Prérequis : Division euclidienne, divisibilité, relation de congruence.
Cadre : Soient n et m des entiers naturels non nuls.

I Structures

1) Structure de groupe

Rappel. *Les sous-groupes de $\mathbb{Z}$ sont les $n\mathbb{Z}$, ce sont aussi ses idéaux.*

Définition 1. $\mathbb{Z}/n\mathbb{Z}$ est le quotient de $\mathbb{Z}$ par le sous-groupe $n\mathbb{Z}$. $(\mathbb{Z}/n\mathbb{Z}, +)$ est muni d'une structure de groupe par : $\overline{x} + \overline{y} = \overline{x+y}$.

Proposition 2. *$(\mathbb{Z}/n\mathbb{Z}, +)$ est cyclique.*

Proposition 3. *Tout groupe monogène est isomorphe soit à $(\mathbb{Z}, +)$ soit à $(\mathbb{Z}/n\mathbb{Z}, +)$ pour un certain entier n, selon son cardinal.*

Exemple 4. *Groupe des racines n-ième de l'unité isomorphe à $\mathbb{Z}/n\mathbb{Z}$.*

Proposition 5.
— *Un sous-groupe d'un groupe cyclique est cyclique.*
— *Tout sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ est engendré par la classe d'un diviseur b de n, ce sous-groupe est d'ordre $a = \frac{n}{b}$.*
— *Réciproquement, si $a|n$ et $b = \frac{n}{a}$, il existe un unique sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ d'ordre a, engendré par la classe b modulo n.*

Exemple 6. *Les sous-groupes de $\mathbb{Z}/6\mathbb{Z}$ sont engendrés par les classes de 1, 2, 3, 6 : $\langle 1\rangle \cong \mathbb{Z}/6\mathbb{Z}$, $\langle 2\rangle \cong \mathbb{Z}/3\mathbb{Z}$, $\langle 3\rangle \cong \mathbb{Z}/2\mathbb{Z}$ et $\langle 6\rangle \cong \{0\}$.*

Définition 7. On appelle indicatrice d'Euler de $n \geqslant 1$ l'entier :

$$\varphi(n) = \text{Card}\left(\left\{k \in [\![1, n]\!] \;\middle|\; k \wedge n = 1\right\}\right)$$

Proposition 8. *Soit $k \in \mathbb{N}$. $\overline{k}$ est inversible $(\mathbb{Z}/n\mathbb{Z}, +)$ si, et seulement si, $k \wedge n = 1$. En particulier, $\varphi(n)$ est le nombre d'inversibles de $\mathbb{Z}/n\mathbb{Z}$.*

Proposition 9. *Les générateurs sont exactement les inversibles.*

Exemple 10. *$\varphi(6) = 2$ et les générateurs de $\mathbb{Z}/6\mathbb{Z}$ sont 1 et 5.*

Proposition 11.
— *Pour $d|n$, $\mathbb{Z}/n\mathbb{Z}$ admet $\varphi(d)$ éléments d'ordre d.*
— *(Formule de Möbius) $n = \sum_{d|n} \varphi(n)$*

Proposition 12. *Les automorphismes de groupe de $\mathbb{Z}/n\mathbb{Z}$ sont les applications $\psi_k : \overline{x} \mapsto k\overline{x}$ pour $1 \leqslant k \leqslant n$ avec $k \wedge n = 1$. On a ainsi $\text{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.*

Exemple 13. $\text{Aut}(\mathbb{Z}/6\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$ *(groupe à deux éléments)*

2) Structure d'anneau

Définition 14. $\mathbb{Z}/n\mathbb{Z}$ est le quotient de $\mathbb{Z}$ par l'idéal $n\mathbb{Z}$. $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ est muni d'une structure d'anneau par : $\overline{x} + \overline{y} = \overline{x+y}$ et $\overline{x} \cdot \overline{y} = \overline{xy}$.

Proposition 15. *Soit $n > 1$ et $a \in \mathbb{Z}$. Alors $\overline{a}$ engendre $\mathbb{Z}/n\mathbb{Z}$ si, et seulement si, $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$.*

Corollaire 16. *L'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps si, et seulement si, n est un nombre premier. On note alors $\mathbb{Z}/n\mathbb{Z} = \mathbb{F}_n$.*

Proposition 17 (Euler)**.** *Soient a et n deux entiers non nuls premiers entre eux. Alors $a^{\varphi(n)} \equiv 1[n]$.*

Corollaire 18 (Fermat)**.** *Soient p un nombre premier et $a \in \mathbb{N}^\star$ non divisible par p. Alors $a^{p-1} \equiv 1[p]$.*

Proposition 19 (Wilson)**.** *Soit $p \in \mathbb{N}^\star$, alors p est premier si, et seulement si, $(p-1)! \equiv -1[p]$.*

Théorème 20 (Bézout)**.** *Soient a et b deux entiers non nuls, alors a et b sont premiers entre eux si, et seulement si, il existe deux entiers u et v tels que $au + bv = 1$.*

Théorème 21 (Restes chinois)**.** *Soit $n = m_1 m_2$ avec $m_1 \wedge m_2 = 1$. Alors*

$$\varphi : \left|\begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \\ \overline{k}^n & \longmapsto & (\overline{k}^{m_1}, \overline{k}^{m_2}) \end{array}\right. \text{ est un isomorphisme d'anneaux.}$$

Généralisation 22. *Le théorème des restes chinois se généralise à tout produit d'entiers premiers entre eux deux à deux.*

Exemple 23. *Résolution de systèmes de congruences :*

$$\begin{cases} x \equiv 1[3] \\ x \equiv 2[4] \\ x \equiv 0[5] \end{cases} \Leftrightarrow x = 10 + 60k,\ k \in \mathbb{Z}$$

Corollaire 24. *Soient $m, n \in \mathbb{N}$ premiers entre eux. On a alors $(\mathbb{Z}/nm\mathbb{Z})^\times = (\mathbb{Z}/n\mathbb{Z})^\times \times (\mathbb{Z}/m\mathbb{Z})^\times$, et donc $\varphi(nm) = \varphi(n)\varphi(m)$.*

Corollaire 25. *Soit $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$. Alors :*

$$\text{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/(p_1^{\alpha_1})\mathbb{Z})^\times \times \dots \times (\mathbb{Z}/(p_k^{\alpha_k})\mathbb{Z})^\times$$

II Arithmétique dans $\mathbb{Z}$

1) Équations diophantiennes

Définition 26. Un équation diophantienne est une équation de la forme $P(x_1, \dots, x_n) = 0$, où P est un polynôme à n variables et à coefficients entiers, et dont on cherche les solutions parmi les entiers.

Exemple 27.
— *Triplets pythagoriciens :* $x^2 + y^2 = z^2$
— *Équation de Pell-Fermat :* $x^2 - ny^2 = 1$
— *Somme de carrés :* $n = x^2 + y^2$

Proposition 28. *Soit a, b et c des entiers. On note (E) l'équation $ax + by = c$. L'équation (E) admet des solution si, et seulement si, le* pgcd *de a et b divise c. Dans ce cas, il y a une infinité de solutions.*

Théorème 29 (Sophie Germain)**.** *Soit p un nombre premier impair tel que $2p + 1$ est premier. Si $x^p + y^p + y^p = 0$, alors $xyz \equiv 0[p]$.*

2) Carrés dans $\mathbb{Z}/p\mathbb{Z}$

Définition 30. Si $q = p^n$ avec p premier, on note $\mathbb{F}_q$ le corps à q éléments.

Définition 31. On pose $(\mathbb{F}_q)^2 = \left\{x^2 \in \mathbb{F}_q \;\middle|\; x \in \mathbb{F}_q\right\}$ l'ensemble des carrés de $\mathbb{F}_q$, et $\mathbb{F}_q^{\star 2} = \mathbb{F}_q^2 \cap \mathbb{F}_q^\star$.

Proposition 32. *Si $q = p^n$, on a :*
— *Si $p = 2$, $\mathbb{F}_q^2 = \mathbb{F}_q$*
— *Si $p > 2$, $|\mathbb{F}_q^2| = \frac{q+1}{2}$ et $|\mathbb{F}_q^{\star 2}| = \frac{q-1}{2}$*

Proposition 33. *Si $q = p^n$ et $p > 2$, on a $x \in \mathbb{F}_q^{\star 2} \Leftrightarrow x^{\frac{q-1}{2}} = 1$.*

Corollaire 34. *Si $q = p^n$ et $p > 2$, -1 est un carré dans $\mathbb{F}_q$ si, et seulement si, q est congru à 1 modulo 4.*

Corollaire 35. *Il y a une infinité de nombres premiers de la forme $4k+1$.*

Définition 36. Soit p un premier impair et $a \in \mathbb{N}$. On définit le symbole de Legendre de a par p par $\left(\frac{a}{p}\right) = \begin{cases} 1 & si\ \overline{a} \in \mathbb{F}_p^{\star 2} \\ -1 & si\ \overline{a} \notin \mathbb{F}_p^{\star 2} \\ 0 & si\ \overline{a} = 0 \end{cases}$.

Proposition 37. *Pour $x, y \in \mathbb{F}_p^\star$, on a $\left(\frac{xy}{p}\right) = \left(\frac{x}{p}\right)\left(\frac{y}{p}\right)$.*
Le symbole de Legendre donne un morphisme $\mathbb{F}_q^\star \to \{\pm 1\}$.

Proposition 38. *Soit p un premier impair et $a \in \mathbb{N}$, alors $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}}[p]$*

Théorème 39 (Réciprocité quadratique)**.** *Soient p et q deux premiers distincts impairs. Alors $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)(-1)^{\frac{q-1}{2}\frac{p-1}{2}}$.*

Proposition 40. $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

Exemple 41. $\left(\frac{29}{43}\right) = \left(\frac{43}{29}\right) = \left(\frac{14}{29}\right) = \left(\frac{2}{29}\right)\left(\frac{7}{29}\right) = -\left(\frac{29}{7}\right) = -\left(\frac{1}{7}\right) = -1$

Exemple 42. *L'équation $x^2 + 59y = 23$ n'a pas de solutions entiers.*

III Applications aux polynômes

1) Irréductibilité des polynômes de $\mathbb{Z}[X]$

Proposition 43. *Soient $P, Q \in \mathbb{F}_p[X]$. Alors :*

$$(P + Q)^p = P^p + Q^p \text{ et } (P(X))^p = P(X^p)$$

Définition 44. On définit le contenu de $P(X) = \sum_{k=0}^{n} a_k X^k \in \mathbb{Z}[X]$ par $c(P) = \text{pgcd}(a_0, \dots, a_n)$. Un polynôme P est dit primitif si $c(P) = 1$.

Proposition 45. *Soient $P, Q \in \mathbb{Z}[X]$, alors $c(PQ) = c(P)c(Q)$.*

Proposition 46. *Les polynômes irréductibles de $\mathbb{Z}[X]$ sont :*
— *Les polynômes constants, irréductibles dans $\mathbb{Z}$ (premiers).*
— *Les polynômes non constants, primitifs et irréductibles dans $\mathbb{Q}[X]$.*

Théorème 47 (Critère d'Eisenstein)**.** *Soit $P(X) = \sum_{k=0}^{n} a_k X^k \in \mathbb{Z}[X]$.*
Soit un nombre premier p tel que $p \nmid a_n$, $\forall i < n, p | a_i$ et $p^2 \nmid a_0$.
Alors P est irréductible dans $\mathbb{Z}[X]$.

2) Polynômes cyclotomiques

Définition 48. Soit $n \in \mathbb{N}^\star$, on définit $\Phi_n \in \mathbb{C}[X]$ le n-ième polynôme cyclotomique par $\Phi_n(X) = \prod_{\xi \in \mu_n^\star} (X - \xi)$, où $\mu_n^\star \subset \mathbb{C}$ désigne les racines primitives n-ième de l'unité.

Proposition 49. *Φ_n est unitaire de degré $\varphi(n)$.*

Proposition 50. $\forall n \in \mathbb{N}^\star, X^n - 1 = \prod_{d|n} \Phi_d(n)$

Exemple 51. $\Phi_1(X) = X - 1$, $\Phi_2(X) = X + 1$, $\Phi_p(X) = \sum_{k=0}^{p-1} X^k$

Proposition 52. *Pour $n \in \mathbb{N}^\star$, Φ_n est à coefficients entiers, et est irréductible dans $\mathbb{Z}[X]$.*

Lemme 53. *Soit $a \in \mathbb{Z}$ et p premier tel que $p|\Phi_n(a)$ et $p \nmid \Phi_d(a)$ pour $d|n$ et $d < n$. Alors $p \equiv 1[n]$.*

Théorème 54 (Dirichlet faible)**.** *Pour $n \geqslant 1$, il existe une infinité de nombres premiers congrus à 1 modulo n.*

Développements

- Théorème de Sophie Germain (29) [FGN]
- Réciprocité quadratique (39) [Ser]
- Forme faible de la progression arithmétique de Dirichlet (53,54) [FGN]

Références

[Gou] Xavier Gourdon. *Les Maths en Tête : Algèbre.* Ellipses, 2e edition
[Per] Daniel Perrin. *Cours d'Algèbre.* Ellipses
[FGN] Serge Francinou, Hervé Gianella, and Serge Nicolas. *Oraux X-ENS Algèbre 1.* Cassini
[Ser] Jean-Pierre Serre. *Cours d'Arithmétiques.* PUF