

Cours — Chapitre 14

Arithmétique dans $\mathbb{Z}$

1^{ère} Bac Sciences Mathématiques · Lycée Qualifiant Ibn Hazm · Prof. El Koudri Hamza · 2026–2027

Plan du chapitre. I. Divisibilité dans $\mathbb{Z}$ — II. Division euclidienne — III. Congruences modulo n — IV. Nombres premiers — V. PGCD et PPCM — VI. L'ensemble $\mathbb{Z}/n\mathbb{Z}$ — Résumé.

Prérequis. Ensembles $\mathbb{N}$ et $\mathbb{Z}$, raisonnement par récurrence, par contraposée et par l'absurde (Ch. 01), dénombrement (Ch. 13) pour compter les diviseurs. Notation : on écrit « a divise b » en toutes lettres.

I. Divisibilité dans $\mathbb{Z}$

1) Définition

Définition 1

Soient $a, b \in \mathbb{Z}$. On dit que a **divise** b (ou que b est un **multiple** de a) s'il existe $k \in \mathbb{Z}$ tel que $b = ka$. L'ensemble des multiples de a est noté $a\mathbb{Z}$.

Exemple 1

3 divise -12 car $-12 = (-4) \times 3$; 0 est multiple de tout entier ; 1 et -1 divisent tout entier.

2) Propriétés

Propriété 1

Soient $a, b, c \in \mathbb{Z}$.
— a divise a ; si a divise b et b divise c , alors a divise c (transitivité).
— Si a divise b et b divise a , alors $|a| = |b|$.
— Si a divise b et a divise c , alors pour tous $u, v \in \mathbb{Z}$, a divise $ub + vc$ (combinaison linéaire).
— Si a divise b et $b \neq 0$, alors $|a| \leq |b|$.

Solution

Preuve de la combinaison linéaire (raisonnement direct). a divise b et a divise $c \implies$ il existe $k, k' \in \mathbb{Z}$ tels que $b = ka$ et $c = k'a \implies ub + vc = (uk + vk')a$ avec $uk + vk' \in \mathbb{Z} \implies a$ divise $ub + vc$.

Exemple 2

Soit $n \in \mathbb{Z}$ tel que $n + 2$ divise $3n + 1$. Comme $n + 2$ divise $3(n + 2)$, il divise $3(n + 2) - (3n + 1) = 5$: donc $n + 2 \in \{-5; -1; 1; 5\}$, soit $n \in \{-7; -3; -1; 3\}$ (on vérifie que ces valeurs conviennent).

II. Division euclidienne

1) Théorème

Théorème 1 (admis)

Soient $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. Il existe un **unique** couple $(q; r) \in \mathbb{Z} \times \mathbb{N}$ tel que $a = bq + r$ et $0 \leq r < b$. q est le **quotient** et r le **reste** de la division euclidienne de a par b .

Exemple 3

$-23 = 5 \times (-5) + 2$: le quotient de -23 par 5 est -5 et le reste 2 (et non -3 , car il faut $0 \leq r < 5$).

2) Conséquence

Propriété 2

Soit $b \in \mathbb{N}^*$. Tout entier a s'écrit sous l'une des formes $bk, bk + 1, \dots, bk + (b - 1)$ avec $k \in \mathbb{Z}$. En particulier tout entier est de la forme $2k$ ou $2k + 1$, et de la forme $3k, 3k + 1$ ou $3k + 2$.

Exemple 4

Pour tout $n \in \mathbb{Z}$, $n(n + 1)(n + 2)$ est divisible par 3 : on traite les trois cas $n = 3k, n = 3k + 1, n = 3k + 2$; dans chaque cas l'un des trois facteurs est multiple de 3.

III. Congruences modulo n

1) Définition

Définition 2

Soient $n \in \mathbb{N}^*$ et $a, b \in \mathbb{Z}$. On dit que a est **congru** à b modulo n , et on note $a \equiv b [n]$, si n divise $a - b$. Cela équivaut à : a et b ont le même reste dans la division euclidienne par n .

Propriété 3

Si r est le reste de la division euclidienne de a par n , alors $a \equiv r [n]$ et $0 \leq r < n$. Réciproquement, si $a \equiv r [n]$ et $0 \leq r < n$, alors r est ce reste.

2) Compatibilité avec les opérations

Propriété 4

Soient $n \in \mathbb{N}^*$ et $a, b, c, d \in \mathbb{Z}$ tels que $a \equiv b [n]$ et $c \equiv d [n]$. Alors :

- $a + c \equiv b + d [n]$ et $a - c \equiv b - d [n]$;
- $ac \equiv bd [n]$;
- pour tout $k \in \mathbb{N}$: $a^k \equiv b^k [n]$;
- la relation $\equiv$ est réflexive, symétrique et transitive.

Solution

Preuve de $a^k \equiv b^k [n]$ (raisonnement par récurrence sur k). Initialisation : pour $k = 0$, on a $a^0 = 1 \equiv 1 = b^0 [n]$. Hérédité : soit $k \in \mathbb{N}$, on suppose $a^k \equiv b^k [n]$; comme $a \equiv b [n]$, la compatibilité avec le produit donne $a^{k+1} = a^k a \equiv b^k b = b^{k+1} [n]$. Conclusion : d'après le principe du raisonnement par récurrence, $a^k \equiv b^k [n]$ pour tout $k \in \mathbb{N}$.

Exemple 5

Reste de 2^{2027} dans la division par 7 : $2^3 = 8 \equiv 1 [7]$ et $2027 = 3 \times 675 + 2$, donc $2^{2027} = (2^3)^{675} \times 2^2 \equiv 1 \times 4 = 4 [7]$. Le reste est 4.

IV. Nombres premiers

1) Définition et critère

Définition 3

Un entier naturel p est **premier** s'il admet exactement deux diviseurs dans $\mathbb{N}$: 1 et p . (1 n'est pas premier.)

Propriété 5

- Tout entier naturel $n \geq 2$ admet au moins un diviseur premier.
- Si $n \geq 2$ n'est pas premier, il admet un diviseur premier p tel que $p^2 \leq n$. Donc si aucun nombre premier p tel que $p^2 \leq n$ ne divise n , alors n est premier.
- L'ensemble des nombres premiers est infini.

Solution

Preuve du dernier point (raisonnement par l'absurde). Supposons qu'il n'y ait qu'un nombre fini de nombres premiers $p_1, \dots, p_k$ et posons $N = p_1 p_2 \cdots p_k + 1 \geq 2$. N admet un diviseur premier, donc un p_i divise N ; comme p_i divise aussi $p_1 \cdots p_k$, il divise la différence 1 : contradiction avec $p_i \geq 2$.

2) Décomposition en facteurs premiers**Théorème 2 (admis)**

Tout entier $n \geq 2$ s'écrit de façon unique (à l'ordre près) $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ où $p_1 < \cdots < p_k$ sont premiers et $\alpha_i \in \mathbb{N}^*$.

Propriété 6 : nombre de diviseurs

Avec la décomposition ci-dessus, les diviseurs positifs de n sont les $p_1^{\beta_1} \cdots p_k^{\beta_k}$ avec $0 \leq \beta_i \leq \alpha_i$; leur nombre est (principe multiplicatif, Ch. 13) $(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1)$.

Exemple 6

$360 = 2^3 \times 3^2 \times 5$ possède $4 \times 3 \times 2 = 24$ diviseurs positifs.

Propriété 7 (lemme d'Euclide, admis)

Si un nombre premier p divise un produit ab ($a, b \in \mathbb{Z}$), alors p divise a ou p divise b .

V. PGCD et PPCM**1) Définitions****Définition 4**

Soient $a, b \in \mathbb{Z}$ non tous deux nuls. Le **PGCD** de a et b , noté $\text{PGCD}(a; b)$ ou $a \wedge b$, est le plus grand diviseur commun de a et b . Pour $a, b \in \mathbb{Z}^*$, le **PPCM**, noté $\text{PPCM}(a; b)$ ou $a \vee b$, est le plus petit multiple commun **strictement positif**. On dit que a et b sont **premiers entre eux** si $a \wedge b = 1$.

2) Propriétés et algorithme d'Euclide**Propriété 8**

Soient $a, b \in \mathbb{Z}^*$.

- Pour tout $k \in \mathbb{Z}$: $a \wedge b = b \wedge (a - kb)$. En particulier, si $a = bq + r$ (division euclidienne), $a \wedge b = b \wedge r$.
- **Algorithme d'Euclide** : on effectue des divisions successives; le PGCD est le dernier reste non nul.
- Les diviseurs communs à a et b sont exactement les diviseurs de $a \wedge b$; les multiples communs sont les multiples de $a \vee b$.
- $(a \wedge b) \times (a \vee b) = |ab|$; pour $k \in \mathbb{N}^*$: $(ka) \wedge (kb) = k(a \wedge b)$.
- Si $d = a \wedge b$, alors $a = da'$ et $b = db'$ avec $a' \wedge b' = 1$.
- Avec les décompositions en facteurs premiers : $a \wedge b$ (resp. $a \vee b$) est le produit des facteurs premiers communs (resp. de tous les facteurs) affectés du plus petit (resp. plus grand) exposant.

Exemple 7

$\text{PGCD}(1071; 462)$: $1071 = 462 \times 2 + 147$, $462 = 147 \times 3 + 21$, $147 = 21 \times 7 + 0$: $1071 \wedge 462 = 21$ et $1071 \vee 462 = \frac{1071 \times 462}{21} = 23\,562$.

VI. L'ensemble $\mathbb{Z}/n\mathbb{Z}$

1) Classes d'équivalence

Définition 5

Soit $n \in \mathbb{N}^*$, $n \geq 2$. La **classe** de $a \in \mathbb{Z}$ modulo n est $\bar{a} = \{b \in \mathbb{Z} / b \equiv a[n]\} = a + n\mathbb{Z}$. On a $\bar{a} = \bar{b} \iff a \equiv b[n]$. L'ensemble des classes est $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}; \bar{1}; \dots; \overline{n-1}\}$; il a n éléments.

2) Opérations

Propriété 9

On définit $\bar{a} + \bar{b} = \overline{a+b}$ et $\bar{a} \times \bar{b} = \overline{ab}$ (ces définitions ne dépendent pas des représentants choisis, d'après la propriété 4). On résout une équation dans $\mathbb{Z}/n\mathbb{Z}$ en testant les n classes, à l'aide d'une **table** d'addition ou de multiplication.

Exemple 8

Dans $\mathbb{Z}/5\mathbb{Z}$: $\bar{3} \times \bar{x} = \bar{2}$. Les produits $\bar{3} \times \bar{0}, \dots, \bar{3} \times \bar{4}$ valent $\bar{0}, \bar{3}, \bar{1}, \bar{4}, \bar{2}$: l'unique solution est $\bar{x} = \bar{4}$.

Résumé

Remarque — l'essentiel

- a divise $b \iff \exists k \in \mathbb{Z}, b = ka$; un diviseur commun divise toute combinaison linéaire.
- Division euclidienne : $a = bq + r, 0 \leq r < b$; $a \equiv b[n] \iff n$ divise $a - b$; congruences compatibles avec $+$, $\times$, puissances.
- Décomposition en facteurs premiers; nombre de diviseurs $\prod(\alpha_i + 1)$.
- $a \wedge b = b \wedge (a - kb)$; algorithme d'Euclide; $(a \wedge b)(a \vee b) = |ab|$.
- $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}; \dots; \overline{n-1}\}$, opérations sur les représentants.