Prérequis : Divisibilité dans $\mathbb{Z}$, congruences, pgcd, ppcm.

I Arithmétique dans $\mathbb{Z}$

1) Définitions et premières propriétés

Définition 1. Un entier naturel est un nombre premier s'il est supérieur ou égal à 2 et si ses seuls diviseurs dans $\mathbb{N}$ sont 1 et lui-même. Un entier qui n'est pas premier est appelé composé. On notera $\mathbb{P}$ l'ensemble des nombres premiers.

Proposition 2. *Soit $n \geqslant 2$ un entier composé, alors il existe $p \in \mathbb{P}$ tel que p divise n et $p^2 \leqslant n$.*

Application 3 (Crible d'Erathostène)**.** *C'est un algorithme qui permet de déterminer dans $\mathbb{N}$ la suite des nombres premiers inférieurs à un nombre donné N. Il consiste à rayer dans la liste $A, \dots, N$ les multiples de 2, puis de 3, et ainsi de suite. Quand on rencontre un entier qui n'est pas encore rayé, il est premier. On supprime ses multiples de la liste et alors apparaît, non rayé, le nombre premier suivant.*

Exemple 4. *401 est premier, mais 403 est composé.*

Théorème 5 (Euclide)**.** *Il existe une infinité de nombres premiers.*

Théorème 6 (admis)**.** *Si on note $\pi(x)$ le nombre de nombres premiers inférieurs ou égaux à x, on a $\pi(x) \underset{x\to\infty}{\sim} \frac{x}{\ln x}$.*

Théorème 7 (Théorème fondamental de l'arithmétique)**.** *Soit n un entier strictement supérieur à 1. Alors ou bien n est premier, ou bien n se décompose de manière unique en un produit de facteurs premiers.*

Application 8. $780 \wedge 1001 = 13$, $780 \vee 1001 = 60060$, *780 a 24 diviseurs.*

2) L'anneau $\mathbb{Z}/n\mathbb{Z}$

Proposition 9. *$\mathbb{Z}/n\mathbb{Z}$ est un corps si, et seulement si, n est premier.*

Proposition 10. *$\mathbb{Z}/n\mathbb{Z}$ est intègre si, et seulement si, n est premier.*

Proposition 11. *Si $p \in \mathbb{P}$, alors $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique d'ordre $p-1$.*

Théorème 12 (Wilson)**.** *Un entier p supérieur ou égal à 2 est premier si, et seulement si, $(p-1)!$ est congru à -1 modulo p.*

Théorème 13 (Petit théorème de Fermat)**.** *Si p est un entier naturel premier, pour tout entier relatif n, on a alors $n^p \equiv n[p]$, et dans le cas où n est premier avec p, on a $n^{p-1} \equiv 1[p]$.*

Contre-exemple 14 (Nombres de Carmichael)**.** *La réciproque du petit théorème de Fermat est rendue fausse par les nombres de Carmichael, comme 561.*

Lemme 15. *Soit p un nombre premier, alors , pour tout entier k compris entre 1 et $p-1$, on a $\binom{p}{k} \equiv 0[p]$ et $\binom{p-1}{k} \equiv (-1)^k[p]$.*

Définition 16. Pour tout $n \in \mathbb{N}$, on note $\varphi(n)$ le nombre d'entiers premiers à n. Alors, $\varphi(n)$ est le cardinal de $(\mathbb{Z}/n\mathbb{Z})^\times$.

Théorème 17 (Euler-Fermat)**.** *Si n est un entier naturel non nul, pour tout entier relatif a, on a alors $a^{\varphi(n)} \equiv a[n]$.*

Théorème 18 (Restes chinois)**.** *Soient m et n deux entiers naturels premiers entre eux. Alors $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.*

Corollaire 19. *φ est multiplicative.*

II Applications de la réduction modulo p

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

Proposition 20. *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 21. 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 22. *Soient $P, Q \in \mathbb{Z}[X]$, alors $c(PQ) = c(P)c(Q)$.*

Proposition 23. *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 24 (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) Résolution d'équations diophantiennes

Définition 25. 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 26.
- *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 27. *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 28 (Sophie Germain)**.** *Soit p un nombre premier impair tel que $2p + 1$ est premier. Si $x^p + y^p + y^p = 0$, alors $xyz \equiv 0[p]$.*

III Les corps finis

1) Propriétés des corps finis

Définition 29. Soit $\mathbb{K}$ un corps, on appelle sous-corps premier de $\mathbb{K}$ l'intersection de tous ses sous-corps non nuls.

Exemple 30. *Le sous-corps premier de $\mathbb{R}$ et $\mathbb{C}$ est $\mathbb{Q}$.*

Définition 31. Soit A un anneau unitaire, il existe un unique morphisme d'anneaux $\varphi : \mathbb{Z} \to A$. Le générateur positif de $\operatorname{Ker}\varphi$ est appelé caractéristique de A, notée $\operatorname{car}(A)$.

Proposition 32. *Si $A = \mathbb{K}$ est un corps, sa caractéristique est nulle ou est un nombre premier.*

Corollaire 33. *Si $\operatorname{car}(K) = 0$, alors $\mathbb{K}$ est infini, mais la réciproque est fausse.*

Théorème 34. *Soit $\mathbb{L}$ une extension de corps de $\mathbb{K}$, alors $\mathbb{L}$ est un $\mathbb{K}$-espace vectoriel.*

Corollaire 35. *Soit $\mathbb{L}$ une extension de corps de $\mathbb{K}$ avec $\mathbb{K}$ et $\mathbb{L}$ finis, alors $\mathbb{L} \cong \mathbb{K}^n$.*

Théorème 36. *Si $\mathbb{K}$ est un corps fini de caractéristique p, alors le sous-corps premier de $\mathbb{K}$ est $\mathbb{Z}/p\mathbb{Z}$. Ainsi $\mathbb{K}$ a pour cardinal une puissance de p.*

Théorème 37. *À $\mathbb{F}_p$-isomorphisme près, il existe un unique corps de cardinal p^n, noté $\mathbb{F}_{p^n}$.*

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

Définition 38. Si $q = p^n$ avec p premier, on note $\mathbb{F}_q$ le corps à q éléments.

Définition 39. 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 40. *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 41. *Si $q = p^n$ et $p > 2$, on a $x \in \mathbb{F}_q^{\star 2} \Leftrightarrow x^{\frac{q-1}{2}} = 1$.*

Corollaire 42. *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 43. *Il y a une infinité de nombres premiers de la forme $4k+1$.*

Définition 44. 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 45. *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 46. *Soit p un premier impair et $a \in \mathbb{N}$, alors $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}}[p]$*

Théorème 47 (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 48. $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

Exemple 49. $\left(\frac{29}{43}\right) = \left(\frac{43}{29}\right) = \left(\frac{14}{29}\right) = \left(\frac{2}{29}\right)\left(\frac{7}{29}\right) = -\left(\frac{29}{7}\right) = -\left(\frac{1}{7}\right) = -1$

Exemple 50. *L'équation $x^2 + 59y = 23$ n'a pas de solutions entiers.*

3) Polynômes cyclotomiques

Définition 51. 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 52. *Φ_n est unitaire de degré $\varphi(n)$.*

Proposition 53. $\forall n \in \mathbb{N}^\star, X^n - 1 = \prod_{d|n} \Phi_d(n)$

Exemple 54. $\Phi_1(X) = X - 1$, $\Phi_2(X) = X + 1$, $\Phi_p(X) = \sum_{k=0}^{p-1} X^k$

Proposition 55. *Pour $n \in \mathbb{N}^\star$, Φ_n est à coefficients entiers, et est irréductible dans $\mathbb{Z}[X]$.*

Lemme 56. *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 57 (Dirichlet faible)**.** *Pour $n \geqslant 1$, il existe une infinité de nombres premiers congrus à 1 modulo n.*

Développements

- Théorème de Sophie Germain (28) [FGN]
- Réciprocité quadratique (47) [Ser]
- Forme faible de la progression arithmétique de Dirichlet (56,57) [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