Plaquette 5 – Synthèse : grandes puissances, clés de contrôle et chiffrement

Divisibilité et congruences — Terminale maths expertes

Corrections détaillées

Boîte à outils

Formules, méthodes et applications.

— **Cycle des puissances.** Les restes de a^n modulo n_0 se répètent : on calcule $a^1, a^2, a^3, \ldots$ jusqu'à retomber sur 1 (ou sur un reste déjà vu). Si $a^p \equiv 1 \pmod{n_0}$, alors

$$a^n \equiv a^r \pmod{n_0} \qquad \text{où } r \text{ est le reste de } n \text{ dans la division par } p$$

— **Méthode en trois temps** : trouver le cycle, diviser l'exposant par la longueur du cycle, conclure avec le reste.

— **Astuce** : chercher -1 plutôt que 1 raccourcit le travail ($2 \equiv -1 \pmod 3$, $10 \equiv -1 \pmod{11}$).

— **Preuve par neuf** : comme $10 \equiv 1 \pmod 9$, un nombre est congru modulo 9 à la somme de ses chiffres. Le reste modulo 9 du produit doit être celui du produit des restes.

— **Clé ISBN-10** : les dix chiffres $d_1, \ldots, d_{10}$ vérifient

$$\sum_{i=1}^{10} i \times d_i \equiv 0 \pmod{11} \qquad (d_{10} = 10 \text{ se note } X)$$

— **Clé EAN-13** : on pondère les douze premiers chiffres par $1, 3, 1, 3, \ldots$ et la clé complète la somme au multiple de 10 supérieur.

— **Clé INSEE** (numéro de sécurité sociale) : clé $= 97 - r$, où r est le reste du numéro à 13 chiffres modulo 97.

— **Chiffrement.** On code les lettres par $A = 0, \ldots, Z = 25$. César : $y \equiv x + k \pmod{26}$. Affine : $y \equiv ax + b \pmod{26}$, **déchiffrable seulement si a possède un inverse modulo 26**, et alors $x \equiv a^{-1}(y - b)$.

Correction de l'exercice 1 – Le cycle des puissances de 2

a) On calcule de proche en proche, en réduisant à chaque étape :

n	1	2	3	4	5	6
$2^n \equiv$	2	4	1	2	4	1

— $2^3 = 8 = 7 + 1 \equiv 1 \pmod 7$: dès que l'on retombe sur 1, tout se répète.

— Le cycle est donc de **longueur 3** : $2, 4, 1, 2, 4, 1, \ldots$

b) On divise l'exposant par la longueur du cycle :

— $2\,026 = 3 \times 675 + 1$, donc $2\,026 \equiv 1 \pmod 3$.

— $2^{2026} = 2^{3 \times 675 + 1} = \left(2^3\right)^{675} \times 2^1 \equiv 1^{675} \times 2 = 2 \pmod 7$.

Conclusion. Le reste de 2^{2026} dans la division par 7 est 2.

— **Le réflexe** : ce n'est pas l'exposant qui compte, c'est son **reste modulo la longueur du cycle**.

Réponse. a) cycle $2, 4, 1$ de longueur 3 · b) reste 2.

Correction de l'exercice 2 – Un exposant gigantesque

Inutile de chercher un cycle : on **réduit d'abord la base**.

— Modulo 9, un nombre est congru à la somme de ses chiffres : $2+0+2+6=10$, puis $1+0=1$.
— Donc $2\,026 \equiv 1 \pmod 9$.
— Par compatibilité avec les puissances : $2\,026^{\,2026} \equiv 1^{\,2026} = 1 \pmod 9$.

Conclusion. Le reste est 1.

— **Contrôle du calcul de départ** : $2\,026 = 9 \times 225 + 1$ ✓.
— La morale : une puissance colossale peut se traiter en deux lignes si la base est congrue à 1 (ou à -1).

Réponse. $2\,026^{\,2026} \equiv 1 \pmod 9$: le reste est 1.

Correction de l'exercice 3 – Les deux derniers chiffres

Les deux derniers chiffres d'un nombre, c'est son reste modulo 100.

— $7^1 \equiv 7$; $7^2 = 49$; $7^3 = 343 \equiv 43$; $7^4 = 2\,401 \equiv 1 \pmod{100}$.
— On retombe sur 1 : le cycle a pour longueur 4.
— $2\,026 = 4 \times 506 + 2$, donc $2\,026 \equiv 2 \pmod 4$.
— $7^{\,2026} = \left(7^4\right)^{506} \times 7^2 \equiv 1^{\,506} \times 49 = 49 \pmod{100}$.

Conclusion. $7^{\,2026}$ se termine par 49.

— Astuce de calcul pour 7^4 : $7^4 = \left(7^2\right)^2 = 49^2 = 2\,401$, dont les deux derniers chiffres sont 01.
— Au passage, le **chiffre des unités** est 9.

Réponse. $7^{\,2026} \equiv 49 \pmod{100}$: les deux derniers chiffres sont 49.

Correction de l'exercice 4 – Longueur d'un cycle

a) On calcule les puissances successives de 3 modulo 7 :

p	1	2	3	4	5	6
$3^p \equiv$	3	2	6	4	5	1

— Détail : $3^2 = 9 \equiv 2$, puis $3^3 \equiv 3 \times 2 = 6$, $3^4 \equiv 3 \times 6 = 18 \equiv 4$, $3^5 \equiv 12 \equiv 5$, $3^6 \equiv 15 \equiv 1$.
— Le plus petit exposant qui donne 1 est donc $p = 6$.
— On remarque que **tous** les restes non nuls apparaissent : 3 est un « générateur » modulo 7.

b) $100 = 6 \times 16 + 4$, donc $100 \equiv 4 \pmod 6$.

— $3^{\,100} = \left(3^6\right)^{16} \times 3^4 \equiv 1^{\,16} \times 4 = 4 \pmod 7$.
— **Conclusion.** Le reste de $3^{\,100}$ dans la division par 7 est 4.

Réponse. a) $p = 6$ · b) reste 4.

Correction de l'exercice 5 – Une somme de deux puissances

On traite **séparément** les deux puissances, puis on additionne les restes.

— Puissances de 2 modulo 5 : $2, 4, 3, 1$ puis répétition (cycle de longueur 4).
— Puissances de 3 modulo 5 : $3, 4, 2, 1$ puis répétition (cycle de longueur 4 également).
— $2\,026 = 4 \times 506 + 2$, donc l'exposant est congru à 2 modulo 4 : on lit la **deuxième** valeur de chaque cycle.
— $2^{2026} \equiv 4 \pmod 5$ et $3^{2026} \equiv 4 \pmod 5$.
— Somme : $4 + 4 = 8 \equiv 3 \pmod 5$.

Conclusion. Le reste est 3.

— **Contrôle sur un petit exposant de même reste** : pour $n = 2$, $2^2 + 3^2 = 13 = 5 \times 2 + 3$ ✓ — le reste est bien 3, comme prévu.

Réponse. $2^{2026} + 3^{2026} \equiv 3 \pmod 5$.

Correction de l'exercice 6 – La preuve par neuf

Le principe : $10 \equiv 1 \pmod 9$, donc un nombre est **congru à la somme de ses chiffres** modulo 9.

— $3\,847 : 3 + 8 + 4 + 7 = 22$, puis $2 + 2 = 4$, donc $3\,847 \equiv 4 \pmod 9$.
— $259 : 2 + 5 + 9 = 16$, puis $1 + 6 = 7$, donc $259 \equiv 7 \pmod 9$.
— Le produit doit donc vérifier : $3\,847 \times 259 \equiv 4 \times 7 = 28 \equiv 1 \pmod 9$.

a) $996\,273 : 9 + 9 + 6 + 2 + 7 + 3 = 36 \equiv 0 \pmod 9$.

— On attendait 1 : le résultat est **faux**.

b) $996\,373 : 9 + 9 + 6 + 3 + 7 + 3 = 37$, puis $3 + 7 = 10 \equiv 1 \pmod 9$ ✓ : la preuve est concluante.

c) $996\,337$: la somme des chiffres est la même (37), donc la preuve par neuf **ne détecte rien**.

— **Limite de la méthode** : elle ne repère jamais une **interversion de chiffres**, ni une erreur de 9 ou d'un multiple de 9.
— La preuve par neuf peut donc invalider un résultat, mais jamais le garantir. C'est exactement pour cela que les clés de contrôle modernes utilisent des **poids différents** selon la position.

Réponse. a) $0 \neq 1$: faux · b) $37 \equiv 1$ ✓ · c) non détectée (interversion de chiffres).

Correction de l'exercice 7 – Calculer une clé ISBN

On calcule la somme pondérée des neuf premiers chiffres, en multipliant chaque chiffre par **son rang**.

Rang i	1	2	3	4	5	6	7	8	9
Chiffre d_i	2	7	1	0	4	3	7	6	5
$i \times d_i$	2	14	3	0	20	18	49	48	45

— Somme : $2 + 14 + 3 + 0 + 20 + 18 + 49 + 48 + 45 = 199$.
— La condition s'écrit $199 + 10k \equiv 0 \pmod{11}$.
— Or $199 = 11 \times 18 + 1$, donc $199 \equiv 1$, et $10 \equiv -1 \pmod{11}$: la condition devient $1 - k \equiv 0$.
— D'où $k \equiv 1 \pmod{11}$, et comme $0 \leq k \leq 10$: $k = 1$.

Vérification. $199 + 10 \times 1 = 209 = 11 \times 19$ ✓.

— **Conclusion.** L'ISBN complet est 2-7104-3765-1.

— Si l'on avait trouvé $k = 10$, on écrirait la clé X : c'est la raison de ce caractère sur certains livres.

Réponse. $k = 1$, soit l'ISBN 2-7104-3765-1.

Correction de l'exercice 8 – Retrouver un chiffre illisible

C'est l'intérêt d'une clé de contrôle : elle permet de **reconstituer** un caractère manquant.

— Somme pondérée des chiffres connus (rangs $1, 2, 3, 4, 6, 7, 8, 9, 10$) :

— $1 \times 2 + 2 \times 7 + 3 \times 1 + 4 \times 0 + 6 \times 3 + 7 \times 7 + 8 \times 6 + 9 \times 5 + 10 \times 1$

— $= 2 + 14 + 3 + 0 + 18 + 49 + 48 + 45 + 10 = 189$.

— Le chiffre manquant est au rang 5, il compte donc pour $5x$: la condition est $189 + 5x \equiv 0 \pmod{11}$.

— $189 = 11 \times 17 + 2$, donc $2 + 5x \equiv 0$, soit $5x \equiv -2 \equiv 9 \pmod{11}$.

— Inverse de 5 modulo 11 : $5 \times 9 = 45 = 44 + 1 \equiv 1$, donc $5^{-1} \equiv 9$.

— $x \equiv 9 \times 9 = 81 \pmod{11}$, et $81 = 77 + 4$, donc $x \equiv 4$.

Conclusion. $x = 4$: l'ISBN est 2-7104-3765-1, ce qui confirme l'exercice précédent.

Réponse. $x = 4$.

Correction de l'exercice 9 – La clé d'un code-barres

On aligne les douze chiffres et leurs poids alternés.

Chiffre	3	0	1	2	3	4	5	6	7	8	9	0
Poids	1	3	1	3	1	3	1	3	1	3	1	3
Produit	3	0	1	6	3	12	5	18	7	24	9	0

— Somme : $3 + 0 + 1 + 6 + 3 + 12 + 5 + 18 + 7 + 24 + 9 + 0 = 88$.

— La clé c vérifie $88 + c \equiv 0 \pmod{10}$, soit $c \equiv -88 \equiv 2 \pmod{10}$.

— Comme c est un chiffre : $c = 2$.

Vérification. $88 + 2 = 90$, multiple de 10 ✓.

— **Conclusion.** Le code-barres complet est 3 012 345 678 902.

— **Pourquoi des poids** 1 **et** 3 **?** Parce qu'ils rendent la clé sensible aux **interversions** de deux chiffres voisins, contrairement à la preuve par neuf : intervertir deux chiffres change la somme de ± 2 fois leur différence.

Réponse. Clé $c = 2$, code complet 3 012 345 678 902.

Correction de l'exercice 10 – La clé d'un numéro de sécurité sociale

On doit obtenir le reste de $N = 1\,850\,675\,114\,287$ modulo 97. Le nombre dépasse la capacité d'affichage d'une calculatrice : on le **découpe** et on réduit chaque morceau.

— On sépare les six derniers chiffres : $N = 1\,850\,675 \times 10^6 + 114\,287$.

— **Premier morceau** : $97 \times 19\,079 = 1\,850\,663$, donc $1\,850\,675 \equiv 12 \pmod{97}$.

— **La puissance de 10** : $10^2 = 100 \equiv 3$, donc $10^4 \equiv 3^2 = 9$ et $10^6 \equiv 9 \times 3 = 27 \pmod{97}$.

— **Second morceau** : $97 \times 1\,178 = 114\,266$, donc $114\,287 \equiv 21 \pmod{97}$.

— On recompose : $N \equiv 12 \times 27 + 21 = 324 + 21 = 345 \pmod{97}$.

— Enfin $345 = 97 \times 3 + 54$, donc $r = 54$.
— Clé : $97 - 54 = 43$.

Conclusion. La clé du numéro est 43, et le numéro complet s'écrit 1 85 06 75 114 287 43.

— **Pourquoi** 97 **?** C'est un nombre premier, plus grand que 10 : toute erreur sur un seul chiffre, et toute interversion de deux chiffres, modifient le reste — donc la clé.

Réponse. $N \equiv 54 \pmod{97}$, donc la clé vaut $97 - 54 = 43$.

Correction de l'exercice 11 – Le chiffre de César

a) On remplace chaque lettre par son rang, on ajoute 3, on réduit modulo 26 :

Lettre	**M**	**A**	**T**	**H**	**S**
x	12	0	19	7	18
$y = x + 3$	15	3	22	10	21
Lettre codée	P	D	W	K	V

— MATHS devient **PDWKV**.

b) Pour déchiffrer, on utilise la transformation réciproque : $x \equiv y - 3 \pmod{26}$.

Lettre	**F**	**D**	**O**	**F**	**X**	**O**
y	5	3	14	5	23	14
$x = y - 3$	2	0	11	2	20	11
Lettre claire	C	A	L	C	U	L

— Le message est **CALCUL**.
— **Pourquoi le modulo** 26 **?** Pour que Z (rang 25) codé donne C (rang 2) : $25 + 3 = 28 \equiv 2$. L'alphabet « boucle ».

Réponse. a) PDWKV · b) CALCUL.

Correction de l'exercice 12 – Le chiffrement affine

a) On applique $y \equiv 5x + 8 \pmod{26}$:

— C : $x = 2$, $y = 10 + 8 = 18 \to$ S.
— L : $x = 11$, $y = 55 + 8 = 63 = 26 \times 2 + 11 \to y = 11 \to$ L.
— E : $x = 4$, $y = 20 + 8 = 28 \equiv 2 \to$ C.
— CLE devient **SLC**.

b) $5 \times 21 = 105 = 26 \times 4 + 1$, donc $5 \times 21 \equiv 1 \pmod{26}$: 21 est bien l'inverse de 5.

— On part de $y \equiv 5x + 8$, donc $5x \equiv y - 8$.
— On multiplie par 21 : $x \equiv 21(y - 8) \pmod{26}$.

c) On applique cette formule lettre par lettre :

Lettre	**V**	**A**	**Q**	**N**	**P**	**C**
y	21	0	16	13	15	2
$y - 8$	13	-8	8	5	7	-6
$x = 21(y - 8)$	13	14	12	1	17	4
Lettre claire	N	O	M	B	R	E

— Détail du premier calcul : $21 \times 13 = 273 = 26 \times 10 + 13$, donc $x = 13$, la lettre N.
— Détail du deuxième : $21 \times (-8) = -168$, et $-168 + 26 \times 7 = -168 + 182 = 14$, donc $x = 14$, la lettre O.
— Le message est **NOMBRE**.

Réponse. a) SLC · b) $x \equiv 21(y - 8) \pmod{26}$ · c) NOMBRE.

Correction de l'exercice 13 – Une clé qui ne convient pas

On calcule quelques images pour voir ce qui se passe :

— $x = 0$: $y = 4 \to$ E. $x = 2$: $y = 26 + 4 = 30 \equiv 4 \to$ E aussi.
— Plus généralement, si x est **pair**, $x = 2k$, alors $13x = 26k \equiv 0$, donc $y \equiv 4$.
— Si x est **impair**, $x = 2k + 1$, alors $13x = 26k + 13 \equiv 13$, donc $y \equiv 17 \to$ R.

Conclusion. Toutes les lettres de rang pair sont codées par E, toutes celles de rang impair par R : le message chiffré ne contient que deux lettres, et le déchiffrement est impossible.

— **La raison de fond** : 13 n'a pas d'inverse modulo 26, car 13 et 26 ont le diviseur commun 13.
— **Règle à retenir** : dans $y \equiv ax + b \pmod{26}$, le coefficient a doit n'avoir aucun diviseur commun avec 26 — donc être impair et différent de 13. Il reste 12 valeurs utilisables.

Réponse. $13x \equiv 0$ ou $13 \pmod{26}$ selon la parité de x : le codage n'est pas injectif.

Correction de l'exercice 14 – Horloge et passages d'un satellite

a) Une horloge de 24 heures, c'est un calcul modulo 24.

— $9 + 1\,009 = 1\,018$.
— $1\,018 = 24 \times 42 + 10$, car $24 \times 42 = 1\,008$.
— Donc $1\,018 \equiv 10 \pmod{24}$: il sera **10 h**.
— Autre présentation : $1\,009 = 24 \times 42 + 1$, on avance donc de 42 jours **et 1 heure**, d'où $9 + 1 = 10$ h.

b) Le 100^{e} passage a lieu $11 \times 100 = 1\,100$ jours après le mardi initial. On travaille modulo 7.

— $1\,100 = 7 \times 157 + 1$, car $7 \times 157 = 1\,099$.
— Donc $1\,100 \equiv 1 \pmod{7}$: on avance d'un seul jour dans la semaine.
— **Conclusion.** Le 100^{e} passage aura lieu un **mercredi**.
— Contrôle sur un petit cas : le 7^{e} passage a lieu 77 jours plus tard, et $77 = 7 \times 11$: c'est bien un mardi ✓.

Réponse. a) 10 h · b) un mercredi.

Correction de l'exercice 15 – Bilan : trois applications

a) On cherche le cycle des puissances de 7 modulo 13 :

— $7^1 \equiv 7$; $7^2 = 49 \equiv 10$; $7^3 \equiv 70 \equiv 5$; $7^4 \equiv 35 \equiv 9$; $7^6 \equiv 7^4 \times 7^2 \equiv 9 \times 10 = 90 \equiv 12 \equiv -1 \pmod{13}$.
— Comme $7^6 \equiv -1$, on obtient $7^{12} \equiv 1$: le cycle a pour longueur 12.
— $2\,026 = 12 \times 168 + 10$, donc $7^{2026} \equiv 7^{10} \pmod{13}$.
— $7^{10} = 7^6 \times 7^4 \equiv (-1) \times 9 = -9 \equiv 4 \pmod{13}$.
— **Le reste est 4.**

b) On applique les poids alternés $1, 3, 1, 3, \ldots$ aux douze premiers chiffres, le dernier (1) étant la clé.

— Chiffres et poids : 4×1, 0×3, 1×1, 2×3, 3×1, 4×3, 5×1, 6×3, 7×1, $y \times 3$, 8×1, 9×3.

— Somme des termes connus : $4 + 0 + 1 + 6 + 3 + 12 + 5 + 18 + 7 + 8 + 27 = 91$.

— La clé 1 complète la somme : $91 + 3y + 1 \equiv 0 \pmod{10}$, soit $3y \equiv -92 \equiv 8 \pmod{10}$.

— Inverse de 3 modulo 10 : $3 \times 7 = 21 \equiv 1$, donc $y \equiv 7 \times 8 = 56 \equiv 6 \pmod{10}$.

— **Le chiffre effacé est** 6**.** Vérification : $91 + 18 + 1 = 110$, multiple de 10 ✓.

c) $3 \times 9 = 27 = 26 + 1 \equiv 1 \pmod{26}$: 9 est bien l'inverse de 3. La formule de déchiffrement est $x \equiv 9(y - 5) \pmod{26}$.

Lettre	**H**	**V**	**P**	**P**	**R**
y	7	21	15	15	17
$y - 5$	2	16	10	10	12
$x = 9(y - 5)$	18	14	12	12	4
Lettre claire	S	O	M	M	E

— Détail de la deuxième lettre : $9 \times 16 = 144 = 26 \times 5 + 14$, donc $x = 14$, la lettre O.

— Détail de la dernière : $9 \times 12 = 108 = 26 \times 4 + 4$, donc $x = 4$, la lettre E.

— Le message clair est **SOMME**.

Réponse. a) reste 4 · b) $y = 6$ · c) SOMME.