

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

[Ber] : *Algèbre, le grand combat*, Grégory Berhuy

[Dem] : *Cours d'algèbre*, Michel Demazure

[Goz] : *Théorie de galois*, Ivan Gozard

[Per] : *Cours d'algèbre*, Daniel Perrin

[Rom] : *Mathématiques pour l'agrégation*, Jean-Étienne Rombaldi

[Sau-Ran] : *Cours de calcul formel. Corps finis, systèmes polynomiaux, applications*,

Phillipe Saux Picart, Eric Rannou

[Ulm] : *Théorie des groupes*, Félix Ulmer

I Partie A - Premiers pas

I.1 Construction [Ber] [Rom] [Per]

■ **Prop 1 (Idéaux de $\mathbb{Z}$) :**

■ **Déf 2 ($\mathbb{Z}/n\mathbb{Z}$) :**

■ **Ex 3 :** Par division euclidienne, $\mathbb{Z}/n\mathbb{Z} = \{0, \dots, n-1\}$.

■ **Thm 4 (Cyclicité) :**

Rem 5 : Sous-groupes

■ **Thm 6 (Classification des groupes cycliques) :**

I.2 Inversibles et indicatrice d'Euler [Rom]

■ **Thm 7 (Critère d'inversibilité) :**

■ **Ex 8 :**

■ **Déf 9 (Groupe multiplicatif) :**

■ **Prop 10 ($\mathbb{Z}/n\mathbb{Z}$ et corps) :**

■ **Déf 11 (Indicatrice d'Euler) :**

■ **Ex 12 :** $\varphi(n)$ pour n premier, pour n petit.

■ **Ex 13 ($\varphi(p^\alpha)$) :**

App 14 (Euler / Fermat) :

■ **Prop 15 (Somme Gauss) :**

■ **Thm 16 (Automorphismes de $\mathbb{Z}/n\mathbb{Z}$) :**

II Partie B - Groupe multiplicatif

■ **Ex 17 :** Exemples et contre-exemples de divers comportements.

II.1 Étude de $(\mathbb{Z}/p\mathbb{Z})^\times$ [Rom] [Per]

■ **Thm 18 (Cyclicité pour p premier) :**

■ **Dév 19 (Cyclicité pour p^α) :**

II.2 Théorème Chinois [Rom] [Gou]

■ **Thm 20 (Théorème Chinois) :**

■ **Prop 21 (Multiplicativité de l'indicatrice d'Euler) :**

■ **Thm 22 (Indicatrice d'Euler) :**

■ **Ex 23 :** Exemple pour des “grands” nombres.

■ **Dév 24 (Structure de $(\mathbb{Z}/n\mathbb{Z})^\times$) :**

App 25 (RSA) :

III Partie C- Cas de n premier [Goz]

III.1 Corps finis

■ **Prop 26 (Caractéristique d'un corps fini) :**

■ **Prop 27 (Sous-corps premiers) :**

■ **Thm 28 (Existence des corps finis) :**

■ **Prop 29 (Structure de $\mathbb{F}_q$) :**

Rem 30 : Construction des corps fini comme corps de rupture.

■ **Ex 31 :** $\mathbb{F}_4$, $\mathbb{F}_8$ et $\mathbb{F}_9$ [Annexe : Table de $\mathbb{F}_4$].

III.2 Carrés dans $\mathbb{F}_p$

■ **Déf 32 (Symbole de Legendre, résidu quadratique) :**

■ **Ex 33 :** Résidus quadratiques dans $\mathbb{F}_5$.

■ **Prop 34 :** On a $\left(\frac{x}{p}\right) = x^{(p-1)/2}$ dans $\mathbb{F}_p$.

■ **App 35 (Réciprocité quadratique) :**

IV Partie D - Applications dans deux domaines de l'arithmétique

IV.1 Test de primalité [Rom] [Dem] [Sau-Ran]

■ **Déf 36 (Nombre de Mersenne) :**

■ **Dév 37 (Critère de primalité 1) :**

■ **Dév 38 (Lucas-Lehmer) :**

■ **Rem 39 :** Test lié au petit théorème de Fermat.

■ **Déf 40 (Nombres de Carmichael) :**

■ **Ex 41 :** Voir [Rom]

■ **Thm 42 (Korselt) :**

■ **Rem 43 :** Test de Miller-Rabin

IV.2 Équations diophantiennes [Rom] [Ulm]

■ **Thm 44 (Équation diophantienne linéaire) :**

■ **Thm 45 (Système d'équations diophantiennes linéaires) :**

■ **Ex 46 :**

■ **Prop 47 (Algo de résolution) :**

■ **Ex 48 :** Voir [Ulm].

■ **Ex 49 :** Mettre des exemples de (non) résolution en réduisant modulo p .