

Algèbre Générale : Arithmétique dans $\mathbb{Z}$

1. Divisibilité et Division Euclidienne

Divisibilité : Soient $a, b \in \mathbb{Z}$. On dit que a divise b ($a \mid b$) s'il existe $k \in \mathbb{Z}$ tel que $b = ka$.

Théorème de la division euclidienne :

Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$. Il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que : $a = bq + r$ avec $0 \leq r < |b|$

2. PGCD, PPCM et Algorithme d'Euclide

Sous-groupes de $\mathbb{Z}$: Tout sous-groupe de $(\mathbb{Z}, +)$ est de la forme $n\mathbb{Z}$ avec $n \in \mathbb{N}$.

PGCD : $a\mathbb{Z} + b\mathbb{Z} = \delta\mathbb{Z}$ avec $\delta = \text{pgcd}(a, b) = a \wedge b$.

☞ $a \wedge b$ est le plus grand diviseur commun à a et b .

☞ L'algorithme d'Euclide calcule $a \wedge b$ via successions de divisions euclidiennes.

PPCM : $a\mathbb{Z} \cap b\mathbb{Z} = \mu\mathbb{Z}$ avec $\mu = \text{ppcm}(a, b) = a \vee b$.

Relation fondamentale : $(a \wedge b) \cdot (a \vee b) = |ab|$.

3. Théorèmes Fondamentaux

Identité de Bézout :

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

Théorème de Gauss :

$$(a \mid bc \text{ et } a \wedge b = 1) \implies a \mid c$$

Lemme d'Euclide :

Si p est premier et $p \mid ab$, alors $p \mid a$ ou $p \mid b$.

Équations diophantiennes : $ax + by = c$ admet des solutions $(x, y) \in \mathbb{Z}^2 \iff (a \wedge b) \mid c$.

4. Nombres Premiers et Décomposition

Théorème Fondamental de l'Arithmétique :

Tout entier $n \geq 2$ se décompose de manière unique (à l'ordre près des facteurs) en produit de nombres premiers :

$$n = \prod_{i=1}^r p_i^{\alpha_i} \quad (\alpha_i \geq 1)$$

Formules de PGCD/PPCM :

Si $a = \prod p_i^{\alpha_i}$ et $b = \prod p_i^{\beta_i}$, alors :

$$a \wedge b = \prod p_i^{\min(\alpha_i, \beta_i)}, \quad a \vee b = \prod p_i^{\max(\alpha_i, \beta_i)}$$

Valuation p -adique :

Si $v_p(n)$ est l'exposant de p dans la décomposition de n , alors :

$$\text{☞ } v_p(ab) = v_p(a) + v_p(b).$$

$$\text{☞ } v_p(a + b) \geq \min(v_p(a), v_p(b)).$$

$$\text{Formule de Legendre : } v_p(n!) = \sum_{k=1}^{+\infty} \left\lfloor \frac{n}{p^k} \right\rfloor.$$

5. Congruences et Anneau $\mathbb{Z}/n\mathbb{Z}$

Structure de $\mathbb{Z}/n\mathbb{Z}$:

$$\text{☞ Élément inversible : } \bar{k} \in (\mathbb{Z}/n\mathbb{Z})^\times \iff k \wedge n = 1.$$

$$\text{☞ } \mathbb{Z}/n\mathbb{Z} \text{ est un corps } \iff n \text{ est premier.}$$

Cyclicité de $(\mathbb{Z}/n\mathbb{Z})^\times$:

$(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique $\iff n \in \{2, 4, p^k, 2p^k\}$ avec p premier impair et $k \geq 1$.

6. Fonction indicatrice d'Euler

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

Définition : $\varphi(n) = \text{card}(\{k \in \llbracket 1, n \rrbracket \text{ tel que } k \wedge n = 1\})$.

Propriétés :

$$\text{☞ } n \wedge m = 1 \implies \varphi(nm) = \varphi(n)\varphi(m).$$

$$\text{☞ Si } p \text{ est premier, alors } \varphi(p) = p - 1, \text{ et en général } \varphi(p^\alpha) = p^\alpha - p^{\alpha-1}, \text{ pour tout } \alpha \in \mathbb{N}^*.$$

$$\text{☞ } \varphi(n) = n \prod_{p \mid n} \left(1 - \frac{1}{p}\right).$$

Théorème d'Euler (Grand Théorème de Fermat) :

Si $a \wedge n = 1$, alors : $a^{\varphi(n)} \equiv 1 \pmod{n}$

Petit Théorème de Fermat : Si p est premier et $a \in \mathbb{Z}$, alors $a^p \equiv a \pmod{p}$ et $a^{p-1} \equiv 1 \pmod{p}$, quand $p \nmid a$.

$$\text{Formule de Gauss : } n = \sum_{d \mid n} \varphi(d).$$

7. Théorème des Restes Chinois

Si $n_1, \dots, n_k$ sont deux à deux premiers entre eux, alors

$$\text{le système } (\mathcal{S}) : \begin{cases} x \equiv a_1 \pmod{n_1} \\ \dots \\ x \equiv a_k \pmod{n_k} \end{cases}$$

On pose $N = \prod_{i=1}^k n_i$ et $N_i = \frac{N}{n_i}$. Comme $n_i \wedge N_i = 1$, on

cherche $u_i \in \mathbb{Z}$ tel que $N_i u_i \equiv 1 \pmod{n_i}$.

Alors $x_0 = \sum a_i N_i u_i$ est une solution de $(\mathcal{S})$ et toutes les autres solutions sont de la forme $x = x_0 + kN$, où $k \in \mathbb{Z}$.