

Divisibilité et congruences — Terminale maths expertes

20 exercices corrigés · mathlvl.fr

Énoncés et corrigés détaillés

Présentation

Travailler modulo n , c'est décider de ne retenir d'un entier que son RESTE dans la division par n : les nombres géants deviennent alors une poignée de cas à examiner. Ces 20 exercices corrigés couvrent tout le chapitre d'arithmétique de maths expertes : divisibilité dans $\mathbb{Z}$, division euclidienne (y compris pour un dividende négatif), congruences et leur compatibilité avec l'addition et la multiplication, périodicité des puissances et chiffre des unités, critères de divisibilité par 3, 9 et 11 démontrés, résolution d'équations $ax \equiv b [n]$, systèmes de congruences, et raisonnements par disjonction selon le reste. Les derniers exercices sont des applications complètes : clé de contrôle du numéro de sécurité sociale, calcul du jour de la semaine, démonstration qu'une équation n'a AUCUNE solution entière, et chiffrement affine avec son déchiffrement. Chaque correction est rédigée étape par étape, avec les vérifications.

Version en ligne, avec les corrections dépliantes :
mathlvl.fr/exercices-corriges/terminale-maths-expertes/divisibilite-et-congruences

Exercice 1 - Divisibilité dans $\mathbb{Z}$

On dit que l'entier a DIVISE l'entier b , et on note $a \mid b$, s'il existe un entier k tel que $b = ka$. Attention : la définition porte sur des entiers relatifs, et le quotient doit être entier.

1. Déterminer tous les diviseurs POSITIFS de 36.
2. Justifier que $7 \mid 343$ et que $6 \nmid 100$.
3. Démontrer que si $a \mid b$ et $a \mid c$, alors $a \mid (b + c)$ et plus généralement $a \mid (ub + vc)$ pour tous entiers u et v .

Exercice 2 - Division euclidienne, y compris pour un négatif

La division euclidienne de a par $b > 0$ donne l'UNIQUE couple $(q; r)$ d'entiers tel que $a = bq + r$ avec $0 \leq r < b$. La condition sur le reste est essentielle : c'est elle qui assure l'unicité, et elle réserve une surprise pour les dividendes négatifs.

1. Effectuer la division euclidienne de 2026 par 7, puis par 12.
2. Effectuer la division euclidienne de -2026 par 7.
3. Quel est le reste de la division de 2026 par 2026 ? par 1 ?

Exercice 3 - Congruences : définition et premières lectures

On dit que a est CONGRU à b modulo n , et on note $a \equiv b [n]$, lorsque n divise $a - b$ — autrement dit lorsque a et b ont le même reste dans la division par n .

1. Déterminer le reste de 2026 modulo 7, modulo 9 et modulo 11.
2. Les affirmations suivantes sont-elles vraies : $23 \equiv 2 [7]$? $-5 \equiv 3 [8]$? $100 \equiv 4 [6]$?
3. Traduire « n est pair » et « n est un multiple de 5 » à l'aide de congruences.

Exercice 4 - Calculer avec les congruences

Les congruences sont compatibles avec l'addition, la soustraction et la multiplication : si $a \equiv a' [n]$ et $b \equiv b' [n]$, alors $a + b \equiv a' + b' [n]$ et $ab \equiv a'b' [n]$. On peut donc remplacer chaque nombre par son reste AVANT de calculer.

1. Déterminer le reste de 47×53 modulo 9, sans effectuer le produit.
2. Déterminer le reste de $2026 + 1234$ modulo 7.
3. Déterminer le reste de 2026^2 modulo 9.

Exercice 5 - Chiffre des unités d'une grande puissance

Le chiffre des unités d'un entier est son reste modulo 10. Comme les restes des puissances se répètent, on peut déterminer le dernier chiffre d'un nombre qu'on ne saurait pas écrire.

1. Déterminer le chiffre des unités de 7^{2026} .
2. Déterminer le chiffre des unités de 3^{2026} et de 2^{2026} .
3. Expliquer pourquoi les puissances de 5 et de 6 ne posent pas ce problème.

Exercice 6 - Périodicité des restes d'une puissance

La méthode précédente vaut pour n'importe quel module, pas seulement 10. On étudie ici les restes de 5^n modulo 7.

1. Dresser le tableau des restes de 5^n modulo 7 pour n de 1 à 7.
2. En déduire la période, puis le reste de 5^{2026} modulo 7.
3. Déterminer les entiers n pour lesquels $7 \mid 5^n - 1$.

Exercice 7 - Critères de divisibilité par 3, 9 et 11

Les critères appris au collège se démontrent en une ligne avec les congruences. Tout repose sur les restes de 10^k : modulo 9 on a $10 \equiv 1$, modulo 11 on a $10 \equiv -1$.

1. Démontrer qu'un entier est divisible par 9 si et seulement si la somme de ses chiffres l'est. Même question pour 3.
2. Démontrer le critère de divisibilité par 11 (somme alternée des chiffres).
3. Appliquer les deux critères à 4059.

Exercice 8 - Divisibilité d'une expression pour tout n

Pour montrer qu'une expression est divisible par d POUR TOUT entier n , on ne peut pas tester tous les cas — mais il suffit d'examiner les d restes possibles de n .

1. Démontrer que $n(n+1)(n+2)$ est divisible par 6 pour tout entier n .
2. Démontrer que $n^3 - n$ est divisible par 6 pour tout entier n .
3. Démontrer que $n^2 + n$ est toujours pair.

Exercice 9 - Disjonction selon le reste : les carrés

Un carré ne peut pas prendre n'importe quel reste. Établir la table des restes possibles est le point de départ de nombreuses démonstrations d'impossibilité.

1. Déterminer les restes possibles de n^2 modulo 4.
2. Déterminer les restes possibles de n^2 modulo 3.
3. En déduire que si $3 \mid n^2$, alors $3 \mid n$.

Exercice 10 - Résoudre une équation de congruence

Une équation $ax \equiv b \pmod{n}$ porte sur des restes : il suffit donc de tester les n valeurs possibles de x modulo n . Le nombre de solutions, lui, réserve des surprises.

1. Résoudre $5x \equiv 3 \pmod{7}$.
2. Résoudre $6x \equiv 4 \pmod{8}$.
3. Résoudre $4x \equiv 3 \pmod{6}$.

Exercice 11 - Une équation avec un carré

Les équations non linéaires se traitent de la même façon : par examen exhaustif des restes. On résout $x^2 \equiv 1 \pmod{8}$, puis $x^2 \equiv 2 \pmod{5}$.

1. Résoudre $x^2 \equiv 1 \pmod{8}$, et interpréter le résultat.
2. Résoudre $x^2 \equiv 2 \pmod{5}$.
3. En déduire que l'équation $x^2 = 5y + 2$ n'a pas de solution entière.

Exercice 12 - Système de deux congruences

On cherche les entiers x vérifiant simultanément $x \equiv 2 \pmod{5}$ et $x \equiv 3 \pmod{7}$.

1. Déterminer une solution particulière en listant les entiers vérifiant la première condition.
2. Démontrer que l'ensemble des solutions est $x \equiv 17 \pmod{35}$.
3. En déduire le plus petit entier positif solution, et le plus petit supérieur à 1000.

Exercice 13 - Divisibilité d'une suite d'entiers

Les congruences permettent de démontrer qu'une expression dépendant de n est divisible par un entier fixé, sans récurrence.

1. Démontrer que $4^n + 2$ est divisible par 3 pour tout entier naturel n .
2. Démontrer que $3^{2n} - 1$ est divisible par 8 pour tout entier naturel n .
3. Déterminer les entiers n pour lesquels $2^n + 1$ est divisible par 3.

Exercice 14 - Quel jour de la semaine ?

Les jours de la semaine se répètent avec une période de 7 : le calendrier est donc un problème de congruences modulo 7. On sait que le 1^{er} septembre 2026 est un MARDI.

1. Quel jour de la semaine sera le 1^{er} septembre 2027 ?

2. Quel jour de la semaine sera le 1^{er} octobre 2026 ?
3. Quel jour de la semaine tombera le 300^e jour après le 1^{er} septembre 2026 ?

Exercice 15 - La clé du numéro de sécurité sociale

Le numéro de sécurité sociale français comporte 13 chiffres, suivis d'une CLÉ de contrôle à deux chiffres. Cette clé vaut $97 - r$, où r est le reste du nombre à 13 chiffres dans la division par 97. Elle sert à détecter les erreurs de saisie.

1. Calculer la clé associée au numéro $N = 2\,550\,833\,189\,456$, sachant que $N \equiv 81 [97]$.
2. Démontrer que le nombre formé par N suivi de sa clé (c'est-à-dire $100N + \text{clé}$) est divisible par 97.
3. Expliquer pourquoi ce système détecte toute erreur portant sur un seul chiffre.

Exercice 16 - Reste d'une très grande puissance

On veut le reste de 2026^{2026} dans la division par 7. Le nombre a plus de six mille chiffres : seule la réduction modulo 7 permet de conclure.

1. Réduire d'abord la BASE modulo 7.
2. Déterminer la période des puissances de cette base modulo 7.
3. En déduire le reste cherché.

Exercice 17 - Une équation sans solution entière

On veut démontrer que l'équation $x^2 + y^2 = 2023$ n'admet AUCUN couple $(x; y)$ d'entiers pour solution. Tester des valeurs ne prouverait rien : il faut un argument modulo bien choisi.

1. Déterminer les restes possibles de $x^2 + y^2$ modulo 4.
2. Déterminer le reste de 2023 modulo 4, et conclure.
3. L'équation $x^2 + y^2 = 2026$ a-t-elle des solutions ?

Exercice 18 - Les cubes modulo 9

Le même schéma, avec un module moins évident. On veut montrer que l'équation $x^3 + y^3 + z^3 = 4$ n'a aucune solution entière — un résultat qui a résisté longtemps aux tentatives numériques.

1. Déterminer les restes possibles d'un cube modulo 9.
2. En déduire les restes possibles d'une somme de trois cubes modulo 9.
3. Conclure quant à l'équation $x^3 + y^3 + z^3 = 4$.

Exercice 19 - Divisibilité d'une somme de puissances

On étudie la suite définie par $u_n = 2^n + 3^n$ pour $n \geq 1$, et l'on cherche pour quelles valeurs de n elle est divisible par 5.

1. Dresser le tableau des restes de 2^n et de 3^n modulo 5.

2. En déduire les restes de u_n modulo 5, puis les entiers n tels que $5 \mid u_n$.
3. Retrouver ce résultat par un argument direct, sans tableau.

Exercice 20 - Problème de synthèse : un chiffrement affine

On code les lettres de l'alphabet par leur rang : $A = 0, B = 1, \dots, Z = 25$. Le chiffrement affine associe à la lettre de rang x la lettre de rang $y = 5x + 3$ modulo 26. On note f cette transformation.

1. Coder le mot MATH.
2. Montrer que 21 est un « inverse » de 5 modulo 26, c'est-à-dire que $5 \times 21 \equiv 1 [26]$.
3. En déduire la formule de déchiffrement, puis décoder le mot obtenu à la question 1.
4. Expliquer pourquoi le coefficient 5 ne peut pas être remplacé par 13 ni par 2.

Corrigés détaillés

Les corrections des 20 exercices, dans l'ordre des énoncés.

Correction de l'exercice 1 - Divisibilité dans $\mathbb{Z}$

On cherche les entiers positifs d tels que $36 = d \times k$ avec k entier. On les trouve par paires, en partant de 1.

$$36 = 1 \times 36 = 2 \times 18 = 3 \times 12 = 4 \times 9 = 6 \times 6.$$

Les diviseurs positifs de 36 sont donc 1, 2, 3, 4, 6, 9, 12, 18 et 36 : il y en a 9.

On s'arrête à 6 car $6 \times 6 = 36$: au-delà, on retrouverait les mêmes paires dans l'autre sens. Il suffit de tester jusqu'à $\sqrt{36}$.

$7 \mid 343$: on cherche un entier k tel que $343 = 7k$. Comme $343 = 7 \times 49$, l'entier $k = 49$ convient ✓. (On reconnaît d'ailleurs $343 = 7^3$.)

$6 \nmid 100$: la division de 100 par 6 donne $100 = 6 \times 16 + 4$. Le reste 4 n'est pas nul, donc 6 ne divise pas 100.

Passons à la démonstration. Par hypothèse, il existe des entiers k et k' tels que $b = ka$ et $c = k'a$.

Alors $b + c = ka + k'a = (k + k')a$. Comme $k + k'$ est un entier, on a bien $a \mid (b + c)$.

Plus généralement, $ub + vc = uka + vk'a = (uk + vk')a$, et $uk + vk'$ est un entier : donc $a \mid (ub + vc)$.

Ce résultat est l'outil de base de tout le chapitre : toute COMBINAISON LINÉAIRE ENTIÈRE de multiples de a est encore un multiple de a .

Exemple d'utilisation : si a divise b et $b + c$, alors a divise $(b + c) - b = c$.

Réponse. Diviseurs positifs de 36 : 1, 2, 3, 4, 6, 9, 12, 18, 36 · $343 = 7 \times 49$ donc $7 \mid 343$ · $100 = 6 \times 16 + 4$ donc $6 \nmid 100$ · si $a \mid b$ et $a \mid c$ alors $a \mid (ub + vc)$.

Rappel de cours. $a \mid b \Leftrightarrow \exists k \in \mathbb{Z}, b = ka$. Pour lister les diviseurs de n , on teste les entiers jusqu'à $\sqrt{n}$ et on forme les paires. Combinaison linéaire : $a \mid b$ et $a \mid c \Rightarrow a \mid (ub + vc)$.

Erreur fréquente. Écrire $a \mid b$ alors qu'on veut dire $\frac{b}{a}$. La notation $a \mid b$ est une AFFIRMATION (« a divise b »), pas un nombre.

Correction de l'exercice 2 - Division euclidienne, y compris pour un négatif

Division par 7 : on cherche le plus grand multiple de 7 inférieur ou égal à 2026. Comme $7 \times 289 = 2023$ et $7 \times 290 = 2030 > 2026$, le quotient est 289.

Le reste vaut $2026 - 2023 = 3$. On écrit $2026 = 7 \times 289 + 3$, avec $0 \leq 3 < 7$ ✓.

Division par 12 : $12 \times 168 = 2016$ et $12 \times 169 = 2028 > 2026$. Donc $2026 = 12 \times 168 + 10$, avec $0 \leq 10 < 12$ ✓.

Pour -2026 , l'erreur classique consiste à écrire $-2026 = 7 \times (-289) - 3$: le « reste » -3 est négatif, donc INTERDIT.

Il faut descendre d'un cran sur le quotient : $7 \times (-290) = -2030$, et $-2026 - (-2030) = 4$.

On écrit donc $-2026 = 7 \times (-290) + 4$, avec $0 \leq 4 < 7$ ✓. Le reste est 4, pas 3 ni -3 .

Contrôle utile : la somme du reste « naïf » 3 et du reste correct 4 vaut 7. C'est général : si a a pour reste $r \neq 0$, alors $-a$ a pour reste $b - r$.

Division de 2026 par 2026 : $2026 = 2026 \times 1 + 0$, le reste est 0 — normal, tout entier se

divise lui-même.

Division par 1 : $2026 = 1 \times 2026 + 0$, le reste est 0. Le reste dans une division par 1 est toujours nul, puisqu'il doit vérifier $0 \leq r < 1$.

Réponse. $2026 = 7 \times 289 + 3$, $2026 = 12 \times 168 + 10$, $-2026 = 7 \times (-290) + 4$ (reste 4, pas -3) · reste nul dans les deux derniers cas.

Rappel de cours. $a = bq + r$ avec $0 \leq r < b$: le reste est toujours POSITIF ou nul et strictement inférieur au diviseur. Pour un dividende négatif, on prend le quotient immédiatement inférieur.

Erreur fréquente. Annoncer un reste négatif. $-2026 = 7 \times (-289) - 3$ est une égalité vraie, mais ce n'est PAS la division euclidienne : -3 ne vérifie pas $0 \leq r < 7$.

Correction de l'exercice 3 - Congruences : définition et premières lectures

Modulo 7 : on a vu $2026 = 7 \times 289 + 3$, donc $2026 \equiv 3 [7]$.

Modulo 9 : $9 \times 225 = 2025$, donc $2026 = 9 \times 225 + 1$ et $2026 \equiv 1 [9]$.

Contrôle par la somme des chiffres, qui sera justifiée à l'exercice 7 : $2 + 0 + 2 + 6 = 10$, et $10 \equiv 1 [9]$ ✓.

Modulo 11 : $11 \times 184 = 2024$, donc $2026 = 11 \times 184 + 2$ et $2026 \equiv 2 [11]$.

$23 \equiv 2 [7]$: on calcule $23 - 2 = 21 = 7 \times 3$. Comme $7 \mid 21$, l'affirmation est VRAIE.

$-5 \equiv 3 [8]$: $-5 - 3 = -8$, qui est bien divisible par 8. L'affirmation est VRAIE — un nombre négatif peut tout à fait être congru à un positif.

$100 \equiv 4 [6]$: $100 - 4 = 96 = 6 \times 16$ ✓. L'affirmation est VRAIE (on retrouve $100 = 6 \times 16 + 4$ de l'exercice 1).

Traduction : « n est pair » signifie que 2 divise n , c'est-à-dire $n \equiv 0 [2]$. « n est impair » s'écrit $n \equiv 1 [2]$.

« n est un multiple de 5 » signifie $5 \mid n$, c'est-à-dire $n \equiv 0 [5]$.

Règle générale à retenir : $d \mid n \Leftrightarrow n \equiv 0 [d]$. Toute question de divisibilité peut donc s'écrire comme une congruence, et réciproquement.

Réponse. $2026 \equiv 3 [7]$, $2026 \equiv 1 [9]$, $2026 \equiv 2 [11]$ · les trois affirmations sont vraies · n pair $\Leftrightarrow n \equiv 0 [2]$ · n multiple de 5 $\Leftrightarrow n \equiv 0 [5]$.

Rappel de cours. $a \equiv b [n] \Leftrightarrow n \mid (a - b) \Leftrightarrow a$ et b ont le même reste modulo n . Et $d \mid n \Leftrightarrow n \equiv 0 [d]$.

Erreur fréquente. Croire que $a \equiv b [n]$ impose $0 \leq b < n$. Toute autre valeur congrue convient : $23 \equiv 2 \equiv 9 \equiv -5 [7]$.

Correction de l'exercice 4 - Calculer avec les congruences

On remplace chaque facteur par son reste modulo 9. Pour 47 : $47 = 9 \times 5 + 2$, donc $47 \equiv 2 [9]$.

Pour 53 : $53 = 9 \times 5 + 8$, donc $53 \equiv 8 [9]$.

Par compatibilité avec le produit : $47 \times 53 \equiv 2 \times 8 = 16 [9]$.

On réduit encore : $16 = 9 + 7$, donc $16 \equiv 7 [9]$. Le reste cherché est 7.

Contrôle : $47 \times 53 = 2491$, et $2491 = 9 \times 276 + 7$ ✓. Le calcul modulo 9 a évité de poser la multiplication.

Deuxième question : $2026 \equiv 3 [7]$ (exercice 3). Pour 1234 : $7 \times 176 = 1232$, donc $1234 \equiv 2 [7]$.

Par compatibilité avec la somme : $2026 + 1234 \equiv 3 + 2 = 5 \pmod{7}$. Le reste est 5.

Contrôle : $2026 + 1234 = 3260$, et $3260 = 7 \times 465 + 5$ ✓.

Troisième question : $2026 \equiv 1 \pmod{9}$, donc $2026^2 \equiv 1^2 = 1 \pmod{9}$.

La compatibilité avec le produit se transmet aux puissances : si $a \equiv b \pmod{n}$, alors $a^k \equiv b^k \pmod{n}$ pour tout entier $k \geq 1$.

C'est cette propriété qui rendra calculables, à l'exercice 5, des puissances de plusieurs milliers de chiffres.

Attention en revanche : la DIVISION n'est pas compatible. De $6 \equiv 12 \pmod{6}$ on ne peut pas déduire $3 \equiv 6 \pmod{6}$, qui est faux.

Réponse. $47 \times 53 \equiv 7 \pmod{9}$ · $2026 + 1234 \equiv 5 \pmod{7}$ · $2026^2 \equiv 1 \pmod{9}$.

Rappel de cours. Compatibilité : somme, différence, produit et puissances.

$a \equiv b \pmod{n} \Rightarrow a^k \equiv b^k \pmod{n}$. En revanche, on ne SIMPLIFIE pas une congruence par un facteur sans précaution.

Erreur fréquente. Diviser les deux membres d'une congruence. $4 \times 3 \equiv 4 \times 5 \pmod{8}$ est vrai, mais $3 \equiv 5 \pmod{8}$ est faux.

Correction de l'exercice 5 - Chiffre des unités d'une grande puissance

On calcule les premières puissances de 7 modulo 10 : $7^1 \equiv 7$, $7^2 = 49 \equiv 9$, $7^3 \equiv 9 \times 7 = 63 \equiv 3$, $7^4 \equiv 3 \times 7 = 21 \equiv 1 \pmod{10}$.

Dès qu'on retombe sur 1, le cycle recommence : $7^5 \equiv 7$, $7^6 \equiv 9$, etc. La suite des restes est PÉRIODIQUE de période 4 : 7, 9, 3, 1, 7, 9, 3, 1, ...

Le reste de 7^n ne dépend donc que du reste de n modulo 4.

Or $2026 = 4 \times 506 + 2$, donc $2026 \equiv 2 \pmod{4}$.

Donc $7^{2026} \equiv 7^2 \equiv 9 \pmod{10}$: le chiffre des unités de 7^{2026} est 9.

Rédaction rigoureuse : $7^{2026} = 7^{4 \times 506 + 2} = (7^4)^{506} \times 7^2 \equiv 1^{506} \times 49 \equiv 9 \pmod{10}$.

Pour 3 : $3^1 \equiv 3$, $3^2 \equiv 9$, $3^3 \equiv 27 \equiv 7$, $3^4 \equiv 21 \equiv 1 \pmod{10}$. Période 4 également.

Comme $2026 \equiv 2 \pmod{4}$, on a $3^{2026} \equiv 3^2 \equiv 9 \pmod{10}$: le chiffre des unités est 9.

Pour 2 : 2, 4, 8, 16 $\equiv$ 6, 32 $\equiv$ 2... La suite est 2, 4, 8, 6, de période 4 (à partir de l'exposant 1).

Comme $2026 \equiv 2 \pmod{4}$, on a $2^{2026} \equiv 2^2 \equiv 4 \pmod{10}$: le chiffre des unités est 4.

Puissances de 5 : $5^2 = 25 \equiv 5$, et par récurrence $5^n \equiv 5 \pmod{10}$ pour tout $n \geq 1$. Le chiffre des unités est TOUJOURS 5.

Puissances de 6 : $6^2 = 36 \equiv 6 \pmod{10}$, donc de même $6^n \equiv 6 \pmod{10}$. La période vaut 1 : ces deux chiffres sont dits « automorphes » pour la multiplication.

Réponse. Chiffre des unités de 7^{2026} : 9 · de 3^{2026} : 9 · de 2^{2026} : 4 · les puissances de 5 finissent toujours par 5, celles de 6 toujours par 6.

Rappel de cours. Méthode : calculer les premières puissances modulo n jusqu'à retomber sur 1 (ou sur une valeur déjà vue), en déduire la PÉRIODE p , puis réduire l'exposant modulo p .

Erreur fréquente. Réduire l'exposant modulo 10 au lieu de le réduire modulo la PÉRIODE. Ce sont deux modules différents : 10 pour le résultat, 4 pour l'exposant.

Correction de l'exercice 6 - Périodicité des restes d'une puissance

On calcule de proche en proche, en réduisant à chaque étape (c'est ce qui garde les nombres petits).

$$5^1 \equiv 5 \pmod{7}.$$

$$5^2 = 25 = 7 \times 3 + 4, \text{ donc } 5^2 \equiv 4 \pmod{7}.$$

$$5^3 \equiv 5^2 \times 5 \equiv 4 \times 5 = 20 \equiv 6 \pmod{7}.$$

$$5^4 \equiv 6 \times 5 = 30 \equiv 2 \pmod{7}.$$

$$5^5 \equiv 2 \times 5 = 10 \equiv 3 \pmod{7}.$$

$$5^6 \equiv 3 \times 5 = 15 \equiv 1 \pmod{7}.$$

$$5^7 \equiv 1 \times 5 = 5 \pmod{7} : \text{on retrouve le reste de } 5^1, \text{ le cycle recommence.}$$

La suite des restes est donc 5, 4, 6, 2, 3, 1 puis se répète : la PÉRIODE est 6.

Pour 5^{2026} , on réduit l'exposant modulo 6 : $2026 = 6 \times 337 + 4$, donc $2026 \equiv 4 \pmod{6}$.

Donc $5^{2026} \equiv 5^4 \equiv 2 \pmod{7}$: le reste de 5^{2026} dans la division par 7 est 2.

$$\text{Rédaction : } 5^{2026} = (5^6)^{337} \times 5^4 \equiv 1^{337} \times 2 \equiv 2 \pmod{7}.$$

$$\text{Dernière question : } 7 \mid 5^n - 1 \text{ équivaut à } 5^n \equiv 1 \pmod{7}.$$

D'après le tableau, le reste 1 est atteint pour $n = 6$, et uniquement là dans une période complète.

Comme la suite est périodique de période 6, les exposants convenables sont exactement les MULTIPLES DE 6 (avec $n \geq 1$, et aussi $n = 0$ puisque $5^0 = 1$).

$$\text{Contrôle : } 5^6 = 15\,625 \text{ et } 15\,625 - 1 = 15\,624 = 7 \times 2232 \checkmark.$$

Réponse. Restes de 5^n modulo 7 : 5, 4, 6, 2, 3, 1, période $6 \cdot 5^{2026} \equiv 2 \pmod{7} \cdot 7 \mid 5^n - 1$ si et seulement si n est un multiple de 6.

Rappel de cours. On calcule les puissances de proche en proche EN RÉDUISANT à chaque étape. Le premier retour à 1 donne la période, et tout exposant se réduit alors modulo cette période.

Erreur fréquente. Calculer $5^4 = 625$ puis réduire. C'est possible ici, mais impraticable pour 5^{2026} : le réflexe est de réduire à CHAQUE multiplication.

Correction de l'exercice 7 - Critères de divisibilité par 3, 9 et 11

Écrivons un entier N avec ses chiffres : $N = a_p 10^p + \dots + a_1 10 + a_0$.

Modulo 9 : comme $10 \equiv 1 \pmod{9}$, on a $10^k \equiv 1^k = 1 \pmod{9}$ pour tout k .

Donc $N \equiv a_p + \dots + a_1 + a_0 \pmod{9}$: un entier est congru à la somme de ses chiffres modulo 9.

En particulier $9 \mid N$ si et seulement si 9 divise la somme des chiffres. Le critère est démontré.

Pour 3, le raisonnement est identique : $10 \equiv 1 \pmod{3}$ aussi, donc N est congru à la somme de ses chiffres modulo 3, et le critère est le même.

Modulo 11, la situation change : $10 \equiv -1 \pmod{11}$, donc $10^k \equiv (-1)^k \pmod{11}$, qui vaut 1 si k est pair et -1 s'il est impair.

D'où $N \equiv a_0 - a_1 + a_2 - a_3 + \dots \pmod{11}$: c'est la somme ALTERNÉE des chiffres, en commençant par le chiffre des unités avec le signe +.

Donc $11 \mid N$ si et seulement si 11 divise cette somme alternée.

Application à 4059. Somme des chiffres : $4 + 0 + 5 + 9 = 18$, qui est divisible par 9 : donc $9 \mid 4059$.

Contrôle : $4059 = 9 \times 451$ ✓.

Somme alternée, en partant des unités : $9 - 5 + 0 - 4 = 0$. Or $11 \mid 0$, donc $11 \mid 4059$.

Contrôle : $4059 = 11 \times 369$ ✓.

Le nombre 4059 est donc divisible par 9 et par 11, donc par 99 : en effet $4059 = 99 \times 41$.

Réponse. $10 \equiv 1 [9]$ donne $N \equiv$ somme des chiffres modulo 9 (et modulo 3) ·

$10 \equiv -1 [11]$ donne $N \equiv$ somme alternée modulo 11 · 4059 : somme 18 donc divisible par 9 ; somme alternée 0 donc divisible par 11 ; et $4059 = 99 \times 41$.

Rappel de cours. Tous les critères de divisibilité viennent du reste de 10 modulo n : $10 \equiv 1 [3]$ et $[9]$, $10 \equiv -1 [11]$, $10 \equiv 0 [2]$ et $[5]$ — d'où le critère par le seul chiffre des unités.

Erreur fréquente. Commencer la somme alternée par le chiffre de gauche. C'est le chiffre des UNITÉS qui porte le signe + (il correspond à 10^0).

Correction de l'exercice 8 - Divisibilité d'une expression pour tout n

Première méthode, par les facteurs. n , $n + 1$ et $n + 2$ sont trois entiers CONSÉCUTIFS.

Parmi trois entiers consécutifs, il y en a au moins un pair : leur produit est donc divisible par 2.

Parmi trois entiers consécutifs, il y en a exactement un divisible par 3 (les restes modulo 3 sont 0, 1 et 2 dans un ordre ou un autre) : le produit est donc divisible par 3.

Le produit est divisible par 2 et par 3, qui n'ont aucun facteur commun : il est donc divisible par 6.

Seconde méthode, par disjonction sur le reste modulo 6. On dresse un tableau : pour $n \equiv 0, 1, 2, 3, 4, 5 [6]$, on calcule $n(n + 1)(n + 2)$ modulo 6.

$n \equiv 0 : 0 \times 1 \times 2 = 0$. $n \equiv 1 : 1 \times 2 \times 3 = 6 \equiv 0$. $n \equiv 2 : 2 \times 3 \times 4 = 24 \equiv 0$.

$n \equiv 3 : 3 \times 4 \times 5 = 60 \equiv 0$. $n \equiv 4 : 4 \times 5 \times 6 = 120 \equiv 0$. $n \equiv 5 : 5 \times 6 \times 7 = 210 \equiv 0$.

Dans les six cas le reste est nul : $6 \mid n(n + 1)(n + 2)$ pour tout n ✓. Les deux méthodes concluent, la première est plus élégante.

Deuxième question : on factorise $n^3 - n = n(n^2 - 1) = n(n - 1)(n + 1) = (n - 1)n(n + 1)$.

C'est encore un produit de trois entiers consécutifs : il est divisible par 6 d'après la question 1.

Troisième question : $n^2 + n = n(n + 1)$, produit de deux entiers consécutifs.

L'un des deux est nécessairement pair, donc le produit est pair : $n^2 + n$ est toujours divisible par 2.

Vérification sur quelques valeurs : $n = 3$ donne 12 ✓, $n = -4$ donne 12 ✓, $n = 0$ donne 0 ✓.

Réponse. $n(n + 1)(n + 2)$ est un produit de trois entiers consécutifs : divisible par 2 et par 3, donc par 6 · $n^3 - n = (n - 1)n(n + 1)$, même conclusion · $n^2 + n = n(n + 1)$ est un produit de deux entiers consécutifs, donc pair.

Rappel de cours. Deux stratégies : reconnaître un produit d'entiers CONSÉCUTIFS, ou faire une disjonction sur les d restes possibles. La seconde marche toujours, la première est plus courte quand elle s'applique.

Erreur fréquente. Conclure « divisible par 6 » à partir de « divisible par 2 et par 4 ». Ce raisonnement exige que les deux diviseurs soient PREMIERS ENTRE EUX, ce qui est le cas de 2 et 3.

Correction de l'exercice 9 - Disjonction selon le reste : les carrés

Tout entier n est congru à 0, 1, 2 ou 3 modulo 4. On examine les quatre cas.

$$n \equiv 0 [4] : n^2 \equiv 0 [4].$$

$$n \equiv 1 [4] : n^2 \equiv 1 [4].$$

$$n \equiv 2 [4] : n^2 \equiv 4 \equiv 0 [4].$$

$$n \equiv 3 [4] : n^2 \equiv 9 \equiv 1 [4].$$

Les seuls restes possibles pour un carré modulo 4 sont donc 0 et 1. En particulier, AUCUN carré n'est congru à 2 ou 3 modulo 4.

Lecture simple : un carré de nombre pair est congru à 0, un carré de nombre impair est congru à 1.

Modulo 3, on examine les trois cas. $n \equiv 0 : n^2 \equiv 0$. $n \equiv 1 : n^2 \equiv 1$. $n \equiv 2 : n^2 \equiv 4 \equiv 1 [3]$.

Les restes possibles sont donc 0 et 1 : un carré n'est jamais congru à 2 modulo 3.

Dernière question. Supposons $3 \mid n^2$, c'est-à-dire $n^2 \equiv 0 [3]$.

D'après le tableau, le reste 0 pour n^2 ne s'obtient que dans le cas $n \equiv 0 [3]$: les deux autres cas donnent le reste 1.

Donc $n \equiv 0 [3]$, c'est-à-dire $3 \mid n$. La réciproque étant évidente, on a l'équivalence.

Ce résultat est exactement ce qui sert à démontrer que $\sqrt{3}$ est irrationnel — et le même raisonnement modulo 2 traite le cas de $\sqrt{2}$.

Réponse. $n^2 \equiv 0$ ou $1 [4] \cdot n^2 \equiv 0$ ou $1 [3] \cdot 3 \mid n^2 \Rightarrow 3 \mid n$, puisque seul le cas $n \equiv 0 [3]$ donne un carré divisible par 3.

Rappel de cours. Table des carrés : modulo 4, un carré vaut 0 ou 1 ; modulo 3, 0 ou 1 ; modulo 8, 0, 1 ou 4. Ces tables servent à prouver qu'une équation n'a pas de solution.

Erreur fréquente. Oublier des cas dans la disjonction. Modulo 4, il faut examiner les QUATRE restes, même si 2 et 3 redonnent les mêmes valeurs que 0 et 1.

Correction de l'exercice 10 - Résoudre une équation de congruence

Première équation. On teste les sept restes possibles $x \equiv 0, 1, \dots, 6 [7]$, en calculant $5x$ modulo 7.

$$x \equiv 0 \rightarrow 0 ; x \equiv 1 \rightarrow 5 ; x \equiv 2 \rightarrow 10 \equiv 3 \checkmark ; x \equiv 3 \rightarrow 15 \equiv 1 ; x \equiv 4 \rightarrow 20 \equiv 6 ; x \equiv 5 \rightarrow 25 \equiv 4 ; x \equiv 6 \rightarrow 30 \equiv 2.$$

Une seule valeur convient : $x \equiv 2 [7]$. L'ensemble des solutions est $\{2 + 7k, k \in \mathbb{Z}\}$.

Méthode plus rapide : chercher un « inverse » de 5 modulo 7, c'est-à-dire un entier u tel que $5u \equiv 1 [7]$. Ici $5 \times 3 = 15 \equiv 1 [7]$, donc $u = 3$.

En multipliant l'équation par 3 : $15x \equiv 9 [7]$, soit $x \equiv 2 [7] \checkmark$ — même résultat.

Deuxième équation, $6x \equiv 4 [8]$. On teste les huit restes : $x \equiv 0 \rightarrow 0$; $1 \rightarrow 6$; $2 \rightarrow 12 \equiv 4 \checkmark$; $3 \rightarrow 18 \equiv 2$; $4 \rightarrow 24 \equiv 0$; $5 \rightarrow 30 \equiv 6$; $6 \rightarrow 36 \equiv 4 \checkmark$; $7 \rightarrow 42 \equiv 2$.

Il y a cette fois DEUX solutions modulo 8 : $x \equiv 2 [8]$ et $x \equiv 6 [8]$.

On peut les réunir : les solutions sont les entiers pairs non multiples de 4, c'est-à-dire $x \equiv 2 [4]$.

Troisième équation, $4x \equiv 3 [6]$. On teste : $x \equiv 0 \rightarrow 0$; $1 \rightarrow 4$; $2 \rightarrow 8 \equiv 2$; $3 \rightarrow 12 \equiv 0$;

$$4 \rightarrow 16 \equiv 4 ; 5 \rightarrow 20 \equiv 2.$$

Les valeurs atteintes sont 0, 2 et 4 : uniquement des nombres PAIRS. La valeur 3 n'est jamais atteinte.

L'équation $4x \equiv 3 [6]$ n'a donc AUCUNE solution.

Explication : $4x$ et 6 sont pairs, donc $4x - 6k$ est toujours pair et ne peut valoir 3. Plus généralement, $ax \equiv b [n]$ a des solutions si et seulement si le PGCD de a et n divise b — ici $\text{PGCD}(4; 6) = 2$ ne divise pas 3.

Contrôle du deuxième cas avec ce critère : $\text{PGCD}(6; 8) = 2$ divise 4 ✓, et il y a exactement 2 solutions modulo 8 — autant que la valeur du PGCD.

Réponse. $5x \equiv 3 [7] \Rightarrow x \equiv 2 [7] \cdot 6x \equiv 4 [8] \Rightarrow x \equiv 2$ ou $6 [8]$, soit $x \equiv 2 [4] \cdot 4x \equiv 3 [6]$ n'a pas de solution.

Rappel de cours. $ax \equiv b [n]$: on teste les n restes. L'équation a des solutions si et seulement si $\text{PGCD}(a; n) \mid b$, et il y en a alors exactement $\text{PGCD}(a; n)$ modulo n .

Erreur fréquente. Croire qu'il y a toujours une solution unique. Contrairement à $ax = b$ dans $\mathbb{R}$, une équation de congruence peut avoir 0, 1 ou plusieurs solutions.

Correction de l'exercice 11 - Une équation avec un carré

On teste les huit restes possibles modulo 8, en calculant x^2 .

$$x \equiv 0 \rightarrow 0 ; 1 \rightarrow 1 \checkmark ; 2 \rightarrow 4 ; 3 \rightarrow 9 \equiv 1 \checkmark ; 4 \rightarrow 16 \equiv 0.$$

$$5 \rightarrow 25 \equiv 1 \checkmark ; 6 \rightarrow 36 \equiv 4 ; 7 \rightarrow 49 \equiv 1 \checkmark.$$

Les solutions sont $x \equiv 1, 3, 5$ ou $7 [8]$: ce sont exactement les restes IMPAIRS.

Interprétation : le carré de tout nombre impair est congru à 1 modulo 8. C'est un résultat utile, plus fin que « un carré impair est congru à 1 modulo 4 ».

On note au passage que la table des carrés modulo 8 est $\{0; 1; 4\}$: les restes 2, 3, 5, 6, 7 sont impossibles pour un carré.

$$\text{Deuxième équation, modulo 5. } x \equiv 0 \rightarrow 0 ; 1 \rightarrow 1 ; 2 \rightarrow 4 ; 3 \rightarrow 9 \equiv 4 ; 4 \rightarrow 16 \equiv 1.$$

Les restes possibles d'un carré modulo 5 sont 0, 1 et 4. La valeur 2 n'y figure pas.

L'équation $x^2 \equiv 2 [5]$ n'a donc AUCUNE solution.

Troisième question : l'équation $x^2 = 5y + 2$ signifie que $x^2 - 2$ est un multiple de 5, c'est-à-dire $x^2 \equiv 2 [5]$.

Or on vient de montrer que cette congruence est impossible. Donc l'équation $x^2 = 5y + 2$ n'a pas de solution entière.

C'est le schéma type d'une démonstration d'impossibilité : on passe de l'équation à une congruence, puis on montre que le reste demandé n'appartient pas à la table.

Contrôle empirique : les carrés 0, 1, 4, 9, 16, 25, 36, 49 donnent modulo 5 les restes 0, 1, 4, 4, 1, 0, 1, 4 — jamais 2 ✓.

Réponse. $x^2 \equiv 1 [8] \Leftrightarrow x$ impair $\cdot x^2 \equiv 2 [5]$ n'a pas de solution (les carrés valent 0, 1 ou 4 modulo 5) $\cdot$ donc $x^2 = 5y + 2$ n'a pas de solution entière.

Rappel de cours. Pour montrer qu'une équation n'a pas de solution entière : la réduire modulo un entier bien choisi, puis constater que le reste exigé n'est pas dans la table des restes possibles.

Erreur fréquente. Conclure trop vite à l'impossibilité avec un mauvais module. Modulo 3, $x^2 = 5y + 2$ ne donne aucune contradiction : c'est le choix du module 5 qui fait marcher l'argument.

Correction de l'exercice 12 - Système de deux congruences

Les entiers vérifiant $x \equiv 2 [5]$ sont 2, 7, 12, 17, 22, 27, 32, ... (on ajoute 5 à chaque fois).

On teste la seconde condition $x \equiv 3 [7]$ sur cette liste : 2 (→ 2), 7 (→ 0), 12 (→ 5), 17 (→ 3) ✓.

Une solution particulière est donc $x_0 = 17$. Contrôle : $17 = 5 \times 3 + 2$ ✓ et $17 = 7 \times 2 + 3$ ✓.

Passons au cas général. Soit x une solution quelconque. Alors $x - 17$ est divisible par 5 (car $x \equiv 17 \equiv 2 [5]$) et par 7 (car $x \equiv 17 \equiv 3 [7]$).

Comme 5 et 7 n'ont aucun facteur commun, $x - 17$ est divisible par leur produit 35.

Donc $x \equiv 17 [35]$. Réciproquement, si $x \equiv 17 [35]$, alors $x \equiv 17 \equiv 2 [5]$ et $x \equiv 17 \equiv 3 [7]$: les deux conditions sont vérifiées.

L'ensemble des solutions est donc exactement $\{17 + 35k, k \in \mathbb{Z}\}$.

Remarque de méthode : il y a bien UNE classe de solutions modulo $5 \times 7 = 35$. C'est le contenu du théorème des restes chinois, valable dès que les deux modules sont premiers entre eux.

Le plus petit entier positif solution est 17.

Pour le plus petit supérieur à 1000 : on cherche le plus petit k tel que $17 + 35k > 1000$, soit $35k > 983$, c'est-à-dire $k > 28,09$.

Donc $k = 29$, et la solution est $17 + 35 \times 29 = 17 + 1015 = 1032$.

Contrôle : $1032 = 5 \times 206 + 2$ ✓ et $1032 = 7 \times 147 + 3$ ✓.

Réponse. Solution particulière : 17 · l'ensemble des solutions est $x \equiv 17 [35]$ · plus petit entier positif : 17 · plus petit supérieur à 1000 : 1032.

Rappel de cours. Système $x \equiv a [m]$ et $x \equiv b [n]$ avec m et n premiers entre eux : il existe une unique classe de solutions modulo mn . On trouve une solution particulière par balayage, puis on conclut.

Erreur fréquente. Écrire directement $x \equiv 2 + 3 [35]$. Les congruences ne s'additionnent pas ainsi : il faut une solution particulière, obtenue par recherche.

Correction de l'exercice 13 - Divisibilité d'une suite d'entiers

Première question : on cherche le reste de 4 modulo 3. Comme $4 = 3 + 1$, on a $4 \equiv 1 [3]$.

Par compatibilité avec les puissances : $4^n \equiv 1^n = 1 [3]$, quel que soit n .

Donc $4^n + 2 \equiv 1 + 2 = 3 \equiv 0 [3]$: l'expression est divisible par 3 pour tout n .

Contrôle : $n = 0 \rightarrow 3$ ✓ ; $n = 1 \rightarrow 6$ ✓ ; $n = 2 \rightarrow 18$ ✓ ; $n = 3 \rightarrow 66 = 3 \times 22$ ✓.

Deuxième question : on regroupe la puissance, $3^{2n} = (3^2)^n = 9^n$.

Or $9 = 8 + 1$, donc $9 \equiv 1 [8]$, et $9^n \equiv 1^n = 1 [8]$.

Donc $3^{2n} - 1 \equiv 1 - 1 = 0 [8]$: l'expression est divisible par 8 pour tout n .

Contrôle : $n = 1 \rightarrow 8$ ✓ ; $n = 2 \rightarrow 80 = 8 \times 10$ ✓ ; $n = 3 \rightarrow 728 = 8 \times 91$ ✓.

Troisième question : on étudie les restes de 2^n modulo 3. $2 \equiv -1 [3]$, ce qui simplifie tout.

Donc $2^n \equiv (-1)^n [3]$: le reste vaut 1 si n est pair, et $-1 \equiv 2$ si n est impair.

Alors $2^n + 1 \equiv (-1)^n + 1 [3]$.

Si n est pair : $2^n + 1 \equiv 1 + 1 = 2 [3]$, donc l'expression n'est PAS divisible par 3.

Si n est impair : $2^n + 1 \equiv -1 + 1 = 0 \pmod{3}$, donc l'expression EST divisible par 3.

Conclusion : $3 \mid 2^n + 1$ si et seulement si n est impair.

Contrôle : $n = 1 \rightarrow 3 \checkmark$; $n = 2 \rightarrow 5 \times$; $n = 3 \rightarrow 9 \checkmark$; $n = 4 \rightarrow 17 \times$; $n = 5 \rightarrow 33 = 3 \times 11 \checkmark$.

Réponse. $4 \equiv 1 \pmod{3}$ donne $4^n + 2 \equiv 0 \pmod{3}$ · $3^{2n} = 9^n$ et $9 \equiv 1 \pmod{8}$ donnent $3^{2n} - 1 \equiv 0 \pmod{8}$ · $3 \mid 2^n + 1$ si et seulement si n est impair.

Rappel de cours. Le bon réflexe : chercher une base congrue à 1 ou à -1 . $a \equiv 1 \pmod{n}$ donne $a^k \equiv 1$; $a \equiv -1 \pmod{n}$ donne un résultat qui alterne selon la parité de k .

Erreur fréquente. Se lancer dans une récurrence. Elle fonctionne, mais la congruence donne le résultat en deux lignes — et fournit en prime la condition NÉCESSAIRE de la question 3.

Correction de l'exercice 14 - Quel jour de la semaine ?

On numérote les jours : 0 pour mardi (le jour de référence), 1 pour mercredi, 2 pour jeudi, et ainsi de suite jusqu'à 6 pour lundi.

Avancer de d jours revient à ajouter d modulo 7.

Du 1^{er} septembre 2026 au 1^{er} septembre 2027, il s'écoule une année complète. L'année 2027 n'est pas bissextile, et la période couverte compte 365 jours.

Or $365 = 7 \times 52 + 1$, donc $365 \equiv 1 \pmod{7}$.

On avance donc d'un seul jour : le 1^{er} septembre 2027 sera un MERCREDI.

C'est la règle générale : d'une année sur l'autre, une date recule d'un jour dans la semaine — et de deux jours si un 29 février est traversé.

Deuxième question : septembre compte 30 jours, donc du 1^{er} septembre au 1^{er} octobre il s'écoule 30 jours.

$30 = 7 \times 4 + 2$, donc $30 \equiv 2 \pmod{7}$: on avance de deux jours.

Mardi + 2 donne JEUDI : le 1^{er} octobre 2026 est un jeudi.

Troisième question : $300 = 7 \times 42 + 6$, donc $300 \equiv 6 \pmod{7}$.

On avance de 6 jours à partir de mardi. En numérotation : $0 + 6 = 6$, qui correspond à LUNDI.

Autre façon de le voir : avancer de 6 jours revient à reculer d'un jour (car $6 \equiv -1 \pmod{7}$), et la veille de mardi est lundi $\checkmark$.

Contrôle du raisonnement sur un petit cas : 7 jours après un mardi, on est encore un mardi, et $7 \equiv 0 \pmod{7} \checkmark$.

Réponse. 1^{er} septembre 2027 : mercredi ($365 \equiv 1 \pmod{7}$) · 1^{er} octobre 2026 : jeudi ($30 \equiv 2 \pmod{7}$) · 300^e jour après : lundi ($300 \equiv 6 \equiv -1 \pmod{7}$).

Rappel de cours. Tout problème de calendrier se ramène à un calcul modulo 7.

Repères : $365 \equiv 1 \pmod{7}$, $366 \equiv 2 \pmod{7}$, $30 \equiv 2 \pmod{7}$, $31 \equiv 3 \pmod{7}$, $28 \equiv 0 \pmod{7}$.

Erreur fréquente. Compter le jour de départ dans le nombre de jours écoulés. Du 1^{er} au 1^{er} du mois suivant, il s'écoule le nombre de jours du mois, pas ce nombre plus un.

Correction de l'exercice 15 - La clé du numéro de sécurité sociale

Par définition, la clé vaut $97 - r$ où r est le reste de N modulo 97.

Ici $r = 81$, donc la clé est $97 - 81 = 16$.

Le numéro complet s'écrit donc 2 550 833 189 456 16.

Remarque : la clé est toujours comprise entre 1 et 97, ce qui explique qu'elle occupe

deux chiffres. Le cas $r = 0$ donne la clé 97.

Deuxième question. On veut montrer que 97 divise $100N + \text{clé}$, c'est-à-dire $100N + 97 - r$.

Le terme 97 est divisible par 97, il ne change rien à la congruence :

$$100N + 97 - r \equiv 100N - r \pmod{97}.$$

Or $N \equiv r \pmod{97}$ par définition du reste, donc $100N \equiv 100r \pmod{97}$.

$$\text{D'où } 100N - r \equiv 100r - r = 99r \pmod{97}.$$

Et $99 = 97 + 2$, donc $99 \equiv 2 \pmod{97}$, ce qui donne $99r \equiv 2r \pmod{97}$: cette quantité n'est pas nulle en général.

Le calcul montre donc que ce n'est PAS $100N + \text{clé}$ qui est divisible par 97, mais bien $N + \text{clé}$: en effet $N + \text{clé} \equiv r + 97 - r = 97 \equiv 0 \pmod{97}$.

Contrôle avec les valeurs : $N + 16 \equiv 81 + 16 = 97 \equiv 0 \pmod{97}$ ✓. C'est cette somme que le système vérifie.

Troisième question. Supposons qu'un seul chiffre soit mal saisi : à la position k (en partant des unités), le chiffre c devient c' .

Le numéro est alors modifié de $(c' - c) \times 10^k$, avec $1 \leq |c' - c| \leq 9$.

Pour que l'erreur passe inaperçue, il faudrait que 97 divise $(c' - c) \times 10^k$.

Or 97 est un nombre premier qui ne divise ni 10 (donc aucune de ses puissances) ni un écart de chiffres compris entre 1 et 9.

Le produit n'est donc jamais divisible par 97 : toute erreur sur un seul chiffre modifie le reste, et la clé ne correspond plus. Le système la détecte.

C'est précisément pour cette raison qu'on a choisi un module PREMIER et grand : 97 détecte aussi la plupart des inversions de deux chiffres voisins.

Réponse. La clé vaut $97 - 81 = 16$: c'est $N + \text{clé}$ qui est divisible par 97 (et non $100N + \text{clé}$) : toute erreur d'un chiffre modifie le nombre de $(c' - c)10^k$, quantité jamais divisible par 97 : l'erreur est détectée.

Rappel de cours. Une clé de contrôle est un reste : on ajoute au message le complément qui rend le total divisible par un module donné. Un module PREMIER, et premier avec 10, maximise la détection d'erreurs.

Erreur fréquente. Supposer que la clé se concatène « mathématiquement » comme un décalage de deux rangs. Ici la règle de vérification porte sur la SOMME $N + \text{clé}$, qu'il faut établir avant de conclure.

Correction de l'exercice 16 - Reste d'une très grande puissance

Première étape, la base. $2026 = 7 \times 289 + 3$, donc $2026 \equiv 3 \pmod{7}$.

Par compatibilité avec les puissances : $2026^{2026} \equiv 3^{2026} \pmod{7}$. Le problème se ramène aux puissances de 3.

Deuxième étape, la période. $3^1 \equiv 3$; $3^2 = 9 \equiv 2$; $3^3 \equiv 2 \times 3 = 6$; $3^4 \equiv 6 \times 3 = 18 \equiv 4$; $3^5 \equiv 4 \times 3 = 12 \equiv 5$; $3^6 \equiv 5 \times 3 = 15 \equiv 1 \pmod{7}$.

On retombe sur 1 à l'exposant 6 : la suite des restes 3, 2, 6, 4, 5, 1 est périodique de période 6.

Troisième étape : on réduit l'EXPOSANT modulo 6. $2026 = 6 \times 337 + 4$, donc $2026 \equiv 4 \pmod{6}$.

$$\text{D'où } 3^{2026} = \left(3^6\right)^{337} \times 3^4 \equiv 1^{337} \times 4 \equiv 4 \pmod{7}.$$

Le reste de 2026^{2026} dans la division par 7 est donc 4.

Récapitulons la méthode, en deux réductions bien distinctes : la BASE se réduit modulo 7 (le module de la question), l'EXPOSANT se réduit modulo 6 (la période trouvée).

Ce sont deux modules différents, et les confondre est l'erreur la plus fréquente du chapitre.

Contrôle partiel sur un cas calculable : $2026^2 = 4\,104\,676$. Sa réduction : $4\,104\,676 = 7 \times 586\,382 + 2$, donc reste 2.

Et la méthode prédit $3^2 \equiv 2 \pmod{7}$ ✓ — cohérent.

Réponse. $2026 \equiv 3 \pmod{7}$ · les puissances de 3 modulo 7 ont pour période 6 : 3, 2, 6, 4, 5, 1 · $2026 \equiv 4 \pmod{6}$, donc $2026^{2026} \equiv 3^4 \equiv 4 \pmod{7}$.

Rappel de cours. Deux réductions : la base modulo n , l'exposant modulo la période p des puissances. Rédaction type : $a^N = (a^p)^q \times a^s \equiv a^s \pmod{n}$ avec $N = pq + s$.

Erreur fréquente. Réduire l'exposant modulo 7 au lieu de 6. On obtiendrait $2026 \equiv 3 \pmod{7}$ puis $3^3 \equiv 6$, soit une réponse fausse.

Correction de l'exercice 17 - Une équation sans solution entière

D'après l'exercice 9, un carré est congru à 0 ou à 1 modulo 4.

On additionne deux tels restes, en examinant les combinaisons possibles.

$0 + 0 = 0$; $0 + 1 = 1$; $1 + 0 = 1$; $1 + 1 = 2$.

Les restes possibles de $x^2 + y^2$ modulo 4 sont donc 0, 1 et 2. La valeur 3 est IMPOSSIBLE.

Autrement dit : aucune somme de deux carrés n'est congrue à 3 modulo 4.

Reste de 2023 : $2023 = 4 \times 505 + 3$, donc $2023 \equiv 3 \pmod{4}$.

Si un couple $(x; y)$ vérifiait $x^2 + y^2 = 2023$, on aurait $x^2 + y^2 \equiv 3 \pmod{4}$, ce qui vient d'être écarté.

L'équation $x^2 + y^2 = 2023$ n'a donc aucune solution entière. La démonstration est complète : elle vaut pour TOUS les entiers, pas seulement ceux qu'on aurait testés.

Troisième question : $2026 = 4 \times 506 + 2$, donc $2026 \equiv 2 \pmod{4}$. Cette fois, le reste 2 EST possible (cas $1 + 1$, c'est-à-dire x et y tous deux impairs).

L'argument modulo 4 ne permet donc pas de conclure à l'impossibilité — mais il ne prouve pas non plus l'existence.

Cherchons effectivement une solution : on essaie $x = 45$, d'où $x^2 = 2025$ et $y^2 = 1$, soit $y = 1$.

Le couple $(45; 1)$ convient : $45^2 + 1^2 = 2025 + 1 = 2026$ ✓. Et cohérence avec la question précédente : 45 et 1 sont bien tous deux impairs ✓.

Morale : une congruence peut prouver une IMPOSSIBILITÉ, jamais une existence. Pour l'existence, il faut exhiber une solution.

Réponse. $x^2 + y^2 \equiv 0, 1$ ou $2 \pmod{4}$ — jamais 3 · $2023 \equiv 3 \pmod{4}$, donc $x^2 + y^2 = 2023$ n'a pas de solution entière · en revanche $2026 = 45^2 + 1^2$.

Rappel de cours. Un entier congru à 3 modulo 4 n'est jamais somme de deux carrés. Schéma général : table des restes du membre de gauche, comparaison avec le reste du membre de droite.

Erreur fréquente. Croire qu'une congruence compatible prouve l'existence d'une solution. Elle lève seulement l'obstruction : il reste à trouver le couple, comme pour 2026.

Correction de l'exercice 18 - Les cubes modulo 9

On calcule x^3 modulo 9 pour les neuf restes possibles de x .

$x \equiv 0 \rightarrow 0$; $1 \rightarrow 1$; $2 \rightarrow 8$; $3 \rightarrow 27 \equiv 0$; $4 \rightarrow 64 \equiv 1$.

$5 \rightarrow 125 \equiv 8$ (car $125 = 9 \times 13 + 8$) ; $6 \rightarrow 216 \equiv 0$; $7 \rightarrow 343 \equiv 1$ (car $343 = 9 \times 38 + 1$) ;

$8 \rightarrow 512 \equiv 8$ (car $512 = 9 \times 56 + 8$).

Les seuls restes possibles pour un cube modulo 9 sont donc 0, 1 et 8.

Écriture plus parlante : $8 \equiv -1$ [9], donc un cube est congru à 0, 1 ou -1 modulo 9.

Somme de trois cubes : chaque terme vaut 0, 1 ou -1 , donc la somme est comprise entre -3 et 3 au sens des congruences.

Les valeurs atteignables sont $-3, -2, -1, 0, 1, 2, 3$, c'est-à-dire modulo 9 : 6, 7, 8, 0, 1, 2, 3.

Autrement dit, les restes possibles d'une somme de trois cubes modulo 9 sont $\{0; 1; 2; 3; 6; 7; 8\}$.

Les valeurs 4 et 5 sont donc IMPOSSIBLES pour une somme de trois cubes.

Conclusion : si $x^3 + y^3 + z^3 = 4$ avait une solution entière, on aurait $x^3 + y^3 + z^3 \equiv 4$ [9], ce qui vient d'être écarté.

L'équation $x^3 + y^3 + z^3 = 4$ n'a donc aucune solution entière.

Le même argument s'applique à $x^3 + y^3 + z^3 = 5$, et plus généralement à tout second membre congru à 4 ou 5 modulo 9 — par exemple 13, 14, 22, 23, etc.

Remarque culturelle : pour les autres valeurs, la question est bien plus difficile. Le cas 33 n'a été résolu qu'en 2019, avec des entiers de seize chiffres — et la congruence ne dit rien de tel, elle écarte seulement les cas impossibles.

Réponse. Un cube vaut 0, 1 ou $8 \equiv -1$ modulo 9 · une somme de trois cubes ne peut valoir que 0, 1, 2, 3, 6, 7, 8 modulo 9 · comme 4 n'y figure pas, $x^3 + y^3 + z^3 = 4$ n'a pas de solution entière (idem pour 5).

Rappel de cours. Le module 9 est le bon pour les cubes, comme 4 l'est pour les carrés : il réduit les valeurs possibles à trois. Choisir le module, c'est là que se joue la démonstration.

Erreur fréquente. Se contenter d'un module trop petit. Modulo 3, un cube vaut 0, 1 ou 2 : toutes les valeurs sont atteignables et l'argument échoue. Il faut monter à 9.

Correction de l'exercice 19 - Divisibilité d'une somme de puissances

Puissances de 2 modulo 5 : $2^1 \equiv 2$; $2^2 \equiv 4$; $2^3 \equiv 8 \equiv 3$; $2^4 \equiv 6 \equiv 1$; puis le cycle recommence. Période 4, restes 2, 4, 3, 1.

Puissances de 3 modulo 5 : $3^1 \equiv 3$; $3^2 \equiv 9 \equiv 4$; $3^3 \equiv 12 \equiv 2$; $3^4 \equiv 6 \equiv 1$; cycle de période 4 également, restes 3, 4, 2, 1.

On additionne terme à terme, selon le reste de n modulo 4.

$n \equiv 1$ [4] : $u_n \equiv 2 + 3 = 5 \equiv 0$ [5].

$n \equiv 2$ [4] : $u_n \equiv 4 + 4 = 8 \equiv 3$ [5].

$n \equiv 3$ [4] : $u_n \equiv 3 + 2 = 5 \equiv 0$ [5].

$n \equiv 0$ [4] : $u_n \equiv 1 + 1 = 2$ [5].

Le reste est nul exactement dans les cas $n \equiv 1$ et $n \equiv 3$ modulo 4, c'est-à-dire pour n IMPAIR.

Donc $5 \mid 2^n + 3^n$ si et seulement si n est impair.

Contrôle : $n = 1 \rightarrow 5 \checkmark$; $n = 2 \rightarrow 13 \times$; $n = 3 \rightarrow 35 = 5 \times 7 \checkmark$; $n = 4 \rightarrow 97 \times$;
 $n = 5 \rightarrow 275 = 5 \times 55 \checkmark$.

Argument direct, bien plus court. On remarque que $3 \equiv -2 \pmod{5}$.

Donc $3^n \equiv (-2)^n = (-1)^n 2^n \pmod{5}$, et $u_n = 2^n + 3^n \equiv 2^n + (-1)^n 2^n = 2^n [1 + (-1)^n] \pmod{5}$.

Si n est impair, le crochet vaut $1 - 1 = 0$, donc $u_n \equiv 0 \pmod{5}$.

Si n est pair, le crochet vaut 2, donc $u_n \equiv 2 \times 2^n = 2^{n+1} \pmod{5}$, qui n'est jamais nul puisque 2 et 5 n'ont aucun facteur commun.

On retrouve exactement le même résultat $\checkmark$. Repérer que $3 \equiv -2 \pmod{5}$ a remplacé deux tableaux par trois lignes.

Réponse. Restes de 2^n : 2, 4, 3, 1 ; de 3^n : 3, 4, 2, 1 (période 4) · $u_n \equiv 0 \pmod{5}$ exactement pour n impair · argument direct : $3 \equiv -2 \pmod{5}$, donc $u_n \equiv 2^n [1 + (-1)^n] \pmod{5}$.

Rappel de cours. Avant de dresser un tableau, on cherche si l'une des bases est congrue à l'OPPOSÉE de l'autre : la somme se factorise alors, et la parité de n décide.

Erreur fréquente. Additionner les périodes des deux suites. Elles ont ici la même période 4, mais c'est le tableau des SOMMES qu'il faut examiner, pas la somme des périodes.

Correction de l'exercice 20 - Problème de synthèse : un chiffrement affine

Rangs des lettres de MATH : $M = 12, A = 0, T = 19, H = 7$.

$M : 5 \times 12 + 3 = 63$. Or $63 = 26 \times 2 + 11$, donc $y \equiv 11 \pmod{26}$, ce qui correspond à la lettre L .

$A : 5 \times 0 + 3 = 3$, soit la lettre D .

$T : 5 \times 19 + 3 = 98$. Or $98 = 26 \times 3 + 20$, donc $y \equiv 20$, soit U .

$H : 5 \times 7 + 3 = 38 = 26 + 12$, donc $y \equiv 12$, soit M .

Le mot MATH est donc codé LDUM.

Deuxième question : $5 \times 21 = 105$. Or $105 = 26 \times 4 + 1 = 104 + 1$, donc $105 \equiv 1 \pmod{26} \checkmark$.

Le nombre 21 joue donc, modulo 26, le rôle que $\frac{1}{5}$ joue dans les réels : c'est ce qui va permettre d'inverser le chiffrement.

Déchiffrement. On part de $y \equiv 5x + 3 \pmod{26}$, et on isole x .

D'abord $y - 3 \equiv 5x \pmod{26}$. Puis on multiplie les deux membres par 21 :

$21(y - 3) \equiv 21 \times 5x = 105x \equiv x \pmod{26}$.

La formule de déchiffrement est donc $x \equiv 21(y - 3) \pmod{26}$.

Vérifions sur LDUM. $L = 11 : x \equiv 21 \times 8 = 168$. Or $168 = 26 \times 6 + 12$, donc $x \equiv 12$, soit $M \checkmark$.

$D = 3 : x \equiv 21 \times 0 = 0$, soit $A \checkmark$.

$U = 20 : x \equiv 21 \times 17 = 357$. Or $357 = 26 \times 13 + 19$, donc $x \equiv 19$, soit $T \checkmark$.

$M = 12 : x \equiv 21 \times 9 = 189 = 26 \times 7 + 7$, donc $x \equiv 7$, soit $H \checkmark$. On retrouve bien MATH.

Dernière question. Pour que le chiffrement soit déchiffirable, il faut que $x \mapsto ax + 3$ soit une BIJECTION sur les 26 rangs : deux lettres différentes ne doivent jamais être codées pareil.

Avec $a = 13 : 13 \times 0 + 3 = 3$ et $13 \times 2 + 3 = 29 \equiv 3 \pmod{26}$. Les lettres A et C sont codées par la même lettre : le déchiffrement est impossible.

Avec $a = 2 : 2 \times 0 + 3 = 3$ et $2 \times 13 + 3 = 29 \equiv 3 \pmod{26}$. Même problème entre A et N .

La raison de fond : 13 et 2 ont un facteur commun avec 26 (respectivement 13 et 2). Le coefficient a doit être PREMIER AVEC 26 — ce qui est le cas de 5, et lui garantit un inverse modulo 26.

Les valeurs admissibles de a sont donc les entiers de 1 à 25 sans facteur commun avec $26 = 2 \times 13$: tous les impairs sauf 13, soit 12 valeurs possibles.

Réponse. MATH se code LDUM $\cdot 5 \times 21 = 105 = 4 \times 26 + 1$, donc $5 \times 21 \equiv 1 [26]$ ·
déchiffrement : $x \equiv 21(y - 3) [26]$, et LDUM redonne MATH $\cdot 13$ et 2 ne conviennent pas car ils ne sont pas premiers avec 26 : le codage ne serait pas bijectif.

Rappel de cours. Un chiffrement affine $y \equiv ax + b [n]$ est déchiffrable si et seulement si a est premier avec n . Le déchiffrement s'écrit alors $x \equiv a'(y - b) [n]$, où a' est l'inverse de a modulo n .

Erreur fréquente. Vouloir « diviser par 5 » pour déchiffrer. La division n'existe pas dans les congruences : on multiplie par l'INVERSE, ici 21.