Leçon 120 : Anneau ZnZ. Applications.

1 L'anneau $\mathbb{Z}/n\mathbb{Z}$ (Rombaldi)

1.1 Construction

- Définition de l'égalité modulo n + c'est une relation d'équivalence
- On définit $\mathbb{Z}/n\mathbb{Z}$ comme l'ensemble de ces classes + cardinal
- Unicité de la structure d'anneau cohérente avec la projection
- Explicitation des lois d'anneau

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

- Cyclique
- Description de ses sous-groupes
- Description des générateurs
- Définition indicatrice d'Euler + propriétés
- Théorème de structure des groupes abéliens finis

1.3 Le groupe des inversibles et l'anneau $\mathbb{Z}/n\mathbb{Z}$

- Définition de $(\mathbb{Z}/n\mathbb{Z})^\times$
- Exemple quand n est premier
- Isomorphisme avec les automorphismes de $\mathbb{Z}/n\mathbb{Z}$
- Équivalence entre être inversible et générateur de $\mathbb{Z}/n\mathbb{Z}$
- Théorème chinois
- Conséquence sur le groupe des inversibles + multiplicativité de l'indicatrice d'Euler
- Dév 1 : Condition pour que $\mathbb{Z}/n\mathbb{Z}$ soit cyclique

2 Applications

2.1 Étude des carrés dans $\mathbb{Z}/p\mathbb{Z}$

- $\mathbb{Z}/n\mathbb{Z}$ corps ssi n premier
- Caractérisation des carrés
- -1 carré ssi $p = 1 \mod [4]$
- Application : théorème des deux carrés de Fermat

2.2 Cryptographie

- Explication du système RSA avec la propriété mathématiques sous-jacente

2.3 Utilisation des polynômes cyclotomiques

- Définition
- Propriétés classiques (irréductibilités, à coeff dans $\mathbb{Z}$ etc.)
- Dév 2 : Théorème de Dirichlet faible

2.4 Système de congruence

- Définition du problème
- Explication de l'utilisation du théorème chinois (existence, unicité)
- Application réciproque du théorème chinois
- Exemple concret