# Chapitre 2

# Congruences, $\mathbb{Z}/n\mathbb{Z}$

## 2.1 La relation de congruence modulo $n$

### 2.1.1 Les définitions

**Définition 2.1.1.** Deux entiers relatifs $x$ et $y$ sont congrus modulo l'entier $n$ si et seulement si $y - x$ est divisible par $n$ : $y - x \in n\mathbb{Z}$. On note :

$$x \equiv y \ (mod\ n)\ .$$

**Proposition 2.1.2.** *Deux entiers relatifs $x$ et $y$ sont congrus modulo l'entier $n$ si et seulement si les deux divisions euclidiennes par $n$ produisent le même reste.*

**Proposition 2.1.3.** *La relation de congruence modulo $n$ est une relation d'équivalence.*

La classe d'équivalence de $x$ est l'ensemble $x + n\mathbb{Z}$ souvent noté $\overline{x}$ s'il n'y a pas d'ambiguïté ( ${}^{n}\overline{x}$ s'il y a lieu de préciser). La classe de $x$ contient un unique élément $r$ tel que $0 \leq r < |n|$ (le reste).

### 2.1.2 Le théorème chinois en termes de congruences

**Théorème 2.1.4** (Théorème chinois)**.** *Si $a$ et $b$ sont premiers entre eux, alors le système de congruence :*

$$\begin{cases} x & \equiv & \alpha & (\text{mod } a) \\ x & \equiv & \beta & (\text{mod } b) \end{cases}$$

*a une solution qui est* unique modulo *$ab$. Plus précisément, étant donné une relation de Bezout $au + bv = 1$, le système est équivalent à :*

$$x \equiv vb\alpha + ua\beta \quad (mod\ ab)\ .$$

Exemples.

## 2.2 Notions de base sur les groupes

### 2.2.1 Lois de composition, structure de groupe

Une loi de composition interne sur un ensemble $E$ est une application $E \times E \to E$. L'image du couple $(x, y)$ est noté avec un symbole : suivant le contexte $x + y$, $x \times y$, $x * y$, $x \top y$ ...
Associativité, commutativité.
Neutre, unicité ; élément symétrique, unicité.
Définition d'un groupe.
Exemples :$(\mathbb{Z}, +)$ est un groupe ; groupe des bijections de $X$ noté $(\mathcal{B}(X), \circ)$, cas du groupe symétrique $\mathcal{S}_n = \mathcal{B}(\{1, \ldots, n\})$.

### 2.2.2 Sous-groupe

**Définition 2.2.1.** Une partie $H$ d'un groupe $(G, *)$ est une sous-groupe si et seulement si elle contient le neutre et elle est stable pour l'opération $*$ et la symétrisation.

*Remarque* 2.2.2. En notation additive : une partie $H$ d'un groupe $(G, +)$ est un sous-groupe si et seulement si elle contient 0 et elle est stable par addition et soustraction.
En notation multiplicative : une partie $H$ d'un groupe $(G, \times)$ est une sous-groupe si et seulement si elle contient 1 et elle est stable par produit et quotient.

### 2.2.3 Ordre d'un élément

**Définition 2.2.3.** Soit $x$ un élément d'un groupe $G$. Le sous-groupe engendré par $x$, noté $< x >$ est le plus petit sous-groupe qui contient $x$ ; on dit alors que $x$ est un générateur du sous-groupe $< x >$.

**Définition 2.2.4.** Un élément $x$ d'un groupe $G$ est d'ordre fini si et seulement si le sous-groupe $< x >$ est fini. Dans ce cas l'ordre de $x$ est le nombre d'éléments du sous-groupe $< x >$, c'est le plus petit $k > 0$ tel que le $k$-ième itéré de $x$ redonne le neutre.

*Remarque* 2.2.5. En notation additive, la composition de $n$ fois $x$ s'écrit $nx$, et pour $n = -m < 0$, $nx$ est l'élément symétrique de $mx$ (l'opposé). Un élément $x$ est d'ordre fini si et seulement s'il existe $m > 0$ tel que $mx$ est nul, l'ordre étant le plus petit tel $m$.
En notation multiplicative, la composition de $n$ fois $x$ s'écrit $x^n$, et pour $n = -m < 0$, $x^n = x^{-m}$ est l'inverse de $x^m$. Un élément $x$ est d'ordre fini si et seulement s'il existe $m > 0$ tel que $x^m$ vaut 1, l'ordre étant le plus petit tel $m$.

### 2.2.4 Morphisme de groupe

**Définition 2.2.6.** Soient $(G, *)$ et $(G', \top)$ deux groupes. Une application $f : G \to G'$ est un morphisme de groupe si et seulement si :

$$\forall x \in G \ , \ \forall y \in G \ , \ , f(x * y) = f(x) \top f(y) \ .$$

*Exemple* 2.2.7. L'application logarithme est un morphisme du groupe $(]0, +\infty[, \times)$ vers le groupe $(\mathbb{R}, +)$.

*Exemple* 2.2.8. Soit $x$ un élément dans un groupe $G$ noté multicativement. L'application $g_x : \mathbb{Z} \to G$ qui à $n$ associe $x^n$ est un morphisme de groupe.

**Définition 2.2.9.** Le noyau d'un morphisme de groupe $f : G \to G'$ est l'ensemble des éléments dont l'image est le neutre $e'$ de $G'$.

**Définition 2.2.10.** L'image d'un morphisme de groupe $f : G \to G'$ est l'ensemble :

$$\mathrm{Im}(f) = f(G) = \{f(x), \ x \in G\} \ .$$

**Proposition 2.2.11.** *Soit $f : G \to G'$ un morphisme de groupe.*
*Le noyau de $f$ est un sous-groupe de $G$ et l'image de $f$ est un sous-groupe de $G'$.*

### 2.2.5 Théorème de Lagrange

**Théorème 2.2.12** (Lagrange)**.** *Dans un groupe fini $G$ de cardinal $N$, tous les sous-groupes ont un cardinal qui divise $N$.*

**Corollaire 2.2.13.** *Dans un groupe fini $G$ de cardinal $N$, l'ordre de tous les éléments divise $N$. En notation multiplicative :*

$$\forall x \in G \ , x^N = 1 \ .$$

## 2.3 Structure sur les classes de congruence

### Le groupe additif $(\mathbb{Z}/n\mathbb{Z}, +)$

**Théorème 2.3.1.** *L'addition est bien définie sur les classes de congruence et munit $\mathbb{Z}/n\mathbb{Z}$ d'une structure de groupe.*

### L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$

**Théorème 2.3.2.** *La multiplication est bien définie sur les classes de congruence et $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ a une structure d'anneau.*

fin du cours du 06/02

### Le théorème chinois en termes de classes de congruence

**Théorème 2.3.3.** *Si $a$ et $b$ sont premiers entre eux, alors l'application*

$$^{ab}\overline{k} \mapsto (^{a}\overline{k}, {}^{b}\overline{k}) \ ,$$

### Le groupe multiplicatif des inversibles de $\mathbb{Z}/n\mathbb{Z}$

**Définition 2.3.4.** La classe $\overline{k} \in \mathbb{Z}/n\mathbb{Z}$ est inversible si et seulement s'il existe $\overline{l} \in \mathbb{Z}/n\mathbb{Z}$ tel que $\overline{k}\,\overline{l} = \overline{1}$.

**Théorème 2.3.5.** *La classe $\overline{k}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $k$ et $n$ sont premiers entre eux.*

**Proposition 2.3.6.** *L'ensemble des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ muni de la multiplication forme un groupe.*

Notation : $(\mathbb{Z}/n\mathbb{Z})^*$.

**Définition 2.3.7.** Pour un entier $n \geq 2$, l'indicateur d'Euler $\phi(b)$ est le nombre d'éléments inversibles dans $\mathbb{Z}/n\mathbb{Z}$ : le nombre d'éléments de $(\mathbb{Z}/n\mathbb{Z})^*$.

**Théorème 2.3.8.** *a) Pour $p$ premier et $\alpha > 0$, $\phi(p^\alpha) = p^\alpha - p^{\alpha-1}$.*
*b) Pour $a$ et $b$ premiers entre eux, $\phi(ab) = \phi(a)\phi(b)$.*

*Exercice* 2.3.9. Montrer qu'un élément de $\mathbb{Z}/n\mathbb{Z}$ est inversible si et seulement s'il est générateur du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$.

**Corollaire 2.3.10.** *$\mathbb{Z}/p\mathbb{Z}$ est un corps si et seulement si $p$ est un nombre premier.*

## 2.4 Petit théorème de Fermat

**Théorème 2.4.1.** *Si $p$ est un nombre premier, alors pour tout $k$ qui est premier avec $p$, on a : $k^{p-1} \equiv 1 \pmod{p}$*

La réciproque de ce théorème est fausse, par exemple : $561 = 3 \times 11 \times 17$ n'est pas premier et pourtant pour tout entier $a$ premier avec 561, on a $a^{560} \equiv 1 \pmod{561}$.

Le théorème de Fermat donne un test de primalité : si pour un entier $a < n$, on a $a^{n-1} \not\equiv 1 \pmod{n}$, alors $n$ n'est pas premier ; si pour plusieurs valeurs de $a$, on a $a^{n-1} \equiv 1 \pmod{n}$, alors $n$ est probablement premier.

**Théorème 2.4.2** (Théorème de Fermat généralisé)**.** *Pour tout entier $k$ premier avec $n$, on a :*

$$k^{\phi(n)} \equiv 1 \pmod{n} \ .$$

**Calcul rapide des puissances modulo $n$.** Le test de Fermat nécessite des calculs de puissances modulo $n$. Pour de grands entiers un calcul naïf sur machine fait apparaître des problèmes de complexité. On améliore grandement l'efficacité avec un algorithme de calcul rapide des puissances.

```
Fonction puissance(a,m,n) // entier, exposant, module
R ← 1 ;
While (m > 0) do
    | If (m est impair) then
    |    | R ← (R × a)mod n ;
    | end If
    | a ← (a × a)mod n ;
    | m ← m/2 ; // division entière
done
Retouner R ;
```

Algorithm 5: Calcul rapide des puissances modulo $n$

**Théorème 2.4.3.** *L'algorithme précédent calcule $a^m$ modulo $n$, avec au plus $2(\log_2(m)+1)$ multiplications modulo $n$.*

*Exercice* 2.4.4. Ecrire une version récursive du calcul rapide des puissances modulo $n$ et coder la fonction correspondante en python.