Plaquette 3 – Calculer avec les congruences : tables modulo n et équations

Divisibilité et congruences — Terminale maths expertes

Corrections détaillées

Boîte à outils

Formules et méthodes pour le calcul modulo n.

— $a \equiv b \pmod{n}$ signifie $n \mid (a-b)$: a et b ont le **même reste** dans la division par n.

— Tout entier est congru modulo n à **exactement un** des entiers $0, 1, \ldots, n-1$: ce sont les n **classes** modulo n.

— **Compatibilités** (la règle qui fait tout marcher) : si $a \equiv a'$ et $b \equiv b' \pmod{n}$, alors

$$a+b \equiv a'+b' \pmod{n} \qquad ab \equiv a'b' \pmod{n} \qquad a^k \equiv a'^k \pmod{n}$$

— **Méthode de calcul** : on **réduit d'abord**, on calcule ensuite. Remplacer 47 par 2 modulo 9 évite de manipuler de grands nombres.

— **Méthode de résolution** d'une équation $ax \equiv b \pmod{n}$: on teste les n classes $x \equiv 0, 1, \ldots, n-1$ dans un tableau. L'ensemble des solutions est une **réunion de classes**.

— **Raccourci** : si a possède un **inverse** modulo n, c'est-à-dire un entier a' tel que $aa' \equiv 1 \pmod{n}$, alors $ax \equiv b \Leftrightarrow x \equiv a'b \pmod{n}$.

— **Interdit** : simplifier une congruence par un facteur k qui a un diviseur commun avec n. On simplifie alors **le module aussi** : $kx \equiv ky \pmod{kn'} \Leftrightarrow x \equiv y \pmod{n'}$.

— **Système** : on écrit la première congruence sous forme $x = n_1 q + r_1$, on reporte dans la seconde, et on obtient une classe unique modulo le produit des modules (lorsqu'ils n'ont pas de diviseur commun).

Correction de l'exercice 1 – Tables modulo 5

a) On additionne, puis on remplace le résultat par son reste modulo 5 :

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

b) Même principe pour le produit : par exemple $3 \times 4 = 12 = 5 \times 2 + 2$, donc $3 \times 4 \equiv 2 \pmod{5}$.

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).

c) Chercher un inverse de a, c'est chercher le nombre 1 dans la ligne de a :

— ligne de 1 : $1 \times 1 \equiv 1$, l'inverse de 1 est 1 ;
— ligne de 2 : $2 \times 3 \equiv 1$, l'inverse de 2 est 3 (et réciproquement) ;
— ligne de 4 : $4 \times 4 \equiv 1$, l'inverse de 4 est 4.
— **Tous** les entiers non nuls ont un inverse modulo 5 : c'est une particularité des modules **premiers**. Modulo 6, par exemple, 2, 3 et 4 n'en ont pas.

Réponse. c) $1^{-1} \equiv 1$, $2^{-1} \equiv 3$, $3^{-1} \equiv 2$, $4^{-1} \equiv 4 \pmod 5$.

Correction de l'exercice 2 – Réduire modulo 7

a) On cherche le multiple de 7 juste en dessous :

— $7 \times 289 = 2\,023$, donc $2\,026 = 7 \times 289 + 3$ et $2\,026 \equiv 3 \pmod 7$.

b) On peut aussi décomposer pour éviter la division :

— $1\,000 = 10^3$ et $10 \equiv 3 \pmod 7$, donc $10^3 \equiv 3^3 = 27 \pmod 7$.
— $27 = 7 \times 3 + 6$, donc $1\,000 \equiv 6 \pmod 7$.
— Contrôle direct : $7 \times 142 = 994$ et $1\,000 - 994 = 6$ ✓.

c) **Le reste doit rester positif**, c'est le piège du cas négatif.

— $-45 = 7 \times (-7) + 4$ car $7 \times (-7) = -49$ et $-49 + 4 = -45$.
— Donc $-45 \equiv 4 \pmod 7$, et non -3 (même si $-45 \equiv -3$ est vrai, -3 n'est pas un reste).

Réponse. a) 3 · b) 6 · c) 4.

Correction de l'exercice 3 – Réduire avant de calculer

On utilise la **compatibilité** des congruences avec le produit et la somme : on remplace chaque nombre par son reste **avant** de calculer.

— $47 = 9 \times 5 + 2$, donc $47 \equiv 2 \pmod 9$.
— $53 = 9 \times 5 + 8$, donc $53 \equiv 8 \pmod 9$.
— $29 = 9 \times 3 + 2$, donc $29 \equiv 2 \pmod 9$.
— Donc

$$47 \times 53 + 29 \equiv 2 \times 8 + 2 = 18 \pmod 9$$

— Et $18 = 9 \times 2$, donc $18 \equiv 0 \pmod 9$.

Conclusion. Le reste est 0 : le nombre est un multiple de 9.

— Contrôle : $47 \times 53 + 29 = 2\,491 + 29 = 2\,520 = 9 \times 280$ ✓.
— On aurait aussi pu utiliser le critère de divisibilité : $2 + 5 + 2 + 0 = 9$.

Réponse. Reste 0 : $47 \times 53 + 29 = 2\,520$ est divisible par 9.

Correction de l'exercice 4 – Une première équation de congruence

Méthode du tableau : tout entier est congru à l'un des sept restes $0, 1, \ldots, 6$ modulo 7. On les teste tous.

$x \equiv$	0	1	2	3	4	5	6
$3x \equiv$	0	3	6	2	5	1	4

— La valeur 4 apparaît une seule fois, pour $x \equiv 6 \pmod 7$.
— **Vérification** : $3 \times 6 = 18 = 7 \times 2 + 4$, donc $3 \times 6 \equiv 4 \pmod 7$ ✓.

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).

Méthode plus rapide (par l'inverse) : $3 \times 5 = 15 \equiv 1 \pmod 7$, donc 5 est l'inverse de 3.

— On multiplie les deux membres par 5 : $x \equiv 5 \times 4 = 20 \equiv 6 \pmod 7$. Même réponse.
— L'ensemble des solutions est $\{6 + 7k,\ k \in \mathbb{Z}\}$: $\ldots, -1, 6, 13, 20, \ldots$

Réponse. $x \equiv 6 \pmod 7$.

Correction de l'exercice 5 – Passer par l'inverse

a) Il suffit de calculer 7×7 :

— $7 \times 7 = 49 = 12 \times 4 + 1$, donc $7 \times 7 \equiv 1 \pmod{12}$.
— 7 est donc bien son propre inverse modulo 12.

b) On multiplie les deux membres de l'équation par 7 — ce qui est licite puisque 7 est inversible :

— $7 \times 7x \equiv 7 \times 5 \pmod{12}$, soit

$$x \equiv 35 \pmod{12}$$

— $35 = 12 \times 2 + 11$, donc $x \equiv 11 \pmod{12}$.
— **Vérification** : $7 \times 11 = 77 = 12 \times 6 + 5$ ✓.
— Autrement dit, les solutions sont les entiers de la forme $12k + 11$, soit $\ldots, -1, 11, 23, 35, \ldots$

Réponse. $x \equiv 11 \pmod{12}$.

Correction de l'exercice 6 – Quand on ne peut pas simplifier

4, 6 et 10 sont tous pairs : on peut simplifier, mais **le module aussi**.

— Par définition, $4x \equiv 6 \pmod{10}$ signifie $10 \mid (4x - 6)$, c'est-à-dire $4x - 6 = 10k$.
— En divisant l'égalité par 2 : $2x - 3 = 5k$, c'est-à-dire $2x \equiv 3 \pmod 5$.
— On résout par table modulo 5 :

$x \equiv$	0	1	2	3	4
$2x \equiv$	0	2	4	1	3

— La valeur 3 correspond à $x \equiv 4 \pmod 5$.

Conclusion. Les solutions sont les $x \equiv 4 \pmod 5$, c'est-à-dire modulo 10 : $x \equiv 4$ ou $x \equiv 9 \pmod{10}$.

— Vérification : $4 \times 4 = 16 \equiv 6$ ✓ et $4 \times 9 = 36 \equiv 6 \pmod{10}$ ✓.
— **Le piège** : écrire $2x \equiv 3 \pmod{10}$ serait faux, car $2x$ est toujours pair alors que 3 est impair : cette équation-là n'a aucune solution.

Réponse. $x \equiv 4 \pmod 5$, soit $x \equiv 4$ ou $x \equiv 9 \pmod{10}$.

Correction de l'exercice 7 – Une équation sans solution

Méthode 1 : la table. On teste les six classes modulo 6.

$x \equiv$	0	1	2	3	4	5
$4x \equiv$	0	4	2	0	4	2

— La valeur 3 n'apparaît jamais : aucune classe ne convient, donc aucun entier ne convient.

Méthode 2 : l'argument de parité.

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).

— Si $4x \equiv 3 \pmod 6$, alors $6 \mid (4x-3)$, donc $4x-3$ est pair.
— Or $4x$ est pair, donc $4x-3$ est **impair** : contradiction.

Conclusion. L'équation n'a pas de solution.

— **Le critère général** : $ax \equiv b \pmod n$ a des solutions si et seulement si tout diviseur commun à a et n divise b. Ici 2 divise 4 et 6 mais pas 3.

Réponse. Aucune solution : $4x-3$ est impair alors que $6 \mid (4x-3)$ l'exigerait pair.

Correction de l'exercice 8 – Les restes possibles d'un carré

a) Il suffit de tester les huit classes : tout entier est congru à l'un des restes 0 à 7.

$x \equiv$	0	1	2	3	4	5	6	7
$x^2 \equiv$	0	1	4	1	0	1	4	1

— Détail de deux cases : $3^2 = 9 \equiv 1$ et $5^2 = 25 = 8 \times 3 + 1 \equiv 1 \pmod 8$.
— Un carré n'est donc congru qu'à 0, 1 ou 4 modulo 8 : les restes $2, 3, 5, 6, 7$ sont **impossibles**.

b) Si $8 \mid (x^2+5)$, alors $x^2 + 5 \equiv 0$, donc $x^2 \equiv -5 \equiv 3 \pmod 8$.

— Or 3 ne figure pas dans la liste $\{0\,;1\,;4\}$ des restes possibles d'un carré.
— **Conclusion.** x^2+5 n'est jamais divisible par 8, quel que soit l'entier x.
— Ce tableau des carrés est un outil à connaître : il sert à démontrer qu'une équation n'a pas de solution entière.

Réponse. a) $x^2 \equiv 0$, 1 ou $4 \pmod 8$ · b) $x^2 \equiv 3$ est impossible, donc $8 \nmid (x^2+5)$.

Correction de l'exercice 9 – Une équation du second degré modulo 12

On teste les douze classes modulo 12 :

$x \equiv$	0	1	2	3	4	5	6	7	8	9	10	11
$x^2 \equiv$	0	1	4	9	4	1	0	1	4	9	4	1

— Détail : $8^2 = 64 = 12 \times 5 + 4 \equiv 4$ et $10^2 = 100 = 12 \times 8 + 4 \equiv 4 \pmod{12}$.
— La valeur 4 apparaît **quatre** fois : $x \equiv 2$, $x \equiv 4$, $x \equiv 8$ ou $x \equiv 10 \pmod{12}$.

Conclusion. Il y a quatre classes solutions, alors que dans $\mathbb{R}$ l'équation $x^2 = 4$ n'a que deux solutions.

— L'arithmétique modulaire ne se comporte pas comme le calcul dans $\mathbb{R}$: un produit peut être nul sans qu'aucun facteur le soit, par exemple $4 \times 3 \equiv 0 \pmod{12}$.
— C'est exactement ce qui se passe ici : $x^2 - 4 = (x-2)(x+2)$ peut être divisible par 12 sans qu'aucun des deux facteurs le soit.

Réponse. $x \equiv 2$, 4, 8 ou $10 \pmod{12}$ (quatre classes).

Correction de l'exercice 10 – Équation affine

On isole d'abord le terme en x, exactement comme dans une équation ordinaire.

— $5x \equiv 1 - 3 = -2 \pmod{11}$, et $-2 \equiv 9 \pmod{11}$: on travaille avec $5x \equiv 9$.
— On cherche l'inverse de 5 modulo 11 : $5 \times 9 = 45 = 11 \times 4 + 1$, donc $5^{-1} \equiv 9 \pmod{11}$.
— On multiplie les deux membres par 9 :

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).

$$x \equiv 9 \times 9 = 81 \pmod{11}$$

— $81 = 11 \times 7 + 4$, donc $x \equiv 4 \pmod{11}$.

Vérification. $5 \times 4 + 3 = 23 = 11 \times 2 + 1 \equiv 1 \pmod{11}$ ✓.

— L'ensemble des solutions est $\{4 + 11k,\ k \in \mathbb{Z}\}$.

Réponse. $x \equiv 4 \pmod{11}$.

Correction de l'exercice 11 – Jamais divisible par 5

La stratégie : puisque n est congru modulo 5 à l'un des restes $0, 1, 2, 3, 4$, il suffit de tester **cinq** cas.

$n \equiv$	0	1	2	3	4
$n^2 \equiv$	0	1	4	4	1
$n^2 + n + 1 \equiv$	1	3	2	3	1

— Détail du cas $n \equiv 3$: $n^2 \equiv 9 \equiv 4$, donc $n^2 + n + 1 \equiv 4 + 3 + 1 = 8 \equiv 3 \pmod{5}$.
— Détail du cas $n \equiv 4$: $n^2 \equiv 16 \equiv 1$, donc $n^2 + n + 1 \equiv 1 + 4 + 1 = 6 \equiv 1 \pmod{5}$.
— Dans les cinq cas, le reste vaut 1, 2 ou 3 : **jamais** 0.

Conclusion. $n^2 + n + 1$ n'est jamais congru à 0 modulo 5, donc n'est jamais divisible par 5.

— Contrôle sur quelques valeurs : $n = 7$ donne 57, $n = 12$ donne 157, $n = 20$ donne 421 : aucun ne se termine par 0 ni par 5 ✓.

Réponse. $n^2 + n + 1 \equiv 1, 2$ ou $3 \pmod{5}$: jamais 0.

Correction de l'exercice 12 – Système de deux congruences

Méthode : on écrit la première condition sous forme d'une expression de x, et on la reporte dans la seconde.

— $x \equiv 1 \pmod{3}$ signifie $x = 3k + 1$, avec $k \in \mathbb{Z}$.
— On reporte : $3k + 1 \equiv 2 \pmod{5}$, donc $3k \equiv 1 \pmod{5}$.
— Inverse de 3 modulo 5 : $3 \times 2 = 6 \equiv 1$, donc $3^{-1} \equiv 2$.
— D'où $k \equiv 2 \times 1 = 2 \pmod{5}$, c'est-à-dire $k = 5m + 2$.
— En remontant :

$$x = 3(5m + 2) + 1 = 15m + 7$$

Conclusion. $x \equiv 7 \pmod{15}$, soit $\ldots, -8, 7, 22, 37, 52, \ldots$

— **Vérification** : $7 = 3 \times 2 + 1$ ✓ et $7 = 5 + 2$ ✓.
— Les deux conditions, portant sur les modules 3 et 5 qui n'ont pas de diviseur commun, se résument à **une seule** condition modulo $15 = 3 \times 5$.

Réponse. $x \equiv 7 \pmod{15}$.

Correction de l'exercice 13 – Des modules qui ont un diviseur commun

Ici 4 et 6 ont le diviseur commun 2 : le produit 24 ne sera pas le bon module, il faut être prudent.

— $x \equiv 3 \pmod{4}$ donne $x = 4k + 3$.
— On reporte : $4k + 3 \equiv 5 \pmod{6}$, donc $4k \equiv 2 \pmod{6}$.

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).

— On ne peut pas simplifier par 2 en gardant le module 6 : on divise **aussi** le module, ce qui donne $2k \equiv 1 \pmod 3$.
— Inverse de 2 modulo 3 : $2 \times 2 = 4 \equiv 1$, donc $k \equiv 2 \pmod 3$, soit $k = 3m + 2$.
— En remontant : $x = 4(3m + 2) + 3 = 12m + 11$.

Conclusion. $x \equiv 11 \pmod{12}$: $\ldots, -1, 11, 23, 35, \ldots$

— **Vérification** : $11 = 4 \times 2 + 3$ ✓ et $11 = 6 + 5$ ✓.
— Le module obtenu est 12 et non 24 : quand les modules ont un diviseur commun, le système se résout modulo leur plus petit multiple commun, et il peut même n'avoir **aucune** solution (essayer $x \equiv 1 \pmod 4$ et $x \equiv 2 \pmod 6$).

Réponse. $x \equiv 11 \pmod{12}$.

Correction de l'exercice 14 – Le sac de billes

On traduit l'énoncé en congruences. Si N est le nombre de billes :

$$N \equiv 3 \pmod 7 \qquad \text{et} \qquad N \equiv 1 \pmod 5$$

— $N \equiv 3 \pmod 7$ donne $N = 7k + 3$.
— On reporte dans la seconde : $7k + 3 \equiv 1 \pmod 5$, donc $2k \equiv -2 \pmod 5$ (car $7 \equiv 2$ et $3 - 1 = 2$).
— Inverse de 2 modulo 5 : $2 \times 3 = 6 \equiv 1$, donc $k \equiv 3 \times (-2) = -6 \equiv 4 \pmod 5$.
— Donc $k = 5m + 4$ et $N = 7(5m + 4) + 3 = 35m + 31$, c'est-à-dire $N \equiv 31 \pmod{35}$.

On sélectionne les valeurs entre 200 et 300 :

— $m = 5$: $N = 206$ · $m = 6$: $N = 241$ · $m = 7$: $N = 276$ ($m = 8$ donnerait 311, trop grand).
— **Vérification** de 206 : $206 = 7 \times 29 + 3$ ✓ et $206 = 5 \times 41 + 1$ ✓.

Conclusion. Le sac peut contenir 206, 241 ou 276 billes.

Réponse. $N \equiv 31 \pmod{35}$, donc 206, 241 ou 276 billes.

Correction de l'exercice 15 – Bilan : trois calculs modulaires

a) 9, 6 et 15 sont divisibles par 3 : on simplifie tout, module compris.

— $9x \equiv 6 \pmod{15} \Leftrightarrow 3x \equiv 2 \pmod 5$.
— Inverse de 3 modulo 5 : $3 \times 2 = 6 \equiv 1$, donc $x \equiv 2 \times 2 = 4 \pmod 5$.
— Modulo 15, cela fait **trois** classes : $x \equiv 4$, $x \equiv 9$ ou $x \equiv 14 \pmod{15}$.
— Vérification : $9 \times 14 = 126 = 15 \times 8 + 6$ ✓.

b) On teste les sept classes modulo 7 :

$n \equiv$	0	1	2	3	4	5	6
$n^2 + 3n \equiv$	0	4	3	4	0	5	5

— Détail du cas $n \equiv 5$: $25 + 15 = 40 = 7 \times 5 + 5 \equiv 5 \pmod 7$.
— Les restes possibles sont donc 0, 3, 4 et 5 : jamais 1.
— Or $7 \mid (n^2 + 3n - 1)$ exigerait $n^2 + 3n \equiv 1 \pmod 7$: impossible.

c) On note T le nombre de tuiles : $T \equiv 5 \pmod 7$ et $T \equiv 3 \pmod 9$.

— $T = 9m + 3$, reporté dans la première : $9m + 3 \equiv 5 \pmod 7$, soit $2m \equiv 2 \pmod 7$.
— 2 est inversible modulo 7 (car $2 \times 4 = 8 \equiv 1$), donc $m \equiv 1 \pmod 7$, soit $m = 7t + 1$.
— $T = 9(7t + 1) + 3 = 63t + 12$, donc $T \equiv 12 \pmod{63}$: 12, 75, 138, 201, …
— Entre 100 et 200, une seule valeur : $T = 138$.
— **Vérification** : $138 = 7 \times 19 + 5$ ✓ et $138 = 9 \times 15 + 3$ ✓.

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).

Réponse. a) $x \equiv 4$, 9 ou 14 $\pmod{15}$ · b) restes $\{0\,;3\,;4\,;5\}$, donc $7 \nmid (n^2+3n-1)$ · c) 138 tuiles.

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).