Algèbre 10 – Nombres premiers. Applications.

1. Généralités

1.1. Définition.

Définition. Un entier $p \geq 2$ est dit *premier* si ses seuls diviseurs dans $\mathbb{N}$ sont 1 et p.

L'ensemble $\mathcal{P}$ des nombres premiers est infini. On note aussi $(p_n)_{n\geq 1}$ la suite croissante des nombres premiers.

Proposition.

(*i*) *Soit* $p \in \mathcal{P}$ *et* $n \in \mathbb{Z}$ *avec* $p \not| n$ *alors* $p \wedge n = 1$

(*ii*) $\forall n \geq 2,\ \exists p \in \mathcal{P}/p|n$

(*iii*) $p \in \mathcal{P} \iff \mathbb{Z}/p\mathbb{Z}$ *corps*

Nombres de Fermat. $F_n = 2^{2^n} + 1$
F_n est premier pour $0 \leq n \leq 4$ mais pas pour $n = 5$.
Si $2^n + 1$ est premier alors il existe $k \geq 0$ tel que $n = 2^k$.

Nombres de Mersenne. $M_p = 2^p - 1$ où $p \in \mathcal{P}$
Si $a^n - 1$ est premier alors $a = 2$ et $n \in \mathcal{P}$.
En revanche $2^{11} - 1$ n'est pas premier.

1.2. Recherche de nombres premiers.

Petit théorème de Fermat. *Si* p *est premier et si* $a \in \mathbb{Z}$ *n'est pas divisible par* p *alors* $a^{p-1} \equiv 1 \pmod{p}$.

La réciproque est fausse : un nombre de Carmichael (par exemple 561) est un entier non premier n tel que pour tout entier a premier avec n on a $a^{n-1} \equiv 1 \pmod{n}$.

Théorème de Wilson. *p est premier si et seulement si on a* $(p-1)! \equiv -1 \bmod p$.

Crible d'Eratosthène. n n'est pas premier si et seulement s'il existe un premier p divisant n tel que $p \leq \sqrt{n}$

Proposition. *Soit* $n \geq 2$ *tel qu'il existe* $a \in \mathbb{Z}$ *avec* $a^{n-1} \equiv 1 \pmod{n}$ *et* $a^q \not\equiv 1 \pmod{n}$ *pour tout diviseur strict premier* q *de* $n-1$. *Alors* n *est premier.*

2. Factorisation en produit de nombres premiers

Théorème. *Tout entier* $n \geq 2$ *s'écrit de façon unique sous la forme* $n = \prod_{p\in\mathcal{P}} p^{v_p(n)}$ *où les* $v_p(n) \in \mathbb{N}$ *sont tous nuls sauf un nombre fini.*

Notons que $v_p(n) = \sup\{k; p^k | n\}$.

Application. $\sum_{p\in\mathcal{P}} \frac{1}{p}$ diverge

Application (théorème des 4 carrés)**.** Tout entier s'écrit comme somme de quatre carrés.

Application. Étude de l'équation de Fermat pour $n = 2$ et 4.

Fonctions multiplicatives. Une fonction $f : \mathbb{N}^* \to \mathbb{C}$ est dite *multiplicative* si pour tous entiers premiers entre eux $m, n \geq 1$, on a $f(mn) = f(m)f(n)$.

Définition. L'*indicatrice d'Euler* définie pour tout $n \geq 1$ par $\varphi(n) = \sharp\mathcal{U}(\mathbb{Z}/n\mathbb{Z})$.

Proposition. *Pour tout* $n \geq 1$, φ *est une fonction multiplicative telle que*

$$\varphi(n) = n \prod_{\substack{p\in\mathcal{P}\\ p|n}} \left(1 - \frac{1}{p}\right)$$

et on a de plus $n = \sum_{d|n} \varphi(d)$.

Application (Principe du codage RSA)**.** Soit p et q deux nombres premiers distincts et c, d deux entiers vérifiant $cd \equiv 1 \pmod{\varphi(pq)}$ alors pour tout $t \in \mathbb{Z}$, on a $t^{cd} \equiv t \pmod{pq}$.

Un autre exemple de fonction multiplicative est donné par la somme $\sigma(n)$ des diviseurs de n.

Application. On dit que $n \geq 1$ est *parfait* si $\sigma(n) = 2n$. Les nombres parfaits pairs sont les $2^{p-1}M_p$ avec M_p premier.

Définition. La *fonction de Möbius* est définie par $\mu(1) = 1$, $\mu(n) = 0$ si n a un facteur carré, et $\mu(q_1 \cdots q_r) = (-1)^r$ si les q_j sont des premiers distincts. Alors μ est multiplicative.

Application. La probabilité r_n que deux entiers de $\{1, \ldots, n\}$ soient premiers entre eux est

$$r_n = \frac{1}{n^2} \sum_{d=1}^{n} \mu(d) E\left(\frac{n}{d}\right)^2$$

et tend vers $\frac{6}{\pi^2}$ lorsque n tend vers l'infini.

3. Répartition de nombres premiers

Définition. Pour tout $x > 0$, on note $\pi(x)$ le nombre de premiers dans $[0, x]$.

Proposition. *Il existe des plages de nombres aussi grandes que l'on veut sans nombre premier.*

Postulat de Bertrand. *Pour tout entier* $n \geq 4$, *il existe un premier* p *vérifiant* $n < p < 2n - 2$.

Application. Si $\sqrt{n!}$ est entier alors $n = 0$ ou 1.

Théorème des nombres premiers. $\pi(x) \sim \dfrac{x}{\log x}$

Forme faible du théorème de Dirichlet. *Pour tout entier* $n \geq 1$, *il existe une infinité de premiers congrus à* 1 *modulo* n.

En fait, pour tous $m, n \geq 1$ premiers entre eux, il existe une infinité de premiers congrus à m modulo n.

Exemple. Il existe une infinité de premiers de la forme $4n + 1$.

4. Quelques applications algébriques

4.1. En théorie des corps.

Proposition. *La caractéristique d'un corps fini est un nombre premier* p *et son cardinal une puissance de* p.

Proposition. *Une extension de degré p d'un corps est simple.*

Un entier p est premier si et seulement si p divise $\binom{p}{k}$ pour tout $k \in \{1, \dots, p-1\}$.

Proposition. *Si K est un corps de caractéristique p alors l'application $K \to K, x \mapsto x^p$ est un homomorphisme (appelé l'homomorphisme de Frobenius de K).*

4.2. **Aux polynômes.**

Critère d'Eisenstein. Soit $P = a_n X^n + \cdots + a_0 \in \mathbb{Z}[X]$ et p un nombre premier. Si

(i) p ne divise pas a_n

(i) p divise $a_0, a_1, \dots, a_{n-1}$

(i) p^2 ne divise pas a_0

Alors P est irréductible dans $\mathbb{Q}[X]$.

Exemple. $\phi_{p,\mathbb{Q}}$ est irréductible.

4.3. **En théorie des groupes.**

Proposition. *Un groupe d'ordre p est cyclique.*

Proposition. *Un groupe d'ordre p^2 est abélien.*

Théorème de Cauchy. *Si un premier p divise l'ordre d'un groupe G alors G admet un élément d'ordre p.*

Application. Un entier $n \geq 1$ est de Carmichael si et seulement si $n = p_1 \cdots p_k$ où les p_i sont des premiers distincts tels que $p_i - 1 | n - 1$ pour tout i.

Théorèmes de Sylow. *Soit G un groupe d'ordre $p^k m$.*

(i) *G admet un p-sous-groupe de Sylow*

(ii) *Tout p-sous-groupe de G est inclus dans un p-sous-groupe de Sylow*

(iii) *Les p-sous-groupes de Sylow de G sont conjugués*

(iv) *Le nombre n_p de p-sous-groupes de Sylow de G divise m et est congru à 1 modulo p.*

Application. Classification des groupes d'ordre pq.

Développements

Probabilité pour que deux entiers soient premiers entre eux.

Forme faible du théorème de Dirichlet.

Classification des groupes d'ordre pq.

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, *Les maths en tête. Algèbre*, Ellipses, 1994.