

Fiche de cours

Arithmétique des entiers relatifs

Divisibilité, division euclidienne, pgcd et ppcm, nombres premiers, valuations, congruences

définitions · théorèmes et hypothèses · méthodes · démonstrations exigibles

1 DIVISIBILITÉ DANS $\mathbb{Z}$

Définition. Soient $a, b \in \mathbb{Z}$. On dit que a **divise** b , et l'on note $a \mid b$, lorsqu'il existe $k \in \mathbb{Z}$ tel que $b = ak$. On dit aussi que a est un **diviseur** de b , ou que b est un **multiple** de a . On note $\mathcal{D}(b) = \{d \in \mathbb{Z}, d \mid b\}$ l'ensemble des diviseurs de b .

Propriété — règles de calcul. Soient $a, b, c, u, v \in \mathbb{Z}$.

■ FORMULAIRE

- $a \mid 0$ pour tout a ; $1 \mid b$ pour tout b ; $0 \mid b \iff b = 0$;
- **transitivité** : si $a \mid b$ et $b \mid c$, alors $a \mid c$;
- **combinaisons linéaires** : si $a \mid b$ et $a \mid c$, alors $a \mid (ub + vc)$ pour tous $u, v \in \mathbb{Z}$;
- si $a \mid b$ et $b \neq 0$, alors $|a| \leq |b|$: tout entier non nul n'a qu'un nombre fini de diviseurs;
- $a \mid b \iff |a| \mid |b|$: la divisibilité ne dépend que des valeurs absolues.

Théorème — entiers associés. Soient $a, b \in \mathbb{Z}$. Alors $a \mid b$ et $b \mid a \iff b = a$ ou $b = -a$. On dit alors que a et b sont **associés**. En particulier, deux entiers *naturels* qui se divisent mutuellement sont égaux.

Idée de preuve (exigible). Si $a = 0$, $a \mid b$ donne $b = 0$. Sinon $|a| \leq |b|$ et $|b| \leq |a|$, donc $|a| = |b|$.

✗ ATTENTION

$a \mid b$ est une *assertion*, pas un nombre : on n'écrit jamais « $a \mid b = c$ », et l'on ne confond pas $a \mid b$ avec $\frac{a}{b}$. La divisibilité est une relation d'ordre sur $\mathbb{N}$, mais pas sur $\mathbb{Z}$: elle n'y est pas antisymétrique ($1 \mid -1$ et $-1 \mid 1$).

2 DIVISION EUCLIDIENNE

Théorème — division euclidienne. Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$. Il existe un *unique* couple $(q, r) \in \mathbb{Z}^2$ tel que

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

L'entier q est le **quotient**, r le **reste** de la division euclidienne de a par b . De plus $b \mid a \iff r = 0$.

Idée de preuve (exigible). Existence pour $b > 0$: $E = \{k \in \mathbb{Z}, bk \leq a\}$ est non vide et majoré, donc admet un plus grand élément q ; alors $bq \leq a < b(q+1)$ et $r = a - bq$ convient. *Unicité* : si $bq + r = bq' + r'$ avec $0 \leq r, r' < b$, alors $b(q - q') = r' - r$ avec $|r' - r| < b$, donc $r = r'$ puis $q = q'$. Le cas $b < 0$ s'en déduit en remplaçant b par $-b$. Pour $b > 0$, $q = \lfloor \frac{a}{b} \rfloor$.

✗ ATTENTION

Le reste est **toujours positif**, même si $a < 0$. Ainsi $-100 = 7 \times (-15) + 5$: le quotient est -15 et le reste 5, pas $-100 = 7 \times (-14) - 2$. Une erreur classique consiste à écrire $q = -14$ parce que « -14 est plus proche ».

Méthode — disjonction selon le reste. pour étudier une propriété de $n \in \mathbb{Z}$ modulo b , écrire $n = bq + r$ avec $r \in \llbracket 0; b-1 \rrbracket$ et traiter les b cas : ils recouvrent $\mathbb{Z}$ sans se chevaucher, par unicité du reste.

3 PGCD, ALGORITHME D'EUCLIDE, PPCM

Théorème — pgcd. Soient $a, b \in \mathbb{Z}$ non tous deux nuls. L'ensemble $\mathcal{D}(a) \cap \mathcal{D}(b)$ des diviseurs communs à a et b admet un plus grand élément, appelé **pgcd** de a et b et noté $a \wedge b$; il appartient à $\mathbb{N}^*$ et vérifie $\mathcal{D}(a) \cap \mathcal{D}(b) = \mathcal{D}(a \wedge b)$. Ainsi $a \wedge b$ est le plus grand des diviseurs communs *au sens de la divisibilité* : tout diviseur commun divise $a \wedge b$.

Propriété — règles de calcul. Pour $a, b, c \in \mathbb{Z}$ non tous nuls et $k \in \mathbb{N}^*$:

■ FORMULAIRE

- $a \wedge b = b \wedge a = |a| \wedge |b|$; $a \wedge 0 = |a|$ ($a \neq 0$); $a \wedge 1 = 1$; $a \mid b \iff a \wedge b = |a|$ (pour $a \neq 0$);
- **homogénéité** : $(ka) \wedge (kb) = k(a \wedge b)$;
- **clé de l'algorithme** : $a \wedge b = b \wedge r$, où r est le reste de la division euclidienne de a par b ($b \neq 0$); plus généralement $a \wedge b = (a - qb) \wedge b$ pour tout $q \in \mathbb{Z}$;
- **associativité** : $(a \wedge b) \wedge c = a \wedge (b \wedge c)$, ce qui autorise la notation $a_1 \wedge \dots \wedge a_n$.

Théorème — algorithme d'Euclide. Soient $a, b \in \mathbb{N}$ avec $b \neq 0$. On pose $r_0 = a, r_1 = b$ et, tant que $r_k \neq 0$, on note r_{k+1} le reste de la division euclidienne de r_{k-1} par r_k . Si $r_{N+1} = 0$ est le premier reste nul, alors $a \wedge b = r_N$: le pgcd est le dernier reste non nul.

Idée de preuve (exigible). Terminaison : $(r_k)_{k \geq 1}$ est une suite d'entiers naturels strictement décroissante tant qu'elle ne s'annule pas, donc elle s'annule. Correction : à chaque étape $r_{k-1} \wedge r_k = r_k \wedge r_{k+1}$ d'après la règle ci-dessus; par récurrence $a \wedge b = r_N \wedge r_{N+1} = r_N \wedge 0 = r_N$.

Théorème — relation de Bézout. Soient $a, b \in \mathbb{Z}$ non tous nuls et $d = a \wedge b$. Il existe $(u, v) \in \mathbb{Z}^2$ tel que

$$au + bv = d.$$

Un tel couple (u, v) , appelé **couple de Bézout** de (a, b) , s'obtient par l'**algorithme d'Euclide étendu** : on remonte les divisions successives en exprimant chaque reste comme combinaison de a et b .

✖ ATTENTION

De $au + bv = c$ on ne peut conclure $a \wedge b = c$, mais seulement $(a \wedge b) \mid c$: ainsi $6 \times 2 + 4 \times (-1) = 8$ alors que $6 \wedge 4 = 2$. Le couple (u, v) n'est jamais unique : $(u + kb', v - ka')$ convient aussi, où $a = da'$ et $b = db'$.

Définition. Soient $a, b \in \mathbb{Z}^*$. L'ensemble des multiples communs strictement positifs de a et b est non vide (il contient $|ab|$) : il admet un plus petit élément, appelé **ppcm** de a et b et noté $a \vee b$. Les multiples communs de a et b sont exactement les multiples de $a \vee b$, et $(a \wedge b)(a \vee b) = |ab|$. En particulier, si $a \wedge b = 1$ alors $a \vee b = |ab|$.

4 ENTIERS PREMIERS ENTRE EUX

Définition. Deux entiers a et b sont **premiers entre eux** lorsque $a \wedge b = 1$, c'est-à-dire lorsque leurs seuls diviseurs communs sont 1 et -1 .

Théorème — théorème de Bézout. Soient $a, b \in \mathbb{Z}$. Alors

$$a \wedge b = 1 \iff \exists (u, v) \in \mathbb{Z}^2, au + bv = 1.$$

Idée de preuve (exigible). $(\Rightarrow)$ c'est la relation de Bézout avec $d = 1$. $(\Leftarrow)$ si $au + bv = 1$, tout diviseur commun d de a et b divise $au + bv = 1$, donc $d \in \{-1, 1\}$: $a \wedge b = 1$.

Théorème — lemme de Gauss. Soient $a, b, c \in \mathbb{Z}$. Si $a \mid bc$ et $a \wedge b = 1$, alors $a \mid c$.

Idée de preuve (exigible). Par Bézout, $au + bv = 1$; en multipliant par c , $c = acu + (bc)v$. Or a divise ac et a divise bc par hypothèse, donc a divise cette combinaison linéaire, c'est-à-dire c .

Propriété — conséquences à connaître. Soient $a, b, c, n \in \mathbb{Z}$.

■ FORMULAIRE

- si $a \mid n, b \mid n$ et $a \wedge b = 1$, alors $ab \mid n$;
- si $a \wedge n = 1$ et $b \wedge n = 1$, alors $(ab) \wedge n = 1$; par récurrence, $a^k \wedge n = 1$ pour tout $k \in \mathbb{N}$;
- si $d = a \wedge b$ et $a = da', b = db'$, alors $a' \wedge b' = 1$ (on « sort » le pgcd);
- **forme irréductible** : tout $x \in \mathbb{Q}$ s'écrit $x = \frac{p}{q}$ avec $p \in \mathbb{Z}, q \in \mathbb{N}^*$ et $p \wedge q = 1$; cette écriture est unique.

Définition. Soient $a_1, \dots, a_n \in \mathbb{Z}$ non tous nuls. Ils sont **premiers entre eux dans leur ensemble** lorsque $a_1 \wedge \dots \wedge a_n = 1$, et **premiers entre eux deux à deux** lorsque $a_i \wedge a_j = 1$ pour tous $i \neq j$. On a la relation de Bézout généralisée : il existe $u_1, \dots, u_n \in \mathbb{Z}$ tels que $\sum_{i=1}^n a_i u_i = a_1 \wedge \dots \wedge a_n$.

✖ ATTENTION

« Deux à deux » entraîne « dans leur ensemble », mais la réciproque est **fausse** : 6, 10, 15 sont premiers entre eux dans leur

ensemble ($6 \wedge 10 \wedge 15 = 1$) alors qu'aucune paire ne l'est ($6 \wedge 10 = 2$, $6 \wedge 15 = 3$, $10 \wedge 15 = 5$). Ne pas confondre non plus « $a \wedge b = 1$ » et « a et b sont premiers » : 8 et 9 sont premiers entre eux sans être premiers.

5 NOMBRES PREMIERS

Définition. Un entier $p \geq 2$ est **premier** lorsque ses seuls diviseurs positifs sont 1 et p . On note $\mathcal{P}$ l'ensemble des nombres premiers : $\mathcal{P} = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, \dots\}$. Un entier $n \geq 2$ non premier est dit **composé**. L'entier 1 n'est pas premier.

Propriété. Tout entier $n \geq 2$ admet un diviseur premier, et son plus petit diviseur > 1 est premier. Si $n \geq 2$ n'a aucun diviseur premier $p \leq \sqrt{n}$, alors n est premier.

Méthode — crible d'Ératosthène. pour lister les nombres premiers $\leq N$: écrire $2, 3, \dots, N$, puis, tant qu'il reste un entier non barré $p \leq \sqrt{N}$, barrer tous les multiples de p strictement supérieurs à p . Les entiers non barrés sont les nombres premiers $\leq N$: on s'arrête à $\sqrt{N}$ car tout composé $n \leq N$ a un diviseur premier $\leq \sqrt{n}$.

Théorème. L'ensemble $\mathcal{P}$ des nombres premiers est **infini**.

Idée de preuve (exigible). Par l'absurde, si $\mathcal{P} = \{p_1, \dots, p_k\}$, l'entier $N = p_1 \cdots p_k + 1$ est ≥ 2 , donc admet un diviseur premier $p = p_i$; alors p divise N et $N - 1$, donc $p \mid 1$: absurde.

Théorème — lemme d'Euclide. Soit $p \in \mathcal{P}$ et $a, b \in \mathbb{Z}$. Alors $p \mid ab \implies p \mid a$ ou $p \mid b$. Plus généralement, si p divise un produit $a_1 \cdots a_n$, il divise l'un des a_i .

Idée de preuve. Si $p \nmid a$, alors $p \wedge a = 1$ (les diviseurs positifs de p sont 1 et p), et le lemme de Gauss donne $p \mid b$.

Théorème — décomposition en facteurs premiers. Tout entier $n \geq 2$ s'écrit

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$$

avec $r \geq 1$, $p_1 < p_2 < \cdots < p_r$ premiers et $\alpha_i \in \mathbb{N}^*$; cette écriture est **unique**.

Idée de preuve (exigible). Existence par récurrence forte : si n est premier c'est fini, sinon $n = ab$ avec $2 \leq a, b < n$ et l'on applique l'hypothèse de récurrence. *Unicité* : si deux décompositions coïncident, un premier p figurant à gauche divise le produit de droite, donc l'un de ses facteurs premiers par le lemme d'Euclide, donc lui est égal; on simplifie par p et l'on conclut par récurrence sur n .

Définition. Soit $p \in \mathcal{P}$ et $n \in \mathbb{Z}^*$. La **valuation p -adique** de n , notée $v_p(n)$, est le plus grand $k \in \mathbb{N}$ tel que $p^k \mid n$; c'est l'exposant de p dans la décomposition de $|n|$ (avec $v_p(n) = 0$ si $p \nmid n$). On convient $v_p(0) = +\infty$. Ainsi, pour $n \geq 2$,

$$n = \prod_{p \in \mathcal{P}} p^{v_p(n)},$$

produit où seuls un nombre fini de facteurs diffèrent de 1.

Théorème — propriétés des valuations. Soient $a, b \in \mathbb{Z}^*$, $p \in \mathcal{P}$ et $k \in \mathbb{N}$.

■ FORMULAIRE

- $v_p(ab) = v_p(a) + v_p(b)$ et $v_p(a^k) = k v_p(a)$;
- $a \mid b \iff \forall p \in \mathcal{P}, v_p(a) \leq v_p(b)$ (pour $a, b \geq 1$);
- $v_p(a \wedge b) = \min(v_p(a), v_p(b))$ et $v_p(a \vee b) = \max(v_p(a), v_p(b))$;
- $a \wedge b = 1 \iff a$ et b n'ont aucun facteur premier commun; de $\min + \max = \text{somme}$, on retrouve $(a \wedge b)(a \vee b) = ab$;
- le nombre de diviseurs positifs de $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ vaut $(\alpha_1 + 1) \cdots (\alpha_r + 1)$.

6 CONGRUENCES ET CALCUL MODULAIRE

Définition. Soient $n \in \mathbb{N}^*$ et $a, b \in \mathbb{Z}$. On dit que a est **congru à b modulo n** , et l'on note $a \equiv b [n]$, lorsque $n \mid (b - a)$. C'est le cas si et seulement si a et b ont le même reste dans la division euclidienne par n .

Propriété. La relation $\equiv [n]$ est réflexive, symétrique et transitive. Elle est **compatible** avec les opérations : si $a \equiv b [n]$ et $c \equiv d [n]$, alors

$$a + c \equiv b + d [n], \quad a - c \equiv b - d [n], \quad ac \equiv bd [n], \quad a^k \equiv b^k [n] \quad (k \in \mathbb{N}).$$

Elle n'est pas compatible avec la division : voir l'encadré ci-dessous. La structure d'anneau $\mathbb{Z}/n\mathbb{Z}$ est hors programme : on calcule uniquement avec les congruences.

✖ ATTENTION

On ne **divise jamais** une congruence sans précaution : $6 \equiv 12 [6]$ mais $1 \not\equiv 2 [6]$. La règle correcte est : si $ac \equiv bc [n]$ et $c \wedge n = 1$, alors $a \equiv b [n]$ (lemme de Gauss). Plus généralement $ac \equiv bc [n] \iff a \equiv b [\frac{n}{n \wedge c}]$.

Théorème — inverse modulo n . Soient $n \in \mathbb{N}^*$ et $a \in \mathbb{Z}$. Il existe $a' \in \mathbb{Z}$ tel que $aa' \equiv 1 [n]$ si et seulement si $a \wedge n = 1$. Un tel a' , unique modulo n , est appelé **inverse de a modulo n** ; on l'obtient par l'algorithme d'Euclide étendu : de $au + nv = 1$ on tire $a' = u$.

Méthode — résoudre $ax \equiv b [n]$. poser $d = a \wedge n$.

- Si $d \nmid b$: aucune solution. En effet $ax \equiv b [n]$ signifie $b = ax - nk$ pour un certain $k \in \mathbb{Z}$; or $d \mid a$ et $d \mid n$, donc d diviserait b .
- Si $d \mid b$: l'équation équivaut à $\frac{a}{d}x \equiv \frac{b}{d} [\frac{n}{d}]$, où $\frac{a}{d}$ est inversible modulo $\frac{n}{d}$; en notant a' son inverse, $x \equiv a' \frac{b}{d} [\frac{n}{d}]$. Il y a alors exactement d classes de solutions modulo n .

Méthode — résoudre $ax + by = c$ dans $\mathbb{Z}^2$. soit $d = a \wedge b$. Si $d \nmid c$, pas de solution. Sinon : (i) trouver une solution particulière (x_0, y_0) par l'algorithme d'Euclide étendu; (ii) soustraire pour obtenir $a(x - x_0) = -b(y - y_0)$, puis simplifier par d et appliquer le lemme de Gauss. On obtient

$$x = x_0 + \frac{b}{d}k, \quad y = y_0 - \frac{a}{d}k, \quad k \in \mathbb{Z},$$

et il faut vérifier que tous ces couples sont bien solutions (la double inclusion est exigée).

Théorème — petit théorème de Fermat. Soit $p \in \mathcal{P}$ et $a \in \mathbb{Z}$.

- Si $p \nmid a$, alors $a^{p-1} \equiv 1 [p]$.
- Sans hypothèse sur a : $a^p \equiv a [p]$.

Idée de preuve (exigible). Pour $p \nmid a$, $k \mapsto$ reste de ak modulo p est une bijection de $\llbracket 1; p-1 \rrbracket$ sur lui-même (si $ak \equiv ak'$ alors $k \equiv k'$ par Gauss, car $a \wedge p = 1$). En multipliant les $p-1$ congruences $ak \equiv r_k [p]$: $a^{p-1}(p-1)! \equiv (p-1)! [p]$, et l'on simplifie par $(p-1)!$, premier à p . La seconde forme s'en déduit en multipliant par a .

✗ ATTENTION

L'hypothèse $p \nmid a$ est indispensable dans la première forme : $2^{3-1} = 4 \equiv 1 [3]$, mais $3^{3-1} = 9 \equiv 0 [3]$. Et la réciproque est fautive : $a^{n-1} \equiv 1 [n]$ pour tout a premier à n n'entraîne pas que n soit premier ($n = 561$).

► SAVOIR-FAIRE

- Effectuer une division euclidienne (y compris à dividende négatif); raisonner par disjonction selon le reste.
- Dérouler l'algorithme d'Euclide, puis le remonter pour obtenir un couple de Bézout; en déduire un inverse modulo n .
- Résoudre $ax + by = c$ dans $\mathbb{Z}^2$ et $ax \equiv b [n]$, en décrivant tout l'ensemble des solutions.
- Décomposer un entier en facteurs premiers; calculer pgcd, ppcm, nombre de diviseurs par les valuations; reconnaître un carré ou un cube.
- Calculer un reste de puissance modulo n (périodicité ou petit théorème de Fermat); montrer $m \mid f(n)$ en factorisant m en facteurs premiers entre eux deux à deux.

★ EXEMPLE — trois calculs types

- **Euclide et Bézout.** $1071 = 2 \times 462 + 147$, $462 = 3 \times 147 + 21$, $147 = 7 \times 21$: donc $1071 \wedge 462 = 21$. En remontant : $21 = 462 - 3 \times 147 = 462 - 3(1071 - 2 \times 462)$, soit $1071 \times (-3) + 462 \times 7 = 21$.
- **Valuations.** $6048 = 2^5 \times 3^3 \times 7$ n'est pas un carré ($v_7 = 1$ est impair); le plus petit $k \geq 1$ tel que $6048k$ soit un carré est $k = 2 \times 3 \times 7 = 42$, et $6048 \times 42 = 254\,016 = 504^2$.
- **Puissance modulo n .** $2^3 = 8 \equiv 1 [7]$, et $2027 = 3 \times 675 + 2$, donc $2^{2027} = (2^3)^{675} \times 2^2 \equiv 4 [7]$.

✗ PIÈGES

- Confondre « $a \wedge b = 1$ » et « a et b premiers »; confondre « deux à deux » et « dans leur ensemble ».
- Écrire un reste négatif, ou arrondir le quotient au plus proche au lieu de prendre la partie entière.
- Lire $au + bv = c$ comme « $a \wedge b = c$ » : elle ne donne que $(a \wedge b) \mid c$.
- Utiliser $a \mid bc \Rightarrow a \mid b$ ou $a \mid c$ sans que a soit premier : $6 \mid 4 \times 9$, mais $6 \nmid 4$ et $6 \nmid 9$.
- Diviser une congruence par un entier non premier à n ; oublier $p \nmid a$ dans le petit théorème de Fermat.
- S'arrêter à une solution particulière d'une équation diophantienne; invoquer une propriété de l'anneau $\mathbb{Z}/n\mathbb{Z}$ (hors programme).