121. Nombres premiers. Applications.

Introduction : Ce sont les briques de base de la théorie des nombres.

1 Généralités

1.1 Définitions et premières propriétés

Définition 1. Soit $p \in \mathbb{N}, p \geq 2$. On dit qu'il est premier si ses seuls diviseurs dans $\mathbb{N}$ sont 1 et p.

***Exemple* 2.** *Les nombres de Fermat* $2^{(2^\beta)}$ *sont premiers pour* $\beta \in [\![1, 4]\!]$.

***Exemple* 3.** *Soient* $a, n \in \mathbb{N}$. *Si le nombre de Mersenne* $a^n - 1$ *est premier, alors* $a = 2$ *et* n *est premier.*

Proposition 4. L'ensemble $\mathcal{P}$ des nombres premiers est infini.

Remarque 5. Si $p \in \mathcal{P}, \alpha \in \mathbb{N}^*$, on a $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$.

Théorème 6 (Fermat)**.** Si $a \in \mathbb{Z}, p \in \mathcal{P}$ et $a \wedge p = 1$, alors $a^p \equiv a[p]$.

***Contre-exemple* 7** (Carmichael)**.** *Pour tout* $a \in \mathbb{Z}$, *si* $a \wedge 561 = 1$, *alors* $a^{561} \equiv a[561]$.

1.2 Factorisation en nombres premiers

Théorème 8. Soit $n \in \mathbb{N}$. Il existe $p_1, \cdots, p_r \in \mathcal{P}$ et $\alpha_1, \cdots, \alpha_r \in \mathbb{N}^*$ tels que $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, et cette décomposition est unique à l'ordre près des facteurs.

***Application* 9.** $\{\ln(p), p$ *premier*$\}$ *forme une famille* $\mathbb{Q}$*-libre dans* $\mathbb{R}$, *et* $[\mathbb{R} : \mathbb{Q}] = \infty$.

***Application* 10.** *Si* $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, *alors* $\varphi(n) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)$.

1.3 Critères de primalité

Théorème 11 (Crible d'Ératosthène)**.** Soit $n \in \mathbb{N}^*$. Si n n'admet pas de diviseur inférieur à $\sqrt{n}$, alors n est premier.

Théorème 12. Soit $n \in \mathbb{N}^*$. n est premier, si et seulement si, $\mathbb{Z}/n\mathbb{Z}$ est un corps (et on le note alors $\mathbb{F}_n$).

Corollaire 13 (Wilson)**.** Soit $p \geq 2$. Alors $p \in \mathcal{P}$ ssi $(p-1)! \equiv -1[p]$.

Remarque 14. Le petit théorème de Fermat donne un test de non-primalité.

Proposition 15. Soit $n \geq 2$. S'il existe $a \in \mathbb{Z}$ tel que $a^{n-1} \equiv 1[n]$ et $\forall q \in \mathcal{P}, q|n-1 \Rightarrow a^q \not\equiv 1[n]$, alors n est premier.

1.4 Répartition des nombres premiers

Proposition 16. Il existe des intervalles de longueur arbitraire ne contenant pas de nombre premier.

Proposition 17 (Bertrand)**.** Pour tout $n \in \mathbb{N}$, il existe $p \in [\![n+1, 2n-1]\!]$ premier.

Définition 18. Pour $n \in \mathbb{N}^*$, on note $\pi(n) = \text{Card}(\mathcal{P} \cap [\![1, n]\!])$.

Théorème 19 (Hadamard, La Vallée Poussin)**.** On a $\pi(n) \underset{n \to +\infty}{\sim} \frac{n}{\ln(n)}$.

Théorème 20 (Dirichlet)**.** Soit $n \geq 2$. Il existe une infinité de nombres premiers congrus à 1 modulo n.

2 Corps finis

2.1 Généralités

Lemme 21. Soit K un corps. Sa caractéristique est soit nulle, soit un nombre premier.

Remarque 22. Soit $p \in \mathcal{P}$. Alors, pour tout $k < p, p$ divise $\binom{p}{k}$.

Proposition 23 (Frobenius)**.** Soit K corps de caractéristique $p \in \mathcal{P}$. Alors $\Phi : K \to K$ défini par $\Phi(x) = x^p$ est un morphisme de corps.

Proposition 24. Soit F corps fini de caractéristique p. Alors son sous-corps premier est isomorphe à $\mathbb{F}_p$. De plus, F possède une structure de $\mathbb{F}_p$-espace vectoriel de dimension finie, il existe donc $r \in \mathbb{N}^*$ tel que $|F| = p^r$.

Proposition 25. Réciproquement, si $p \in \mathcal{P}$ et $r \in \mathbb{N}^*$, il existe un unique corps de cardinal p^r à isomorphisme près.

***Exemple* 26.** $\mathbb{F}_4 \simeq \mathbb{F}_2[X]/(X^2 + X + 1)$.

Proposition 27. Si $\mathbb{F}_q$ est un corps fini, $\mathbb{F}_q^*$ est un groupe cyclique.

2.2 Résidus quadratiques

Soit $p \in \mathcal{P}$.

Définition 28. On définit pour $a \in \mathbb{F}_p^*$ le symbole de Legendre $\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{si } a \in \mathbb{F}_p^2 \\ -1 & \text{sinon} \end{cases}$.

Proposition 29. On a, pour tout $a \in \mathbb{F}_p^*$, $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}$.

Corollaire 30. -1 est un carré dans $\mathbb{F}_p$ ssi $p \equiv 1[4]$.

***Application* 31.** *Soit $\Sigma = \{n \in \mathbb{N}, \exists (a,b) \in \mathbb{N}^2, n = a^2 + b^2\}$. Soit $p \geq 3$ premier. Alors $p \in \Sigma \Leftrightarrow p \equiv 1 \mod 4$.*
Soit $n \geq 2$, de décomposition en facteurs premiers $n = \prod_{p \in \mathcal{P}} p^{v_p(n)}$. Alors $n \in \Sigma \Leftrightarrow$ $v_p(n)$ pair pour tout $p \equiv 3 \mod 4$.

Théorème 32. Soit $\mathbb{F}_q$ un corps fini de caractéristique différente de 2. Alors il y a $2n+1$ orbites pour l'action de congruence sur $S_n(\mathbb{F}_q)$, représentées par les matrices $A = \begin{pmatrix} I_r & \\ & 0_{n-r} \end{pmatrix}$ et $B = \begin{pmatrix} I_{r-1} & & \\ & \alpha & \\ & & 0_{n-r} \end{pmatrix}$, où α n'est pas un carré dans $\mathbb{F}_q$.

Théorème 33 (Frobenius-Zolotarev)**.** Soit $p \geq 3$ premier, soit $u \in GL_n(\mathbb{F}_p)$. Alors $\varepsilon(u) = \left(\frac{\det(u)}{p}\right)$.

Théorème 34 (Réciprocité quadratique)**.** Soient p, q premiers.
Alors $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

***Exemple* 35.** *65 est un carré dans $\mathbb{F}_{29}$.*

3 Applications

3.1 Polygones réguliers constructibles

Théorème 36 (Wantzel)**.** Soit $x \in \mathbb{R}$. x est constructible à la règle et au compas si et seulement si il existe une suite finie $L_0, \cdots, L_q$ de sous-corps de $\mathbb{R}$ tels que $L_0 = \mathbb{Q}, x \in L_q$ et $\forall k \leq q-1, [L_{k+1} : L_k] = 2$.

Théorème 37 (Gauss-Wantzel)**.** Soit p premier, soit $\alpha \in \mathbb{N}^*$. L'angle $\frac{2\pi}{p^\alpha}$ est constructible ssi $p = 2$ ou ($\alpha = 1$ et p est un nombre de Fermat, soit $p = 1 + 2^{(2^\beta)}$).

Corollaire 38. Si un polygone régulier est constructible, son nombre de côtés est de la forme $2^\alpha p_1 \cdots p_r$ où les p_i sont des nombres premiers de la forme ci-dessus.

***Exemple* 39.** *Les polygones réguliers à 5 et 17 côtés sont constructibles.*

3.2 En théorie des groupes

Proposition 40. Tout groupe d'ordre premier est cyclique.

Remarque 41. L'équation aux classes permet de prouver plusieurs résultats sur les groupes d'ordre premier.

***Application* 42** (Lemme de Cauchy)**.** *Si p est un nombre premier, un p-groupe possède un élément d'ordre p.*

***Application* 43.** *Si p est un nombre premier, un p-groupe a un centre non trivial.*

Définition 44. Soit p nombre premier, soit G un groupe d'ordre multiple de p. On appelle p-Sylow de G tout sous-groupe de G d'ordre égal à $\max\{k \in \mathbb{N}, p^k \mid |G|\}$.

Théorème 45 (Théorèmes de Sylow)**.** Soit G groupe d'ordre $p^k m$, p premier, $m \nmid p$.

(i). G possède un p-Sylow.

(ii). Tous les p-Sylow de G sont conjugués.

(iii). Si on note c_p le nombre de p-Sylow de G, on a $c_p \mid m$ et $c_p \equiv 1\ [p]$.

***Application* 46.** *Il n'existe pas de groupe simple à 30 ou 42 éléments.*

3.3 Cryptage RSA

Soient p, q deux nombres premiers distincts. Soit $n = pq$, soient c, d tels que $cd \equiv 1[\varphi(n)]$. Les applications $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ définies par $c : \overline{x} \mapsto \overline{x}^c$ et $d : \overline{x} \mapsto \overline{x}^d$ sont respectivement appelées fonction de chiffrement et de déchiffrement. On a $c \circ d = d \circ c = \mathrm{Id}_{\mathbb{Z}/n\mathbb{Z}}$. On peut ainsi transmettre des messages cryptés à l'aide de la clé publique (n, c) et de la clé privée d.

3.4 Irréductibilité de polynômes

Théorème 47. Soit $P \in \mathbb{Z}[X]$, soit p premier. On note $\overline{P}$ le polynôme obtenu en réduisant modulo p les coefficients de P. Alors, si $\overline{P}$ est irréductible dans $\mathbb{F}_p[X]$ et $\deg(\overline{P}) = \deg(P)$, alors P est irréductible dans $\mathbb{Q}[X]$.

***Exemple* 48.** *$P = 3X^2 + 17X - 11$ est irréductible dans $\mathbb{Q}[X]$.*

***Contre-exemple* 49.** *X^4+1 est irréductible dans $\mathbb{Z}[X]$ mais réductible dans $\mathbb{F}_p[X]$ pour tout $p \in \mathbb{N}^*$ premier.*

Développements

— Théorème des deux carrés.
— Loi de réciprocité quadratique.
— Théorème de Gauss-Wantzel.

Références

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

[2] X. Gourdon, Les maths en tête - Algèbre, Ellipses.

[3] X. Gourdon, Les maths en tête - Analyse, Ellipses.

[4] I. Gozard, Théorie de Galois, Ellipses.

[5] A. Paugam, Questions délicates en algèbre et géométrie, Dunod.