

Arithmétique dans $\mathbb{Z}$ Licence 1 - Fiche de révision

1. Divisibilité

$a \mid b \iff \exists k \in \mathbb{Z}, b = ak.$

Si $a \mid b$ et $a \mid c$, alors

$$a \mid (ub + vc) \quad (\forall u, v \in \mathbb{Z}).$$

2. Division euclidienne

Pour $b \neq 0$, il existe un unique (q, r) :

$$a = bq + r, \quad 0 \leq r < |b|.$$

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

3. PGCD / PPCM

$d = \text{pgcd}(a, b) > 0$ divise a, b et est multiple de tout diviseur commun.

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

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

4. Euclide et Bézout

Euclide : le dernier reste non nul est le PGCD.

Si $d = \text{pgcd}(a, b)$:

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

En particulier

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

Les coefficients se trouvent en remontant Euclide.

5. Équation $ax + by = c$

Solutions entières ssi

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

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

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

avec $k \in \mathbb{Z}.$

6. Lemme de Gauss

$$a \mid bc, \text{ pgcd}(a, b) = 1 \Rightarrow a \mid c.$$

Si p est premier :

$$p \mid ab \Rightarrow p \mid a \text{ ou } p \mid b.$$

7. Facteurs premiers

Tout $n \geq 2$: $n = \prod p^{\alpha_p}$ de manière unique.

Si $a = \prod p^{\alpha_p}, b = \prod p^{\beta_p}$:

$$\text{pgcd}(a, b) = \prod p^{\min(\alpha_p, \beta_p)},$$

$$\text{ppcm}(a, b) = \prod p^{\max(\alpha_p, \beta_p)}.$$

Primalité : tester les premiers $p \leq \sqrt{n}.$

8. Congruences

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

Compatibles avec $+, -, \times$, puissances.

Attention à la simplification

De $ac \equiv bc \pmod{n}$, on peut conclure $a \equiv b \pmod{n}$ si

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

Sinon, il faut adapter le module. Ex. :

$$2x \equiv 2y \pmod{4} \Rightarrow x \equiv y \pmod{2},$$

pas forcément modulo 4.

9. $\mathbb{Z}/n\mathbb{Z}$ et inverses

Classes : $\bar{0}, \dots, \bar{n-1}.$

$$\bar{a} \text{ inversible} \iff \text{pgcd}(a, n) = 1.$$

Si $au + nv = 1$, alors

$$a^{-1} \equiv u \pmod{n}.$$

10. Résoudre $ax \equiv b \pmod{n}$

Poser $d = \text{pgcd}(a, n).$

- $d \nmid b$: aucune solution.
- $d \mid b$: diviser a, b, n par d , puis inverser a/d modulo n/d .

Il y a alors d classes de solutions modulo n .

11. Petit théorème de Fermat

Si p premier et $p \nmid a$:

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

Pour tout $a \in \mathbb{Z}$:

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

Méthodes, exemples et pièges

A. Euclide étendu

Pour 252, 198 :

$$252 = 198 + 54,$$

$$198 = 3 \cdot 54 + 36, \quad 54 = 36 + 18.$$

Donc $\text{pgcd} = 18$ et

$$18 = 54 - 36 = 4 \cdot 54 - 198$$

$$= \boxed{4 \cdot 252 - 5 \cdot 198}.$$

B. Trouver un inverse

Inverse de 7 modulo 15 :

$$1 = 15 - 2 \cdot 7.$$

Donc

$$\boxed{7^{-1} \equiv -2 \equiv 13 \pmod{15}}.$$

C. Congruence linéaire

$6x \equiv 9 \pmod{15}$. Comme $d = 3$:

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

Or $2^{-1} \equiv 3 \pmod{5}$, donc

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

Modulo 15 :

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

D. Fermat - exemple

$3^{2026} \pmod{7}$. Comme $3^6 \equiv 1$ et

$$2026 = 6 \cdot 337 + 4,$$

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

E. Divisibilité par combinaison

Si $d \mid a$ et $d \mid b$, alors

$$\boxed{d \mid (ua + vb) \quad \forall u, v \in \mathbb{Z}}.$$

C'est le mécanisme central d'Euclide et de Bézout.

F. Réflexes d'examen

- PGCD : Euclide.
- Inverse modulo n : Bézout.
- $p \mid ab$: Gauss.
- $ax \equiv b$: calculer $\text{pgcd}(a, n)$.
- Grande puissance modulo p premier : Fermat/cycles.
- Simplifier : vérifier l'inversibilité.

G. 6 pièges classiques

- $a \equiv b \pmod{n}$ signifie $n \mid (a - b)$.
- Ne pas diviser une congruence sans condition.
- Fermat : le module doit être premier.
- Dans a^{p-1} , il faut aussi $p \nmid a$.
- $\text{pgcd}(a, b)$ est positif par convention.
- $ax \equiv b \pmod{n}$ peut avoir plusieurs classes solutions.

H. Formules à savoir

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

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

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

$$\boxed{\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^\times \iff \text{pgcd}(a, n) = 1}$$

$$\boxed{p \nmid a \Rightarrow a^{p-1} \equiv 1 \pmod{p}}$$

I. Mini-checklist rédaction

Avant de conclure, écrire explicitement :

- le module considéré ;
- le PGCD utile ;
- l'hypothèse de coprimalité si Gauss/-simplification ;
- l'identité de Bézout si un inverse est utilisé ;
- la classe finale sous la forme $x \equiv r \pmod{n}$.