# Arithmétique : divisibilité et congruences

## Prélude - Historique et contexte

L'arithmétique, étude des nombres entiers, est l'une des plus anciennes branches des mathématiques : le livre VII des *Éléments* d'Euclide (vers 300 av. J.-C.) expose déjà la division euclidienne. En 1801, Gauss introduit dans ses *Disquisitiones arithmeticae* la notion de congruence, qui permet de calculer « sur les restes ». Ces outils sont au cœur des clés de contrôle (numéro de sécurité sociale, ISBN, IBAN) et de la cryptographie.

## I Divisibilité dans $\mathbb{Z}$

### Définition

Soit $a$ et $b$ deux entiers relatifs. On dit que $a$ **divise** $b$ (ou que $b$ est un **multiple** de $a$) s'il existe un entier relatif $k$ tel que $b = ka$. On note $a \mid b$.

### Exemple

$7 \mid 91$ car $91 = 13 \times 7$ ; $-4 \mid 12$ ; tout entier divise 0. Les diviseurs de 12 dans $\mathbb{Z}$ sont $\pm 1$, $\pm 2$, $\pm 3$, $\pm 4$, $\pm 6$, $\pm 12$.

### Propriété

Soit $a$, $b$, $c$ des entiers relatifs.

- Transitivité : si $a \mid b$ et $b \mid c$, alors $a \mid c$.
- Combinaison linéaire : si $a \mid b$ et $a \mid c$, alors pour tous entiers $u$ et $v$, $a \mid ub + vc$.

Démonstration du second point : $b = ka$ et $c = k'a$ donnent $ub + vc = (uk + vk')a$.

### Méthode - Utiliser une combinaison linéaire

Déterminer les entiers $n$ tels que $n+2$ divise $3n+11$. Si $n+2 \mid 3n+11$, comme $n+2 \mid 3(n+2)$, alors $n+2 \mid (3n+11) - 3(n+2) = 5$. Donc $n+2 \in \{-5\ ;\ -1\ ;\ 1\ ;\ 5\}$, soit $n \in \{-7\ ;\ -3\ ;\ -1\ ;\ 3\}$, et on vérifie que ces valeurs conviennent.

## II Division euclidienne

### Propriété - Théorème (admis)

Soit $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. Il existe un unique couple d'entiers $(q\ ;\ r)$ tel que

$$a = bq + r \quad \text{et} \quad 0 \leqslant r < b.$$

$q$ est le **quotient** et $r$ le **reste** de la division euclidienne de $a$ par $b$. $b$ divise $a$ si et seulement si $r = 0$.

### Exemple

$75 = 7 \times 10 + 5$ : quotient 10, reste 5. $-17 = 5 \times (-4) + 3$ : quotient $-4$, reste 3 (et non $-2$).
En Python : `a // b` donne le quotient et `a % b` le reste.

# III Congruences

## Définition

Soit $n \geqslant 2$. Deux entiers $a$ et $b$ sont **congrus modulo** $n$ s'ils ont le même reste dans la division euclidienne par $n$, ce qui équivaut à $n \mid a-b$. On note $a \equiv b\ [n]$.

## Exemple

$23 \equiv 2\ [7]$ ; $-1 \equiv 6\ [7]$ ; $a \equiv 0\ [n] \iff n \mid a$.

## Propriété - Compatibilité avec les opérations

Si $a \equiv b\ [n]$ et $c \equiv d\ [n]$, alors pour tout $k \in \mathbb{N}$ :

$$a+c \equiv b+d\ [n] \qquad ac \equiv bd\ [n] \qquad a^k \equiv b^k\ [n].$$

Attention : on ne peut pas « diviser » une congruence en général ($2 \times 3 \equiv 2 \times 0\ [6]$ mais $3 \not\equiv 0\ [6]$).

## Méthode - Reste d'une grande puissance

Reste de $3^{2026}$ dans la division par 8 : $3^2 = 9 \equiv 1\ [8]$, donc $3^{2026} = \left(3^2\right)^{1013} \equiv 1^{1013} = 1\ [8]$. Le reste est 1.

## Méthode - Tableau de congruences

Montrer que pour tout entier $n$, $n(n^2+2)$ est divisible par 3 : on étudie les restes possibles modulo 3.

| $n \equiv \ldots\ [3]$ | 0 | 1 | 2 |
|---|---|---|---|
| $n^2+2 \equiv \ldots\ [3]$ | 2 | 0 | 0 |
| $n(n^2+2) \equiv \ldots\ [3]$ | 0 | 0 | 0 |

## Méthode - Résoudre une congruence

Résoudre $3x \equiv 2\ [5]$. On teste les restes 0 à 4 : $3 \times 4 = 12 \equiv 2\ [5]$, seul $x \equiv 4\ [5]$ convient. Les solutions sont les entiers $x = 4+5k$, $k \in \mathbb{Z}$.