Algèbre et Arithmétique Effectives — 30/09/25
Cours 4

Rappels de la dernières fois

Déf : Soit $n \in \mathbb{Z}_{>0}$.
Soient $a, b \in \mathbb{Z}$.

On dit que <u>a est congruent à b modulo n</u>
et on écrit :

$$a \equiv b \pmod{n} \qquad (\text{ou } a \equiv_n b)$$

si $n \mid a-b$.

Ceci est une relation d'équivalence (voir TD 2).
$\forall a \in \mathbb{Z}$, on note

$$[a]_n := \{ b \in \mathbb{Z} \; : \; b \equiv a \bmod n \}$$

la classe d'équivalence de a.

Déf : L'ensemble des classes d'équivalence, i.e. l'ensemble quotient, par rapport à la relation de congruence modulo n est noté

$$\mathbb{Z}/n\mathbb{Z}.$$

Théorème : Soit $n \in \mathbb{Z}_{>0}$. Alors $\mathbb{Z}/n\mathbb{Z}$ est l'ensemble des n classes d'équivalence

$$[0]_n, [1]_n, \ldots, [n-1]_n$$

Ainsi, toute classe d'équivalence possède un représentant compris entre 0 et $n-1$.

Démo

Soit $a \in \mathbb{Z}$.

Alors, en effectuant la division euclidienne de n par a, on obtient :

$\exists\, q, r \in \mathbb{Z},\ 0 \leq r < n$ tels que

$$a = qn + r$$

$\Rightarrow a - r = qn \Rightarrow n \mid a - r \Rightarrow a \equiv r \bmod n.$

$\Rightarrow a \in [r]_n,\ 0 \leq r < n.$

On montre maintenant que si $0 \leq a < b \leq n-1$ alors $[a]_n \neq [b]_n$.

Si, par l'absurde, $[a]_n = [b]_n \Rightarrow$

$\Rightarrow n \mid b - a$, $0 < b - a \leq n-1$ et cela est impossible.

Remarque : La démo du théorème nous dit aussi que $\forall a \in \mathbb{Z}$, $[a]_n = [r]_n$, où r est le reste de la division de a par n.

Donc :

$$\mathbb{Z}/_{n\mathbb{Z}} = \{[0]_n, [1]_n, \dots, [n-1]_n\}$$

On va définir deux opérations binaires sur $\mathbb{Z}/_{n\mathbb{Z}}$.

ADDITION : $+ : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$

$$([a]_n, [b]_n) \longmapsto [a]_n + [b]_n := [a+b]_n$$

MULTIPLICATION : $\cdot : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$

$$([a]_n, [b]_n) \longmapsto [a]_n \cdot [b]_n := [ab]_n$$

Quand on travaille avec des classes d'équivalence il faut montrer que les opérations sont bien définies.

Dans notre cas cela signifie que :

si $a' \in [a]_n$, $b' \in [b]_n$, alors $[a'+b']_n = [a+b]_n$ et $[a'b']_n = [ab]_n$.

Cela est conséquence du résultat suivant :

<u>Proposition</u> : Soient $a, b, a', b' \in \mathbb{Z}$, $n \in \mathbb{Z}_{>0}$.

Si $a \equiv a' \bmod n$ et $b \equiv b' \bmod n$ alors :

1) $a+b \equiv a'+b' \bmod n$.
2) $ab \equiv a'b' \bmod n$.

<u>Dem</u>

1) $a \equiv a' \pmod n \Rightarrow \exists\, k_1 \in \mathbb{Z}$ t.q. $a - a' = k_1 n$

$b \equiv b' \pmod n \Rightarrow \exists\, k_2 \in \mathbb{Z}$ t.q. $b - b' = k_2 n$

Donc, en sommant on obtient :

$$a - a' + b - b' = n(k_1 + k_2)$$

$$\Downarrow$$

$$(a+b)-(a'+b')=n(k_1+k_2)$$

$$\Downarrow$$

$$a+b \equiv a'+b' \pmod n.$$

2) Par exercice.

<u>Propriétés de l'addition</u>

1) commutativité : $\forall\ [a]_n, [b]_n \in \mathbb{Z}/_{n\mathbb{Z}}$,
$[a]_n+[b]_n = [b]_n+[a]_n$.
(conséquence du fait que + est commutative dans $\mathbb{Z}$)

2) associativité : $\forall\ [a]_n, [b]_n, [c]_n \in \mathbb{Z}/_{n\mathbb{Z}}$
$([a]_n+[b]_n)+[c]_n = [a]_n+([b]_n+[c]_n)$

3) $\exists$ élément neutre $[0]_n$ tel que
$\forall\ [a]_n \in \mathbb{Z}/_{n\mathbb{Z}}$, $[a]_n+[0]_n = [0]_n+[a]_n = [a]_n$.

4) $\forall\ [a]_n \in \mathbb{Z}/_{n\mathbb{Z}}$, $\exists$ un élément opposé $[-a]_n$ tel que :
$$[a]_n+[-a]_n = [-a]_n+[a]_n = [0]_n.$$

Donc $(\mathbb{Z}/_{n\mathbb{Z}}, +)$ est un groupe abélien (ou commutatif).

<u>Propriétés de la multiplication</u>

1) commutativité

2) associativité

3) $\exists$ élément neutre $[1]_n$

En plus $\cdot$ est distributive sur $+$:

$\forall\ [a]_n, [b]_n, [c]_n \in \mathbb{Z}/_{n\mathbb{Z}}$

$$[a]_n \left([b]_n + [c]_n\right) = [a]_n [b]_n + [a]_n [c]_n$$
$$\left([a]_n + [b]_n\right) [c]_n = [a]_n [c]_n + [b]_n [c]_n$$

Donc $\left(\mathbb{Z}/_{n\mathbb{Z}}, +, \cdot\right)$ est un anneau commutatif et unitaire.

<u>Question</u> : Est-ce que $\mathbb{Z}/_{n\mathbb{Z}}$ est un corps ?

Non, car en général <u>ce n'est pas vrai que</u>

$\forall\ [a]_n \in \mathbb{Z}/_{n\mathbb{Z}},\ [a]_n \neq [0]_n,$
$\exists\ [b]_n \in \mathbb{Z}/_{n\mathbb{Z}}$ t.q. $[a]_n [b]_n = [1]_n$.

<u>Exemple</u> : $\mathbb{Z}/_{8\mathbb{Z}}$, l'élément $[2]_n$ n'a pas d'inverse par rapport à la multiplication.

<u>Notation</u> : Lorsque le contexte est clair, on note $[a]_n$ simplement $[a]$, ou encore, par abus de notation, juste a.

<u>Déf</u> : Un élément $a \in \mathbb{Z}/_{n\mathbb{Z}}$ est <u>inversible</u> s'il existe $b \in \mathbb{Z}/_{n\mathbb{Z}}$ t.q. $ab = 1$.

$\Updownarrow$

$ab \equiv 1 \mod n$

Exemple : 3 est inversible mod 4, car $3 \cdot 3 \equiv 1 \bmod 4$.

Remarque : on peut facilement montrer que si a est inversible alors son inverse est unique et on le note a^{-1}.

Proposition : Un élément $a \in \mathbb{Z}/_{n\mathbb{Z}}$ est inversible si et seulement si $\mathrm{pgcd}(a,n) = 1$.

Dém

$\Rightarrow$) Si $a \in \mathbb{Z}/_{n\mathbb{Z}}$ est inversible $\Rightarrow \exists\, b \in \mathbb{Z}/_{n\mathbb{Z}}$ tel que $ab \equiv 1 \bmod n \Rightarrow n \mid (ab-1)$

$\Rightarrow \exists\, k \in \mathbb{Z}$ t.q. $ab - 1 = nk \Rightarrow$

$\Rightarrow ab - nk = 1 \Rightarrow \mathrm{pgcd}(a,n) \mid 1 \Rightarrow$

exo 5.1 TD1

$\Rightarrow \mathrm{pgcd}(a,n) = 1$.

$\Leftarrow$) Si $\mathrm{pgcd}(a,n) = 1 \Rightarrow \exists\, u,v \in \mathbb{Z}$ tels que

$au + nv = 1 \Rightarrow au - 1 = n(-v) \Rightarrow$

$\Rightarrow au \equiv 1 \pmod n$

Donc a est inversible et u est l'inverse de a.

La démonstration nous suggère un algorithme d'inversion modulaire.

Algorithme : InverseMod(a,n)

Entrées : Deux entiers $a, n \neq 0$

Sortie : Un entier b, $0 < b < n$, tel que $ab \equiv 1 \bmod n$ s'il existe, une erreur sinon.

1. $(d, u, v) \leftarrow$ EuclideEtendu (a, n)

2. Si $d \neq 1$. Renvoyer une erreur
« a n'est pas inversible modulo n »

3. Renvoyer $u \bmod n$.

<u>Exemple</u> : 1) Calculer l'inverse de 20 modulo 63.

$$63 = 3 \cdot 20 + 3 \quad ③$$

$$20 = 6 \cdot 3 + 2 \quad ②$$

$$3 = 1 \cdot 2 + 1 \quad ①$$

$$2 = 2 \cdot 1$$

$\Rightarrow$ $\operatorname{pgcd}(20, 63) = 1 \Rightarrow 20$ est inversible modulo 63.

$$1 \overset{①}{=} 3 - 1 \cdot 2 \overset{②}{=} 3 - (20 - 6 \cdot 3) =$$

$$= -20 + 7 \cdot 3 = -20 + 7(63 - 3 \cdot 20) =$$

$$\overset{③}{=} \underbrace{-22}_{u} \cdot 20 + \underbrace{7}_{v} \cdot 63$$

$\Rightarrow 1 = -22 \cdot 20 + 7 \cdot 63$ (identité de Bézout)

$\Rightarrow -22 \equiv 41 \bmod 63$ est l'inverse de 20 modulo 63.

2) Calculer l'inverse de 3 mod 7.
C'est plus rapide de procéder par "force brute"

$3 \cdot 5 = 15 \equiv 1 \bmod 7 \Rightarrow 5$ est l'inverse de 3 mod 7.

<u>Notation</u> : L'ensemble des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ est noté $(\mathbb{Z}/n\mathbb{Z})^*$.

Remarque : $\left| \left(\mathbb{Z}/n\mathbb{Z} \right)^\times \right| \underset{\substack{\uparrow \\ \text{proposition} \\ \text{précédente}}}{=} \left| \{ a \in \mathbb{Z},\ 1 \leq a \leq n\ , \text{ tel que } \operatorname{pgcd}(a,n) = 1 \} \right| =$

$= \varphi(n)$ (fonction φ d'Euler)

Exemple : Si $n = p$ est un nombre premier, alors $\forall\ 0 < a \leq p-1$ on a $\operatorname{pgcd}(a,p) = 1$ et donc

$\varphi(p) = p - 1.$

Remarque : Soit p un nombre premier. Alors tous les éléments non nuls de $\mathbb{Z}/p\mathbb{Z}$ sont inversibles, et donc $\mathbb{Z}/p\mathbb{Z}$ est un corps (commutatif).

Exemple

$n = 36$

$$\left(\mathbb{Z}/36\mathbb{Z} \right)^\times = \{ 1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35 \}.$$