

Arithmétique dans $\mathbb{Z}$

Licence 1 (L1) - Cours complet

Division euclidienne, PGCD, Bézout, Gauss, nombres premiers et congruences

Idée directrice. L'arithmétique dans $\mathbb{Z}$ étudie la divisibilité et les calculs “modulo n ”. À partir de la division euclidienne, on construit le PGCD et l'algorithme d'Euclide, puis les théorèmes de Bézout et de Gauss. Ils conduisent à la décomposition unique en facteurs premiers et à la structure de l'anneau $\mathbb{Z}/n\mathbb{Z}$.

1. Divisibilité dans $\mathbb{Z}$

Définition

Pour $a, b \in \mathbb{Z}$, on dit que a **divise** b , et on écrit $a \mid b$, s'il existe $k \in \mathbb{Z}$ tel que

$$b = ak.$$

Sinon, on écrit $a \nmid b$.

Propriétés immédiates, pour $a, b, c \in \mathbb{Z}$:

- $a \mid a$, $1 \mid a$, et $a \mid 0$;
- si $a \mid b$ et $b \mid c$, alors $a \mid c$;
- 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 $b \mid a$, alors $|a| = |b|$.

Exemple

$6 \mid 42$ car $42 = 6 \times 7$. De plus, si $6 \mid b$ et $6 \mid c$, alors 6 divise toute combinaison linéaire $3b - 5c$.

2. Division euclidienne

Théorème - Division euclidienne

Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z} \setminus \{0\}$. Il existe un **unique** couple $(q, r) \in \mathbb{Z}^2$ tel que

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

q est le quotient et r le reste.

Exemple

Pour $a = -37$ et $b = 5$:

$$-37 = 5 \times (-8) + 3,$$

donc $q = -8$ et $r = 3$. Le reste doit toujours satisfaire $0 \leq r < 5$.

La division euclidienne donne immédiatement :

$$b \mid a \iff r = 0.$$

Elle est aussi à la base du calcul des congruences : deux entiers ont même reste modulo n exactement lorsqu'ils sont congrus modulo n .

3. PGCD et PPCM

Définition

Pour $a, b \in \mathbb{Z}$ non tous deux nuls, le **plus grand commun diviseur** $d = \text{pgcd}(a, b)$ est l'unique entier $d > 0$ tel que :

- $d \mid a$ et $d \mid b$;
- tout diviseur commun de a et b divise d .

On dit que a et b sont **premiers entre eux** si $\text{pgcd}(a, b) = 1$.

Le PGCD ne dépend pas des signes :

$$\text{pgcd}(a, b) = \text{pgcd}(|a|, |b|).$$

Il est invariant par ajout d'un multiple :

$$\boxed{\text{pgcd}(a, b) = \text{pgcd}(b, a - qb)} \quad (q \in \mathbb{Z}).$$

Définition

Pour $a, b \neq 0$, le **PPCM** $m = \text{ppcm}(a, b)$ est le plus petit entier strictement positif divisible par a et b .

Relation fondamentale :

$$\boxed{\text{pgcd}(a, b) \text{ ppcm}(a, b) = |ab|}.$$

4. Algorithme d'Euclide

On effectue des divisions euclidiennes successives :

$$\begin{aligned} a &= bq_1 + r_1, \\ b &= r_1q_2 + r_2, \\ r_1 &= r_2q_3 + r_3, \\ &\vdots \\ r_{k-2} &= r_{k-1}q_k + r_k, \\ r_{k-1} &= r_kq_{k+1}. \end{aligned}$$

Le dernier reste non nul est le PGCD :

$$\boxed{\text{pgcd}(a, b) = r_k}.$$

Exemple

Calculons $\text{pgcd}(252, 198)$:

$$252 = 198 + 54, \quad 198 = 3 \times 54 + 36, \quad 54 = 36 + 18, \quad 36 = 2 \times 18.$$

Donc $\text{pgcd}(252, 198) = 18$.

Algorithme d'Euclide étendu

Pour trouver des entiers u, v tels que $au + bv = \text{pgcd}(a, b)$:

1. exécuter Euclide jusqu'au dernier reste non nul ;
2. remonter les égalités en remplaçant chaque reste ;
3. regrouper les coefficients de a et b .

Exemple

Avec le calcul précédent :

$$18 = 54 - 36 = 54 - (198 - 3 \times 54) = 4 \times 54 - 198 = 4 \times 252 - 5 \times 198.$$

Ainsi $18 = 4 \times 252 - 5 \times 198$.

5. Théorème de Bézout

Théorème de Bézout

Pour $a, b \in \mathbb{Z}$ non tous deux nuls, si $d = \text{pgcd}(a, b)$, alors il existe $u, v \in \mathbb{Z}$ tels que

$$au + bv = d.$$

Plus précisément,

$$\{au + bv; u, v \in \mathbb{Z}\} = d\mathbb{Z}.$$

Le cas $d = 1$ est particulièrement important :

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

Exemple

Comme $\text{pgcd}(35, 12) = 1$, il existe une identité de Bézout. Euclide donne

$$1 = 3 \times 12 - 35.$$

Donc $u = -1$ et $v = 3$ conviennent dans $35u + 12v = 1$.

Résolution d'une équation diophantienne linéaire

Considérons

$$ax + by = c, \quad x, y \in \mathbb{Z}.$$

Théorème

L'équation admet des solutions entières si et seulement si

$$\text{pgcd}(a, b) \mid c.$$

Si (x_0, y_0) est une solution et $d = \text{pgcd}(a, b)$, toutes les solutions sont

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

Exemple

Résoudre $14x + 21y = 35$. Comme $\text{pgcd}(14, 21) = 7$ et $7 \mid 35$, il existe des solutions. Une solution est $(x_0, y_0) = (1, 1)$, et toutes les solutions sont

$$x = 1 + 3k, \quad y = 1 - 2k, \quad k \in \mathbb{Z}.$$

6. Lemme de Gauss

Lemme de Gauss

Si $a, b, c \in \mathbb{Z}$, si $a \mid bc$ et si $\text{pgcd}(a, b) = 1$, alors

$$a \mid c.$$

Preuve type. Par Bézout, il existe u, v tels que $au + bv = 1$. En multipliant par c :

$$auc + bvc = c.$$

Or $a \mid auc$ et $a \mid bvc$ car $a \mid bc$. Donc $a \mid c$.

Conséquence essentielle : si p est premier et $p \mid ab$, alors

$$p \mid a \quad \text{ou} \quad p \mid b.$$

7. Nombres premiers

Définition

Un entier $p \geq 2$ est **premier** si ses seuls diviseurs positifs sont 1 et p . Un entier $n \geq 2$ non premier est dit **composé**.

Théorème fondamental de l'arithmétique

Tout entier $n \geq 2$ s'écrit, de manière unique à l'ordre des facteurs près,

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

où $p_1, \dots, p_r$ sont des nombres premiers distincts et $\alpha_i \geq 1$.

Cette décomposition permet de lire directement PGCD et PPCM. Si

$$a = \prod_p p^{\alpha_p}, \quad b = \prod_p p^{\beta_p},$$

alors

$$\text{pgcd}(a, b) = \prod_p p^{\min(\alpha_p, \beta_p)}, \quad \text{ppcm}(a, b) = \prod_p p^{\max(\alpha_p, \beta_p)}.$$

Exemple

$360 = 2^3 \cdot 3^2 \cdot 5$ et $504 = 2^3 \cdot 3^2 \cdot 7$. Donc

$$\text{pgcd}(360, 504) = 2^3 \cdot 3^2 = 72,$$

$$\text{ppcm}(360, 504) = 2^3 \cdot 3^2 \cdot 5 \cdot 7 = 2520.$$

Critère élémentaire de primalité

Si $n \geq 2$ est composé, il possède un diviseur premier $p \leq \sqrt{n}$. Ainsi, pour tester si n est premier, il suffit d'essayer les nombres premiers $p \leq \sqrt{n}$.

8. Congruences modulo n

Définition

Soit $n \geq 1$. Pour $a, b \in \mathbb{Z}$, on écrit

$$a \equiv b \pmod{n}$$

si et seulement si $n \mid (a - b)$.

Equivalent : a et b ont le même reste dans la division euclidienne par n .

La congruence modulo n est une relation d'équivalence. Elle est compatible avec l'addition et la multiplication :

$$a \equiv b \pmod{n}, \quad c \equiv d \pmod{n}$$

implique

$$a + c \equiv b + d \pmod{n}, \quad ac \equiv bd \pmod{n}.$$

On peut aussi élever à une puissance :

$$a \equiv b \pmod{n} \implies a^k \equiv b^k \pmod{n} \quad (k \in \mathbb{N}).$$

9. Calcul modulo n

Exemple

Calculer le reste de 7^{100} modulo 10. Comme

$$7^1 \equiv 7, \quad 7^2 \equiv 9, \quad 7^3 \equiv 3, \quad 7^4 \equiv 1 \pmod{10},$$

le cycle est de longueur 4. Or $100 \equiv 0 \pmod{4}$, donc

$$\boxed{7^{100} \equiv 1 \pmod{10}}.$$

Simplification d'une congruence

De

$$ac \equiv bc \pmod{n},$$

on ne peut pas toujours "diviser par c ".

Théorème

Si $\text{pgcd}(c, n) = 1$, alors

$$ac \equiv bc \pmod{n} \implies a \equiv b \pmod{n}.$$

Plus généralement, si $d = \text{pgcd}(c, n)$, alors

$$ac \equiv bc \pmod{n} \implies a \equiv b \pmod{n/d}.$$

Piège classique

$2x \equiv 2y \pmod{4}$ signifie $4 \mid 2(x - y)$, donc seulement $2 \mid (x - y)$:

$$x \equiv y \pmod{2},$$

mais pas nécessairement modulo 4. Par exemple, $x = 1$ et $y = 3$ conviennent à la première congruence, alors que $1 \not\equiv 3 \pmod{4}$.

10. L'anneau $\mathbb{Z}/n\mathbb{Z}$

Les classes de congruence modulo n sont

$$\overline{0}, \overline{1}, \dots, \overline{n-1}.$$

On note leur ensemble $\mathbb{Z}/n\mathbb{Z}$. Les opérations sont définies par

$$\overline{a} + \overline{b} = \overline{a + b}, \quad \overline{a} \overline{b} = \overline{ab}.$$

Elles sont bien définies grâce à la compatibilité des congruences avec $+$ et $\times$.

Définition

Une classe $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ est **inversible** s'il existe $\overline{b}$ tel que

$$\overline{a} \overline{b} = \overline{1}.$$

Théorème

$$\boxed{\overline{a} \text{ est inversible modulo } n \iff \text{pgcd}(a, n) = 1.}$$

Preuve. Si $\text{pgcd}(a, n) = 1$, Bézout donne $au + nv = 1$, donc $au \equiv 1 \pmod{n}$: $\overline{u}$ est l'inverse de $\overline{a}$. La réciproque se déduit de la même identité.

11. Résoudre une congruence linéaire

On cherche les $x \in \mathbb{Z}$ tels que

$$ax \equiv b \pmod{n}.$$

Cette congruence équivaut à l'existence de $k \in \mathbb{Z}$ tel que

$$ax - nk = b.$$

C'est donc une équation diophantienne.

Théorème

Posons $d = \text{pgcd}(a, n)$. La congruence

$$ax \equiv b \pmod{n}$$

admet une solution si et seulement si

$$d \mid b.$$

Si $d \mid b$, elle possède exactement d classes de solutions modulo n .

Exemple

Résoudre $6x \equiv 9 \pmod{15}$. Ici $d = \text{pgcd}(6, 15) = 3$ et $3 \mid 9$. En divisant l'équation par 3 tout en divisant le module par 3 :

$$2x \equiv 3 \pmod{5}.$$

L'inverse de 2 modulo 5 est 3, donc

$$x \equiv 9 \equiv 4 \pmod{5}.$$

Modulo 15, les trois classes solutions sont

$$x \equiv 4, 9, 14 \pmod{15}.$$

Résoudre $ax \equiv b \pmod{n}$

1. Calculer $d = \text{pgcd}(a, n)$.
2. Si $d \nmid b$, il n'y a aucune solution.
3. Si $d \mid b$, diviser a, b, n par d .
4. Dans le nouveau module n/d , calculer l'inverse de a/d par Bézout.
5. Revenir aux d classes de solutions modulo n .

12. Petit théorème de Fermat

Petit théorème de Fermat

Si p est premier et $p \nmid a$, alors

$$a^{p-1} \equiv 1 \pmod{p}.$$

Equivalent, pour tout $a \in \mathbb{Z}$:

$$a^p \equiv a \pmod{p}.$$

Exemple

Calculer $3^{2026} \pmod{7}$. Comme $3^6 \equiv 1 \pmod{7}$ et $2026 = 6 \times 337 + 4$,

$$3^{2026} \equiv 3^4 = 81 \equiv 4 \pmod{7}.$$

13. Ordres, cycles et puissances modulo n

Lorsque $\text{pgcd}(a, n) = 1$, les puissances de a modulo n finissent par revenir à 1. Le plus petit entier $r \geq 1$ tel que

$$a^r \equiv 1 \pmod{n}$$

est appelé **ordre multiplicatif** de a modulo n .

Pour un nombre premier p avec $p \nmid a$, le petit théorème de Fermat assure que cet ordre divise $p - 1$.

Exemple

Modulo 7, les puissances de 2 donnent

$$2, 4, 1, 2, 4, 1, \dots$$

Donc l'ordre de 2 modulo 7 est 3. Ainsi, pour réduire $2^m \pmod{7}$, on peut réduire m modulo 3.

14. Méthodes de démonstration typiques

Prouver une divisibilité

Pour montrer $d \mid N$, on cherche à écrire explicitement $N = dk$ avec $k \in \mathbb{Z}$, ou à utiliser une combinaison linéaire de quantités déjà divisibles par d .

Prouver que deux entiers sont premiers entre eux

Plusieurs méthodes :

- calculer le PGCD par Euclide ;
- produire une identité de Bézout $au + bv = 1$;
- utiliser les facteurs premiers.

Prouver une congruence

On peut partir de la définition :

$$a \equiv b \pmod{n} \iff n \mid (a - b),$$

ou calculer directement dans $\mathbb{Z}/n\mathbb{Z}$ en réduisant les termes au fur et à mesure.

15. Erreurs fréquentes à éviter

Piège classique

- **Diviser une congruence sans vérifier l'inversibilité.** On peut simplifier par c modulo n seulement si $\text{pgcd}(c, n) = 1$, ou alors il faut aussi adapter le module.
- **Confondre Bézout et Gauss.** Bézout caractérise le PGCD par une combinaison linéaire ; Gauss permet de retirer un facteur premier avec une hypothèse de coprimauté.
- **Oublier les signes dans le PGCD.** Par convention, $\text{pgcd}(a, b) > 0$.
- **Utiliser Fermat avec un module non premier.** Le petit théorème de Fermat exige un module premier.
- **Dire qu'un entier est premier sans tester jusqu'à $\sqrt{n}$.** Tester quelques petits diviseurs ne suffit pas en général.

16. Exercices corrigés

Exercice 1 - Euclide et Bézout

Calculer $\text{pgcd}(414, 662)$ et trouver $u, v \in \mathbb{Z}$ tels que $414u + 662v = \text{pgcd}(414, 662)$.

Correction.

$$\begin{aligned} 662 &= 414 + 248, \\ 414 &= 248 + 166, \\ 248 &= 166 + 82, \\ 166 &= 2 \times 82 + 2, \\ 82 &= 41 \times 2. \end{aligned}$$

Donc $\text{pgcd}(414, 662) = 2$. En remontant :

$$\begin{aligned} 2 &= 166 - 2 \times 82 = 166 - 2(248 - 166) = 3 \times 166 - 2 \times 248, \\ &= 3(414 - 248) - 2 \times 248 = 3 \times 414 - 5 \times 248, \\ &= 3 \times 414 - 5(662 - 414) = 8 \times 414 - 5 \times 662. \end{aligned}$$

Ainsi $u = 8$ et $v = -5$.

Exercice 2 - Congruence linéaire

Résoudre $14x \equiv 8 \pmod{30}$.

Correction. $d = \text{pgcd}(14, 30) = 2$ et $2 \mid 8$. On divise par 2 :

$$7x \equiv 4 \pmod{15}.$$

L'inverse de 7 modulo 15 vaut 13 car $7 \times 13 = 91 \equiv 1 \pmod{15}$. Donc

$$x \equiv 52 \equiv 7 \pmod{15}.$$

Modulo 30, on obtient deux classes :

$$\boxed{x \equiv 7 \text{ ou } 22 \pmod{30}}.$$

Exercice 3 - Fermat

Déterminer le reste de 11^{1000} dans la division par 13.

Correction. Comme 13 est premier et $13 \nmid 11$,

$$11^{12} \equiv 1 \pmod{13}.$$

Or $1000 = 12 \times 83 + 4$, donc

$$11^{1000} \equiv 11^4 \pmod{13}.$$

Comme $11^2 = 121 \equiv 4 \pmod{13}$, on a $11^4 \equiv 16 \equiv 3 \pmod{13}$.

Exercice 4 - Nombres premiers

Montrer que si p est premier et $p \mid a^2$, alors $p \mid a$.

Correction. Comme $p \mid a \cdot a$, le lemme de Gauss appliqué à un nombre premier donne immédiatement $p \mid a$.

17. Synthèse à connaître

- Division euclidienne : $a = bq + r$, $0 \leq r < |b|$.
- Euclide calcule le PGCD ; Euclide étendu produit une identité de Bézout.
- Bézout : $\text{pgcd}(a, b) = d \iff d$ est le générateur positif des combinaisons $au + bv$.
- Gauss : $a \mid bc$ et $\text{pgcd}(a, b) = 1 \Rightarrow a \mid c$.
- Tout entier $n \geq 2$ possède une décomposition unique en facteurs premiers.
- $a \equiv b \pmod{n} \iff n \mid (a - b)$.
- $\bar{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z} \iff \text{pgcd}(a, n) = 1$.
- $ax \equiv b \pmod{n}$ est soluble ssi $\text{pgcd}(a, n) \mid b$.
- Si p est premier et $p \nmid a$, alors $a^{p-1} \equiv 1 \pmod{p}$.