

## 120 : Anneaux $\mathbb{Z}/n\mathbb{Z}$ . Applications.

**Cadre** :  $n \in \mathbb{N}^*$ .

### I) Généralités

A) Le groupe  $\mathbb{Z}/n\mathbb{Z}$

Sous-groupe  $n\mathbb{Z}$ , caractérisation des sous-groupes de  $\mathbb{Z}$ . Relation de congruence. Sous-groupe de  $\mathbb{Z}/n\mathbb{Z}$ . Groupe des inversibles de  $\mathbb{Z}/n\mathbb{Z}$ . Isomorphisme avec les groupes cycliques d'ordre  $n$ .

B) Automorphismes de  $\mathbb{Z}/n\mathbb{Z}$

Fonction d'EULER, exemples. Isomorphisme avec les automorphismes de  $\mathbb{Z}/n\mathbb{Z}$ . **DEV 1** : ÉTUDE DE  $(\mathbb{Z}/n\mathbb{Z})^*$ .

C) L'anneau  $\mathbb{Z}/n\mathbb{Z}$

Structure d'anneau. Théorème chinois, contre-exemple dans le cas où les entiers sont seulement "premiers dans leur ensemble". passage à l'isomorphisme des inversibles.

### II) Application à l'arithmétique de $\mathbb{Z}$

Théorème d'EULER puis de FERMAT. Somme des  $\varphi(d)$ , où  $d$  divise  $n$ . Théorème de WILSON, théorème de LIOUVILLE.

### III) Application à la résolution d'équations diophantiennes

Résolution de  $ax \equiv b \pmod{n}$  dans le cas particulier où  $a \wedge n = 1$ . Résolution dans le cas général. Utilisation du théorème chinois pour un système d'équations diophantiennes :  $k \equiv a_j \pmod{n_j}$  ( $1 \leq j \leq r$ ). **DEV 2** : SYSTÈME DE CONGRUENCES. Exemple.

### IV) Application aux corps finis

A) Les carrés de  $\mathbb{F}_q$

Carrés de  $(\mathbb{F}_q)^*$  et de  $\mathbb{F}$ . Existence d'une solution à  $ax^2 +$

$by^2 = 1$ . Étude du groupe  $SO(\mathbb{F}_q)$ . Cas de la caractéristique 2.

B) Vers la loi de réciprocité quadratique

Symbole de LEGENDRE, loi de réciprocité quadratique. Cas de 2. Exemple.

### V) Cyclotomie

Sous-groupes de l'unité, définition du  $n$ -ième polynôme cyclotomique  $\Phi_{n,k}$ , exemples. Degré de  $\Phi_{n,k}$ , relations avec  $X^n - 1$ , irréductibilité de  $\Phi_{n,k} \in \mathbb{Z}[X]$ , application au degré de l'extension de  $\mathbb{Q} \subset \mathbb{Q}(\xi)$ .

### Références :

- ROMBALDI
- PERRIN
- GOURDON
- CALDERO