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

Soit $n \geq 2$ un entier et p un premier.

I/ Construction de l'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$.

A/ Groupe $(\mathbb{Z}/n\mathbb{Z}, +)$. [ROM]

Définition 1 : Congruence mod n.

Proposition 2 : Somme et produit de congruences.

Définition 3 : Définition de $\mathbb{Z}/n\mathbb{Z}$ et groupe avec l'addition mod n.

Proposition 4 : $\mathbb{Z}/n\mathbb{Z}$ est cyclique d'ordre n et tout groupe cyclique d'ordre n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Application 5 : $\mathbb{U}_n \simeq \mathbb{Z}/n\mathbb{Z}$.

Théorème 6 : Les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$.

Théorème 7 : Théorème de structure des groupes abéliens finis.

Exemple 8 : Les groupes abéliens d'ordre 24.

B/ L'anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$. [ROM]

Proposition 9 : $\mathbb{Z}$ est principal et ses idéaux sont les $n\mathbb{Z}$.

Corollaire 10 : Il existe une unique structure d'anneau sur $\mathbb{Z}/n\mathbb{Z}$ rendant la surjection canonique un morphisme d'anneaux.

Théorème 11 : $a \wedge n = 1 \Leftrightarrow \overline{a}$ est générateur de $\mathbb{Z}/n\mathbb{Z} \Leftrightarrow \overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$.

Application 12 : $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$.

Définition 13 : Indicatrice d'Euler.

Exemple 14 : $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$, $\varphi(p) = p-1$ et $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$.

Exemple 15 : $n = \sum_{d|n} \varphi(d)$.

Corollaire 16 : Les diviseurs de 0 dans $\mathbb{Z}/n\mathbb{Z}$ sont $\mathbb{Z}/n\mathbb{Z} \backslash ((\mathbb{Z}/n\mathbb{Z})^\times \cup \{0\})$.

Corollaire 17 : Les idéaux de $\mathbb{Z}/n\mathbb{Z}$.

Théorème 18 : $\mathbb{Z}/n\mathbb{Z}$ intègre $\Leftrightarrow \mathbb{Z}/n\mathbb{Z}$ corps $\Leftrightarrow n$ premier.

Théorème 19 : Théorème chinois général et expression explicite de l'inverse.

Application 20 : Calcul du déterminant sur $\mathbb{Z}$ informatiquement : soit $M \in \mathrm{M}_n(\mathbb{Z})$, on considère $H = \max_{i,j \in [\![1,n]\!]} |m_{i,j}|$ et prenons $p_1, \dots, p_r$ des premiers distincts tels que $p_1 \dots p_r > 2n! H^n$ (de telle sorte à ce que $\det(M) < p_1 \dots p_r$), on calcule $\det(\overline{M})$ dans $\mathbb{F}_{p_i}$ pour tout i et par le théorème chinois on a donc $\det(M)$ dans $\mathbb{Z}$.

Corollaire 21 : φ est multiplicative.

Application 22 : Avec le théorème de structure des groupes abéliens et le théorème chinois, on peut trouver à isomorphisme près tous les groupes abéliens d'ordre fini.

Théorème 23 : $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique.

Théorème 24 : $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique ssi $n = 2, 4, p^\alpha, 2p^\alpha$.

II/ Application dans différents domaines des mathématiques

A/ Test de primalité et RSA. [ROM] [G]

Théorème 25 : Euler.

Théorème 26 : Fermat.

Remarque 27 : Réciproque fausse, nombres de Carmichaël.

Application 28 : RSA.

Application 29 : Test de primalité de Fermat.

B/ Équations arithmétiques. [ROM]

Théorème 30 : Résolution de $ax \equiv b[n]$.

Application 31 : Application du théorème chinois à la résolution de systèmes de congruences.

Exemple 32 : Résolution du système de congruences $k \equiv 2[4], 3[5], 1[9]$.

C/ Application à la théorie des corps. [PER]

Proposition 33 : Caractéristique et $\mathbb{F}_p$ sous-corps premier des $\mathbb{K}$ de caractéristique p.

Corollaire 34 : Les corps finis sont de cardinalité une puissance d'un nombre premier.

Théorème 35 : Existence et unicité des corps finis.

Exemple 36 : Construction explicite de $\mathbb{F}_4 = \mathbb{Z}/2\mathbb{Z}[X]/(X^2 + X + 1)$.

D/ Étude des carrés de $\mathbb{Z}/p\mathbb{Z}$. [ROM]

Proposition 37 : Nombres de carrés dans $\mathbb{F}_p$.

Proposition 38 : Caractérisation des carrés.

Application 39 : Algorithme pour trouver des carrés dans $\mathbb{F}_p$.

Corollaire 40 : -1 est un carré mod $p \Leftrightarrow p \equiv 1[4]$.

Développement 1

Application 41 : Théorème des deux carrés.

Définition 42 : Symbole de Legendre.

Théorème 43 : C'est un morphisme.

Lemme 44 : Réduction des formes quadratiques sur $\mathbb{F}_p$.

Développement 2

Théorème 45 : Loi de réciprocité quadratique.

Proposition 46 : $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

Application 47 : On peut calculer tous les symboles de Legendre, exemple de calcul d'un d'entre eux.

Références :

- [PER] Perrin p. 72
- [ROM] Rombaldi Algèbre 2nd éd. p. 279-294 et p. 426
- [G] Gourdon Algèbre p. 34-37