Arithmétique Modulaire

Plan

Dans toute cette section n est un entier **strictement positif**

Congruences modulo n

On définit une **relation d'équivalence**, notée $\equiv$, sur $\mathbb{Z}$ par

$$x \equiv y \mod n \text{ (« } x \text{ congru à } y \text{ modulo } n \text{ »)}$$
$$\text{si } n \text{ divise } x - y$$

L'ensemble des classes d'équivalences est noté $\mathbb{Z}/n\mathbb{Z}$.
On note $\dot{a} \in \mathbb{Z}/n\mathbb{Z}$, ou encore $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$, la classe de l'entier $a \in \mathbb{Z}$.

Proposition

Pour tous entiers a, et b, on a équivalence de

1. $a \equiv b \mod n$
2. a et b ont le même reste dans la division euclidienne par n.

Par conséquent, un système « naturel » de représentants des classes est l'ensemble des entiers compris entre 0 et $n-1$:
chaque entier est représenté par son reste dans la division euclidienne par n.

Remarque.

Il peut être intéressant (surtout pour les calculs « à la main ») de travailler avec un autre système de représentants :

$$\begin{aligned}\mathbb{Z}/5\mathbb{Z} &= \{\overline{0},\overline{1},\overline{2},\overline{3},\overline{4}\} \\ &= \{\overline{-2},\overline{-1},\overline{0},\overline{1},\overline{2}\}\end{aligned}$$

Structure d'anneau

Pour $n \geq 2$, l'ensemble $\mathbb{Z}/n\mathbb{Z}$ « hérite » de $\mathbb{Z}$ une structure d'anneau commutatif, c'est-à-dire de deux lois internes $+$ et $\times$ qui partagent les propriétés de l'addition et de la multiplication des entiers.
Plus précisément, on définit sur $\mathbb{Z}/n\mathbb{Z}$:

$$\begin{cases} + : & \overline{a} + \overline{b} = \overline{a+b} \\ \times : & \overline{a} \times \overline{b} = \overline{ab} \end{cases}$$

vérifiant

- $+$ est une loi de groupe abélien sur $\mathbb{Z}/n\mathbb{Z}$: loi interne, associative, $\overline{0}$ est élément neutre, toute classe admet une classe opposée : $-\overline{x} = \overline{-x}$, commutative
- $\times$ est une loi interne, associative, et commutative, admettant $\overline{1}$ pour élément neutre
- l'addition est distributive par rapport à la multiplication

Remarques.

1. Chacune de ces propriétés mérite une vérification, la plus importante étant de s'assurer que les opération sont **bien définies** : le résultat ne dépend que des classes et non des représentants particuliers choisis.
2. À partir de ces lois, de la multiplication en particulier, on peut définir
   - l'élévation au carré $a \mapsto a^2$
   - plus généralement, l'élévation à la puissance n, $n \geq 2$: $a \mapsto a^n$
   - l'exponentiation de base B : $a \mapsto B^a$

   puis éventuellement, avec quelques précautions, leurs réciproques : « racine carrée », racine n^e^, logarithme en base B ...

Plan

Soit a, b deux entiers strictement positifs, soit $x \in \mathbb{Z}$.
Si l'on connaît la classe x_{ab} de x modulo ab, on peut obtenir la classe x_a de x modulo a, en réduisant x_{ab} modulo a.
Et de même modulo b !
En fait, si a et b sont premiers entre eux, on a une sorte de réciproque :

Théorème chinois des restes

Soit a, b des entiers strictement positifs tels que $\text{pgcd}(a, b) = 1$, et soit u, v des entiers tels que $au + bv = 1$.
L'application

$$\begin{array}{rccc} \varphi : & \mathbb{Z}/(ab)\mathbb{Z} & \longrightarrow & \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} \\ & x \mod (ab) & \mapsto & (x \mod a,\ x \mod b) \end{array}$$

est un isomorphisme d'anneau (une bijection respectant la structure d'anneau), de réciproque :

$$\begin{array}{rcc} \psi : \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} & \longrightarrow & \mathbb{Z}/(ab)\mathbb{Z} \\ (x_a, x_b) & \mapsto & x_a bv + x_b au \end{array}$$

Exemple.

avec $a = 7$, $b = 5$ (noter que $3 \times 7 - 4 \times 5 = 1$)

$$\begin{cases} x \equiv 3 \mod 7 \\ x \equiv 1 \mod 5 \end{cases} \Leftrightarrow \quad x \equiv 3 \times (-4) \times 5 + 1 \times 3 \times 7 \equiv 31 \mod 35$$

Démonstration.

- Pour la partie morphisme, il y a beaucoup de choses faciles à vérifier.
- Le plus important est de saisir que la structure d'anneau sur un produit cartésien d'anneaux, est celle qu'on pense (addition et multiplication composante par composante).
- Pour l'aspect « bijection », on vérifie facilement que $\varphi \circ \psi = \mathrm{Id}_{\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}}$ grâce à l'identité de Bézout
- Et réciproquement, il faut voir que $\psi \circ \varphi(x) = x_a bv + x_b au \mod ab$. On peut calculer avec des représentants dans $\mathbb{Z}$

$$\begin{aligned} x_a bv + x_b au &= (x + ak)bv + (x + b\ell)au \\ &= x(au + bv) + ab(kv + \ell u) \end{aligned}$$

$\square$

Plan

Définition

Soit $a \in \mathbb{Z}/n\mathbb{Z}$.
On dit que a est un (élément) inversible s'il existe $b \in \mathbb{Z}/n\mathbb{Z}$ tel que $ab = 1 \in \mathbb{Z}/n\mathbb{Z}$.

Par exemple $7 \times 8 = 1 + 5 \times 11$ implique que 7 et 8 sont inverses modulo 11.

Remarques.

- Un tel élément b est un inverse de a, et il est facile de voir que si a est inversible, l'inverse est unique.
- $\overline{0}$ n'est jamais inversible, $\overline{1}$ l'est toujours.
- Si $a \neq \overline{0}$, et s'il existe $b \in \mathbb{Z}/n\mathbb{Z}$, $b \neq \overline{0}$, tel que $ab = 0 \in \mathbb{Z}/n\mathbb{Z}$, on dit que a est un diviseur de zéro, et on voit facilement que a n'est alors pas inversible.

On note $(\mathbb{Z}/n\mathbb{Z})^\times$ l'ensemble des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$.

Proposition

L'ensemble $(\mathbb{Z}/n\mathbb{Z})^\times$ est stable par multiplication et passage à l'inverse.

Remarques.

- La démonstration est une vérification immédiate.
- On résume cette propriété en disant que $((\mathbb{Z}/n\mathbb{Z})^\times, \times)$ est un **groupe abélien** (avec la classe de 1 pour élément neutre).

Proposition

Soit $n \in \mathbb{N}^*$ et $a \in \mathbb{Z}$. On a équivalence entre

1. $\overline{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$
2. $\text{pgcd}(a, n) = 1$

Démonstration.
C'est simplement l'Identité de Bézout ! $\square$

Corollaire

On a équivalence entre

1. p est un nombre premier
2. tout élément non nul de $\mathbb{Z}/p\mathbb{Z}$ est inversible

Autrement dit, si si n est premier, $(\mathbb{Z}/n\mathbb{Z})^\times = \mathbb{Z}/n\mathbb{Z} \setminus \{\overline{0}\}$:
$\mathbb{Z}/n\mathbb{Z}$ est alors un corps
(un anneau dont tout élément non nul est inversible).

Définition

Soit $n \in \mathbb{Z}$.
On appelle indicatrice d'Euler de n ,et on note $\phi(n)$,le nombre d'éléments de $(\mathbb{Z}/n\mathbb{Z})^{\times}$.

Remarques.

- $\phi(n)$ est simplement le nombre d'entiers m, tels que $0 < m < n$, et $\text{pgcd}(m, n) = 1$
- Pour un nombre premier p, $\phi(p) = p - 1$
- si p et q sont des nombres premiers distincts, et $n = pq$, $\phi(n) = (p - 1)(q - 1)$ (simple comptage, ou théorème chinois)
- mais le comportement (et le calcul) général de $\phi(n)$ ne semble ni simple, ni prévisible : il reflète la complexité de la relation de divisibilité dans $\mathbb{Z}$ ...
  Calculer par exemple : $\phi(11)$, $\phi(12)$, $\phi(13)$, $\phi(14)$.

Théorème d'Euler

Soit n un entier. Pour tout entier a, premier à n, on a

$$a^{\phi(n)} \equiv 1 \mod n.$$

Démonstration.

Soit $a \in (\mathbb{Z}/n\mathbb{Z})^\times$, on considère l'application :

$$\begin{array}{rccc} \mu_a : (\mathbb{Z}/n\mathbb{Z})^\times & \longrightarrow & (\mathbb{Z}/n\mathbb{Z})^\times \\ x & \mapsto & ax \end{array}$$

C'est une bijection de $(\mathbb{Z}/n\mathbb{Z})^\times$ (d'inverse $\mu_{a^{-1}}$), donc

$$\prod_{x\in(\mathbb{Z}/n\mathbb{Z})^\times} x = \prod_{x\in(\mathbb{Z}/n\mathbb{Z})^\times} \mu_a(x) = \prod_{x\in(\mathbb{Z}/n\mathbb{Z})^\times} ax = a^{\phi(n)} \left(\prod_{x\in(\mathbb{Z}/n\mathbb{Z})^\times} x \right)$$

Et on simplifie par $\prod_{x\in(\mathbb{Z}/n\mathbb{Z})^\times} x$ aux deux extrémités des égalités ! $\square$

Corollaire : Petit théorème de Fermat

Pour tout nombre premier p, et tout entier a tel que $0 < a < p$,
on a : $a^{p-1} \equiv 1 \mod p$.