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

➤ Références	[Perrin], [H2G2.1], [Gozard], [UlmG], [UlmA], [Obj_pas_chômage], [Saux-picard], [Berhuy], [ROM_AG]
📁 Section	Algèbre
📅 Date	@11 février 2025
☰ Statut leçon	Plan détaillé ok
☰ Enseignant	Lionel Fourquaux
➤ Développements choisis	Chevalley Warning et EGZ, Dirichlet faible et app $\mathbb{Z}/n\mathbb{Z}$
🔍 Nb choisis	2
➤ Développements	Chevalley Warning et EGZ

Rapport de Jury

Introduction

- permet de répondre à la négative à des équations arithmétiques, équations diophantiennes
- (théo groupe abéliens)

Plans

▼ Plan

- I. Construction et éléments remarquables
 1. Construction
 2. Éléments remarquables
 3. Idéaux
 4. Utilisation du passage au quotient
- II. Indicatrice d'Euler et théo chinois
 1. Indicatrice d'Euler
 2. Théorème chinois
- III. Le corps $\mathbb{Z}/p\mathbb{Z}$ pour p premier
 1. Corps finis
 2. Carrés dans $\mathbb{Z}/p\mathbb{Z}$

▼ Plan détaillé

- ▼ I.1. Construction de $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$
 - Comment ?
 - def et prop anneau
 - prop : idéaux de $(\mathbb{Z}, +, \cdot)$
 - def de $\mathbb{Z}/n\mathbb{Z}$ comme anneau quotient. Il est commutatif unitaire
- ▼ I. 2. Éléments remarquables
 - ° Inversibles
 - prop : générateurs $(\mathbb{Z}/n\mathbb{Z}, +) =$ éléments premier avec $n =$ inversible de $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$
 - ° Diviseurs de zéros
 - prop diviseurs de zéros (Berhuy)
 - ° Lien:
 - $\mathbb{Z}/n\mathbb{Z}$ corps ssi intègre ssi n premier
 - c-ex
 - Dirichlet faible DEV 1.1
 - ° Nilpotents et idempotents
 - def : indicatrice d'Euler + ex petits nombres
 - prop : $\phi_n =$ cardinal des générateurs de $\mathbb{Z}/n\mathbb{Z}$
 - prop : Automorphismes de $\mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z}$ (pk ici?)
 - prop : Relation avec ϕ : $n = \sum \phi(d)$
 - thrm : si k corps alors tt sg fini de k^* est cyclique (k^*, x) est un groupe + $\mathbb{F}_p^*$ iso à $\mathbb{Z}/(p-1)\mathbb{Z}$
- ▼ I.3. Idéaux
 - prop : idéaux de $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$, ce sont des idéaux principaux mais **attention** $\mathbb{Z}/n\mathbb{Z}$ pas forcément principal car pas intègre !!

▼ I.4. Utilisation du passage au quotient

- ex 2 carrés
- ex 3 carrés
- critère de divisibilité par 3 et 9
- réduction modulo p ? Eisenstein ?

▼ II.1. Indicatrice d'Euler

- def
- lien avec prop
- corol : $\text{Card}(\mathbb{Z}/n\mathbb{Z}^*) = \phi(n)$
- Euler: si $a \in \mathbb{Z}$, $\text{pgcd}(a,n)=1$ ssi $a^{\phi(n)} \equiv 1 \pmod{n}$
- Fermat : Soit p 1er et $a \in \mathbb{Z}$ $a^p \equiv a \pmod{p}$
- $n = \text{somme}(\phi(d))$ + sgrp multiplicatif est cyclique

▼ II. 2. Théorème chinois

- prop : morphismes d'anneaux de $\mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z}$
- th chinois + rq?
- Corollaire: tout groupe abélien est un quotient d'un groupe $\mathbb{Z}/n\mathbb{Z}^*$ DEV1.2.
- résolution des systèmes de congruences + les deux algo de résolution

°Retour à l'indicatrice d'Euler

- prop : indicatrice d'Euler est un morphisme d'anneaux
- calcul $\phi(n)$ n quelconque
- app origine RSA (Gourdon)

▼ III. 1 Corps finis

- prop : $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ est un corps ssi n est 1er
- prop : Wilson n est 1er ssi $(n-1)! \equiv -1 \pmod{n}$
- thm : Soit k un corps fini de Kq p 1er. Alors il peut être vu comme un F_p -e.v de dimension n / def corps finis
- Chevalley warning + EGZ DEV2

▼ III.2. Carrés dans F_p

- Def carré, plus F_{p^2}
- prop : Carré de $F_{p^2} = F_p + \text{cardinal de } F_p^2 \text{ et } F_p^{*2}$
- app: Perrin: $ax^2 + by^2 = 1$ a des solutions
- prop : x est un carré dans $F_{p \setminus \{0\}}$ ssi $x^{(p-1)/2} = 1$ dans F_p
- Def symbole de Legendre + ppté
- Lemme réciprocité quadratique
- thm : loi de réciprocité quadratique + exemple (17/23) + app l'équation $x^2 + 23y^2 = 17$ n'a pas de solutions dans $\mathbb{Z}$

Garder en tête: thm de structure des groupes abéliens