

Plaquette 4 – Congruences, anneaux $\mathbb{Z}/n\mathbb{Z}$ et applications

Arithmétique dans $\mathbb{Z}$ — Licence 1 (L1)

Corrections détaillées

Boîte à outils

Calcul modulo n . Si $a \equiv a'$ et $b \equiv b' \pmod{n}$, alors $a + b \equiv a' + b'$, $ab \equiv a'b'$ et $a^k \equiv a'^k$.

- a est **inversible** modulo $n \Leftrightarrow a \wedge n = 1$; l'inverse se lit dans une relation de Bézout $au + nv = 1$: c'est u .
- $\mathbb{Z}/n\mathbb{Z}$ est un **corps** $\Leftrightarrow n$ est premier ; sinon il a des **diviseurs de zéro** ($\overline{a}\overline{b} = \overline{0}$ avec $\overline{a}, \overline{b} \neq \overline{0}$).

Indicatrice d'Euler $\varphi(n)$ = nombre d'entiers de $\{1, \dots, n\}$ premiers avec n :

$$\varphi(p^k) = p^k - p^{k-1}, \quad \varphi(mn) = \varphi(m)\varphi(n) \text{ si } m \wedge n = 1, \quad a \wedge n = 1 \Rightarrow a^{\varphi(n)} \equiv 1 \pmod{n}$$

- **Ordre** de a modulo n : le plus petit $k \geq 1$ tel que $a^k \equiv 1$; alors $a^m \equiv 1 \Leftrightarrow \text{ordre} \mid m$, et l'ordre divise $\varphi(n)$.
- **Théorème chinois** : si $m \wedge n = 1$, le système $x \equiv a \pmod{m}$, $x \equiv b \pmod{n}$ a une unique solution modulo mn .
- **Carrés** : modulo 4, $x^2 \in \{0, 1\}$; modulo 8, $x^2 \in \{0, 1, 4\}$; modulo 3, $x^2 \in \{0, 1\}$.

Correction de l'exercice 1 - Réduire une grande puissance

a) $7^2 = 49$ et $7^4 = 2401 \equiv 1 \pmod{100}$. On divise l'exposant par 4 : $2026 = 4 \times 506 + 2$, donc

$$7^{2026} = (7^4)^{506} \times 7^2 \equiv 1^{506} \times 49 = 49 \pmod{100}$$

— Les deux derniers chiffres de 7^{2026} sont 49.

b) Par le petit théorème de Fermat (7 premier, $7 \nmid 3$) : $3^6 \equiv 1 \pmod{7}$. Or $2026 = 6 \times 337 + 4$:

— $3^{2026} \equiv 3^4 = 81 = 11 \times 7 + 4 \equiv 4 \pmod{7}$. Le reste est 4.

c) Les puissances de 2 modulo 10 : $2, 4, 8, 16 \equiv 6, 32 \equiv 2, \dots$: cycle 2, 4, 8, 6 de longueur 4 **à partir de l'exposant 1**.

— $2026 = 4 \times 506 + 2$: 2^{2026} se termine par le même chiffre que 2^2 , soit 4.

— $2026^{2026} \equiv 6^{2026} \pmod{10}$, et $6^k \equiv 6$ pour tout $k \geq 1$ ($6 \times 6 = 36$) : chiffre des unités 6.

d) Si $a^k \equiv 1$, alors $a^{kq+r} = (a^k)^q a^r \equiv a^r$: il suffit de connaître le **reste de l'exposant modulo k** . Fermat (ou Euler) fournit un tel k quand a est premier avec le module ; sinon (comme 2 modulo 10) on observe directement le cycle.

— **Piège** : $2^4 = 16 \not\equiv 1 \pmod{10}$; le cycle existe mais il ne passe pas par 1, car 2 n'est pas inversible modulo 10.

Réponse. $7^{2026} \equiv 49 \pmod{100}$; $3^{2026} \equiv 4 \pmod{7}$; unités de 2^{2026} : 4, de 2026^{2026} : 6.

Correction de l'exercice 2 - Indicatrice d'Euler

a) Parmi $1, \dots, p^k$, les entiers **non** premiers avec p^k sont ceux divisibles par p : $p, 2p, \dots, p^{k-1} \cdot p$, au nombre de p^{k-1} . D'où $\varphi(p^k) = p^k - p^{k-1}$.

b) $100 = 2^2 \times 5^2 : \varphi(100) = (4 - 2)(25 - 5) = 2 \times 20 = 40$.

— $360 = 2^3 \times 3^2 \times 5 : \varphi(360) = 4 \times 6 \times 4 = 96$.

— **Formule compacte** : $\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$; par exemple $360 \times \frac{1}{2} \times \frac{2}{3} \times \frac{4}{5} = 96 \checkmark$

c) Soient $r_1, \dots, r_m$ ($m = \varphi(n)$) les entiers de $\{1, \dots, n\}$ premiers avec n . Chaque ar_i est premier avec n ; et $ar_i \equiv ar_j$ entraîne $r_i \equiv r_j$ (on multiplie par l'inverse de a). Donc les ar_i sont, modulo n , les r_i **dans un autre ordre**, et :

$$\prod_{i=1}^m (ar_i) \equiv \prod_{i=1}^m r_i \Leftrightarrow a^m \prod_{i=1}^m r_i \equiv \prod_{i=1}^m r_i \pmod{n}$$

— $\prod r_i$ est inversible (produit d'inversibles) : on simplifie, $a^{\varphi(n)} \equiv 1 \pmod{n}$.

— Pour $n = p$ premier, $\varphi(p) = p - 1$: on retrouve **Fermat**.

d) $7 \wedge 100 = 1$ et $\varphi(100) = 40 : 7^{40} \equiv 1$. Or $2026 = 40 \times 50 + 26$, donc $7^{2026} \equiv 7^{26}$.

— $7^{26} = (7^4)^6 \times 7^2 \equiv 49 \checkmark$ Euler donne un exposant (40) plus grand que l'ordre réel (4) : c'est un multiple de l'ordre, pas forcément l'ordre lui-même.

Réponse. $\varphi(p^k) = p^k - p^{k-1}$; $\varphi(100) = 40$, $\varphi(360) = 96$; $a^{\varphi(n)} \equiv 1 \pmod{n}$ si $a \wedge n = 1$.

Correction de l'exercice 3 - Inverse modulaire par Bézout

a) 31 est premier et ne divise pas 17 : $17 \wedge 31 = 1$, donc 17 est inversible modulo 31.

b) Euclide : $31 = 1 \times 17 + 14$; $17 = 1 \times 14 + 3$; $14 = 4 \times 3 + 2$; $3 = 1 \times 2 + 1$. On remonte :

— $1 = 3 - 2 = 3 - (14 - 4 \times 3) = 5 \times 3 - 14$

— $= 5(17 - 14) - 14 = 5 \times 17 - 6 \times 14 = 5 \times 17 - 6(31 - 17) = 11 \times 17 - 6 \times 31$.

$$11 \times 17 - 6 \times 31 = 1 \implies 11 \times 17 \equiv 1 \pmod{31}$$

— L'inverse de 17 est 11. **Contrôle** : $187 = 6 \times 31 + 1 \checkmark$

c) On multiplie par l'inverse : $x \equiv 11 \times 5 = 55 \equiv 24 \pmod{31}$.

— **Vérification** : $17 \times 24 = 408 = 13 \times 31 + 5 \checkmark$

d) La seconde équation donne $y \equiv x$; on reporte : $20x \equiv 1 \pmod{31}$.

— Inverse de 20 : $31 = 20 + 11$, $20 = 11 + 9$, $11 = 9 + 2$, $9 = 4 \times 2 + 1$. On remonte :

— $1 = 9 - 4 \times 2 = 9 - 4(11 - 9) = 5 \times 9 - 4 \times 11$;

— $= 5(20 - 11) - 4 \times 11 = 5 \times 20 - 9 \times 11$;

— $= 5 \times 20 - 9(31 - 20) = 14 \times 20 - 9 \times 31$.

— Donc $x \equiv 14$ et $y \equiv 14 \pmod{31}$. **Vérification** : $17 \times 14 + 3 \times 14 = 280 = 9 \times 31 + 1 \checkmark$

Réponse. $17^{-1} \equiv 11 \pmod{31}$; $x \equiv 24 \pmod{31}$; système : $x \equiv y \equiv 14 \pmod{31}$.

Correction de l'exercice 4 - Le problème de Sunzi

a) 3, 5, 7 sont deux à deux premiers entre eux : le théorème chinois (appliqué deux fois) donne une unique solution modulo $3 \times 5 \times 7 = 105$.

b) e_1 est multiple de 35 et $\equiv 1 \pmod{3}$: $35 \equiv 2 \pmod{3}$, $70 \equiv 1 \pmod{3}$, donc $e_1 = 70$.

— e_2 multiple de 21 et $\equiv 1 \pmod{5}$: $21 \equiv 1 \pmod{5}$, donc $e_2 = 21$.

— e_3 multiple de 15 et $\equiv 1 \pmod{7}$: $15 \equiv 1 \pmod{7}$, donc $e_3 = 15$.

c) $x = 2e_1 + 3e_2 + 2e_3$ vérifie chaque congruence : modulo 3, seul $2e_1 \equiv 2$ compte, et ainsi de suite.

$$x = 2 \times 70 + 3 \times 21 + 2 \times 15 = 140 + 63 + 30 = 233 \equiv 233 - 210 = 23 \pmod{105}$$

- **Vérification** : $23 = 7 \times 3 + 2 \checkmark$; $23 = 4 \times 5 + 3 \checkmark$; $23 = 3 \times 7 + 2 \checkmark$
 - Les solutions sont les $x = 23 + 105k$.
 - d)** On cherche $23 + 105k \in [1\,000; 1\,100]$: $105k \in [977; 1\,077]$, donc $k = 10$ (1 050).
 - L'armée compte 1 073 soldats. **Contrôle** :
 $1\,073 = 357 \times 3 + 2 = 214 \times 5 + 3 = 153 \times 7 + 2 \checkmark$
 - **Méthode** : les e_i forment une « base » : chaque e_i vaut 1 modulo un des modules et 0 modulo les autres.
- Réponse.** $e_1 = 70$, $e_2 = 21$, $e_3 = 15$; $x \equiv 23 \pmod{105}$; l'armée compte 1 073 soldats.

Correction de l'exercice 5 - Sommes de carrés impossibles

- a)** On calcule les carrés des restes. Modulo 4 : $0, 1, 4 \equiv 0, 9 \equiv 1$. Modulo 8 : $0, 1, 4, 9 \equiv 1, 16 \equiv 0, 25 \equiv 1, 36 \equiv 4, 49 \equiv 1$.
- $$x^2 \equiv 0 \text{ ou } 1 \pmod{4}, \quad x^2 \equiv 0, 1 \text{ ou } 4 \pmod{8}$$
- b)** $a^2 + b^2$ modulo 4 prend les valeurs $0 + 0, 0 + 1, 1 + 1$, soit 0, 1 ou 2 : **jamais** 3.
- **Exemples** : 3, 7, 11, 15 ne sont pas sommes de deux carrés.
- c)** Trois carrés modulo 8 : on additionne trois valeurs parmi $\{0, 1, 4\}$. Sommes possibles : 0, 1, 2, 3, 4, 5, 6 (par exemple $6 = 1 + 1 + 4$) — mais **pas** 7 : il faudrait $4 + 1 + 1 + 1$ ou $4 + 4 - 1$, impossible avec trois termes pris dans $\{0, 1, 4\}$ (le plus proche, $4 + 4 + 4 = 12 \equiv 4$).
- Les plus petits exemples : 7, 15, 23.
 - **Contrôle** pour 7 : les carrés ≤ 7 sont 0, 1, 4, et aucune somme de trois d'entre eux ne fait 7 $\checkmark$
- d)** Modulo 3 : $x^2 - 3y^2 \equiv x^2$. Il faudrait $x^2 \equiv 2 \pmod{3}$, alors qu'un carré vaut 0 ou 1 modulo 3. **Aucune solution.**
- **Méthode** : pour prouver qu'une équation n'a pas de solution entière, on cherche un **module** où elle devient impossible.
- Réponse.** Carrés : $\{0, 1\} \pmod{4}$, $\{0, 1, 4\} \pmod{8}$; $4k + 3$ n'est pas somme de deux carrés ; $8k + 7$ pas de trois carrés (7, 15, 23) ; $x^2 - 3y^2 = 2$ impossible.

Correction de l'exercice 6 - Ordre d'un élément

- a)** Par le théorème d'Euler, $a^{\varphi(n)} \equiv 1$: l'ensemble des $k \geq 1$ tels que $a^k \equiv 1$ est non vide ; il a un plus petit élément.
- b)** Écrivons $m = dq + r$ avec $0 \leq r < d$. Alors $a^m = (a^d)^q a^r \equiv a^r$.
- Si $a^m \equiv 1$, alors $a^r \equiv 1$ avec $0 \leq r < d$: par minimalité de d , $r = 0$, donc $d \mid m$. La réciproque est immédiate.
- $$a^m \equiv 1 \pmod{n} \Leftrightarrow d \mid m$$
- Avec $m = \varphi(n)$ (Euler) : $d \mid \varphi(n)$.
- c)** Modulo 7 ($\varphi(7) = 6$, ordres possibles 1, 2, 3, 6) :
- 1 : ordre 1 ; 2 : $2^3 = 8 \equiv 1$, ordre 3 ; 3 : 3, 2, 6, 4, 5, 1, ordre 6 ;
 - 4 : $4^3 = 64 \equiv 1$ (et $4^2 = 16 \equiv 2$), ordre 3 ; 5 : ordre 6 ; 6 $\equiv -1$: ordre 2.
 - **Générateurs** : 3 et 5 ; leurs puissances parcourent tous les inversibles.
- d)** $10 \equiv 3 \pmod{7}$: l'ordre de 10 est 6.

- La période du développement décimal de $\frac{1}{n}$ (n premier avec 10) est l'ordre de 10 modulo n : ici 6. En effet $\frac{1}{7} = 0,142857 \checkmark$ ($10^6 - 1 = 999\,999 = 7 \times 142\,857$).

Réponse. $a^m \equiv 1 \Leftrightarrow \text{ordre} \mid m$; modulo 7 : ordres 1, 3, 6, 3, 6, 2, générateurs 3 et 5 ; période de $\frac{1}{7}$: 6.

Correction de l'exercice 7 - Racine carrée de -1 modulo p

a) On écrit $(p-1)! = \prod_{k=1}^{(p-1)/2} k \times \prod_{k=1}^{(p-1)/2} (p-k)$ (les facteurs de $\frac{p+1}{2}$ à $p-1$ s'écrivent $p-k$). Or $p-k \equiv -k \pmod{p}$:

$$(p-1)! \equiv \prod_{k=1}^{(p-1)/2} k \times \prod_{k=1}^{(p-1)/2} (-k) = (-1)^{\frac{p-1}{2}} \left(\left(\frac{p-1}{2} \right)! \right)^2 \pmod{p}$$

b) Wilson donne $(p-1)! \equiv -1$. Si $p \equiv 1 \pmod{4}$, $\frac{p-1}{2}$ est **pair** et $(-1)^{(p-1)/2} = 1$:

— $\left(\left(\frac{p-1}{2} \right)! \right)^2 \equiv -1 \pmod{p}$: $x = \left(\frac{p-1}{2} \right)!$ convient.

c) $p = 13$: $x = 6! = 720 = 55 \times 13 + 5$, donc $x \equiv 5$.

— **Vérification** : $5^2 = 25 = 26 - 1 \equiv -1 \pmod{13} \checkmark$ (et $8 \equiv -5$ est l'autre racine).

d) Le sens direct a été vu (exercice « Diviseurs premiers de $n^2 + 1$ », plaquette 3) ; b) donne la réciproque.

— **Conséquence** : un premier $p \equiv 1 \pmod{4}$ divise un nombre de la forme $x^2 + 1$; c'est le point de départ du **théorème des deux carrés** de Fermat ($p = a^2 + b^2$, par exemple $13 = 4 + 9$).

Réponse. $(p-1)! \equiv (-1)^{(p-1)/2} \left(\left(\frac{p-1}{2} \right)! \right)^2$; pour $p = 13$: $6! \equiv 5$ et $5^2 \equiv -1$.

Correction de l'exercice 8 - Chiffrement RSA miniature

a) $\varphi(55) = \varphi(5)\varphi(11) = 4 \times 10 = 40$; $3 \wedge 40 = 1 \checkmark$

b) On cherche d avec $3d \equiv 1 \pmod{40}$: $3 \times 27 = 81 = 2 \times 40 + 1$, donc $d = 27$.

— (Par Euclide : $40 = 13 \times 3 + 1$, donc $1 = 40 - 13 \times 3$ et $d \equiv -13 \equiv 27$.)

c) $7^3 = 343 = 6 \times 55 + 13$: $c = 13$.

d) On calcule $13^{27} \pmod{55}$ par carrés successifs :

— $13^2 = 169 \equiv 4$; $13^4 \equiv 16$; $13^8 \equiv 256 \equiv 36$; $13^{16} \equiv 1\,296 \equiv 31$ ($1\,296 = 23 \times 55 + 31$).

— $27 = 16 + 8 + 2 + 1$: $13^{27} \equiv 31 \times 36 \times 4 \times 13$. On réduit pas à pas :
 $31 \times 36 = 1\,116 \equiv 16$; $16 \times 4 = 64 \equiv 9$; $9 \times 13 = 117 \equiv 7$.

— Alice retrouve $m = 7 \checkmark$

Justification. $ed = 1 + k\varphi(n)$, donc, par Euler ($m \wedge n = 1$) :

$$m^{ed} = m \times \left(m^{\varphi(n)} \right)^k \equiv m \times 1^k = m \pmod{n}$$

— **Sécurité** : connaître d demande $\varphi(n)$, donc la factorisation de n . Avec $n = 55$ c'est trivial ; avec n de 600 chiffres, personne ne sait le faire en temps raisonnable.

Réponse. $\varphi(55) = 40$, $d = 27$, $c = 13$, $13^{27} \equiv 7 \pmod{55}$.

Correction de l'exercice 9 - Critère de divisibilité par 7

a) $-2 \times 10 = -20 = -21 + 1 \equiv 1 \pmod{7}$: -2 est l'**inverse** de 10 modulo 7. Multiplier par un inversible ne change pas la nullité :

$$10a + b \equiv 0 \Leftrightarrow -2(10a + b) \equiv 0 \Leftrightarrow a - 2b \equiv 0 \pmod{7}$$

b) $2\,023 : 202 - 2 \times 3 = 196$, puis $19 - 12 = 7$: divisible par 7 ✓ ($2\,023 = 7 \times 289$).

— $4\,165 : 416 - 10 = 406$, puis $40 - 12 = 28$: divisible ✓ ($4\,165 = 7 \times 595$).

c) On cherche l'inverse de 10 modulo 13 : $4 \times 10 = 40 = 39 + 1 \equiv 1$. Donc

— $10a + b \equiv 0 \Leftrightarrow 4(10a + b) \equiv 0 \Leftrightarrow a + 4b \equiv 0 \pmod{13}$ (car $40a \equiv a$).

— **Test** : $1\,001 : 100 + 4 = 104 = 8 \times 13$ ✓

d) $7 \times 11 = 77$ et $77 \times 13 = 1\,001$ ✓ Donc $1\,000 \equiv -1$ modulo 7, 11 et 13.

— En découpant n en tranches de trois chiffres depuis la droite,

$$n = t_0 + 1\,000t_1 + 1\,000^2t_2 + \dots \equiv t_0 - t_1 + t_2 - \dots$$

— **Exemple** : $123\,456\,789 : 789 - 456 + 123 = 456 = 7 \times 65 + 1$; donc $123\,456\,789$ n'est pas divisible par 7 (reste 1). Modulo 13 : $456 = 35 \times 13 + 1$, reste 1 également.

Réponse. $7 \mid 10a + b \Leftrightarrow 7 \mid a - 2b$; $2\,023$ et $4\,165$ divisibles par 7 ;

$13 \mid 10a + b \Leftrightarrow 13 \mid a + 4b$; tranches de trois chiffres alternées.

Correction de l'exercice 10 - Calendrier perpétuel

a) $365 = 52 \times 7 + 1 \equiv 1 \pmod{7}$ et $366 \equiv 2 \pmod{7}$. Une année plus tard, la même date est décalée de 1 jour de semaine, ou de 2 si l'on a franchi un 29 février.

b) Entre le 28/09/2026 et le 28/09/2030 : 4 ans, dont le passage par le 29/02/2028.

$$4 \times 365 + 1 = 1\,461 = 208 \times 7 + 5 \equiv 5 \pmod{7}$$

— Lundi (0) +5 : **samedi**.

c) Cent ans avec 24 années bissextiles : $100 \times 365 + 24 = 36\,524$ jours.

— $36\,524 = 5\,217 \times 7 + 5$: décalage de 5 jours. Le 28/09/2126 sera un **samedi**.

— (2100 n'est pas bissextile : c'est pourquoi on compte 24 et non 25 années bissextiles.)

d) Sur 400 ans : 97 années bissextiles, soit $400 \times 365 + 97 = 146\,097$ jours, et $146\,097 = 20\,871 \times 7$ exactement.

— Le décalage est **null** : le calendrier grégorien est périodique de 400 ans, jours de la semaine compris.

— **Méthode** : un problème de calendrier est un calcul de **somme modulo 7**.

Réponse. $365 \equiv 1$, $366 \equiv 2 \pmod{7}$; 28/09/2030 : samedi ; 28/09/2126 : samedi ; $146\,097 = 7 \times 20\,871$.

Correction de l'exercice 11 - Suites périodiques modulo m

a) Les $m + 1$ termes $u_0, \dots, u_m$ prennent au plus m valeurs : deux sont égaux, $u_i = u_j$ avec $i < j$ (**principe des tiroirs**). Comme chaque terme ne dépend que du précédent, $u_{i+k} = u_{j+k}$ pour tout k : la suite est périodique à partir du rang i , de période $j - i$.

b) Ici chaque terme dépend des **deux** précédents : on applique le même argument au couple (F_n, F_{n+1}) , qui prend au plus 9 valeurs. De plus on peut **remonter** ($F_n = F_{n+2} - F_{n+1}$), donc la suite est périodique **dès le rang 0**. Calcul :

$$0, 1, 1, 2, 0, 2, 2, 1, \quad 0, 1, 1, 2, \dots$$

— Le couple $(0, 1)$ réapparaît au rang 8 : la période est 8.

c) $2026 = 8 \times 253 + 2$, donc $F_{2026} \equiv F_2 = 1 \pmod{3}$.

d) Dans une période, les termes nuls sont aux rangs 0 et 4 : $3 \mid F_n \Leftrightarrow 4 \mid n$.

— **Contrôle** : $F_4 = 3$, $F_8 = 21$, $F_{12} = 144$ sont multiples de 3 ✓ ; $F_6 = 8$ ne l'est pas ✓

— **Lien** : c'est cohérent avec $\text{pgcd}(F_m, F_n) = F_{\text{pgcd}(m, n)}$ et $F_4 = 3$.

Réponse. Périodicité par les tiroirs ; Fibonacci mod 3 : période 8 ; $F_{2026} \equiv 1 \pmod{3}$; $3 \mid F_n \Leftrightarrow 4 \mid n$.

Correction de l'exercice 12 - Nombres pseudo-premiers

a) $11 \times 31 = 341$ ✓ et $2^{10} = 1024 = 3 \times 341 + 1$ ✓

b) $2^{340} = (2^{10})^{34} \equiv 1^{34} = 1 \pmod{341}$.

— 341 n'est pas premier et pourtant $2^{341-1} \equiv 1$: la **réci-proque** de Fermat est **fausse**. On dit que 341 est **pseudo-premier en base 2** (le plus petit).

c) Modulo 11 : $3^{10} \equiv 1$ et $340 = 34 \times 10$, donc $3^{340} \equiv 1$.

— Modulo 31 : $3^{30} \equiv 1$ et $340 = 11 \times 30 + 10$, donc $3^{340} \equiv 3^{10}$. Or $3^5 = 243 = 7 \times 31 + 26 \equiv -5$, d'où $3^{10} \equiv 25 \pmod{31}$.

— $3^{340} \equiv 25 \not\equiv 1 \pmod{31}$, donc $3^{340} \not\equiv 1 \pmod{341}$ (sinon on aurait $\equiv 1$ modulo 31).

$$3^{340} \not\equiv 1 \pmod{341} \Rightarrow 341 \text{ n'est pas premier}$$

d) Si n est premier, **toutes** les bases a premières avec n vérifient $a^{n-1} \equiv 1$. Trouver une base qui échoue (ici 3) **prouve** que n est composé.

— À l'inverse, réussir le test pour quelques bases ne prouve rien : il existe même des nombres (de **Carmichael**, comme $561 = 3 \times 11 \times 17$) qui passent le test pour toutes les bases premières avec eux.

Réponse. $2^{340} \equiv 1 \pmod{341}$ alors que $341 = 11 \times 31$; $3^{340} \equiv 25 \pmod{31}$, donc $3^{340} \not\equiv 1 \pmod{341}$.

Correction de l'exercice 13 - Diviseurs de zéro dans $\mathbb{Z}/12\mathbb{Z}$

a) $\overline{3} \times \overline{4} = \overline{12} = \overline{0}$, avec $\overline{3} \neq \overline{0}$ et $\overline{4} \neq \overline{0}$: ce sont des **diviseurs de zéro**. L'anneau n'est pas intègre. (Autres exemples : $\overline{2} \times \overline{6}$, $\overline{6} \times \overline{6}$.)

b) $\overline{k}$ est inversible $\Leftrightarrow k \wedge 12 = 1$: $k \in \{1, 5, 7, 11\}$, soit $\varphi(12) = \varphi(4)\varphi(3) = 2 \times 2 = 4$ éléments ✓

— $5 \times 5 = 25 \equiv 1$, $7 \times 7 = 49 \equiv 1$, $11 \times 11 = 121 \equiv 1$: **chaque inversible est son propre inverse**.

c) On teste les 12 classes : $x^2 \equiv 1 \pmod{12}$ pour $x \in \{1, 5, 7, 11\}$, et seulement pour elles (un x tel que $x^2 \equiv 1$ est inversible, d'inverse x).

$$x^2 = \overline{1} \Leftrightarrow x \in \{\overline{1}, \overline{5}, \overline{7}, \overline{11}\}$$

— **Quatre** solutions. Dans un corps, $x^2 - 1 = (x - 1)(x + 1) = 0$ n'a que les deux solutions ± 1 (pas de diviseur de zéro). Ici $(x - 1)(x + 1) = \overline{0}$ peut arriver avec deux facteurs non nuls : $(\overline{5} - \overline{1})(\overline{5} + \overline{1}) = \overline{4} \times \overline{6} = \overline{0}$.

d) Si $n = p$ est premier, tout $k \in \{1, \dots, p - 1\}$ est premier avec p , donc inversible : c'est un corps.

— Si $n = ab$ avec $1 < a, b < n$, alors $\overline{a}\overline{b} = \overline{0}$ avec $\overline{a}, \overline{b} \neq \overline{0}$: $\overline{a}$ n'est pas inversible (sinon $\overline{b} = \overline{a}^{-1}\overline{a}\overline{b} = \overline{0}$). Ce n'est pas un corps.

Réponse. $\overline{3} \times \overline{4} = \overline{0}$; inversibles $\overline{1}, \overline{5}, \overline{7}, \overline{11}$ (involutifs) ; $x^2 = \overline{1}$ a 4 solutions ; corps $\Leftrightarrow n$ premier.

Correction de l'exercice 14 - Cubes modulo 9

a) Il suffit de tester les restes modulo 3 : si $x = 3k + r$, alors

$$x^3 = 27k^3 + 27k^2r + 9kr^2 + r^3 \equiv r^3 \pmod{9}.$$

$$0^3 = 0, \quad 1^3 = 1, \quad 2^3 = 8 \equiv -1 \pmod{9}$$

b) Somme de trois termes pris dans $\{-1, 0, 1\}$: on obtient tous les entiers de -3 à 3 , soit modulo 9 : $0, \pm 1, \pm 2, \pm 3$. Les restes 4 et 5 (c'est-à-dire ± 4) sont **impossibles**.

c) $2\,030 = 225 \times 9 + 5 \equiv 5 \pmod{9}$: pas de solution.

— $2\,026 \equiv 1 \pmod{9}$: l'argument ne dit rien ; la question reste ouverte par cette méthode (elle ne prouve que l'impossibilité).

— **Culture** : la décomposition de 33 et de 42 en sommes de trois cubes n'a été trouvée qu'en 2019, avec des nombres de 16 et 17 chiffres.

d) Trois entiers consécutifs ont les trois restes 0, 1, 2 modulo 3, donc leurs cubes ont les restes 0, 1, -1 modulo 9 (par a)).

— La somme est $\equiv 0 + 1 - 1 = 0 \pmod{9}$ ✓

— **Contrôle** : $n = 1 : 1 + 8 + 27 = 36 = 4 \times 9$ ✓ ; $n = 2 : 8 + 27 + 64 = 99 = 11 \times 9$ ✓

Réponse. Cubes $\equiv 0, \pm 1 \pmod{9}$; $x^3 + y^3 + z^3 \not\equiv \pm 4 \pmod{9}$; $2\,030 \equiv 5$ impossible ;

$$9 \mid n^3 + (n+1)^3 + (n+2)^3.$$

Correction de l'exercice 15 - Synthèse : clé de contrôle ISBN

a) Somme pondérée des douze premiers chiffres 9, 7, 8, 2, 7, 0, 1, 1, 9, 3, 6, 1 avec les poids 1, 3, 1, 3, ... :

— $9 + 21 + 8 + 6 + 7 + 0 + 1 + 3 + 9 + 9 + 6 + 3 = 82$.

— Il faut $82 + a_{13} \equiv 0 \pmod{10}$: $a_{13} = 8$. ISBN complet : 978 2 7011 9361 8.

b) Si le chiffre a_i (de poids $w \in \{1, 3\}$) est remplacé par $a'_i \neq a_i$, la somme change de $w(a'_i - a_i)$. L'erreur passe inaperçue seulement si

$$w(a'_i - a_i) \equiv 0 \pmod{10}$$

— w est **inversible** modulo 10 ($1 \wedge 10 = 3 \wedge 10 = 1$), donc cela impose $a'_i \equiv a_i \pmod{10}$, soit $a'_i = a_i$ (chiffres entre 0 et 9) : contradiction. Toute erreur simple est détectée.

c) Échanger a_i et a_{i+1} (poids 1 et 3 ou 3 et 1) change la somme de $\pm(3-1)(a_{i+1} - a_i) = \pm 2(a_{i+1} - a_i)$.

— Non détecté $\Leftrightarrow 10 \mid 2(a_{i+1} - a_i) \Leftrightarrow 5 \mid a_{i+1} - a_i \Leftrightarrow |a_{i+1} - a_i| = 5$ (chiffres distincts entre 0 et 9).

— **Exemple** non détecté : ...16... $\rightarrow$...61... ($|1 - 6| = 5$).

d) 2 n'est **pas inversible** modulo 10 : une erreur $a_i \rightarrow a_i + 5$ sur un chiffre de poids 2 changerait la somme de $10 \equiv 0$, sans être détectée. Le bon choix d'un poids est un nombre **premier avec le module**.

Réponse. Clé 8 ; erreur simple toujours détectée (poids inversibles) ; transposition non détectée $\Leftrightarrow |a_i - a_{i+1}| = 5$.