Plaquette 1 – Division euclidienne, congruences et critères

Divisibilité et congruences — Terminale maths expertes

Corrections détaillées

Boîte à outils

Définitions et théorèmes du cours.

— $b \mid a$ (« b divise a ») s'il existe $k \in \mathbb{Z}$ tel que $a = bk$.

— Propriétés : si $b \mid a$ et $b \mid a'$, alors $b \mid (au + a'v)$ pour tous entiers u, v (**combinaison linéaire**).

— **Division euclidienne** : pour $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$, il existe un unique couple $(q\,;r)$ tel que

$$a = bq + r \qquad \text{avec} \qquad 0 \leq r < b$$

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

— **Compatibilités** : si $a \equiv b \pmod{n}$ et $c \equiv d \pmod{n}$, alors

$$a + c \equiv b + d \pmod{n} \qquad ac \equiv bd \pmod{n} \qquad a^k \equiv b^k \pmod{n}$$

— **Attention** : on ne peut pas « diviser » une congruence par un entier quelconque.

— Pour déterminer un reste de a^k modulo n, on cherche d'abord un **cycle** des puissances de a modulo n.

— Critères classiques : $10 \equiv 1 \pmod{9}$ (somme des chiffres), $10 \equiv 1 \pmod{3}$, $10 \equiv -1 \pmod{11}$ (somme alternée).

Correction de l'exercice 1 – Divisibilité et combinaison linéaire

a) $7 \mid n$ donc $n = 7k$ pour un entier k.

— $3n + 14 = 21k + 14 = 7(3k + 2)$: c'est un multiple de 7, donc $7 \mid (3n + 14)$.

b) On utilise la propriété des **combinaisons linéaires** :

— $a = 5k$ et $b = 5k'$, donc

$$4a - 3b = 20k - 15k' = 5(4k - 3k')$$

— C'est un multiple de 5 : $5 \mid (4a - 3b)$.

— Cette propriété est l'outil de base de l'arithmétique : un diviseur commun divise toute combinaison linéaire.

Réponse. a) $3n + 14 = 7(3k + 2)$ · b) $4a - 3b = 5(4k - 3k')$.

Correction de l'exercice 2 – Division euclidienne

a) $7 \times 289 = 2\,023$, et $2\,026 - 2\,023 = 3$.

— Donc $2\,026 = 7 \times 289 + 3$, avec $q = 289$ et $r = 3$ (bien compris entre 0 et 6).

b) **Attention au cas négatif** : le reste doit rester **positif**.

— $5 \times (-10) = -50$, donc $-47 = 5 \times (-10) + 3$, avec $q = -10$ et $r = 3$.

— L'écriture $-47 = 5 \times (-9) - 2$ n'est **pas** la division euclidienne, car -2 n'est pas dans $[0\,;5[$.

Réponse. a) $2\,026 = 7 \times 289 + 3$ · b) $-47 = 5 \times (-10) + 3$.

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).

Correction de l’exercice 3 – Congruences élémentaires

On cherche le reste r avec $0 \leq r < 9$.

— a) $47 = 9 \times 5 + 2$, donc $47 \equiv 2 \pmod 9$.
— b) $100 = 9 \times 11 + 1$, donc $100 \equiv 1 \pmod 9$.
— c) $-13 = 9 \times (-2) + 5$, donc $-13 \equiv 5 \pmod 9$.
— Contrôle de c) : -13 et 5 diffèrent de 18, qui est bien un multiple de 9.

Réponse. a) 2 · b) 1 · c) 5.

Correction de l’exercice 4 – Opérations sur les congruences

On applique les compatibilités du cours, en remplaçant a et b par leurs restes.

— a) $a + b \equiv 3 + 5 = 8 \equiv 1 \pmod 7$.
— b) $ab \equiv 3 \times 5 = 15 \equiv 1 \pmod 7$ (car $15 = 14 + 1$).
— c) $a^2 \equiv 9 \equiv 2$ et $b^2 \equiv 25 \equiv 4$, donc $a^2 + b^2 \equiv 2 + 4 = 6 \pmod 7$.
— **Méthode** : on réduit à chaque étape pour garder de petits nombres.

Réponse. a) 1 · b) 1 · c) 6.

Correction de l’exercice 5 – Reste d’une puissance

On cherche un **cycle** des puissances de 3 modulo 7.

— $3^1 \equiv 3$; $3^2 \equiv 2$; $3^3 \equiv 6$; $3^4 \equiv 4$; $3^5 \equiv 5$; $3^6 \equiv 1 \pmod 7$.
— Le cycle est de longueur 6 : $3^6 \equiv 1$.
— On divise l’exposant par 6 : $100 = 6 \times 16 + 4$.

$$3^{100} = \left(3^6\right)^{16} \times 3^4 \equiv 1^{16} \times 4 = 4 \pmod 7$$

— Le reste est donc 4.

Réponse. Le reste est 4.

Correction de l’exercice 6 – Chiffre des unités

Le chiffre des unités est le reste modulo 10.

— Cycle des puissances de 7 : $7^1 \equiv 7$; $7^2 \equiv 9$; $7^3 \equiv 3$; $7^4 \equiv 1 \pmod{10}$.
— Le cycle est de longueur 4.
— $2026 = 4 \times 506 + 2$, donc

$$7^{2026} = \left(7^4\right)^{506} \times 7^2 \equiv 1 \times 9 = 9 \pmod{10}$$

— Le chiffre des unités de 7^{2026} est 9.

Réponse. 9.

Correction de l’exercice 7 – Critère de divisibilité par 9

a) $10 - 1 = 9$ est divisible par 9, donc $10 \equiv 1 \pmod 9$.

— Par compatibilité avec les puissances : $10^k \equiv 1^k = 1 \pmod 9$.

b) Un entier s’écrit $N = \sum a_k 10^k$ où les a_k sont ses chiffres.

— Comme $10^k \equiv 1$, on obtient $N \equiv \sum a_k \pmod 9$: **un entier est congru à la somme de ses chiffres modulo** 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).

— Donc $9 \mid N$ si et seulement si 9 divise la somme des chiffres.

c) Somme des chiffres de 47 835 : $4 + 7 + 8 + 3 + 5 = 27$, et $9 \mid 27$.

— Donc 47 835 est divisible par 9. Contrôle : $47\,835 = 9 \times 5\,315$.

Réponse. c) Oui : la somme des chiffres vaut 27, multiple de 9.

Correction de l'exercice 8 – Critère de divisibilité par 11

a) $10 - (-1) = 11$ est divisible par 11, donc $10 \equiv -1 \pmod{11}$.

b) On en déduit $10^k \equiv (-1)^k \pmod{11}$: les puissances alternent entre 1 et -1.

— Donc $N \equiv a_0 - a_1 + a_2 - a_3 + \cdots \pmod{11}$: c'est la **somme alternée** des chiffres, en partant des unités.

c) Pour 8 591 : chiffres 8, 5, 9, 1 (des milliers aux unités).

— Somme alternée depuis les unités : $1 - 9 + 5 - 8 = -11$.

— -11 est divisible par 11, donc 8 591 l'est aussi.

— Contrôle : $8\,591 = 11 \times 781$. Correct.

Réponse. c) Oui : la somme alternée vaut -11, multiple de 11.

Correction de l'exercice 9 – Discussion selon le reste

On distingue les cas selon le reste de n modulo 4 — ou plus simplement selon sa parité.

— Si n est **pair**, $n = 2k$, alors $n^2 = 4k^2 \equiv 0 \pmod{4}$.

— Si n est **impair**, $n = 2k + 1$, alors

$$n^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1 \equiv 1 \pmod{4}$$

— Les seuls restes possibles sont donc 0 et 1.

— **Conséquence utile** : un carré parfait n'est jamais congru à 2 ou 3 modulo 4. Par exemple, 4 003 n'est pas un carré, car $4\,003 \equiv 3 \pmod{4}$.

Réponse. $n^2 \equiv 0$ ou $1 \pmod{4}$.

Correction de l'exercice 10 – Démontrer une divisibilité

— **Par** 2 : parmi deux entiers **consécutifs**, l'un est nécessairement pair, donc le produit $n(n + 1)$ est divisible par 2.

— **Par** 6 : parmi trois entiers consécutifs, l'un au moins est pair (donc le produit est divisible par 2) et exactement un est divisible par 3 (les multiples de 3 se succèdent tous les trois entiers).

— Le produit est donc divisible par 2 **et** par 3. Comme 2 et 3 sont premiers entre eux, il est divisible par $2 \times 3 = 6$.

— Contrôle : pour $n = 4$, $4 \times 5 \times 6 = 120 = 6 \times 20$. Correct.

Réponse. Deux entiers consécutifs ⇒ un pair ; trois consécutifs ⇒ divisible par 2 et par 3, donc par 6.

Correction de l'exercice 11 – Résoudre une congruence

On ne peut pas « diviser par 3 » : on teste donc les cinq restes possibles modulo 5.

$x \pmod 5$	**0**	**1**	**2**	**3**	**4**
$3x \pmod 5$	0	3	1	4	2

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).

— La valeur 2 est obtenue pour $x \equiv 4 \pmod 5$.
— L'ensemble des solutions est donc $\{4 + 5k\,;\, k \in \mathbb{Z}\}$.
— Contrôle : $3 \times 4 = 12 = 10 + 2 \equiv 2 \pmod 5$. Correct.
— Astuce équivalente : $3 \times 2 = 6 \equiv 1 \pmod 5$, donc 2 est l'inverse de 3 modulo 5 ; en multipliant la congruence par 2, on obtient $x \equiv 4 \pmod 5$.

Réponse. $x \equiv 4 \pmod 5$.

Correction de l'exercice 12 – Application : jour de la semaine

Les jours de la semaine se répètent avec une période de 7 : on travaille **modulo** 7.

— $1\,000 = 7 \times 142 + 6$, donc $1\,000 \equiv 6 \pmod 7$.
— Il suffit donc d'avancer de 6 jours à partir du lundi : mardi, mercredi, jeudi, vendredi, samedi, **dimanche**.
— Réponse : ce sera un dimanche.
— Contrôle : $7 \times 142 = 994$ jours ramènent au même lundi, puis 6 jours de plus donnent dimanche.

Réponse. Un dimanche ($1\,000 \equiv 6 \pmod 7$).

Correction de l'exercice 13 – Divisibilité de n³ − n par 3

On factorise d'abord : $n^3 - n = n(n^2 - 1) = n(n-1)(n+1)$. On étudie ensuite les trois restes possibles de n modulo 3.

— Si $n \equiv 0 \pmod 3$, le facteur n est divisible par 3.
— Si $n \equiv 1 \pmod 3$, alors $n - 1 \equiv 0 \pmod 3$.
— Si $n \equiv 2 \pmod 3$, alors $n + 1 \equiv 3 \equiv 0 \pmod 3$.

Dans les trois cas, l'un des trois facteurs est divisible par 3, donc le produit aussi :

$$n^3 - n = (n-1)\,n\,(n+1) \equiv 0 \pmod 3$$

C'est naturel : parmi trois entiers consécutifs, il y a toujours un multiple de 3. **Contrôle** : pour $n = 5$, $125 - 5 = 120 = 3 \times 40$.

Réponse. $n^3 - n = (n-1)n(n+1)$: l'un des trois entiers consécutifs est multiple de 3.

Correction de l'exercice 14 – Chiffre des unités d'un carré

a) Le chiffre des unités d'un entier est son reste dans la division par 10, et $n^2 \pmod{10}$ ne dépend que de $n \pmod{10}$. On teste les dix restes :

$n \bmod 10$	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
$n^2 \bmod 10$	0	1	4	9	6	5	6	9	4	1

Un carré se termine donc toujours par 0, 1, 4, 5, 6 ou 9 ; jamais par 2, 3, 7 ou 8.

b) On a

$$2\,027 \equiv 7 \pmod{10} \qquad 13\,578 \equiv 8 \pmod{10}$$

Aucun de ces deux nombres n'a un chiffre des unités possible pour un carré : ce ne sont pas des carrés d'entiers. **Contrôle** : $45^2 = 2\,025 < 2\,027 < 2\,116 = 46^2$.

Réponse. a) 0, 1, 4, 5, 6 ou 9 · b) ils se terminent par 7 et 8, impossible pour un carré.

Correction de l'exercice 15 – Synthèse : suite et congruences

a) $u_0 = 1 + 5 = 6$; $u_1 = 4 + 5 = 9$; $u_2 = 16 + 5 = 21$; $u_3 = 64 + 5 = 69$.

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).

— Restes modulo 3 : $6 \equiv 0$; $9 \equiv 0$; $21 \equiv 0$; $69 \equiv 0$. Tous nuls : on conjecture que $3 \mid u_n$.

b) **Démonstration par les congruences.**

— $4 \equiv 1 \pmod 3$, donc par compatibilité avec les puissances : $4^n \equiv 1^n = 1 \pmod 3$.
— Ainsi $u_n = 4^n + 5 \equiv 1 + 5 = 6 \equiv 0 \pmod 3$.
— Conclusion : 3 divise u_n pour **tout** entier naturel n.
— Cette méthode est bien plus rapide qu'une récurrence : elle traite tous les cas d'un coup.

Réponse. a) 6, 9, 21, 69, tous divisibles par 3 · b) $4^n \equiv 1 \pmod 3$ donc $u_n \equiv 6 \equiv 0$.

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).