

Fiche A1.3 : Congruences dans $\mathbb{Z}$

1 - Définition et premières propriétés

- Nous sommes mercredi : quel jour serons-nous dans 100 jours ? Seul compte le reste de 100 dans la division par 7 : $100 = 7 \times 14 + 2$, donc ce sera un vendredi. Gauss a introduit en 1801 la notion de **congruence**, qui permet de calculer directement sur les restes.

Définition : Soit n un entier naturel, $n \geq 2$. On dit que deux entiers relatifs a et b sont **congrus modulo n** si n divise $a-b$. On note $a \equiv b [n]$ (ou $a \equiv b \pmod{n}$).

Propriété 1 : $a \equiv b [n]$ si et seulement si a et b ont le **même reste** dans la division euclidienne par n .

Démonstration :

- Écrivons $a = nq + r$ et $b = nq' + r'$ avec $0 \leq r < n$ et $0 \leq r' < n$. Alors $a-b = n(q-q') + (r-r')$.

Si $r = r'$, alors $a-b = n(q-q')$: n divise $a-b$.

- Réciproquement, si $a \equiv b [n]$, c'est à dire si $n|a-b$, alors n divise $(a-b) - n(q-q') = r-r'$.

Or $-n < r-r' < n$, donc $r-r' = 0$ (comme dans la fiche A1.2) : $r = r'$. $\square$

Conséquences :

- Si $0 \leq r < n$: $a \equiv r [n] \Leftrightarrow r$ est le reste de la division euclidienne de a par n .
- $a \equiv 0 [n] \Leftrightarrow n|a$.
- Tout entier est congru modulo n à **un et un seul** entier de $\{0 ; 1 ; \dots ; n-1\}$: son reste dans la d.e. par n

Exemple 1 :

a) Vérifier que $38 \equiv 3 [5]$ et $-7 \equiv 5 [12]$.

$$38-3 = 35 = 5 \times 7 \checkmark ; \quad -7-5 = -12 = 12 \times (-1) \checkmark$$

b) Déterminer le reste de 2026 modulo 10, et celui de -23 modulo 4.

$2026 = 10 \times 202 + 6$ donc $2026 \equiv 6 [10]$: modulo 10, un entier est congru à son chiffre des unités.

$-23 = 4 \times (-6) + 1$ donc $-23 \equiv 1 [4]$: le reste est 1.

Point de vigilance : $a \equiv r [n]$ donne le reste **seulement si** $0 \leq r < n$.

Par exemple $38 \equiv 13 [5]$ est vrai, mais le reste de 38 modulo 5 est 3, et non 13.

Propriété 2 : Soient $n \geq 2$ et a, b, c trois entiers relatifs.

- $a \equiv a [n]$ (réflexivité).
- Si $a \equiv b [n]$, alors $b \equiv a [n]$ (symétrie).
- Si $a \equiv b [n]$ et $b \equiv c [n]$, alors $a \equiv c [n]$ (transitivité).

Démonstration (transitivité) : $a-c = (a-b) + (b-c)$ est la somme de deux multiples de n : c'est un multiple de n (propriété 3 de la fiche A1.1). $\square$

2 - Compatibilité avec les opérations

Propriété 3 : Soient $n \geq 2$ et a, b, a', b' des entiers relatifs tels que $a \equiv b [n]$ et $a' \equiv b' [n]$. Alors :

- $a + a' \equiv b + b' [n]$ et $a - a' \equiv b - b' [n]$;
- $ka \equiv kb [n]$ pour tout $k \in \mathbb{Z}$;
- $aa' \equiv bb' [n]$;
- $a^p \equiv b^p [n]$ pour tout $p \in \mathbb{N}$.

Démonstration :

- $(a + a') - (b + b') = (a - b) + (a' - b')$ est une somme de deux multiples de n , donc un multiple de n .

De même pour la différence, et $ka - kb = k(a - b)$.

- $aa' - bb' = aa' - ab' + ab' - bb' = a(a' - b') + b'(a - b)$: c'est une combinaison linéaire de $a' - b'$ et $a - b$, qui sont multiples de n . Donc $n | aa' - bb'$.

- Par récurrence sur p : $a^0 = b^0 = 1$, et si $a^p \equiv b^p [n]$, alors $a^{p+1} = a^p \times a \equiv b^p \times b = b^{p+1} [n]$. $\square$

Remarque : dans une somme, un produit ou une puissance, on peut donc **remplacer** un nombre par n'importe quel nombre qui lui est congru : son reste, ou un nombre négatif plus simple (ex : $99 \equiv -1 [100]$).

Exemple 2 : Déterminer le reste de la division euclidienne de $2025 \times 2026 + 2027$ par 7.

$2023 = 7 \times 289$, donc $2025 \equiv 2 [7]$, $2026 \equiv 3 [7]$ et $2027 \equiv 4 [7]$.

Ainsi $2025 \times 2026 + 2027 \equiv 2 \times 3 + 4 = 10 \equiv 3 [7]$: le reste est 3.

Point de vigilance :

- on ne peut **pas diviser** : $2 \times 3 \equiv 2 \times 1 [4]$ (car $6 \equiv 2 [4]$), mais $3 \not\equiv 1 [4]$.
- on ne remplace **pas un exposant** par un nombre congru : $4 \equiv 1 [3]$, mais $2^4 = 16 \equiv 1 [3]$ alors que $2^1 = 2$.

Méthode (reste de a^p modulo n) : On cherche une petite puissance a^k congrue à 1 (ou à -1) modulo n .

Puis, on effectue la division euclidienne de l'exposant : $p = kq + r$. Alors $a^p = (a^k)^q \times a^r \equiv 1^q \times a^r = a^r [n]$.

Exemple 3 :

a) Étudier les restes de 2^n modulo 7.

$2^0 \equiv 1$; $2^1 \equiv 2$; $2^2 \equiv 4$; $2^3 = 8 \equiv 1 [7]$. Les restes se répètent avec une période 3 : 1 ; 2 ; 4 ; 1 ; 2 ; 4 ; ...

b) En déduire le reste de 2^{2026} modulo 7.

$2026 = 3 \times 675 + 1$, donc $2^{2026} = (2^3)^{675} \times 2 \equiv 1^{675} \times 2 = 2 [7]$: le reste est 2.

c) Montrer que pour tout $n \in \mathbb{N}$, 7 divise $2^{3n} - 1$.

$2^{3n} = (2^3)^n = 8^n \equiv 1^n = 1 [7]$, donc $2^{3n} - 1 \equiv 0 [7]$: 7 divise $2^{3n} - 1$.

Exemple 4 : Déterminer le chiffre des unités de 7^{2027} .

Le chiffre des unités est le reste modulo 10. $7^1 \equiv 7 [10]$; $7^2 = 49 \equiv 9 \equiv -1 [10]$;

$2027 = 2 \times 1013 + 1$, donc $7^{2027} = (7^2)^{1013} \times 7 \equiv (-1)^{1013} \times 7 \equiv -7 \equiv 3 [10]$: le chiffre des unités est 3.

Exemple 5 : Montrer que pour tout $n \in \mathbb{N}$, $3^{2n+1} + 2^{n+2}$ est divisible par 7.

$3^{2n+1} = 3 \times (3^2)^n = 3 \times 9^n \equiv 3 \times 2^n [7]$ et par ailleurs $2^{n+2} = 4 \times 2^n$.

Donc $3^{2n+1} + 2^{n+2} \equiv 3 \times 2^n + 4 \times 2^n = 7 \times 2^n \equiv 0 [7]$: $3^{2n+1} + 2^{n+2}$ est divisible par 7.