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

I Construction et propriétés de $\mathbb{Z}/n\mathbb{Z}$

1 Congruences dans $\mathbb{Z}$

- Définition, classes d'équivalence
- Construction de $\mathbb{Z}/n\mathbb{Z}$
- Exemples

2 Structure d'anneau

- $\exists!$ structure d'anneau sur $\mathbb{Z}/n\mathbb{Z}$ telle que $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ soit un morphisme
- $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe cyclique, théorème de structure des groupes abéliens finis
- Générateurs de $(\mathbb{Z}/n\mathbb{Z}, +)$

3 Cas $n = p$ premier

- $\mathbb{Z}/n\mathbb{Z}$ est intègre $\iff$ $\mathbb{Z}/n\mathbb{Z}$ est un corps $\iff$ n est premier
- Ce résultat est à la base de la théorie des corps finis

II Etude de $\mathbb{Z}/n\mathbb{Z}$ et $(\mathbb{Z}/n\mathbb{Z})^\times$

1 Théorème des restes chinois

- DEV 1 : Théorème des restes chinois
- Exemples

2 Groupe $((\mathbb{Z}/n\mathbb{Z})^\times, \cdot)$

- Exemples
- $\bar{k} \in (\mathbb{Z}/n\mathbb{Z})^\times \iff \mathrm{pgcd}(n,k) = 1$
- Critère de cyclicité de $(\mathbb{Z}/n\mathbb{Z})^\times$

3 Fonction indicatrice d'Euler

- Définition
- Lien avec $(\mathbb{Z}/n\mathbb{Z})^\times$
- Propriété de multiplicativité via le théorème chinois
- $n = \sum_{d|n} \varphi(d), \varphi(n) = \sum_{d|n} \mu(d)\frac{n}{d}$

III Applications

1 Arithmétique

- DEV 1 suite : Système de congruence
- Petit théorème de Fermat et variantes
- Critères de divisibilité

2 Irréductibilité de polynômes

- $\bar{P}$ unitaire irréductible sur $\mathbb{Z}/p\mathbb{Z} \implies P$ irréductible sur $\mathbb{Z}$
- DEV 2 : Lemme des contenus + P irréductible sur $\mathbb{Z} \implies P$ irréductible sur $\mathbb{Q}$ + Critère d'Eisenstein