Chapitre 4 : Arithmétique des entiers, arithmétique modulaire

1 Divisibilité dans $\mathbb{Z}$

Définition 1.1 (Divisibilité)**.** Soit $a, b \in \mathbb{Z}$. On dit que a divise b ou que b est un multiple de a (et on note $a \mid b$) s'il existe un entier $q \in \mathbb{Z}$ tel que $b = aq$.

Théorème 1.2 (Division euclidienne)**.** *Soit $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$. Il existe un unique couple $(q, r) \in \mathbb{Z}^2$ tel que $a = bq + r$ et $0 \leq r < b$. Les entiers q et r sont respectivement appelés quotient et reste de la division euclidienne de a par b.*

Théorème 1.3 (Représentation des entiers en base b)**.** *Soit $n, b \in \mathbb{N}$, $b \geq 2$. Alors il existe un unique entier m et un unique $(m+1)$-uplet $(a_0, \ldots, a_m)$ d'entiers appartenant à $\{0, \ldots, b-1\}$ tel que $a_m \neq 0$ et :*

$$n = \sum_{i=0}^{m} a_i b^i.$$

On note alors $n = (a_m \ldots a_1 a_0)_b$ et on parle de l'écriture en base b de l'entier n.

2 Relation de congruence

2.1 Calculs modulo n

Définition 2.1 (Congruence)**.** Soit $n \in \mathbb{Z}$. On définit sur $\mathbb{Z}$ la relation $\equiv$, dite de congruence modulo n par :

$$\forall (a, b) \in \mathbb{Z}^2, \quad a \equiv b \bmod n \iff n \mid a - b.$$

On dit alors que a est congru à b modulo n.

Proposition 2.2. *Soit $a \in \mathbb{Z}$ et $n \in \mathbb{N}^*$. Notons $a = nq + r$ la division euclidienne de a par n. Alors $a \equiv r \bmod n$.*

Proposition 2.3. — *La relation de congruence modulo n est une relation d'équivalence.*

- *Cette relation partitionne $\mathbb{Z}$ en n classes d'équivalence qui sont $\overline{0} = 0 + n\mathbb{Z}, \overline{1} = 1 + n\mathbb{Z}, \ldots, \overline{n-1} = (n-1) + n\mathbb{Z}$.*
- *Pour tout $x, y \in \mathbb{Z}$, $\overline{x} = \overline{y}$ si et seulement si $x \equiv y \bmod n$.*

Proposition 2.4 (Calculs modulo n)**.** *Soit $n \in \mathbb{Z}^*$ et $a, b, c, d \in \mathbb{Z}$. Alors*

1. *Si $a \equiv c \bmod n$ et $b \equiv d \bmod n$ alors $a + b \equiv c + d \bmod n$*
2. *Si $a \equiv c \bmod n$ et $b \equiv d \bmod n$ alors $ab \equiv cd \bmod n$*
3. *Si $a \equiv c \bmod n$ alors pour tout $k \in \mathbb{Z}$, $ka \equiv kc \bmod n$.*
4. *Si $a \equiv c \bmod n$ alors pour tout $k \in \mathbb{Z}$, $a^k \equiv c^k \bmod n$.*

2.2 Arithmétique sur $\mathbb{Z}/n\mathbb{Z}$

Corollary 2.5 (Propriétés de $\mathbb{Z}/n\mathbb{Z}$)**.** *Soit $n \in \mathbb{Z}^*$ et $a, b, c, d \in \mathbb{Z}$. Alors*

1. *Si $\overline{a} = \overline{c}$ et $\overline{b} = \overline{d}$ alors $\overline{a+b} = \overline{c+d}$.*
2. *Si $\overline{a} = \overline{c}$ et $\overline{b} = \overline{d}$ alors $\overline{a \times b} = \overline{c \times d}$.*

Définition 2.6. Soit $n \in \mathbb{Z}$. On définit l'addition et la multiplication sur $\mathbb{Z}/n\mathbb{Z}$ comme suit :

$$\begin{aligned} +\colon \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} &\to \mathbb{Z}/n\mathbb{Z}, \\ \overline{a} + \overline{b} &\mapsto \overline{a+b}. \end{aligned}$$

$$\begin{aligned} \times\colon \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} &\to \mathbb{Z}/n\mathbb{Z}, \\ \overline{a} + \overline{b} &\mapsto \overline{a \times b}. \end{aligned}$$

Autrement dit $\overline{a} + \overline{c} = \overline{a \times c}$ et $\overline{a} + \overline{c} = \overline{a \times c}$.

3 Structures algébriques

Définition 3.1 (Loi)**.** Soit E un ensemble. Une loi (de composition (interne)) est une application de $E \times E$ vers E.

Définition 3.2 (Groupe)**.** Soit $(G, \circ)$ un ensemble muni d'une loi de composition. On dit que $(G, \circ)$ est un groupe si les propriétés suivantes sont vérifiées :

(i) La loi est associative : $\forall a, b, c \in G, \quad (a \circ b) \circ c = a \circ (b \circ c)$.

(ii) Il existe un élément neutre pour $\circ$: $\exists e \in G, \quad \forall a \in E, a \circ e = e \circ a = a$.

(iii) Tous les éléments admettent un inverse pour $\circ$: $\forall a \in G, \exists b \in G \quad a \circ b = b \circ a = e$. L'inverse de a est souvent noté a^{-1}.

Définition 3.3 (Groupe abélien)**.** Soit $(G, \circ)$ un groupe. On dit que G est un groupe abélien si la loi $\circ$ est commutative : $\forall a, b \in G, \quad a \circ b = b \circ a$.

Définition 3.4 (Anneau)**.** Soit $(A, +, \times)$ un ensemble muni de deux lois. $(A, +, \times)$ est un anneau si :

(i) $(A, +)$ est un groupe abélien. On note 0_A son élément neutre.

(ii) La loi $\times$ est associative : $\forall a, b, c \in A, \quad (a \times b) \times c = a \times (b \times c)$.

(iii) Il existe un élément neutre pour $\times$: $\exists f \in A, \ \forall a \in A, \quad a \times f = f \times a = a$. On note souvent le neutre pour la deuxième loi 1_A.

(iv) La loi $\times$ est distributive sur la loi $+$: $\forall a, b, c \in A, \quad a \times (b + c) = (a \times b) + (a \times c)$ et $(b + c) \times a = (b \times a) + (b \times c)$.

Définition 3.5 (Anneau commutatif)**.** Un anneau $(A, +, \times)$ est dit commutatif si la loi $\times$ est de plus commutatif : $\forall a, b \in A, \quad a \times b = b \times a$.

Définition 3.6 (Corps)**.** On dit qu'un ensemble muni de deux lois $(A, +, \times)$ est un corps si :

(i) $(A, +, \times)$ est un anneau commutatif.

(ii) Tous les éléments non nuls admettent un inverse pour $\times$: $\forall a \in A \setminus \{0_A\}, \quad \exists b \in A, \quad a \times b = b \times a = 1_A$.

Pour résumer, il faut respectivement prouver 3, 4, 7, 8 et 9 propriétés pour montrer qu'un ensemble est groupe, groupe abélien, anneau, anneau commutatif ou un corps.

Théorème 3.7 (Structure de $\mathbb{Z}/n\mathbb{Z}$)**.** **(i)** *$(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau commutatif.*

(ii) *$(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un corps si et seulement si n est un nombre premier.*

4 PGCD, algorithme d'Euclide, théorème de Bezout

Définition 4.1 (PGCD)**.** Soit $a, b \in \mathbb{Z}$. Le PGCD (plus grand commun diviseur) de a et b est le plus grand entier qui divise à la fois a et à la fois b.

Définition 4.2 (Nombre premiers entre eux)**.** Soit $a, b \in \mathbb{Z}$. Les entiers a et b sont dits premiers entre eux si $\text{pgcd}(a, b) = 1$.

Proposition 4.3. *Soit $a, b \in \mathbb{Z}$. Alors pour tout entier $k \in \mathbb{Z}$ on a :*

1. *L'ensemble des diviseurs communs à a et b est égale à l'ensemble des diviseurs commun à $a + bk$ et b : $D_{a,b} = D_{a+bk,b}$.*
2. $\text{pgcd}(a, b) = \text{pgcd}(a + bk, b)$
3. *Si (q, r) sont le quotient et le reste de la division euclidenne de a par b alors on a* $\text{pgcd}(a, b) = \text{pgcd}(b, r)$.

Théorème 4.4. *Soit $a, b \in \mathbb{Z}$. Alors :*

(i) *$a\mathbb{Z} + b\mathbb{Z} = \text{pgcd}(a, b)\mathbb{Z}$. Autrement dit, tout multiple du pgcd(a, b) peut s'écrire comme une combinaison linéaire de a et b et le pgcd(a, b) divise toute combinaison linéaire de a et de b.*

(ii) Identité de Bézout *Il existe $u, v \in \mathbb{Z}$ tels que $au + bv = \text{pgcd}(a, b)$.*

(iii) Théorème de Bézout *a et b sont premiers entre eux si et seulement si il existe $u, v \in \mathbb{Z}$ tels que $au + bv = 1$.*

Il est possible de modifier l'algorithme d'Euclide pour obtenir à la fois le pgcd et une identité de Bézout en observant qu'à chaque étape de calcul, on manipule des combinaisons linéaires de a et de b.

5 Retour sur le cas $\mathbb{Z}/n\mathbb{Z}$

Théorème 5.1. *Soit $a, n \in \mathbb{Z}$. Alors :*

(i) *a admet un inverse multiplicatif modulo n si et seulement si* $\text{pgcd}(a, b) = 1$.

(ii) *$\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est un nombre premier.*