1. Congruence modulo n : définition et reste

Ex. 1 ★☆☆ **Restes, y compris d'entiers négatifs**

(a) $158 = 9 \times 17 + 5$ avec $0 \leqslant 5 \leqslant 8$: le reste vaut 5.

(b) $-31 = 8 \times (-4) + 1$ avec $0 \leqslant 1 \leqslant 7$: le reste vaut 1.

(c) $-59 = 9 \times (-7) + 4$ avec $0 \leqslant 4 \leqslant 8$: le reste vaut 4. On a aussi $-59 \equiv -5\ [9]$, mais -5 n'est pas un reste.

(d) $1\,000 = 19 \times 52 + 12$ avec $0 \leqslant 12 \leqslant 18$: le reste vaut 12.

(e) $-7 = 15 \times (-1) + 8$ avec $0 \leqslant 8 \leqslant 14$: le reste vaut 8.

(f) $-86 = 11 \times (-8) + 2$ avec $0 \leqslant 2 \leqslant 10$. L'instruction renvoie donc 2, le reste, même si -86 est négatif.

Ex. 2 ★☆☆ **Congruence vraie ou fausse ?**

(a) $71 - 8 = 63 = 9 \times 7$: 9 divise la différence, donc la congruence est vraie.

(b) $101 - 1 = 100 = 10 \times 10$: la congruence est vraie. Peu importe que $101 \neq 1 + 10$: il suffit d'avoir $a = b + kn$ avec k entier.

(c) $62 - 7 = 55$ et $54 < 55 < 60$, deux multiples consécutifs de 6 : 6 ne divise pas 55, donc la congruence est fausse.

(d) $-19 - 9 = -28 = 7 \times (-4)$: la congruence est vraie.

(e) $-40 - (-4) = -36 = 12 \times (-3)$: la congruence est vraie.

(f) $-11 - 11 = -22$ et $-24 < -22 < -20$, deux multiples consécutifs de 4 : 4 ne divise pas -22, donc la congruence est fausse.

Ex. 3 ★★☆ **Les erreurs de Maëlle**

(a) $77 - 22 = 55 = 5 \times 11$, donc la congruence est vraie. Mais un reste par 5 est compris entre 0 et 4 : $77 = 5 \times 15 + 2$. Le reste vaut donc 2, pas 22.

(b) Un reste n'est jamais négatif. On écrit $-38 = 6 \times (-7) + 4$ avec $0 \leqslant 4 \leqslant 5$, donc le reste vaut 4. On peut écrire $-38 \equiv -2\ [6]$, mais -2 n'est pas le reste.

(c) La définition demande $a - b = kn$ avec k entier quelconque, pas seulement $k = 1$. Or $125 - 5 = 120 = 8 \times 15$, donc $125 \equiv 5\ [8]$ est vraie.

(d) Le module doit vérifier $n \geqslant 2$. Modulo 1, tous les entiers seraient congrus entre eux : cela ne donne aucune information. On ne travaille donc jamais modulo 1.

Ex. 3 (suite)

(e) Une congruence n'est pas une égalité : $x \equiv 3\ [4]$ veut dire $x = 3 + 4k$ avec $k \in \mathbb{Z}$. Par exemple $x = 7$ ($7 - 3 = 4$) ou $x = -1$ ($-1 - 3 = -4$). Donc x n'est pas forcément égal à 3.

Ex. 4 ★★☆ **Vrai ou faux pour tout entier**

(a) Vrai. $10 \mid a - 7$ et $5 \mid 10$, donc $5 \mid a - 7$, c'est-à-dire $a \equiv 7\ [5]$. Comme $7 - 2 = 5$, on a $7 \equiv 2\ [5]$. Par transitivité, $a \equiv 2\ [5]$.

(b) Faux. Contre-exemple : $a = 2$ vérifie $2 \equiv 2\ [5]$, mais $2 - 7 = -5$ n'est pas un multiple de 10. Donc $2 \not\equiv 7\ [10]$ et l'affirmation est fausse.

(c) Vrai. Si $a = 2k + 1$ avec $k \in \mathbb{Z}$, alors $a - (-1) = 2k + 2 = 2(k + 1)$, donc $a \equiv -1\ [2]$. Réciproquement, si $a + 1 = 2m$ avec $m \in \mathbb{Z}$, alors $a = 2(m - 1) + 1$ est impair. L'équivalence est démontrée.

(d) Vrai. $(5n + 15) - (n + 3) = 4n + 12 = 4(n + 3)$ et $n + 3$ est un entier. Donc 4 divise la différence : pour tout entier naturel n, $5n + 15 \equiv n + 3\ [4]$.

Ex. 5 ★★☆ **Les vendredis de Yanis**

(a) Les vendredis reviennent tous les 7 jours à partir du jour 1. Le jour j est donc un vendredi si et seulement si $j - 1$ est un multiple de 7, c'est-à-dire $7 \mid j - 1$, soit $j \equiv 1\ [7]$.

(b) $195 - 1 = 194 = 7 \times 27 + 5$: le jour 195 tombe 5 jours après un vendredi (samedi, dimanche, lundi, mardi, mercredi). Le 14 juillet 2027 est donc un mercredi.

(c) On a $j = 1 + 7k$ avec $k \in \mathbb{Z}$. Alors $200 \leqslant 1 + 7k \leqslant 230 \iff \frac{199}{7} \leqslant k \leqslant \frac{229}{7}$, donc $k \in \{29\,;30\,;31\,;32\}$. Les vendredis cherchés sont les jours 204, 211, 218 et 225.

(d) $1 \leqslant 1 + 7k \leqslant 365 \iff 0 \leqslant k \leqslant 52$, car $1 + 7 \times 52 = 365$. Il y a 53 valeurs de k : l'année 2027 compte donc 53 vendredis.

Ex. 6 ★★★ **Tous les entiers congrus à 13 modulo 17**

(a) 13 lui-même convient : $13 - 13 = 0 = 17 \times 0$, donc $13 \equiv 13\ [17]$, mais $13 \neq 13 + 17$. Par définition, $x \equiv 13\ [17]$ signifie que $17 \mid x - 13$, c'est-à-dire qu'il existe un entier relatif k tel que $x = 13 + 17k$. Le cas $k = 1$ n'est que l'un d'eux.

Ex. 6 **(suite)**

(b) On a $x \equiv 13\ [17]$ si et seulement si $x = 13 + 17k$ avec $k \in \mathbb{Z}$. On veut $-60 \leqslant 13 + 17k \leqslant 60$, soit $-73 \leqslant 17k \leqslant 47$. Comme $17 \times (-5) = -85$, $17 \times (-4) = -68$, $17 \times 2 = 34$ et $17 \times 3 = 51$, on obtient $-4 \leqslant k \leqslant 2$. Les entiers cherchés sont donc -55, -38, -21, -4, 13, 30 et 47.

(c) On veut $-1\,000 \leqslant 13 + 17k \leqslant 1\,000$, soit $-1\,013 \leqslant 17k \leqslant 987$. On a $17 \times (-60) = -1\,020$, $17 \times (-59) = -1\,003$, $17 \times 58 = 986$ et $17 \times 59 = 1\,003$, donc $-59 \leqslant k \leqslant 58$. Cela fait $58 - (-59) + 1 = 118$ valeurs de k, et chacune donne un x différent. Il y a donc 118 entiers.

(d) « x est impair » se traduit par $x \equiv 1\ [2]$. Sens direct : on a $x - 13 = 17k$ avec $k \in \mathbb{Z}$. Comme $x \equiv 1\ [2]$ et $13 \equiv 1\ [2]$, on a $x - 13 \equiv 0\ [2]$, donc $2 \mid 17k$. Comme 2 et 17 sont premiers entre eux, le théorème de Gauss donne $2 \mid k$. On écrit $k = 2k'$, d'où $x - 13 = 34k'$ et $x \equiv 13\ [34]$. Réciproque : si $x = 13 + 34k$, alors $x - 13 = 17 \times (2k)$, donc $x \equiv 13\ [17]$. De plus, $x = 2(17k + 6) + 1$ est impair. L'équivalence est démontrée.

(e) D'après la question précédente, on compte les entiers $x = 13 + 34k$ de l'intervalle. On veut $-1\,013 \leqslant 34k \leqslant 987$. On a $34 \times (-30) = -1\,020$, $34 \times (-29) = -986$, $34 \times 29 = 986$ et $34 \times 30 = 1\,020$, donc $-29 \leqslant k \leqslant 29$. Il y a donc 59 entiers impairs de ce type.

Ex. 7 ★★★ **Opposés et restes**

(a) On écrit la division euclidienne $a = nq + r$. Alors $-a = -nq - r = n(-q - 1) + (n - r)$. Comme $1 \leqslant r \leqslant n - 1$, on a $1 \leqslant n - r \leqslant n - 1$, donc $0 \leqslant n - r \leqslant n - 1$. Par unicité de la division euclidienne, le reste de $-a$ est $n - r$. Si $r = 0$, alors $-a = n \times (-q)$ et le reste de $-a$ vaut 0.

(b) On a $2\,027 = 13 \times 155 + 12$, donc $2\,027 \equiv 12\ [13]$ et $-2\,027 \equiv -12\ [13]$. La congruence est donc juste. Mais -12 n'est pas un reste, car un reste est compris entre 0 et 12. Comme $12 \neq 0$, la question précédente donne un reste égal à $13 - 12 = 1$. Vérification : $-2\,027 = 13 \times (-156) + 1$.

(c) $21 \equiv -21\ [n]$ équivaut à $n \mid 21 - (-21)$, c'est-à-dire $n \mid 42$. Les diviseurs de 42 supérieurs ou égaux à 2 sont 2, 3, 6, 7, 14, 21 et 42. Ce sont donc les valeurs de n cherchées.

Ex. 7 **(suite)**

(d) Si $a \equiv -a\ [n]$, alors $n \mid a - (-a) = 2a$. Comme n est impair, n et 2 sont premiers entre eux. Le théorème de Gauss donne alors $n \mid a$, c'est-à-dire $a \equiv 0\ [n]$. Pour n pair, c'est faux. Contre-exemple : $n = 6$ et $a = 3$. On a $3 - (-3) = 6$, donc $3 \equiv -3\ [6]$, mais le reste de 3 par 6 vaut 3, donc $3 \not\equiv 0\ [6]$.

Ex. 8 ★★★ **Le pion de Sacha**

(a) On a $125 = 12 \times 10 + 5$ avec $0 \leqslant 5 \leqslant 11$: le pion est sur la case 5. On a $-50 = 12 \times (-5) + 10$ avec $0 \leqslant 10 \leqslant 11$: le pion est sur la case 10. Ce n'est pas la case -2, même si $-50 \equiv -2\ [12]$ est vraie, car un reste est compris entre 0 et 11.

(b) `case(125)` renvoie 113 et `case(-50)` renvoie -38. La fonction ajoute ou retire 12 une seule fois. Le nombre obtenu reste congru à s modulo 12, mais il n'est pas forcément compris entre 0 et 11. Ce n'est donc pas toujours le reste.

(c) Il faut répéter l'opération tant que le nombre n'est pas compris entre 0 et 11 :

```
def case(s):
    while s >= 12:
        s = s - 12
    while s < 0:
        s = s + 12
    return s
```

On obtient alors `case(125)` $= 5$ et `case(-50)` $= 10$.

(d) On a $s \equiv r\ [12]$. Comme 3 divise 12, on en déduit $s \equiv r\ [3]$. Si le pion est sur une case rouge, alors $r \in \{0; 3; 6; 9\}$, donc $r \equiv 0\ [3]$ et, par transitivité, $s \equiv 0\ [3]$. Réciproquement, si $s \equiv 0\ [3]$, alors $r \equiv s \equiv 0\ [3]$: r est un multiple de 3 compris entre 0 et 11, donc $r \in \{0; 3; 6; 9\}$. Le pion est donc sur une case rouge.

(e) On a $s \equiv r\ [12]$ et 2 divise 12, donc $s \equiv r\ [2]$. Comme s est impair, $s \equiv 1\ [2]$, donc $r \equiv 1\ [2]$: le numéro r de la case est impair. Or $4 \equiv 0\ [2]$. Le pion ne peut donc pas être sur la case 4.

2. *Compatibilité avec l'addition et la multiplication*

Ex. 9 ★☆☆ **Des représentants commodes**

(a) $199 \equiv -1 \pmod{10}$ et $98 \equiv -2 \pmod{10}$, donc $199 \times 98 \equiv (-1) \times (-2) = 2 \pmod{10}$. Le reste vaut 2.

(b) $49 \equiv -1 \pmod{50}$, donc $49^3 \equiv (-1)^3 = -1 \equiv 49 \pmod{50}$. Le reste vaut 49.

Ex. 9 **(suite)**

(c) $59 \equiv -1 \pmod{60}$ et $61 \equiv 1 \pmod{60}$, donc $59 \times 61 \equiv -1 \equiv 59 \pmod{60}$. Le reste vaut 59.

(d) $-17 = 6 \times (-3) + 1$, donc $-17 \equiv 1 \pmod{6}$. De plus $23 \equiv -1 \pmod{6}$. Ainsi $(-17) \times 23 \equiv -1 \equiv 5 \pmod{6}$. Le reste vaut 5.

(e) $13 \equiv -2 \pmod{15}$, donc $13^4 \equiv (-2)^4 = 16 \equiv 1 \pmod{15}$. Le reste vaut 1.

(f) $2025 \equiv 1 \pmod{4}$ et $2023 \equiv -1 \pmod{4}$, donc $2025^2 - 2023^2 \equiv 1 - (-1)^2 = 0 \pmod{4}$. Le reste vaut 0.

Ex. 10 ★☆☆ **Le reste d'une expression en a**

(a) $3a + 7 \equiv 3 \times 5 + 7 = 22 \equiv 0 \pmod{11}$. Le reste vaut 0.

(b) $a^2 \equiv 25 = 2 \times 11 + 3 \pmod{11}$, donc $a^2 \equiv 3 \pmod{11}$. Le reste vaut 3.

(c) $a^2 - 2a + 6 \equiv 25 - 10 + 6 = 21 \equiv 10 \pmod{11}$. Le reste vaut 10.

(d) $a^3 = a^2 \times a \equiv 3 \times 5 = 15 \equiv 4 \pmod{11}$. Le reste vaut 4.

(e) $2a^3 + a \equiv 2 \times 4 + 5 = 13 \equiv 2 \pmod{11}$. Le reste vaut 2.

(f) $a^4 = a^3 \times a \equiv 4 \times 5 = 20 \equiv 9 \pmod{11}$, donc $a^4 + 10 \equiv 19 \equiv 8 \pmod{11}$. Le reste vaut 8.

Ex. 11 ★★☆ **Un produit nul sans facteur nul**

(a) Pour $x = 5$: $6 \times 5 = 30 = 3 \times 8 + 6$, donc $6 \times 5 \equiv 6 \pmod{8}$. Ligne complète, pour x allant de 0 à 7 : 0, 6, 4, 2, 0, 6, 4, 2.

(b) Pour $x = 4$: $6 \times 4 = 24 = 3 \times 8$, donc $6 \times 4 \equiv 0 \pmod{8}$. Pourtant, ni 6 ni 4 n'est divisible par 8. Modulo 8, un produit peut donc être nul sans qu'aucun de ses facteurs ne le soit.

(c) Dans le tableau, $6x \equiv 2 \pmod{8}$ pour $x = 3$ et $x = 7$. Tout entier x est congru modulo 8 à un entier de 0 à 7. D'après la compatibilité avec la multiplication, $6x$ a alors le même reste que $6r$, où r est le reste de x. Les solutions sont donc les entiers $x \equiv 3 \pmod{8}$ ou $x \equiv 7 \pmod{8}$, c'est-à-dire $x = 3 + 4k$ avec $k \in \mathbb{Z}$.

(d) Tout entier x est congru modulo 8 à un entier de 0 à 7. Par compatibilité, $6x$ est donc congru à 0, 2, 4 ou 6 modulo 8, jamais à 5. L'équation $6x \equiv 5 \pmod{8}$ n'a donc pas de solution dans $\mathbb{Z}$.

Ex. 12 ★★☆ **Deux copies à corriger**

(a) $2^2 = 4 \equiv -1 \pmod{5}$. Comme $11 = 2 \times 5 + 1$, la compatibilité avec les puissances et la multiplication donne $2^{11} = (2^2)^5 \times 2 \equiv (-1)^5 \times 2 = -2 \equiv 3 \pmod{5}$. Le reste vaut 3 et non 2 : Inès a tort.

(b) Inès a remplacé l'exposant 11 par son reste modulo 5. La compatibilité permet seulement de remplacer la base : si $a \equiv b \pmod{n}$, alors $a^m \equiv b^m \pmod{n}$, avec le même exposant m. On ne réduit jamais un exposant modulo n.

(c) Pour $x = 2$: $28 - 4 \times 2 = 20 = 2 \times 10$, donc $4 \times 2 \equiv 28 \pmod{10}$. Pourtant $2 \not\equiv 7 \pmod{10}$. Malo a tort : il a « divisé par 4 », ce qui est interdit pour une congruence.

(d) $4x \equiv 28 \pmod{10}$ équivaut à : il existe $k \in \mathbb{Z}$ tel que $4(x - 7) = 10k$, c'est-à-dire $2(x - 7) = 5k$. Donc $5 \mid 2(x - 7)$. Comme $\text{PGCD}(2; 5) = 1$, le théorème de Gauss donne $5 \mid x - 7$. Réciproquement, si $x = 7 + 5k$, alors $4x - 28 = 20k$, qui est divisible par 10. Les solutions sont donc les entiers $x = 7 + 5k$, avec $k \in \mathbb{Z}$.

Ex. 13 ★★☆ **Une divisibilité pour tout n**

(a) $9 = 7 + 2$, donc $9 \equiv 2 \pmod{7}$. Par compatibilité avec les puissances, pour tout entier naturel n, $9^n \equiv 2^n \pmod{7}$.

(b) $3^{2n+1} = 3 \times (3^2)^n = 3 \times 9^n$ et $2^{n+2} = 4 \times 2^n$. D'après la question précédente et la compatibilité avec la multiplication et l'addition, $3^{2n+1} + 2^{n+2} \equiv 3 \times 2^n + 4 \times 2^n = 7 \times 2^n \equiv 0 \pmod{7}$. Donc, pour tout entier naturel n, 7 divise $3^{2n+1} + 2^{n+2}$.

(c) Faux. Pour $n = 0$: $3^1 + 2^2 = 7$, qui n'est pas divisible par 14. De façon générale, 3^{2n+1} est impair et 2^{n+2} est pair : la somme est impaire, donc jamais divisible par 14.

Ex. 14 ★★★ **Les deux derniers chiffres**

(a) $99 \equiv -1 \pmod{100}$. Par compatibilité avec les puissances, $99^{2027} \equiv (-1)^{2027} = -1 \pmod{100}$. Or $-1 \equiv 99 \pmod{100}$. Le reste de 99^{2027} modulo 100 est donc 99.

(b) $49^2 = 2\,401 \equiv 1 \pmod{100}$. Comme $2027 = 2 \times 1013 + 1$, on a $49^{2027} = (49^2)^{1013} \times 49 \equiv 1^{1013} \times 49 = 49 \pmod{100}$. Le reste vaut 49.

(c) Par compatibilité avec l'addition, $N \equiv 99 + 49 + 52 = 200 \equiv 0 \pmod{100}$. Les deux derniers chiffres de N sont donc 00.

Ex. 14 **(suite)**

(d) Soit n un entier naturel. On a $99^{2n} = (99^2)^n$ et $99^2 \equiv (-1)^2 = 1 \pmod{100}$, donc $99^{2n} \equiv 1 \pmod{100}$. De même, $49^{2n} = (49^2)^n \equiv 1^n = 1 \pmod{100}$. Ainsi $99^{2n} + 49^{2n} - 2 \equiv 1 + 1 - 2 = 0 \pmod{100}$. Pour tout entier naturel n, 100 divise donc $99^{2n} + 49^{2n} - 2$.

(e) $99^n \times 49^n \equiv (-1)^n \times 49^n \pmod{100}$. Si $n = 2k$ est pair, on obtient $1 \times (49^2)^k \equiv 1 \pmod{100}$: le nombre se termine par 01. Si $n = 2k + 1$ est impair, on obtient $-1 \times (49^2)^k \times 49 \equiv -49 \equiv 51 \pmod{100}$: il se termine par 51.

Ex. 15 ★★★ **Un vendredi et des puissances de 3**

(a) $365 = 7 \times 52 + 1$ et $366 = 7 \times 52 + 2$, donc $365 \equiv 1$ et $366 \equiv 2 \pmod 7$. Du 1er janvier 2027 au 1er janvier 2031, il s'écoule $3 \times 365 + 366$ jours, et $3 \times 365 + 366 \equiv 3 \times 1 + 2 = 5 \pmod 7$. Cinq jours après un vendredi, on est un mercredi. Le 1er janvier 2031 est donc un mercredi.

(b) $1\,000 = 7 \times 142 + 6$, donc $1\,000 \equiv 6 \pmod 7$. Six jours après un vendredi, on est un jeudi.

(c) $3^3 = 27 = 28 - 1$, donc $3^3 \equiv -1 \pmod 7$. Comme $100 = 3 \times 33 + 1$, on a $3^{100} = (3^3)^{33} \times 3 \equiv (-1)^{33} \times 3 = -3 \pmod 7$. Or $-3 \equiv 4 \pmod 7$, donc le reste de 3^{100} modulo 7 est 4. Quatre jours après un vendredi, on est un mardi.

(d) Yanis a tort. La compatibilité permet de réduire la base, pas l'exposant : $100 \equiv 2 \pmod 7$ n'entraîne pas $3^{100} \equiv 3^2 \pmod 7$. D'ailleurs $3^2 \equiv 2 \pmod 7$, alors que $3^{100} \equiv 4 \pmod 7$.

(e) $10 \equiv 3 \pmod 7$, donc $10^6 \equiv 3^6 = (3^3)^2 \equiv (-1)^2 = 1 \pmod 7$. Pour tout entier naturel n, $10^{6n} = (10^6)^n \equiv 1^n = 1 \pmod 7$. On est donc toujours un samedi.

Ex. 16 ★★★ **Quand 12 divise-t-il un produit ?**

(a) $(n+2)(n+3) = n^2 + 3n + 2n + 6 = n^2 + 5n + 6 = A_n$. Si $n \equiv 7 \pmod{12}$, alors $n \equiv -5 \pmod{12}$. Par compatibilité, $A_n \equiv (-5+2)(-5+3) = (-3) \times (-2) = 6 \pmod{12}$. Le reste de A_n modulo 12 est 6.

(b) Si $n \equiv 0 \pmod 2$, alors $n + 2 \equiv 0 \pmod 2$. Si $n \equiv 1 \pmod 2$, alors $n + 3 \equiv 0 \pmod 2$. Dans les deux cas, par compatibilité avec la multiplication, $A_n = (n+2)(n+3) \equiv 0 \pmod 2$. Pour tout entier naturel n, A_n est donc pair.

Ex. 16 **(suite)**

(c) Si $n \equiv r \pmod{12}$, la compatibilité donne $A_n \equiv r^2 + 5r + 6 \pmod{12}$.
Donc $12 \mid A_n$ si et seulement si $12 \mid A_r$, et tester r de 0 à 11 suffit. Les restes de A_r modulo 12 pour $r = 0, 1, \ldots, 11$ sont : $6, 0, 8, 6, 6, 8, 0, 6, 2, 0, 0, 2$. Le programme affiche donc $[1, 6, 9, 10]$.

(d) C'est faux. Contre-exemple : $n = 1$. On a $A_1 = 12 \equiv 0 \pmod{12}$ et $n + 3 = 4 \not\equiv 0 \pmod{12}$. Pourtant $n + 2 = 3 \not\equiv 0 \pmod{12}$. Gabin « simplifie » par $n + 3$ comme dans une égalité, mais on ne divise pas une congruence.

(e) D'après le résultat du programme et la compatibilité, 12 divise A_n si et seulement si $n \equiv 1, 6, 9$ ou $10 \pmod{12}$. Entre 20 et 35, ce sont les entiers 21, 22, 25, 30, 33 et 34.

3. *Restes des puissances : cycles*

Ex. 17 ★☆☆ **Restes de grandes puissances**

(a) $4^1 \equiv 4$, $4^2 = 16 \equiv 2$, $4^3 \equiv 2 \times 4 = 8 \equiv 1 \pmod 7$: le cycle a pour longueur 3. $2\,018 = 3 \times 672 + 2$, donc $4^{2018} = (4^3)^{672} \times 4^2 \equiv 1 \times 16 \equiv 2 \pmod 7$. Le reste vaut 2.

(b) $5^2 = 25 \equiv -1 \pmod{13}$, donc $5^4 \equiv (-1)^2 = 1 \pmod{13}$. $1\,000 = 4 \times 250 + 0$, donc $5^{1000} = (5^4)^{250} \equiv 1^{250} = 1 \pmod{13}$. Le reste vaut 1.

(c) $17 \equiv 2 \pmod 5$, donc $17^{43} \equiv 2^{43} \pmod 5$. $2^4 = 16 \equiv 1 \pmod 5$ et $43 = 4 \times 10 + 3$, donc $2^{43} \equiv 2^3 = 8 \equiv 3 \pmod 5$. Le reste vaut 3.

(d) $4 \equiv -1 \pmod 5$, donc $4^{131} \equiv (-1)^{131} = -1 \equiv 4 \pmod 5$, car 131 est impair. Le reste vaut 4.

(e) $10 \equiv -1 \pmod{11}$, donc $10^{2025} \equiv (-1)^{2025} = -1 \equiv 10 \pmod{11}$, car 2 025 est impair. Le reste vaut 10.

Ex. 18 ★☆☆ **Derniers chiffres**

(a) Modulo 10 : $7^1 \equiv 7$, $7^2 \equiv 9$, $7^3 \equiv 3$, $7^4 \equiv 1$.
$1\,001 = 4 \times 250 + 1$, donc $7^{1001} \equiv 7^1 = 7 \pmod{10}$: il se termine par 7.

(b) $13 \equiv 3 \pmod{10}$ et $3^4 = 81 \equiv 1 \pmod{10}$.
$2\,028 = 4 \times 507 + 0$, donc $13^{2028} \equiv (3^4)^{507} \equiv 1 \pmod{10}$: il se termine par 1.

(c) $9 \equiv -1 \pmod{10}$ et 2 027 est impair, donc $9^{2027} \equiv -1 \equiv 9 \pmod{10}$: il se termine par 9.

Ex. 18 **(suite)**

(d) $7^4 = 2\,401 \equiv 1 \pmod{100}$ et $82 = 4 \times 20 + 2$, donc $7^{82} \equiv 7^2 = 49 \pmod{100}$: ses deux derniers chiffres sont 49.

(e) $51^2 = 2\,601 \equiv 1 \pmod{100}$ et $37 = 2 \times 18 + 1$, donc $51^{37} \equiv 51 \pmod{100}$: ses deux derniers chiffres sont 51.

Ex. 19 ★★☆ **Trois copies à corriger**

(a) Léa confond le reste de l'exposant et le reste de la puissance. Le reste nul signifie seulement que 2 032 est un multiple de 4.
Donc $3^{2032} = (3^4)^{508} \equiv 1^{508} = 1 \pmod{16}$. D'ailleurs, 3^{2032} est impair, donc il ne peut pas être divisible par 16. Le reste de 3^{2032} dans la division par 16 vaut 1.

(b) On ne réduit jamais l'exposant modulo 7. Modulo 7, les puissances de 5 valent $5, 4, 6, 2, 3, 1$: le cycle a pour longueur 6. $23 = 6 \times 3 + 5$, donc $5^{23} \equiv 5^5 \equiv 3 \pmod{7}$. Le reste vaut 3.

(c) $15 = 3 \times 5$ n'est pas premier : on ne peut pas appliquer le petit théorème de Fermat. Or $2^4 = 16 \equiv 1 \pmod{15}$ et $2\,030 = 4 \times 507 + 2$, donc $2^{2030} \equiv 2^2 = 4 \pmod{15}$. Le reste vaut 4.

Ex. 20 ★★☆ **Une divisibilité pour tout entier**

(a) $3^{2n} = (3^2)^n = 9^n$ et $9 \equiv 2 \pmod{7}$. Par compatibilité avec les puissances, $9^n \equiv 2^n \pmod{7}$, donc $3^{2n} - 2^n \equiv 0 \pmod{7}$. Pour tout entier naturel n, 7 divise $3^{2n} - 2^n$.

(b) $2^1 \equiv 2$, $2^2 \equiv 4$, $2^3 = 8 \equiv 1 \pmod{7}$: le cycle a pour longueur 3. Si $n = 3q + r$, alors $2^n = (2^3)^q \times 2^r \equiv 2^r \pmod{7}$. Le reste de 2^n vaut 1 si $r = 0$, 2 si $r = 1$ et 4 si $r = 2$.

(c) $3^{2026} = 3^{2 \times 1013} \equiv 2^{1013} \pmod{7}$ d'après la question 1. $1\,013 = 3 \times 337 + 2$, donc $2^{1013} \equiv 4 \pmod{7}$. Le reste de 3^{2026} dans la division par 7 vaut 4.

(d) Écrivons $n = 3q + r$, avec $r \in \{0; 1; 2\}$. D'après la question 1, $3^{2n} + 2^n + 3 \equiv 2 \times 2^n + 3 \pmod{7}$, et d'après la question 2, $2^n \equiv 2^r \pmod{7}$. Si $r = 0$: $2 + 3 = 5$; si $r = 1$: $4 + 3 = 7 \equiv 0$; si $r = 2$: $8 + 3 = 11 \equiv 4$.
Donc 7 divise $3^{2n} + 2^n + 3$ si et seulement si $n = 3q + 1$, avec $q \in \mathbb{N}$.

Ex. 21 ★★☆ **Une fonction qui cherche le cycle**

(a) Modulo 11 : $3^1 \equiv 3$, $3^2 \equiv 9$, $3^3 = 27 \equiv 5$, $3^4 \equiv 15 \equiv 4$, $3^5 \equiv 12 \equiv 1$. La boucle s'arrête quand `m` vaut 5 : la fonction renvoie 5, la longueur du cycle.

(b) $3^5 \equiv 1 \pmod{11}$ et $2\,033 = 5 \times 406 + 3$, donc $3^{2033} = (3^5)^{406} \times 3^3 \equiv 27 \equiv 5 \pmod{11}$. Le reste vaut 5.

(c) $12 = 11 + 1$, donc `r` vaut 1 dès le départ : la boucle n'est jamais exécutée et `cycle(12, 11)` renvoie 1. En effet, $12^1 \equiv 1 \pmod{11}$. Ensuite, $14 \equiv 3 \pmod{11}$, donc $14^m \equiv 3^m \pmod{11}$ pour tout entier $m \geqslant 1$. Les restes successifs sont ceux de la question 1, $3, 9, 5, 4, 1$, donc `cycle(14, 11)` renvoie 5.

Ex. 22 ★★★ **Puissances de 2 : un cycle qui démarre en retard**

(a) On multiplie chaque reste par 2 puis on réduit modulo 40 :

m	**1**	**2**	**3**	**4**
$2^m \pmod{40}$	2	4	8	16

m	**5**	**6**	**7**	**8**
$2^m \pmod{40}$	32	24	8	16

Si $2^m \equiv 1 \pmod{40}$, alors 40 divise $2^m - 1$. Or $2^m - 1$ est impair (pour $m \geqslant 1$) et 40 est pair : c'est impossible. Aucune puissance 2^m avec $m \geqslant 1$ n'est donc congrue à 1 modulo 40.

(b) Soit $m \geqslant 3$. $2^{m+4} - 2^m = 2^m \times (16 - 1) = 15 \times 2^m = 15 \times 8 \times 2^{m-3} = 40 \times 3 \times 2^{m-3}$. Comme $m - 3 \geqslant 0$, $3 \times 2^{m-3}$ est un entier, donc 40 divise $2^{m+4} - 2^m$. Ainsi, pour tout entier $m \geqslant 3$, $2^{m+4} \equiv 2^m \pmod{40}$.

(c) $2026 = 4 \times 505 + 6$ avec $6 \geqslant 3$. En appliquant 505 fois la question 2 : $2^{2026} \equiv 2^{2022} \equiv \cdots \equiv 2^6 = 64 \equiv 24 \pmod{40}$. Le reste de 2^{2026} dans la division par 40 est 24.

(d) Élodie fait comme si $2^4 \equiv 1 \pmod{40}$, alors que $2^4 = 16$. Le cycle de longueur 4 ne commence qu'au rang 3, donc on ne peut pas descendre jusqu'à l'exposant 0. On écrit $2024 = 4 \times 505 + 4$ avec $4 \geqslant 3$: la question 2 donne $2^{2024} \equiv 2^4 = 16 \pmod{40}$. Le reste vaut 16.

(e) D'après la question 3, $2^{2026} = 40q + 24$ avec q entier, donc $2^{2026} = 10(4q + 2) + 4$ avec $0 \leqslant 4 < 10$. Le reste modulo 10 vaut 4 : 2^{2026} se termine par 4.

Ex. 23 ★★★ **Modulo 11 : le signe moins et le théorème de Fermat**

(a) $32 = 3 \times 11 - 1$ et $54 = 5 \times 11 - 1$, donc $32 \equiv -1$ et $54 \equiv -1 \pmod{11}$. Par compatibilité avec les puissances, $32^{2027} \equiv (-1)^{2027} = -1$ car 2 027 est impair, et $54^{2026} \equiv (-1)^{2026} = 1$ car 2 026 est pair. Par compatibilité avec l'addition, $32^{2027} + 54^{2026} \equiv -1 + 1 = 0 \pmod{11}$. Le reste vaut 0.

(b) Le théorème exige que p ne divise pas a. Or $33 = 3 \times 11$: 11 divise 33, donc le théorème ne s'applique pas. On a $33 \equiv 0 \pmod{11}$, donc $33^{10} \equiv 0^{10} = 0 \pmod{11}$. Le reste de 33^{10} dans la division par 11 est 0.

(c) $13 \equiv 2 \pmod{11}$, donc $13^{2040} \equiv 2^{2040} \pmod{11}$. 11 est premier et ne divise pas 2, donc le petit théorème de Fermat donne $2^{10} \equiv 1 \pmod{11}$. Or $2\,040 = 10 \times 204 + 0$, donc $2^{2040} = (2^{10})^{204} \equiv 1^{204} = 1 \pmod{11}$. Le reste vaut 1.

(d) Restes de 2^r modulo 11 pour $r = 0, 1, \ldots, 9$: $1, 2, 4, 8, 5, 10, 9, 7, 3, 6$. Comme $2^{10} \equiv 1 \pmod{11}$ (question 3), si $n = 10q + r$ avec $0 \leqslant r \leqslant 9$, alors $2^n = (2^{10})^q \times 2^r \equiv 2^r \pmod{11}$. Or $11 \mid 2^n + 1 \iff 2^n \equiv -1 \equiv 10 \pmod{11} \iff 2^r \equiv 10 \pmod{11} \iff r = 5$. Les entiers cherchés sont les $n = 10k + 5$, avec $k \in \mathbb{N}$.

Ex. 24 ★★★ **Un programme, un calendrier et une boucle sans fin**

(a) Les restes successifs de 5^m modulo 7 : 5, puis $5 \times 5 = 25 \equiv 4$, $4 \times 5 = 20 \equiv 6$, $6 \times 5 = 30 \equiv 2$, $2 \times 5 = 10 \equiv 3$, $3 \times 5 = 15 \equiv 1$. La boucle s'arrête quand on obtient 1, qui est ajouté en dernier. La fonction renvoie `[5, 4, 6, 2, 3, 1]`.

(b) Les jours reviennent tous les 7 jours : il faut le reste de 5^{2027} modulo 7. D'après la question 1, $5^6 \equiv 1 \pmod{7}$ (première puissance égale à 1). $2027 = 6 \times 337 + 5$, donc $5^{2027} = (5^6)^{337} \times 5^5 \equiv 5^5 \equiv 3 \pmod{7}$. Dans 5^{2027} jours, on sera trois jours après mercredi : un samedi.

(c) Pour $m \geqslant 1$, 4^m est pair. Si $4^m = 10q + r$, alors $r = 4^m - 10q$ est pair, donc $r \neq 1$. La condition `r != 1` reste toujours vraie : la boucle ne s'arrête jamais. C'est le cas où 4 et 10 ont le diviseur commun 2.

(d) $r = 4$ n'est pas dans la liste vide : la liste devient `[4]` et $r = 16\%10 = 6$. 6 n'est pas dans la liste : la liste devient `[4, 6]` et $r = 24\%10 = 4$. 4 est déjà dans la liste, donc la boucle s'arrête. La fonction renvoie `[4, 6]`.

Ex. 24 **(suite)**

(e) D'après la question 4, $4^3 \equiv 4^1 \pmod{10}$: les restes alternent entre 4 (exposant impair) et 6 (exposant pair), à partir de $m = 1$. 2027 est impair, donc $4^{2027} \equiv 4 \pmod{10}$. Le chiffre des unités de 4^{2027} est 4.

4. *Critères de divisibilité et tableaux de congruences*

Ex. 25 ★☆☆ **Restes sans poser la division**

(a) Comme $10 \equiv 1\ [9]$, on a $581\,276 \equiv 5 + 8 + 1 + 2 + 7 + 6 = 29 \equiv 2\ [9]$. Le reste vaut 2.

(b) Comme $10 \equiv -1\ [11]$, on part des unités : $5 - 9 + 3 - 0 + 6 - 1 + 7 - 4 = 7$. Le reste vaut 7.

(c) Comme $100 \equiv 0\ [4]$, on a $93\,718 \equiv 18 \equiv 2\ [4]$. Le plus grand multiple de 4 inférieur ou égal à 93 718 est donc $93\,718 - 2 = 93\,716$.

(d) Comme $100 \equiv 0\ [25]$, on a $40\,863 \equiv 63 \equiv 13\ [25]$. Il manque $25 - 13 = 12$: on ajoute 12, et en effet $40\,875 = 25 \times 1\,635$.

(e) $1\,000 = 8 \times 125$, donc $1\,000 \equiv 0\ [8]$. Or $6\,024\,517 = 6\,024 \times 1\,000 + 517$, donc par compatibilité $6\,024\,517 \equiv 0 + 517 = 517\ [8]$. Comme $517 = 8 \times 64 + 5$, le reste vaut 5.

(f) La somme des chiffres vaut $17 + a$. Il faut $17 + a \equiv 0\ [9]$ avec $0 \leqslant a \leqslant 9$, donc $a = 1$: le nombre est 51 732.

(g) En partant des unités : $4 - 1 + 8 - b + 3 = 14 - b$. Il faut $14 - b \equiv 0\ [11]$ avec $0 \leqslant b \leqslant 9$, donc $b = 3$: le nombre est 33 814.

Ex. 26 ★☆☆ **Vrai ou faux sur les congruences**

(a) Vrai : $10 \equiv 1\ [9]$, donc par compatibilité avec les puissances $10^5 \equiv 1^5 = 1\ [9]$.

(b) Faux : $10 \equiv -1\ [11]$, donc $10^5 \equiv (-1)^5 = -1 \equiv 10\ [11]$, et $10 \not\equiv 1\ [11]$.

(c) Faux : $100 \equiv 0\ [4]$, donc il faut garder les deux derniers chiffres : $5\,934 \equiv 34 \equiv 2\ [4]$, alors que $4 \equiv 0\ [4]$.

(d) Vrai : par compatibilité avec les puissances, $n^2 \equiv 3^2 = 9 \equiv 2\ [7]$.

(e) Faux : $-17 = 7 \times (-3) + 4$, donc $-17 \equiv 4\ [7]$, et $4 \not\equiv 3\ [7]$.

(f) Vrai : si $n \equiv 0\ [2]$, alors $n^2 - n \equiv 0\ [2]$; si $n \equiv 1\ [2]$, alors $n^2 - n \equiv 1 - 1 = 0\ [2]$. Dans les deux cas, $n^2 - n$ est pair.

Ex. 27 ★★☆ **Démontrer les critères de 9, de 11 et de 4**

(a) $10 - 1 = 9$, donc $9 \mid 10 - 1$, c'est-à-dire $10 \equiv 1\ [9]$. Par compatibilité avec les puissances, $10^i \equiv 1\ [9]$ pour tout i. Par compatibilité avec le produit et la somme, $a_i \times 10^i \equiv a_i\ [9]$, donc $N \equiv a_k + \cdots + a_0\ [9]$. Conclusion : N et la somme de ses chiffres ont le même reste modulo 9.

(b) $10 + 1 = 11$, donc $10 \equiv -1\ [11]$. Par compatibilité, $10^i \equiv (-1)^i\ [11]$, donc $N \equiv \sum_{i=0}^{k} (-1)^i a_i\ [11]$. Conclusion : le signe $+$ va au chiffre des unités ($i = 0$), puis les signes alternent.

(c) $100 = 4 \times 25$, donc $100 \equiv 0\ [4]$. Pour $i \geqslant 2$, on a $10^i = 100 \times 10^{i-2} \equiv 0\ [4]$, donc tous les termes de rang $i \geqslant 2$ sont nuls modulo 4. Conclusion : $N \equiv 10a_1 + a_0\ [4]$. Le reste se lit sur le nombre formé par les deux derniers chiffres.

(d) Non. D'après la deuxième question, on part des unités : $3 - 9 + 2 - 5 = -9 \equiv -9 + 11 = 2\ [11]$. Le reste vaut 2. Le nombre a quatre chiffres : en partant de la gauche, Lina a donné à chaque chiffre le signe opposé. Elle obtient l'opposé $9 \equiv -2\ [11]$, pas le reste.

Ex. 28 ★★☆ **Tableaux de congruences à exploiter**

(a)

$n \equiv \ldots\ [3]$	**0**	**1**	**2**
$n(n+1)(n+2) \equiv \ldots\ [3]$	0	0	0

Par exemple, pour $n \equiv 2\ [3]$: $2 \times 3 \times 4 = 24 \equiv 0\ [3]$. La ligne ne contient que des 0 : $n(n+1)(n+2)$ est divisible par 3 pour tout entier n.

(b)

$n \equiv \ldots\ [2]$	**0**	**1**
$n(n+1)(n+2) \equiv \ldots\ [2]$	0	0

Pour $n \equiv 1\ [2]$: $1 \times 2 \times 3 = 6 \equiv 0\ [2]$.
Donc $2 \mid n(n+1)(n+2)$. D'après la question précédente, on peut écrire $n(n+1)(n+2) = 3k$ avec $k \in \mathbb{Z}$. Alors $2 \mid 3k$ et $\text{PGCD}(2\,;3) = 1$, donc $2 \mid k$ par le théorème de Gauss. Conclusion : 6 divise $n(n+1)(n+2)$ pour tout entier n.

Ex. 28 (suite)

(c)

$n \equiv \ldots\ [4]$	**0**	**1**	**2**	**3**
$2n^2 \equiv \ldots\ [4]$	0	2	0	2
$3n \equiv \ldots\ [4]$	0	3	2	1
$2n^2 + 3n + 1 \equiv \ldots\ [4]$	1	2	3	0

Par exemple, pour $n \equiv 3\ [4]$: $2 \times 9 = 18 \equiv 2$, $3 \times 3 = 9 \equiv 1$, et $2 + 1 + 1 = 4 \equiv 0\ [4]$. Le reste 0 n'apparaît que pour $n \equiv 3\ [4]$. Conclusion : $4 \mid 2n^2 + 3n + 1$ si et seulement si $n = 3 + 4k$ avec $k \in \mathbb{Z}$.

(d) Vrai.

$n \equiv \ldots\ [8]$	**0**	**1**	**2**	**3**
$n^2 \equiv \ldots\ [8]$	0	1	4	1

$n \equiv \ldots\ [8]$	**4**	**5**	**6**	**7**
$n^2 \equiv \ldots\ [8]$	0	1	4	1

Par exemple, $5^2 = 25 = 3 \times 8 + 1$ et $7^2 = 49 = 6 \times 8 + 1$. Un entier impair est congru à 1, 3, 5 ou 7 modulo 8, et dans ces quatre cas $n^2 \equiv 1\ [8]$. Conclusion : Sami a raison.

Ex. 29 ★★☆ **Choisir le bon modulo**

(a)

$x \equiv \ldots\ [4]$	**0**	**1**	**2**	**3**
$x^2 \equiv \ldots\ [4]$	0	1	0	1

Un carré est congru à 0 ou à 1 modulo 4, jamais à 2 ni à 3.

(b) Si $(x\,;y)$ était solution, on aurait $x^2 = 2\,027 - 4y^2 \equiv 2\,027 \equiv 27 \equiv 3\ [4]$, puisque $100 \equiv 0\ [4]$. C'est impossible pour un carré d'après la question précédente. Conclusion : l'équation n'a pas de solution entière.

(c) Modulo 4, $3y + 2$ prend toutes les valeurs : pour $y \equiv 0, 1, 2, 3$, on obtient $2, 1, 0, 3$. Les restes 0 et 1 sont donc compatibles avec un carré, et le modulo 4 ne permet pas de conclure. Modulo 3 : $x^2 \equiv 2\ [3]$, mais $0^2 = 0$, $1^2 = 1$ et $2^2 = 4 \equiv 1\ [3]$. Conclusion : l'équation n'a pas de solution entière.

(d)

$x \equiv \ldots\ [7]$	**-3**	**-2**	**-1**	**0**
$x^3 \equiv \ldots\ [7]$	1	-1	-1	0

$x \equiv \ldots\ [7]$	**1**	**2**	**3**
$x^3 \equiv \ldots\ [7]$	1	1	-1

Par exemple, $3^3 = 27 \equiv -1\ [7]$. Un cube est donc congru à 0, 1 ou $-1 \equiv 6$ modulo 7. Or une solution donnerait $x^3 \equiv 3\ [7]$. Conclusion : l'équation n'a pas de solution entière.

Ex. 30 ★★★ **Un critère de divisibilité par 7**

(a) $-20 - 1 = -21 = 7 \times (-3)$, donc $-20 \equiv 1\ [7]$. Par compatibilité avec l'addition et la multiplication : $-2N = -20a - 2b \equiv 1 \times a - 2b\ [7]$.
Donc $a - 2b \equiv -2N\ [7]$ pour tous entiers a et b.

(b) Si $7 \mid N$, alors $N \equiv 0\ [7]$, donc $a - 2b \equiv -2 \times 0 = 0\ [7]$: $7 \mid a - 2b$. Réciproquement, si $7 \mid a - 2b$, alors $7 \mid -2N$, donc $7 \mid 2N$. Comme $\text{PGCD}(7\,;2) = 1$, le théorème de Gauss donne $7 \mid N$. Conclusion : $7 \mid N \iff 7 \mid a - 2b$.

(c) N prend les valeurs $59\,836$, puis $5\,983 - 2 \times 6 = 5\,971$, puis $597 - 2 \times 1 = 595$, puis $59 - 2 \times 5 = 49$. Comme $49 < 100$, la boucle s'arrête et la fonction renvoie 49. D'après la question précédente, chaque étape conserve la divisibilité par 7. Or $49 = 7 \times 7$, donc $59\,836$ est divisible par 7.

(d) Faux. Contre-exemple : $N = 10$, avec $a = 1$ et $b = 0$. Alors $a - 2b = 1$, de reste 1 modulo 7, mais $10 = 7 + 3$ a pour reste 3. Le critère conserve la divisibilité par 7, pas le reste : en fait $a - 2b \equiv -2N\ [7]$.

(e) On a $-6 \equiv 1\ [7]$. Par compatibilité : $3(a - 2b) \equiv 3 \times (-2N) = -6N \equiv N\ [7]$. Pour $4\,852$: $a = 485$, $b = 2$, donc $a - 2b = 481$ et $3 \times 481 = 1\,443 = 7 \times 206 + 1$. Donc $4\,852 \equiv 1\ [7]$: le reste vaut 1.

Ex. 31 ★★★ **Les diviseurs de $n^2 + n + 1$**

(a) Par compatibilité avec l'addition et la multiplication, si $n \equiv r\ [5]$, alors $A \equiv r^2 + r + 1\ [5]$.

$n \equiv \ldots\ [5]$	**0**	**1**	**2**
$A \equiv \ldots\ [5]$	1	3	2

$n \equiv \ldots\ [5]$	**3**	**4**
$A \equiv \ldots\ [5]$	3	1

Par exemple, pour $r = 3$: $9 + 3 + 1 = 13 \equiv 3\ [5]$. Le reste 0 n'apparaît jamais : A n'est jamais un multiple de 5.

(b)

$n \equiv \ldots\ [3]$	**0**	**1**	**2**
$A \equiv \ldots\ [3]$	1	0	1

Pour $n \equiv 1$: $1 + 1 + 1 = 3 \equiv 0\ [3]$; pour $n \equiv 2$: $4 + 2 + 1 = 7 \equiv 1\ [3]$. Le reste 0 n'apparaît que pour $n \equiv 1\ [3]$. Conclusion : $3 \mid A$ si et seulement si $n \equiv 1\ [3]$.

(c) Pour $n \equiv 0, 1, 2, 3, 4, 5, 6\ [7]$, on trouve $A \equiv 1, 3, 0, 6, 0, 3, 1\ [7]$ (par exemple $16 + 4 + 1 = 21 \equiv 0$ et $25 + 5 + 1 = 31 \equiv 3$).
Donc $7 \mid A$ si et seulement si $n \equiv 2$ ou $n \equiv 4\ [7]$.

Ex. 31 **(suite)**

(d) $21 = 3 \times 7$ avec $\text{PGCD}(3\,;7) = 1$, donc $21 \mid A \iff 3 \mid A$ et $7 \mid A$ (si $3 \mid A$ et $7 \mid A$, alors $A = 3k$ et $7 \mid 3k$, donc $7 \mid k$ par Gauss). Les $n < 21$ avec $n \equiv 2$ ou $4\ [7]$ sont $2, 4, 9, 11, 16, 18$. Parmi eux, seuls 4 et 16 vérifient $n \equiv 1\ [3]$. Les solutions sont $n = 4$ ($A = 21$) et $n = 16$ ($A = 273 = 21 \times 13$).

(e) Si $9 \mid A$, alors $3 \mid A$, donc $n \equiv 1\ [3]$: $n = 3k + 1$ avec $k \in \mathbb{N}$. Alors $A = 9k^2 + 6k + 1 + 3k + 1 + 1 = 9k^2 + 9k + 3 \equiv 3\ [9]$, ce qui contredit $9 \mid A$.
Donc A n'est divisible par 9 pour aucun entier naturel n.

Ex. 32 ★★★ **Les chiffres manquants d'un numéro de lot**

(a) Soit M un entier naturel. On écrit $M = 100q + r$, où r est le nombre formé par ses deux derniers chiffres ($0 \leqslant r \leqslant 99$). Or $100 = 4 \times 25$, donc $100 \equiv 0\ [25]$. Par compatibilité avec la multiplication et l'addition, $M \equiv 0 \times q + r = r\ [25]$. Conclusion : M et r ont le même reste modulo 25.

(b) Soit $M = \overline{a_4 a_3 a_2 a_1 a_0}$. Comme $10 \equiv -1\ [11]$, on a $10^i \equiv (-1)^i\ [11]$, donc $M \equiv a_0 - a_1 + a_2 - a_3 + a_4\ [11]$: le signe $+$ va aux unités. En partant de la gauche, Hugo calcule $a_4 - a_3 + a_2 - a_1 + a_0$. C'est la même somme, car le chiffre de gauche a le rang 4, qui est pair : il porte le signe $+$. Conclusion : avec cinq chiffres, sa méthode donne le bon résultat. Avec un nombre pair de chiffres, il obtiendrait l'opposé.

(c) Divisibilité par 4 : comme $100 \equiv 0\ [4]$, $\overline{2b}$ doit être un multiple de 4, donc $b \in \{0\,;4\,;8\}$. Divisibilité par 11 : la somme alternée à partir des unités vaut $b - 2 + 5 - a + 4 = b - a + 7$. Si $b = 0$: $7 - a \equiv 0\ [11]$, donc $a = 7$. Si $b = 4$: $11 - a \equiv 0\ [11]$, donc $a = 0$. Si $b = 8$: $15 - a \equiv 0\ [11]$, donc $a = 4$. Les couples sont $(7\,;0)$, $(0\,;4)$ et $(4\,;8)$, soit $N = 47\,520$, $40\,524$ ou $44\,528$.

(d) $396 = 4 \times 9 \times 11$, et 4, 9, 11 sont premiers entre eux deux à deux. D'après le théorème de Gauss, $396 \mid N$ si et seulement si 4, 9 et 11 divisent N. Comme $10 \equiv 1\ [9]$, un nombre est congru modulo 9 à la somme de ses chiffres. Les sommes valent 18 pour $47\,520$, 15 pour $40\,524$ et 23 pour $44\,528$. Seul 18 est multiple de 9 : le numéro cherché est $47\,520 = 396 \times 120$.

Ex. 32 **(suite)**

(e) $275 = 25 \times 11$ avec $\text{PGCD}(25\,;11) = 1$. Il faut donc $25 \mid N$ et $11 \mid N$. D'après la première question, $\overline{2b}$ doit valoir 00, 25, 50 ou 75, donc $b = 5$. Ensuite $b - a + 7 = 12 - a \equiv 0\ [11]$, donc $a = 1$. Le seul numéro est $N = 41\,525 = 275 \times 151$.

5. *Résoudre $ax \equiv b\ [n]$, inverse modulo n, systèmes*

Ex. 33 ★☆☆ **Trouver un inverse par essais**

(a) $\text{pgcd}(3\,;11) = 1$. Par essais : $3 \times 4 = 12 = 11 + 1$, donc $3 \times 4 \equiv 1\ [11]$. L'inverse de 3 modulo 11 est 4.

(b) $\text{pgcd}(5\,;12) = 1$. $5 \times 5 = 25 = 2 \times 12 + 1$, donc l'inverse de 5 modulo 12 est 5 lui-même.

(c) $\text{pgcd}(9\,;13) = 1$. $9 \times 3 = 27 = 2 \times 13 + 1$: l'inverse de 9 modulo 13 est 3.

(d) $\text{pgcd}(6\,;15) = 3 \neq 1$: 6 n'a pas d'inverse modulo 15. En effet, $6u - 15v = 3(2u - 5v)$ est un multiple de 3 et ne peut pas valoir 1.

(e) $\text{pgcd}(10\,;17) = 1$ car 17 est premier et ne divise pas 10. $10 \times 12 = 120 = 7 \times 17 + 1$: l'inverse de 10 modulo 17 est 12.

(f) Non : $4 \times 5 = 20 = 2 \times 9 + 2$, donc $4 \times 5 \equiv 2\ [9]$ et pas 1. L'opposé n'est pas l'inverse. Par contre $4 \times 7 = 28 = 3 \times 9 + 1$: l'inverse de 4 modulo 9 est 7.

Ex. 34 ★☆☆ **Résoudre en multipliant par l'inverse**

(a) $3 \times 5 = 15 \equiv 1\ [7]$, donc l'inverse de 3 est 5. En multipliant par 5 : $x \equiv 25 \equiv 4\ [7]$. Vérification : $3 \times 4 = 12 \equiv 5\ [7]$. Solutions : $x = 4 + 7k$, $k \in \mathbb{Z}$.

(b) $-7 = -9 + 2$, donc $-7 \equiv 2\ [9]$ et l'équation s'écrit $5x \equiv 2\ [9]$. $5 \times 2 = 10 \equiv 1\ [9]$: l'inverse est 2. $x \equiv 2 \times 2 = 4\ [9]$. Vérification : $5 \times 4 - (-7) = 27 = 3 \times 9$. Solutions : $x = 4 + 9k$, $k \in \mathbb{Z}$.

(c) $7 \times 7 = 49 = 4 \times 12 + 1$: l'inverse de 7 est 7. $x \equiv 7 \times 5 = 35 \equiv 11\ [12]$. Vérification : $7 \times 11 = 77 = 6 \times 12 + 5$. Solutions : $x = 11 + 12k$, $k \in \mathbb{Z}$.

(d) $26 = 2 \times 11 + 4$, donc $26 \equiv 4\ [11]$ et l'équation s'écrit $4x \equiv 6\ [11]$. $4 \times 3 = 12 \equiv 1\ [11]$: l'inverse est 3. $x \equiv 18 \equiv 7\ [11]$. Vérification : $26 \times 7 = 182 = 16 \times 11 + 6$. Solutions : $x = 7 + 11k$, $k \in \mathbb{Z}$.

(e) On soustrait 4 : $9x \equiv 5\ [16]$. $9 \times 9 = 81 = 5 \times 16 + 1$: l'inverse est 9. $x \equiv 45 \equiv 13\ [16]$. Vérification : $9 \times 13 + 4 = 121 = 7 \times 16 + 9$. Solutions : $x = 13 + 16k$, $k \in \mathbb{Z}$.

Ex. 34 **(suite)**

(f) On ne divise pas dans une congruence : $\frac{7}{2}$ n'est pas un entier. On multiplie par l'inverse de 2 modulo 15, qui est 8 car $2 \times 8 = 16 \equiv 1\ [15]$. $x \equiv 56 \equiv 11\ [15]$. Vérification : $2 \times 11 = 22 \equiv 7\ [15]$. Solutions : $x = 11 + 15k$, $k \in \mathbb{Z}$.

Ex. 35 ★★☆ **Un inverse par l'algorithme d'Euclide**

(a) 23 est premier et ne divise pas 60, donc $\text{pgcd}(23\,;60) = 1$. D'après le critère du cours, 23 admet un inverse modulo 60.

(b) $60 = 2 \times 23 + 14$; $23 = 1 \times 14 + 9$; $14 = 1 \times 9 + 5$; $9 = 1 \times 5 + 4$; $5 = 1 \times 4 + 1$. On remonte : $1 = 5 - 4 = 2 \times 5 - 9 = 2 \times 14 - 3 \times 9 = 5 \times 14 - 3 \times 23 = 5 \times 60 - 13 \times 23$.
Donc $u = -13$ et $v = 5$. Ainsi $23 \times (-13) \equiv 1\ [60]$ et $-13 \equiv 47\ [60]$: l'inverse de 23 modulo 60 est 47 (contrôle : $23 \times 47 = 1081 = 18 \times 60 + 1$).

(c) En multipliant par 47 : $23x \equiv 7\ [60] \iff x \equiv 47 \times 7 = 329\ [60]$, soit $x \equiv 29\ [60]$. Vérification : $23 \times 29 = 667 = 11 \times 60 + 7$. Les solutions sont les entiers $x = 29 + 60k$, $k \in \mathbb{Z}$: c'est une classe entière, pas une seule valeur.

(d) $37 = 60 - 23$, donc $37 \equiv -23\ [60]$. Alors $37 \times (-47) \equiv (-23) \times (-47) = 23 \times 47 \equiv 1\ [60]$. Or $-47 \equiv 13\ [60]$. L'inverse de 37 modulo 60 est donc 13. Contrôle : $37 \times 13 = 481 = 8 \times 60 + 1$.

Ex. 36 ★★☆ **Quand pgcd(a ; n) n'est pas égal à 1**

(a) $\text{pgcd}(12\,;20) = 4$. Si $12x - 9 = 20k$ avec $k \in \mathbb{Z}$, alors $9 = 12x - 20k = 4(3x - 5k)$, donc 4 diviserait 9 : c'est impossible. L'équation n'a aucune solution.

(b) $12x \equiv 8\ [20] \iff$ il existe $k \in \mathbb{Z}$ tel que $12x - 8 = 20k \iff 4(3x - 2) = 4 \times 5k \iff 3x - 2 = 5k \iff 3x \equiv 2\ [5]$. Les deux équations sont donc équivalentes.

(c) $3 \times 2 = 6 \equiv 1\ [5]$: l'inverse de 3 modulo 5 est 2. Donc $x \equiv 4\ [5]$ (vérification : $3 \times 4 = 12 \equiv 2\ [5]$). Les solutions de $12x \equiv 8\ [20]$ sont les $x = 4 + 5k$; entre 0 et 19, ce sont 4, 9, 14 et 19 (par exemple $12 \times 9 = 108 = 5 \times 20 + 8$). Modulo 20, il y a donc quatre classes de solutions.

(d) S'il y a une solution, $12x - 20y = b$ pour un entier y, donc 4 divise b. Réciproquement, si $b = 4c$, l'équation équivaut (comme à la question 2) à $3x \equiv c\ [5]$, qui a des solutions car $\text{pgcd}(3\,;5) = 1$: $x \equiv 2c\ [5]$. Conclusion : $b \in \{0\,;4\,;8\,;12\,;16\}$.

Ex. 37 ★★☆ **Les cartes de Sacha**

(a) $x \equiv 3\ [7]$ et $x \equiv 5\ [9]$.

(b) $x \equiv 3\ [7]$ signifie que 7 divise $x-3$: il existe $k \in \mathbb{Z}$ tel que $x = 3+7k$. Alors $x \equiv 5\ [9] \iff 3+7k \equiv 5\ [9] \iff 7k \equiv 2\ [9]$.

(c) $7 \times 4 = 28 = 3 \times 9 + 1$: l'inverse de 7 modulo 9 est 4. Donc $k \equiv 4 \times 2 = 8\ [9]$, soit $k = 8+9j$ avec $j \in \mathbb{Z}$. Alors $x = 3+7(8+9j) = 59+63j$. Réciproquement, $59 = 8 \times 7 + 3$ et $59 = 6 \times 9 + 5$, et 63 est un multiple de 7 et de 9. Les solutions du système sont les entiers $x \equiv 59\ [63]$.

(d) Entre 100 et 200 : $59+63 = 122$ et $59+2\times 63 = 185$ (car $59 < 100$ et $59+3\times 63 = 248 > 200$). 122 est pair. Sacha possède donc 185 cartes. Contrôle : $185 = 26 \times 7 + 3 = 20 \times 9 + 5$.

Ex. 38 ★★★ **Un système aux modules non premiers entre eux**

(a) $x \equiv 4\ \pmod 9$ équivaut à : il existe $k \in \mathbb{Z}$ tel que $x = 4+9k$. Pour un tel x, $x \equiv 7\ \pmod{12} \iff 4+9k \equiv 7\ \pmod{12} \iff 9k \equiv 3\ \pmod{12}$.
Donc x est solution de (S) si et seulement si $x = 4+9k$ avec $9k \equiv 3\ \pmod{12}$.

(b) $12 = 1\times 9 + 3$ et $9 = 3 \times 3$, donc $\text{pgcd}(9\,;12) = 3$, qui divise 3. $9k \equiv 3\ \pmod{12} \iff$ il existe $m \in \mathbb{Z}$ tel que $9k - 3 = 12m \iff 3k - 1 = 4m$ (on divise par 3) $\iff 3k \equiv 1\ \pmod 4$. Or $3 \times 3 = 9 \equiv 1\ \pmod 4$: l'inverse de 3 modulo 4 est 3. On multiplie par 3 : $k \equiv 3\ \pmod 4$, soit $k = 3+4j$, $j \in \mathbb{Z}$.

(c) $x = 4+9(3+4j) = 31+36j$, $j \in \mathbb{Z}$. Réciproquement, $31 = 3\times 9 + 4$ et $31 = 2 \times 12 + 7$, et 36 est un multiple de 9 et de 12. Les solutions de (S) sont donc les entiers $x \equiv 31\ \pmod{36}$.

(d) Il a tort. 31 et $31+36 = 67$ sont deux solutions ($67 = 7\times 9 + 4 = 5 \times 12 + 7$), et leur écart n'est que de 36. Comme $\text{pgcd}(9\,;12) = 3 \neq 1$, les solutions ne se répètent pas tous les 108 entiers mais tous les 36, le plus petit multiple commun de 9 et de 12.

(e) Si $x \equiv 4\ \pmod 9$, alors 9, donc 3, divise $x-4$: $x \equiv 4 \equiv 1\ \pmod 3$. Si $x \equiv 6\ \pmod{12}$, alors 3 divise $x-6$: $x \equiv 0\ \pmod 3$. Un entier n'a qu'un seul reste dans la division par 3, donc ce système n'a aucune solution.

Ex. 39 ★★★ **Les deux jets d'eau du parc**

(a) $x \equiv 5\ \pmod 8$ équivaut à : il existe $k \in \mathbb{Z}$ tel que $x = 5+8k$. Pour un tel x, $x \equiv 7\ \pmod{15} \iff 5+8k \equiv 7\ \pmod{15} \iff 8k \equiv 2\ \pmod{15}$.
Donc x est solution si et seulement si $x = 5+8k$ avec $8k \equiv 2\ \pmod{15}$.

(b) $\text{pgcd}(8\,;15) = 1$ ($8 = 2^3$ et $15 = 3\times 5$), donc 8 admet un inverse modulo 15. Essais : $8 \times 1 = 8$, $8 \times 2 = 16 = 15+1$, donc cet inverse est 2. En multipliant par 2 : $16k \equiv 4\ \pmod{15}$, donc $k \equiv 4\ \pmod{15}$. Réciproquement, $8 \times 4 = 32 = 2\times 15 + 2$. Les solutions sont $k = 4+15j$, $j \in \mathbb{Z}$.

(c) $x = 5+8(4+15j) = 37+120j$, $j \in \mathbb{Z}$. Les solutions forment donc la seule classe $x \equiv 37\ \pmod{120}$, avec $120 = 8\times 15$. Vérification : $37 = 4\times 8 + 5$ et $37 = 2\times 15 + 7$.

(d) Elle a tort. $37+23 = 60$ et $60 = 7\times 8 + 4$, donc $60 \not\equiv 5\ \pmod 8$: à la minute 60, le jet A ne part pas. Les départs communs reviennent toutes les 120 minutes, car 8 et 15 sont premiers entre eux et $8\times 15 = 120$.

(e) Le parc est ouvert 12 h, soit 720 minutes. On cherche j tel que $0 \leqslant 37+120j \leqslant 720$, donc $j \in \{0,1,2,3,4,5\}$ ($37+600 = 637$ et $37+720 = 757 > 720$). Les deux jets partent ensemble 6 fois : à 10 h 37, 12 h 37, 14 h 37, 16 h 37, 18 h 37 et 20 h 37.

Ex. 40 ★★★ **Chercher un inverse : essais ou Euclide ?**

(a) La fonction renvoie le plus petit u entre 0 et 17 tel que $5u \equiv 1\ \pmod{18}$. Pour u de 0 à 10, les produits $5u$ ont pour restes $0, 5, 10, 15, 2, 7, 12, 17, 4, 9, 14$, jamais 1. En revanche, $5 \times 11 = 55 = 3\times 18 + 1$. Elle renvoie donc 11.

(b) Elle renvoie -1. En effet, $\text{pgcd}(12\,;18) = 6 \neq 1$, donc 12 n'a pas d'inverse modulo 18. D'ailleurs, $12u - 18v$ est toujours un multiple de 6 et ne peut pas valoir 1. Aucun test ne réussit, et la boucle se termine sur `return -1`.

Ex. 40 (suite)

(c)
```
def inverse(a, n):
    for u in range(n):
        if (a * u) % n == 1:
            return u
    return -1

for a in range(1, 18):
    if inverse(a, 18) != -1:
        print(a)
```

Le programme affiche 1, 5, 7, 11, 13 et 17. Ce sont les entiers premiers avec 18 : il y en a 6.

(d) $5 \times 77 = 385 = 21 \times 18 + 7$: 77 est bien une solution, mais ce n'est pas la seule. L'inverse de 5 modulo 18 est 11, donc $5x \equiv 7 \pmod{18} \iff x \equiv 77 \pmod{18}$. Comme $77 = 4 \times 18 + 5$, cela s'écrit $x \equiv 5 \pmod{18}$. Vérification : $5 \times 5 = 25 = 18 + 7$. Les solutions forment une classe entière : $x = 5 + 18k$, $k \in \mathbb{Z}$.

(e) $1000 = 23 \times 43 + 11$, $43 = 3 \times 11 + 10$, $11 = 1 \times 10 + 1$, donc $\text{pgcd}(43\,;1000) = 1$. Remontée : $1 = 11 - 10 = 11 - (43 - 3 \times 11) = 4 \times 11 - 43 = 4(1000 - 23 \times 43) - 43 = 4 \times 1000 - 93 \times 43$. Donc $43 \times (-93) \equiv 1 \pmod{1000}$, et $-93 \equiv 907 \pmod{1000}$. L'inverse de 43 modulo 1000 est 907. Vérification : $43 \times 907 = 39\,001 = 39 \times 1000 + 1$.

6. *Chiffrements et clés de contrôle*

Ex. 41 ★☆☆ **Chiffrer avec une clé affine**

(a) E a le rang $x = 4$: $15 \times 4 + 8 = 68 = 2 \times 26 + 16$, donc $y = 16$. E est chiffrée en Q.

(b) K a le rang $x = 10$: $15 \times 10 + 8 = 158 = 6 \times 26 + 2$, donc $y = 2$. K est chiffrée en C.

(c) $25 - (-1) = 26$ est divisible par 26, donc $25 \equiv -1 \pmod{26}$. Par compatibilité avec la multiplication et l'addition, $15 \times 25 + 8 \equiv 15 \times (-1) + 8 = -7 \pmod{26}$. Or $-7 + 26 = 19$ avec $0 \leqslant 19 \leqslant 25$, donc $y = 19$: Z est chiffrée en T.

(d) A (rang 0) : $15 \times 0 + 8 = 8$, ce qui donne I. M (rang 12) : $15 \times 12 + 8 = 188 = 7 \times 26 + 6$, ce qui donne G. I (rang 8) : $15 \times 8 + 8 = 128 = 4 \times 26 + 24$, ce qui donne Y. AMI est chiffré en IGY.

(e) Avec $x = 2$, Nora obtient $15 \times 2 + 8 = 38 = 26 + 12$, soit M. Son erreur : la numérotation commence à A $= 0$, donc B a le rang 1 et non 2 (M est en réalité le chiffré de C). Le bon calcul est $15 \times 1 + 8 = 23$: B est chiffrée en X.

Ex. 42 ★☆☆ **Calculer une clé de Luhn**

(a) En partant de la droite : 9 reste 9 ; 3 doublé donne 6 ; 7 reste 7 ; 4 doublé donne 8. Somme : $9 + 6 + 7 + 8 = 30 \equiv 0 \pmod{10}$. Le numéro est valide.

(b) 6 reste 6 ; 1 doublé donne 2 ; 2 reste 2 ; 8 doublé donne $16 - 9 = 7$; 5 reste 5. Somme : $22 \equiv 2 \pmod{10}$. Le numéro n'est pas valide.

(c) c n'est pas doublé ; 8 doublé donne $16 - 9 = 7$; 7 reste 7 ; 5 doublé donne $10 - 9 = 1$; 6 reste 6. Somme : $c + 21$. Il faut $c + 21 \equiv 0 \pmod{10}$, donc $c = 9$.

(d) c ; 7 doublé donne $14 - 9 = 5$; 1 ; 4 doublé donne 8 ; 9 ; 2 doublé donne 4 ; 5 ; 3 doublé donne 6. Somme : $c + 38$. Il faut $c + 38 \equiv 0 \pmod{10}$, donc $c = 2$.

(e) Non. On double en partant de la droite : c ; 6 doublé donne $12 - 9 = 3$; 4 ; 2 doublé donne 4 ; 7. Somme : $c + 18$, donc $c = 2$. En partant de la gauche, Théo double 7, 4 et c : il obtient $5 + 2 + 8 + 6 + (2c - 9) \equiv 0$, soit $c = 9$, ce qui est faux.

Ex. 43 ★★☆ **Déchiffrer un message affine**

(a) $21 = 3 \times 7$ et $26 = 2 \times 13$ n'ont aucun facteur premier commun, donc $\text{pgcd}(21\,;26) = 1$ et 21 a un inverse modulo 26. On teste : 27, 53 et 79 ne sont pas multiples de 21, mais $105 = 4 \times 26 + 1 = 21 \times 5$. Donc $21 \times 5 \equiv 1 \pmod{26}$: l'inverse de 21 est 5.

(b) Si $y \equiv 21x + 11$, en multipliant par 5 : $5y \equiv 105x + 55 \equiv x + 55 \pmod{26}$, donc $x \equiv 5y - 55 \equiv 5y + 23 \pmod{26}$. Réciproquement, si $x \equiv 5y + 23$, alors $21x + 11 \equiv 105y + 494 \equiv y \pmod{26}$, car $105 \equiv 1$ et $494 = 19 \times 26$. On a donc $c = 5$ et $d = 23$.

(c) Y : $5 \times 24 + 23 = 143 = 5 \times 26 + 13$, ce qui donne N. P : $5 \times 15 + 23 = 98 = 3 \times 26 + 20$, ce qui donne U. X : $5 \times 23 + 23 = 138 = 5 \times 26 + 8$, ce qui donne I. U : $5 \times 20 + 23 = 123 = 4 \times 26 + 19$, ce qui donne T. Le mot clair est NUIT.

(d) $\frac{13}{21}$ n'est pas un entier : on ne divise pas dans une congruence. Il faut multiplier par l'inverse de 21 : $x \equiv 5 \times (24 - 11) = 65 \equiv 13 \pmod{26}$, ce qui donne N.

(e) A : $8 \times 0 + 11 = 11$, ce qui donne L. N : $8 \times 13 + 11 = 115 = 4 \times 26 + 11$, ce qui donne aussi L. Deux lettres différentes ont le même chiffré, donc on ne peut pas retrouver le clair à partir de L. Cela vient de $\text{pgcd}(8\,;26) = 2 \neq 1$: 8 n'a pas d'inverse modulo 26, et la clé n'est pas déchiffrable.

Ex. 44 ★★☆ **Une clé qui ignore les permutations**

(a) $3+8+5+6=22\equiv 2 \pmod{10}$. La clé vaut 2.

(b) Si un chiffre a est remplacé par $a'\neq a$, la somme change de $a'-a$. Comme $0\leqslant a\leqslant 9$ et $0\leqslant a'\leqslant 9$, on a $-9\leqslant a'-a\leqslant 9$ avec $a'-a\neq 0$, donc 10 ne divise pas $a'-a$. Les deux sommes ne sont pas congrues modulo 10 : la clé change et l'erreur est détectée.

(c) $8+3+5+6=22$: la clé vaut encore 2. L'addition est commutative, donc permuter des chiffres ne change pas la somme. La clé reste la même : aucune permutation n'est détectée.

(d) $3+2\times 8+3\times 5+4\times 6=58=5\times 11+3$, donc la clé vaut 3. $3+2\times 5+3\times 8+4\times 6=61=5\times 11+6$, donc la clé vaut 6. Les clés sont différentes : cet échange est détecté.

(e) On échange deux chiffres $u\neq v$ placés aux rangs de poids i et j, avec $1\leqslant i<j\leqslant 4$. Leur contribution passe de $iu+jv$ à $iv+ju$: la somme varie de $(j-i)(u-v)$. La clé reste la même si et seulement si $11\mid (j-i)(u-v)$. Or 11 est premier et $1\leqslant j-i\leqslant 3$, donc $\text{pgcd}(11\,;j-i)=1$. D'après le théorème de Gauss, on aurait $11\mid u-v$, ce qui est impossible car $0<|u-v|\leqslant 9$. L'échange change donc toujours la clé : cette clé détecte toute permutation de deux chiffres.

Ex. 45 ★★☆ **Un programme de chiffrement à corriger**

(a) L (rang 11) : $7\times 11+2=79=3\times 26+1$, ce qui donne B. O (rang 14) : $100=3\times 26+22$, ce qui donne W. U (rang 20) : $142=5\times 26+12$, ce qui donne M. P (rang 15) : $107=4\times 26+3$, ce qui donne D. La fonction renvoie "BWMD".

(b) En Python, `%` est prioritaire sur `+`. La ligne calcule donc $7\times 11+(2\%26)=79$, sans réduire modulo 26. `alphabet[79]` n'existe pas et le programme s'arrête sur une erreur (IndexError). Il faut écrire `y = (a * x + b) % 26`.

(c) Avec cette ligne, A prend le rang 1 au lieu de 0 : $7\times 1+2=9$, donc la fonction renvoie "J". Le bon chiffré de A est C, car $7\times 0+2=2$. Les lettres se numérotent à partir de 0.

Ex. 45 **(suite)**

(d) $7\times 15=105=4\times 26+1$, donc 15 est un inverse de 7 modulo 26. Ainsi $y\equiv 7x+2\ [26]\iff x\equiv 15(y-2)\ [26]$: on multiplie par l'inverse, on ne divise pas. En Python, `%` renvoie un reste positif même si $y-2<0$.

```
def dechiffre(mot):
    alphabet = "ABCDEFGHIJKLMNOPQRSTUVWXYZ"
    resultat = ""
    for lettre in mot:
        y = alphabet.index(lettre)
        x = (15 * (y - 2)) % 26
        resultat = resultat + alphabet[x]
    return resultat
```

Par exemple, `dechiffre("BWMD")` renvoie "LOUP".

Ex. 46 ★★★ **Retrouver la clé d'un espion**

(a) E a le rang 4, Y le rang 24, S le rang 18 et W le rang 22. On a donc $4a+b\equiv 24 \pmod{26}$ et $18a+b\equiv 22 \pmod{26}$.

(b) On soustrait la première congruence de la seconde (compatibilité avec l'addition) : $14a\equiv -2\equiv 24 \pmod{26}$. Or $26\mid 14a-24\iff 13\mid 7a-12$, d'où $7a\equiv 12 \pmod{13}$. Parmi $14, 27\ldots, 14=7\times 2 : 7\times 2\equiv 1 \pmod{13}$, donc 2 est un inverse de 7 modulo 13. En multipliant par 2 : $a\equiv 24\equiv 11 \pmod{13}$. Ainsi, $a\equiv 11 \pmod{13}$.

(c) Entre 0 et 25, $a\equiv 11 \pmod{13}$ donne $a=11$ ou $a=24$. Ensuite, $b\equiv 24-4a \pmod{26}$. Pour $a=11$: $b\equiv -20\equiv 6$. Pour $a=24 : b\equiv -72\equiv 6$. On vérifie la seconde congruence : $18\times 11+6=204\equiv 22$ et $18\times 24+6=438\equiv 22 \pmod{26}$. Les deux clés possibles sont $(11\,;6)$ et $(24\,;6)$.

(d) Avec $a=24$, A ($x=0$) donne $y=6$ et N ($x=13$) donne $24\times 13+6=318=12\times 26+6$, donc $y=6$ aussi. A et N sont donc tous deux chiffrés G. Cela vient de $\text{pgcd}(24\,;26)=2$: cette clé ne se déchiffre pas. La clé de l'espion est donc $a=11$ et $b=6$.

(e) Parmi $27, 53, 79, \ldots$, le premier multiple de 11 est $209=11\times 19$, donc $11\times 19\equiv 1 \pmod{26}$: 19 est un inverse de 11 modulo 26. On ne divise pas, on multiplie par 19 : $y\equiv 11x+6\iff x\equiv 19(y-6) \pmod{26}$. L : $19\times 5=95\equiv 17$, soit R. Q : $19\times 10=190\equiv 8$, soit I. D : $19\times(-3)=-57\equiv 21$, soit V. Y : $19\times 18=342\equiv 4$, soit E. Le message clair est RIVE.

Ex. 47 ★★★ **Le code ISBN-13 sous la loupe**

(a) Sans la clé : $9+21+8+6+7+0+1+3+9+9+8+12=93$. La clé a_{13}, de poids 1, vérifie $93+a_{13}\equiv 0 \pmod{10}$, soit $a_{13}\equiv 7 \pmod{10}$. Comme $0\leqslant a_{13}\leqslant 9$, la clé vaut 7 et le code complet est 9782701193847 ($S=100$).

(b) Supposons qu'un chiffre c de poids $p\in\{1;3\}$ soit remplacé par $c'\neq c$. La nouvelle somme vaut $S'=S+p(c'-c)$. L'erreur passe inaperçue si et seulement si $10\mid p(c'-c)$. Or $\operatorname{pgcd}(p;10)=1$, donc d'après le théorème de Gauss $10\mid c'-c$. C'est impossible, car $0<|c'-c|\leqslant 9$. Une erreur sur un seul chiffre est donc toujours détectée.

(c) Si c est au rang de poids 1 et d au rang suivant, de poids 3, leur contribution passe de $c+3d$ à $d+3c$: S varie de $2(c-d)$. Dans l'autre cas, S varie de $2(d-c)$. L'échange passe inaperçu si et seulement si $10\mid 2(c-d)$, c'est-à-dire $5\mid c-d$. Comme $c\neq d$ et $|c-d|\leqslant 9$, la condition est $|c-d|=5$.

(d) Dans 9782701193847, les seuls voisins dont l'écart vaut 5 sont 2 et 7 (rangs 4 et 5) et 3 et 8 (rangs 10 et 11). Ce sont donc les deux seuls échanges non détectés. Vérification pour 9787201193847 : $S=9+21+8+21+2+0+1+3+9+9+8+12+7=110\equiv 0 \pmod{10}$. Le contrôle passe bien.

(e) Avec les poids 1 et 2, remplaçons le 7 du rang 2 (poids 2) par un 2. La somme varie de $2\times(2-7)=-10\equiv 0 \pmod{10}$. Elle ne change pas modulo 10, donc le contrôle rend le même verdict que pour le code exact : l'erreur passe inaperçue. Cela vient de $\operatorname{pgcd}(2;10)=2\neq 1$.

Ex. 48 ★★★ **Toutes les clés affines au banc d'essai**

(a) $13\times 0+5=5$ et $13\times 2+5=31\equiv 5 \pmod{26}$: A et C sont tous deux chiffrés F. Au tour $x=2$, la valeur 5 est déjà dans `images`, donc `injective(13, 5)` renvoie `False`.

(b) Si $a=2m$ avec m entier, alors $a(x+13)+b-(ax+b)=13a=26m\equiv 0 \pmod{26}$. Les lettres de rangs x et $x+13$ ont donc la même image. En particulier, A ($x=0$) et N ($x=13$) ont la même image : la fonction renvoie `False`.

Ex. 48 **(suite)**

(c) Si $\operatorname{pgcd}(a;26)=1$, le théorème de Bézout donne des entiers u et v tels que $au+26v=1$, donc $au\equiv 1 \pmod{26}$. Si $ax+b\equiv ax'+b \pmod{26}$, alors $ax\equiv ax'$; en multipliant par u, on obtient $x\equiv x' \pmod{26}$. Comme $0\leqslant x,x'\leqslant 25$, on a $x=x'$. Deux lettres distinctes ont donc des images distinctes.

(d) Comme $26=2\times 13$, $\operatorname{pgcd}(a;26)\neq 1$ équivaut, pour $0\leqslant a\leqslant 25$, à « a pair ou $a=13$ ». Pour a pair, la question précédente montre que la fonction renvoie `False`. Pour $a=13$, les rangs 0 et 2 ont la même image quel que soit b, car $13\times 2=26$. Les valeurs retenues sont donc les nombres impairs de 1 à 25 sauf 13 : il y en a $13-1=12$. Le programme affiche 12.

(e)
```
def dechiffre(mot, a, b):
    alphabet = "ABCDEFGHIJKLMNOPQRSTUVWXYZ"
    u = 1
    while (a * u) % 26 != 1:
        u = u + 1
    clair = ""
    for lettre in mot:
        y = alphabet.index(lettre)
        x = (u * (y - b)) % 26
        clair = clair + alphabet[x]
    return clair
```

Comme $\operatorname{pgcd}(a;26)=1$, a a un inverse modulo 26 et la boucle s'arrête. On déchiffre en multipliant par l'inverse, sans diviser par a : $x\equiv u(y-b) \pmod{26}$. Ici $17\times 23=391=15\times 26+1$, donc $u=23$. Q : $23\times(-4)=-92\equiv 12$, soit M. K : $23\times(-10)=-230\equiv 4$, soit E. X : $23\times 3=69\equiv 17$, soit R. Comme `%` renvoie un reste positif même si `y - b` est négatif, la fonction renvoie "MER".