 1$. **Ce PGCD vaut donc 1**.
- On calcule $2(n + 5) - (2n + 3) = 7$. Soit $d = (n + 5) \wedge (2n + 3)$. Alors d divise 7. Comme 7 est premier, d **vaut 1 ou 7**.
- Si $d = 7$, alors 7 divise $n + 5$. Réciproquement, si 7 divise $n + 5$, alors 7 divise aussi $2n + 3 = 2(n + 5) - 7$, donc $d = 7$. Or $7 \mid n + 5$ équivaut à $\begin{matrix} n \equiv -5 \equiv 2 \\ , [7] \end{matrix}$. **Le PGCD vaut 7 si et seulement si $\begin{matrix} n \equiv 2 \\ , [7] \end{matrix}$** . Par exemple, pour $n = 2$, on trouve $7 \wedge 7 = 7$.

Corrigé de l'exercice 9 : Lemme de Gauss et divisibilité

1. Le nombre 7 est premier et ne divise pas 5, donc $7 \wedge 5 = 1$. Comme 7 divise $5n$, le lemme de Gauss s'applique. **Donc 7 divise n .**
2. On a $12 = 2^2 \times 3$ et $35 = 5 \times 7$, donc $12 \wedge 35 = 1$. Si $12x = 35y$, alors 35 divise $12x$, et le lemme de Gauss donne $x = 35k$. En reportant, $12 \times 35k = 35y$, donc $y = 12k$. Réciproquement, ces couples conviennent. **Les solutions sont les couples $(35k, 12k)$, $k \in \mathbb{Z}$.**
3. D'abord, $n(n+1)$ est pair, comme vu à l'exercice 1, donc le produit est divisible par 2. Ensuite, on raisonne modulo 3. Si $n \equiv 0$, alors $3 \mid n$. Si $n \equiv 1$, alors $2n+1 \equiv 3 \equiv 0$. Si $n \equiv 2$, alors $n+1 \equiv 0$. **Dans tous les cas, $n(n+1)(2n+1)$ est divisible par 2 et par 3.**
4. On utilise le corollaire du lemme de Gauss : si $a \mid c$, $b \mid c$ et $a \wedge b = 1$, alors $ab \mid c$. Ici $a = 2$, $b = 3$ et $2 \wedge 3 = 1$. **Ainsi 6 divise $n(n+1)(2n+1)$ pour tout entier n .**

Corrigé de l'exercice 10 : PGCD et PPCM imposés

1. On a $d(a' \wedge b') = (da') \wedge (db') = d$, et $d \geq 1$, donc $a' \wedge b' = 1$. Soit ensuite m un multiple commun de a et b . On écrit $m = da'k$. Comme db' divise $da'k$, on obtient $b' \mid a'k$. Par le lemme de Gauss, $b' \mid k$, donc m est multiple de $da'b'$. Enfin $da'b'$ est un multiple commun de a et b . **Par conséquent $a \vee b = da'b'$.**
2. On pose $a = 12a'$ et $b = 12b'$, avec $a' \wedge b' = 1$. D'après la question 1, $12a'b' = 360$, donc $a'b' = 30 = 2 \times 3 \times 5$. Comme 30 n'a pas de facteur carré, tout couple de produit 30 est formé d'entiers premiers entre eux. Les couples (a', b') sont donc $(1, 30)$, $(2, 15)$, $(3, 10)$, $(5, 6)$ et leurs symétriques. Réciproquement, ils conviennent tous. **Les solutions sont $(12, 360)$, $(24, 180)$, $(36, 120)$, $(60, 72)$ et les couples obtenus en échangeant a et b .**
3. De même, $a = 12a'$ et $b = 12b'$ avec $a' \wedge b' = 1$, et la condition devient $a' + b' = 7$. Pour $1 \leq a' \leq 6$, on a $a' \wedge (7 - a') = a' \wedge 7 = 1$, car 7 est premier.

Tous les couples conviennent donc. **Les solutions sont** $(12, 72)$, $(24, 60)$, $(36, 48)$, $(48, 36)$, $(60, 24)$ **et** $(72, 12)$.

Corrigé de l'exercice 11 : Test de primalité

1. Le plus petit diviseur $p \geq 2$ de n est premier. En effet, un diviseur strict de p supérieur à 1 diviserait n et serait plus petit que p . Si n est composé, on écrit $n = pm$ avec $m \geq 2$. Par minimalité, $m \geq p$. **Donc** $n = pm \geq p^2$.
2. On a $14^2 = 196$ et $15^2 = 225$. Si 223 était composé, il aurait donc un diviseur premier $p \leq 14$, soit $p \in \{2, 3, 5, 7, 11, 13\}$. Or 223 est impair ; la somme de ses chiffres vaut 7 , donc $3 \nmid 223$; il ne se termine ni par 0 ni par 5 . De plus, $223 = 7 \times 31 + 6 = 11 \times 20 + 3 = 13 \times 17 + 2$. **Aucun essai ne réussit, donc 223 est premier.**
3. Pour 221 , on teste les premiers jusqu'à 14 : on trouve $221 = 13 \times 17$. Pour 391 , on teste de même jusqu'à 19 , car $20^2 = 400$: on trouve $391 = 17 \times 23$. **Ainsi $221 = 13 \times 17$ et $391 = 17 \times 23$.**

Corrigé de l'exercice 12 : Décomposition en facteurs premiers de 2520 et 3780

1. On divise successivement par les petits nombres premiers. D'abord $2520 = 2^3 \times 315$, puis $315 = 3^2 \times 35$ et $35 = 5 \times 7$. Ensuite $3780 = 2^2 \times 945$, puis $945 = 3^3 \times 35$. **Ainsi $2520 = 2^3 \times 3^2 \times 5 \times 7$ et $3780 = 2^2 \times 3^3 \times 5 \times 7$.**
2. On prend le minimum, puis le maximum, des exposants :
$$2520 \wedge 3780 = 2^2 \times 3^2 \times 5 \times 7 = 1260, \quad 2520 \vee 3780 = 2^3 \times 3^3 \times 5 \times 7 = 7560.$$

On vérifie : $1260 \times 7560 = 9\,525\,600 = 2520 \times 3780$. **Le PGCD vaut 1260 et le PPCM 7560.**
3. Un diviseur positif s'écrit $2^\alpha 3^\beta 5^\gamma 7^\delta$ avec $0 \leq \alpha \leq 3$, $0 \leq \beta \leq 2$, $\gamma, \delta \in \{0, 1\}$. Par

unicité de la décomposition, ces choix donnent des diviseurs distincts. **Il y en a**
 $4 \times 3 \times 2 \times 2 = 48$.

Corrigé de l'exercice 13 : Carrés parfaits et irrationalité

1. Si $n = m^2$, alors $v_p(n) = 2v_p(m)$ pour tout p premier, donc tous les exposants sont pairs. Réciproquement, si $n = \prod_i p_i^{2\beta_i}$, alors $n = \left(\prod_i p_i^{\beta_i}\right)^2$. **L'équivalence est démontrée.**
2. On a $2520 = 2^3 \times 3^2 \times 5 \times 7$. Pour que $2520k$ soit un carré, il faut que $3 + v_2(k)$, $1 + v_5(k)$ et $1 + v_7(k)$ soient pairs. Ainsi k est multiple de $2 \times 5 \times 7 = 70$. Réciproquement, $2520 \times 70 = 2^4 \times 3^2 \times 5^2 \times 7^2$. **Le plus petit entier est $k = 70$, et $2520 \times 70 = 176400 = 420^2$.**
3. Supposons $\sqrt{6} = a/b$ avec $a, b \in \mathbb{N}^*$. Alors $a^2 = 6b^2$. En prenant la valuation 2-adique, on obtient $2v_2(a) = 1 + 2v_2(b)$. Le membre de gauche est pair et celui de droite impair. C'est absurde. **Donc $\sqrt{6}$ est irrationnel.**

Corrigé de l'exercice 14 : Valuation p-adique de n! et zéros de 100!

1. Les multiples positifs de p^j sont les kp^j avec $k \geq 1$. La condition $kp^j \leq n$ équivaut à $k \leq n/p^j$, donc à $k \leq \lfloor n/p^j \rfloor$, car k est entier. **Il y a donc $\lfloor n/p^j \rfloor$ multiples de p^j entre 1 et n .**
2. Comme la valuation d'un produit est la somme des valuations, $v_p(n!) = \sum_{m=1}^n v_p(m)$. Or $v_p(m)$ est le nombre d'entiers $j \geq 1$ tels que $p^j \mid m$. On compte donc les couples (m, j) tels que $p^j \mid m$. En regroupant selon j , puis en utilisant la question 1, on obtient

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

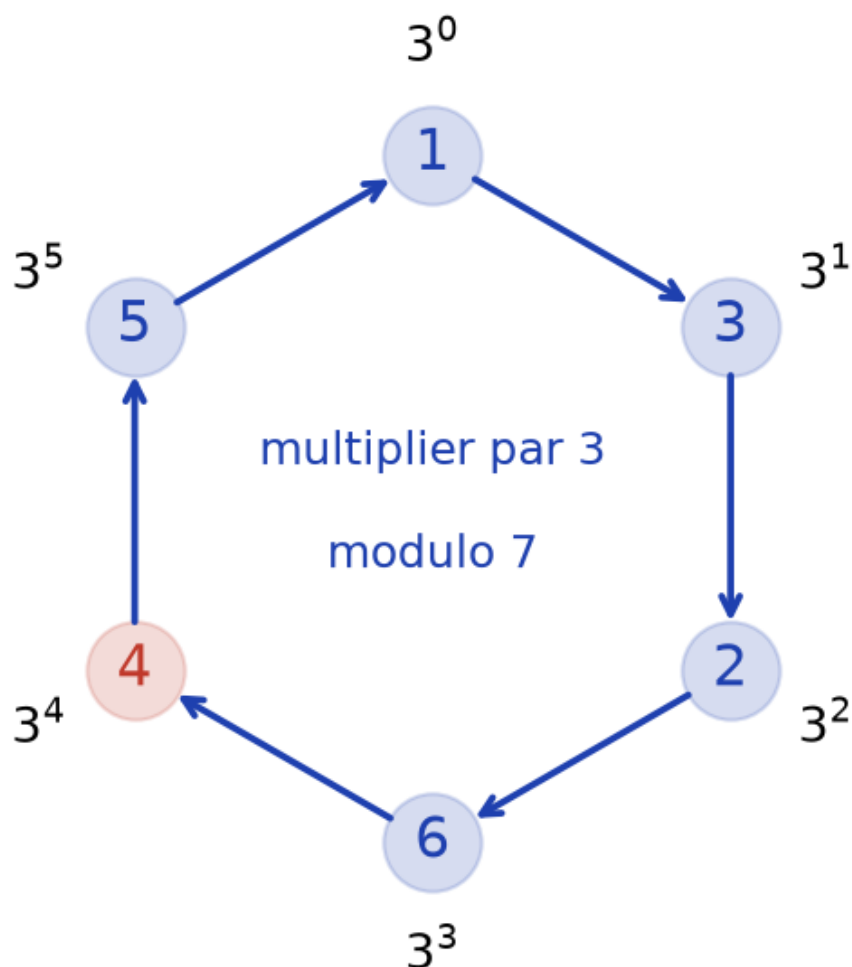
La somme est finie, car les termes sont nuls dès que $p^j > n$.

3. Pour $p = 2$, on trouve $50 + 25 + 12 + 6 + 3 + 1 = 97$. Pour $p = 5$, on trouve $20 + 4 = 24$. **Ainsi $v_2(100!) = 97$ et $v_5(100!) = 24$.**

4. L'écriture se termine par k zéros si 10^k divise $100!$ et 10^{k+1} ne le divise pas. Or $10^k = 2^k 5^k$ divise $100!$ si et seulement si $k \leq 97$ et $k \leq 24$. **L'entier $100!$ se termine donc par 24 zéros.**

Corrigé de l'exercice 15 : Calcul de restes par congruences

1. Le nombre 7 est premier et ne divise pas 3. Le petit théorème de Fermat donne donc $3^6 \equiv 1 \pmod{7}$. Or $100 = 6 \times 16 + 4$, d'où $3^{100} \equiv 3^4 = 81 \pmod{7}$. Enfin $81 = 11 \times 7 + 4$. **Le reste vaut 4.** La figure ci-dessous montre le cycle des puissances de 3 modulo 7, de période 6.



$$3^{100} = (3^6)^{16} \times 3^4 \equiv 4 \text{ modulo } 7$$

2. On a $2^3 = 8 \equiv -1$, donc $2^6 \equiv 1$. Ensuite $2026 = 6 \times 337 + 4$. Ainsi $2^{2026} \equiv 2^4 = 16 \equiv 7$. **Le reste vaut 7.**

3. Le chiffre des unités est le reste modulo 10. Or $7^2 = 49 \equiv -1$, donc $7^4 \equiv 1$. Comme $2026 = 4 \times 506 + 2$, on obtient $7^{2026} \equiv 7^2 \equiv 9$. **Le chiffre des unités est 9.**

4. On a $2^{3n} = 8^n$ et $8 \equiv 1$. Par compatibilité avec les puissances, $8^n \equiv 1^n = 1$. **Donc 7 divise $2^{3n} - 1$.**

Corrigé de l'exercice 16 : Critères de divisibilité par 9 et par 11

1. On a $10 \equiv 1 \pmod{9}$, donc $10^k \equiv 1 \pmod{9}$ pour tout k . Par compatibilité avec la somme et le produit, $N \equiv \sum_{[9]} c_k$.
2. De même, $10 \equiv -1 \pmod{11}$, donc $10^k \equiv (-1)^k \pmod{11}$. Ainsi $N \equiv \sum_{[11]} (-1)^k c_k$.
3. La somme des chiffres de 123456789 vaut $45 = 5 \times 9$. Le nombre est donc divisible par 9. Pour 11, on part du chiffre des unités : $9 - 8 + 7 - 6 + 5 - 4 + 3 - 2 + 1 = 5$. **Le reste modulo 9 vaut 0 et le reste modulo 11 vaut 5 : le nombre est divisible par 9, pas par 11.**
4. Pour 918082, la somme alternée à partir des unités vaut $2 - 8 + 0 - 8 + 1 - 9 = -22$. Or $-22 \equiv 0 \pmod{11}$. **Donc 11 divise 918082.** On vérifie d'ailleurs : $918082 = 11 \times 83462$.
5. La somme des chiffres vaut $7 + x + 3 + 6 = 16 + x$. Elle doit être multiple de 9, avec $0 \leq x \leq 9$. Donc $16 + x = 18$. **Le chiffre cherché est $x = 2$: $7236 = 9 \times 804$.**

Corrigé de l'exercice 17 : Équations de congruence

1. On calcule $17 \times 19 = 323 = 14 \times 23 + 1$. Ainsi 19 est un inverse de 17 modulo 23. En multipliant par 19, la congruence équivaut à $x \equiv 95 \pmod{23}$. Or $95 = 4 \times 23 + 3$. Réciproquement, $17 \times 3 = 51 = 2 \times 23 + 5$. **Les solutions sont les $x \equiv 3 \pmod{23}$.**
2. La congruence signifie qu'il existe k tel que $6x - 4 = 10k$, soit $3x - 2 = 5k$. Elle équivaut donc à $3x \equiv 2 \pmod{5}$. Or $3 \times 2 = 6 \equiv 1 \pmod{5}$, donc 2 est l'inverse de 3. On obtient $x \equiv 4 \pmod{5}$. **Les solutions sont les entiers $x \equiv 4 \pmod{10}$ ou $x \equiv 9 \pmod{10}$.** On vérifie : 24 et 54 sont congrus à 4 modulo 10.
3. Pour tout entier x , le nombre $6x - 3$ est impair. Or un multiple de 10 est pair. **La**

congruence $6x \equiv 3 \pmod{10}$ n'a donc pas de solution.

4. La congruence $ax \equiv c \pmod{n}$ équivaut à l'existence de y tel que $ax + ny = c$. C'est une équation diophantienne. **Elle a une solution si et seulement si $a \wedge n$ divise c** . On retrouve les cas précédents : $6 \wedge 10 = 2$ divise 4 , mais pas 3 .

Corrigé de l'exercice 18 : Système de congruences

- Si $x \equiv 2 \pmod{21}$, alors 21 divise $x - 2$, donc 3 et 7 aussi. Réciproquement, si 3 et 7 divisent $x - 2$, le corollaire du lemme de Gauss s'applique, car $3 \wedge 7 = 1$. Donc 21 divise $x - 2$. **Les deux conditions équivalent à $x \equiv 2 \pmod{21}$** .
- On écrit $x = 2 + 21k$. Comme $21 \equiv 1 \pmod{5}$, on a $x \equiv 2 + k \pmod{5}$. La condition $x \equiv 3 \pmod{5}$ équivaut donc à $k \equiv 1 \pmod{5}$. **Autrement dit, $k = 1 + 5j$ avec $j \in \mathbb{Z}$** .
- On obtient $x = 2 + 21(1 + 5j) = 23 + 105j$. On vérifie :
 $23 = 7 \times 3 + 2 = 4 \times 5 + 3 = 3 \times 7 + 2$. **Les solutions sont les $x \equiv 23 \pmod{105}$, et la plus petite solution positive est 23** .

Corrigé de l'exercice 19 : Divisibilité de $n^7 - n$ par 42

- Le nombre 7 est premier. D'après le petit théorème de Fermat, $n^7 \equiv n \pmod{7}$ pour tout entier n .
Donc 7 divise $n^7 - n$.
- Modulo 2 , le petit théorème de Fermat donne $n^2 \equiv n \pmod{2}$. Par récurrence, $n^k \equiv n \pmod{2}$ pour tout $k \geq 1$, car $n^{k+1} = n^k \times n \equiv n^2 \equiv n \pmod{2}$. En particulier $n^7 \equiv n \pmod{2}$. Modulo 3 , on a

$n^3 \equiv n$. Ainsi $\begin{matrix} n^7 \\ ,[3] \end{matrix} = n^3 \times n^3 \times n \equiv n^3 \equiv n$. **Donc** $n^7 - n$ est divisible par 2 et par 3.

3. Comme $2 \wedge 3 = 1$, le corollaire du lemme de Gauss donne $6 \mid n^7 - n$. Ensuite $6 \wedge 7 = 1$ et $7 \mid n^7 - n$, donc $42 \mid n^7 - n$. **Ainsi** 42 divise $n^7 - n$ pour tout entier n .

Corrigé de l'exercice 20 : Une démonstration du petit théorème de Fermat

1. Pour $1 \leq k \leq p-1$, on a $k \binom{p}{k} = p \binom{p-1}{k-1}$. Ainsi p divise $k \binom{p}{k}$. De plus $p \wedge k = 1$, car p est premier et $1 \leq k < p$. **Le lemme de Gauss donne** $p \mid \binom{p}{k}$.

2. La formule du binôme donne

$$(a+1)^p = a^p + 1 + \sum_{k=1}^{p-1} \binom{p}{k} a^k.$$

Chaque terme de la somme est multiple de p d'après la question 1. **Donc**

$$\begin{matrix} (a+1)^p \\ ,[p] \end{matrix} \equiv a^p + 1.$$

3. On raisonne par récurrence sur $a \in \mathbb{N}$. Pour $a = 0$, l'égalité $0^p = 0$ convient. Supposons $\begin{matrix} a^p \\ ,[p] \end{matrix} \equiv a$. Alors $\begin{matrix} (a+1)^p \\ ,[p] \end{matrix} \equiv a^p + 1 \equiv a + 1$. Soit maintenant $a \in \mathbb{Z}$ quelconque. On

choisit $m \in \mathbb{N}$ tel que $b = a + mp \geq 0$. Comme $\begin{matrix} b \\ ,[p] \end{matrix} \equiv a$, on a $\begin{matrix} a^p \\ ,[p] \end{matrix} \equiv b^p \equiv b \equiv a$.

Ainsi $\begin{matrix} a^p \\ ,[p] \end{matrix} \equiv a$ pour tout $a \in \mathbb{Z}$.

4. Le nombre p divise $a^p - a = a(a^{p-1} - 1)$. Si $p \nmid a$, alors $p \wedge a = 1$, car p est premier. **Le lemme de Gauss donne** $\begin{matrix} a^{p-1} \\ ,[p] \end{matrix} \equiv 1$.

5. On a $2^{10} = 1024 = 3 \times 341 + 1$, donc $\begin{matrix} 2^{10} \\ ,[341] \end{matrix} \equiv 1$. Ensuite $2^{340} = (2^{10})^{34} \equiv 1$.

Pourtant $341 = 11 \times 31$ n'est pas premier. La propriété $2^{n-1} \equiv 1 \pmod{n}$ n'entraîne donc pas que n soit premier.

Corrigé de l'exercice 21 : Infinité des nombres premiers de la forme $4k+3$

1. Un entier est congru à 0, 1, 2 ou 3 modulo 4. S'il est congru à 0 ou 2, il est pair. **Un premier impair est donc congru à 1 ou à 3 modulo 4.**

2. Par compatibilité de la congruence avec le produit, si $a_i \equiv 1 \pmod{4}$ pour tout i , alors $\prod_{i=1}^k a_i \equiv 1 \pmod{4}$.

Le résultat se prouve par récurrence sur le nombre de facteurs.

3. La liste contient 3, donc $N \geq 4 \times 3 - 1 = 11$. De plus $N \equiv -1 \equiv 3 \pmod{4}$, donc N est impair. Ses facteurs premiers sont donc impairs. S'ils étaient tous congrus à 1 modulo 4, leur produit N serait congru à 1 d'après la question 2. C'est faux. **Donc N possède un diviseur premier $q \equiv 3 \pmod{4}$.**

4. Par hypothèse, q est l'un des p_i . Il divise alors $4p_1 \cdots p_k$ et N , donc leur différence 1. C'est absurde, car $q \geq 3$. **Il existe donc une infinité de nombres premiers congrus à 3 modulo 4.**

Corrigé de l'exercice 22 : PGCD des nombres de Mersenne

1. Écrivons $n = dm$ et posons $x = 2^d$. La factorisation $x^m - 1 = (x - 1)(1 + x + \dots + x^{m-1})$ donne

$$2^n - 1 = (2^d - 1)(1 + 2^d + 2^{2d} + \dots + 2^{(m-1)d}).$$

Donc M_d divise M_n .

- Supposons M_n premier. Alors $M_n \geq 2$, donc $n \geq 2$. Si n était composé, on écrirait $n = dm$ avec $2 \leq d < n$. Alors M_d diviserait M_n , avec $3 \leq M_d < M_n$, ce qui contredit la primalité. **Donc n est premier.** La réciproque est fausse : 11 est premier, mais $M_{11} = 2047 = 23 \times 89$.
- On calcule $2^r(2^{bq} - 1) + 2^r - 1 = 2^{bq+r} - 1 = M_a$. D'après la question 1, M_b divise M_{bq} , ce qui reste vrai si $q = 0$, car $M_0 = 0$. On écrit $M_{bq} = K M_b$, d'où $M_a = 2^r K M_b + M_r$. D'après le lemme clé de l'algorithme d'Euclide, $M_a \wedge M_b = M_b \wedge M_r$.
- On démontre par récurrence forte sur $b \in \mathbb{N}$ que $M_a \wedge M_b = M_{a \wedge b}$ pour tout a . Pour $b = 0$, on a $M_a \wedge 0 = M_a = M_{a \wedge 0}$. Pour $b \geq 1$, la question 3 et l'hypothèse de récurrence appliquée à $r < b$ donnent $M_a \wedge M_b = M_b \wedge M_r = M_b \wedge r$. Or $b \wedge r = a \wedge b$. **Ainsi $M_a \wedge M_b = M_{a \wedge b}$.** Autrement dit, l'algorithme d'Euclide sur les exposants se reflète sur les nombres de Mersenne.
- On a $12 \wedge 18 = 6$. **Donc $M_{12} \wedge M_{18} = M_6 = 63$.** On vérifie : $4095 = 63 \times 65$ et $262143 = 63 \times 4161$, avec $65 \wedge 4161 = 1$.

Point de méthode : pour calculer le PGCD d'une suite d'expressions, cherchez une relation qui imite la division euclidienne, puis appliquez le lemme $a \wedge b = b \wedge r$.

Corrigé de l'exercice 23 : Problème, un chiffrement RSA

miniature

- On a $40 = 2^3 \times 5$, et 3 ne divise pas 40, donc $3 \wedge 40 = 1$. On cherche d tel que $3d \equiv 1 \pmod{40}$. Or $3 \times 27 = 81 = 2 \times 40 + 1$. L'inverse est unique modulo 40. **On obtient $d = 27$.**
- Pour $x = 2$, on a $2^3 = 8$, déjà inférieur à 55. Pour $x = 7$, on a $7^3 = 343 = 6 \times 55 + 13$. **Le message 2 est chiffré en 8 et le message 7 en 13.**
- On a $ed = 81 = 1 + 20 \times 4$. Si 5 divise x , alors $x^{81} \equiv 0 \equiv x \pmod{5}$. Sinon, le petit théorème de Fermat donne $x^4 \equiv 1 \pmod{5}$, donc $x^{81} = x \times (x^4)^{20} \equiv x \pmod{5}$. **Dans les deux cas,**

$$x^{ed} \equiv x \pmod{5}.$$

4. De même, $81 = 1 + 8 \times 10$. Si $11 \mid x$, les deux membres sont nuls modulo 11. Sinon, $x^{10} \equiv 1 \pmod{11}$ et $x^{81} = x \times (x^{10})^8 \equiv x \pmod{11}$. Ainsi $x^{ed} \equiv x \pmod{11}$.

5. Les entiers 5 et 11 divisent $x^{81} - x$, et $5 \wedge 11 = 1$. Le corollaire du lemme de Gauss donne $55 \mid x^{81} - x$. Soit maintenant c le chiffré de x , donc $c \equiv x^3 \pmod{55}$. Alors $c^{27} \equiv x^{81} \equiv x \pmod{55}$. Comme $0 \leq x \leq 54$, **le message x est exactement le reste de c^{27} modulo 55.**

6. On calcule 13^{27} modulo 5 : $13 \equiv 3$, $3^4 \equiv 1$ et $27 = 4 \times 6 + 3$, donc $13^{27} \equiv 3^3 = 27 \equiv 2 \pmod{5}$. Modulo 11 : $13 \equiv 2$, $2^{10} \equiv 1$ et $27 = 20 + 7$, donc $13^{27} \equiv 2^7 = 128 \equiv 7 \pmod{11}$. On cherche donc $x \in \{0, 5, 10, \dots, 54\}$ avec $x \equiv 7 \pmod{11}$ et $x \equiv 2 \pmod{5}$. Les candidats 7, 18, 29, 40, 51 ont pour restes modulo 5 respectivement 2, 3, 4, 0, 1. **Le message déchiffré est $x = 7$** , ce qui confirme la question 2.

Point de méthode : pour calculer une puissance modulo un produit de deux premiers distincts, on calcule séparément modulo chaque premier avec le théorème de Fermat, puis on recolle grâce au lemme de Gauss.

[Revenir aux énoncés des exercices](#)

Pour aller plus loin en L1

- Le cours : [arithmétique dans Z, cours de maths en L1](#)
- Les énoncés : [exercices de maths en L1 sur arithmétique dans Z](#)
- À maîtriser avant : [Entiers naturels, récurrence et dénombrement](#)

- Chapitre précédent : [Fonctions usuelles et fonctions réciproques](#)
- Chapitre suivant : [Polynômes et fractions rationnelles](#)
- Le même thème en maths sup : [arithmétique dans \$\mathbb{Z}\$, exercices de maths sup](#)
- Tester vos connaissances : [QCM de maths en L1 par chapitre](#)
- Le sommaire : [tous les chapitres de maths de L1](#) et la [licence de maths de L1 à L3](#)