Algèbre 09 – Congruences dans $\mathbb{Z}$, anneau $\mathbb{Z}/n\mathbb{Z}$. Applications.

1. Congruences et classes modulo un entier

Définitions des congruences et classes.

Théorèmes classiques (Fermat-Euler, Wilson,...)

Application aux équations diophantiennes.
⟶ Théorème de Fermat pour $n = 2$ et 4

2. Arithmétique dans $\mathbb{Z}/n\mathbb{Z}$

Théorème de Bézout et restes chinois.
⟶ Classification des groupes d'ordre pq

Application au codage RSA.

Indicatrice d'Euler et intégrité.

Inversibles et automorphismes.

Résidus quadratiques et loi de réciprocité.

3. Application aux nombres premiers

Tests de primalité.

Racines de l'unité et polynômes cyclotomique.

Application : progression arithmétique.
⟶ Forme faible du théorème de Dirichlet

4. Quelques autres applications

Polynômes irréductibles.

Application : le critère d'Eisenstein.

Application aux codes correcteurs : le minitel.

Anneaux d'entiers quadratiques et équation de Pell.
⟶ Unités des corps quadratiques

Développements

Théorème de Fermat pour $n = 2$ et 4.

Classification des groupes d'ordre pq.

Forme faible du théorème de Dirichlet.

Unités des corps quadratiques.

Références

[1] F. Combes, *Algèbre et géométrie*, Bréal, 1998.

[2] S. Francinou et H. Gianella, *Exercices d'algèbre 1*, Masson, 1993.

[3] S. Francinou, H. Gianella et S. Nicolas, *Oraux X-ENS, algèbre 1*, Cassini, 2001.

[4] X. Gourdon, *Algèbre*, Ellipses, 1994.

[5] D. Perrin, *Cours d'algèbre*, Ellipses, 1996.