110 – Nombres Premiers. Applications.

1 Généralités sur les nombres premiers

Définition 1.1 (Nombre premier) *Un entier $p \in \mathbb{N}^*$ est dit* premier *s'il possède exactement deux diviseurs dans $\mathbb{N}$, à savoir 1 et lui-même. Les nombres premiers sont donc les irréductibles de $\mathbb{Z}$ positifs. On note $\mathbb{P}$ l'ensemble des nombres premiers.*

Remarque. $\mathbb{P} \neq \emptyset$, car $2, 3, 5, 89, 113 \in \mathbb{P}$ par exemple. En fait, $\mathbb{P}$ est infini : un diviseur premier de $n! + 1$ est strictement supérieur à n.

Proposition 1.2 *Un nombre n est premier ssi $\mathbb{Z}/n\mathbb{Z}$ est intègre, auquel cas c'est un corps.*

Remarque. Soit A un anneau. Par extension, un idéal I de A est dit *premier* si le quotient A/I est intègre.

Théorème 1.3 (Théorème fondamental de l'arithmétique) *Tout entier non nul n peut s'écrire de manière unique sous la forme $n = \prod_{p\in\mathbb{P}} p^{v_p(n)}$ où $v_p(n)$ est nulle pour presque tout p. Autrement dit l'anneau $\mathbb{Z}$ est factoriel.*

Applications. Si on connaît la décomposition de m et de n : $m = \prod p_i^{\alpha_i}$ et $n = \prod p_i^{\beta_i}$, alors on a $m \wedge n = \prod p_i^{\min(\alpha_i,\beta_i)}$ et $m \vee n = \prod p_i^{\max(\alpha_i,\beta_i)}$.
Soit G un groupe de type fini commutatif et $m, n \in G$ qui commutent d'ordres resp. a et b. Alors il existe dans G un élément d'ordre $a \vee b$. Ainsi le maximum des ordres des éléments d'un groupe est aussi le ppcm de ces ordres ; c'est l'*exposant* du groupe.

Exemples. Les nombres de Fermat $F_n = 2^{2^n} + 1$ sont premiers pour n dans $\{0, 1, 2, 3, 4\}$, mais F_5 est divisible par 641. Les nombres $a^n - 1$ ne peuvent être premiers que si $a = 2$ et $n \in \mathbb{P}$. On les appelle nombres de Mersenne ; ils ne sont pas tous premiers ($2^{11} - 1$ est divisible par 23).

2 Répartition des nombres premiers

Définition 2.1 *Pour tout $x \in \mathbb{R}_+$, on note $\pi(x)$ le cardinal de $\mathbb{P} \cap [0, x]$.*

Théorème 2.2 (Tchebychev) *On a pour tout x : $A\frac{x}{\ln(x)} \leq \pi(x) \leq B\frac{x}{\ln(x)}$.*

Corollaire 2.3 (Postulat de Bertrand) *Il existe au moins un nombre premier entre un entier et son double.*

Définition 2.4 *La fonction ζ !*

Proposition 2.5 *Représentation en produit infini.*

Théorème 2.6 *Prolongement sur $\mathbb{C}$.*

Proposition 2.7 *La série* $\sum_{p\in\mathbb{P}} \frac{1}{p}$ *diverge.*

Théorème 2.8 (Théorème des nombres premiers) *On a* $\pi(x) \sim \frac{x}{\ln(x)}$*, quand* $x \to \infty$*.*

Applications. Densité des fractions de $\mathbb{Q}$ dont le numérateur et le dénominateur sont premiers ; tout nombre supérieur à 7 est somme de nombres premiers distincts ? ? ? ? ? ? ? ? ? ? ? ?,

Corollaire 2.9 *Si* p_n *désigne le* n*-ième nombre premier, on a* $p_n \sim n\ln(n)$ *quand* $n \to \infty$*.*

Théorème 2.10 (Théorème de la progression arithmétique de Dirichlet) *Soient* a *et* b *deux entiers premiers entre eux. Il existe une infinité de nombres premiers* p *tels que* $p \equiv a \mod b$*.*

Remarque. Ce théorème peut se démontrer de manière purement algébrique dans certains cas particuliers, comme $(a,b) = (\pm 1, 4)$, $(a,b) = (-1,3)$, $(a,b) = (-1,5)$, $(a,b) = (-1,8)$ ou $a = 1$.

Application. Irréductibilité des polynômes cyclotomiques sur $\mathbb{Z}/p\mathbb{Z}$; soit $a \in \mathbb{Z}$. Si $X^2 - a = 0$ a une solution modulo p pour presque tout p, elle a une solution dans $\mathbb{Z}$. ? Revoir...

3 Applications algébriques

3.1 Théorie des groupes

Théorème 3.1 (Théorèmes de Sylow) *Soit* G *un groupe de cardinal* $n = p^a m$*, où* m *est premier à* p*. Il existe alors des sous-groupes de* G *de cardinal* p^a*, appelés* p*-groupes de Sylow. De plus :*

(i) Tout sous-groupe de G *de cardinal une puissance de* p *est inclus dans un* p*-Sylow.*

(ii) Tous les p*-Sylow sont conjugués.*

(iii) Leur nombre divise n*.*

(iv) Leur nombre est congru à 1 modulo p *(donc leur nombre divise* m*).*

Applications. Classification des groupes d'ordre pq, simplicité de ceux d'ordre pq^2, tout groupe d'ordre 255 n'est pas simple.

p-groupes : centre, sous-groupes distingués.

Décomposition des groupes abéliens finis.

3.2 Théorie des corps, carrés et cryptographie

Proposition 3.2 *La caractéristique d'un corps est* 0 *ou un nombre premier.*

Applications. Morphisme de Frobenius.

Proposition 3.3 *Pour tout entier q puissance d'un nombre premier p, il existe un unique corps de cardinal q, à isomorphisme près. Dans une clôture algébrique de $\mathbb{Z}/p\mathbb{Z}$, il existe un unique corps de cardinal q.*

Remarque. Les corps finis sont exactement les corps de la proposition ci-dessus.

Proposition 3.4 *Le groupe multiplicatif d'un corps fini est cyclique.*

Proposition 3.5 (Critère d'Eisenstein) *Soit $P = a_nX^n + \cdots + a_0 \in Z[X]$ et $p \in \mathbb{P}$. On suppose que $p \nmid a_n$, $p|a_i \forall i < n$ et que $p^2 \nmid a_0$. Alors P est irréductible sur $\mathbb{Q}[X]$, donc sur $\mathbb{Z}[X]$ s'il est primitif.*

Proposition 3.6 (Réduction) *Soit $p \in \mathbb{P}$ et $P = a_nX^n + \cdots + a_0 \in Z[X]$. On suppose que $p \nmid a_n$; si la réduction de P modulo p est irréductible sur $\mathbb{F}_p$, alors il est irréductible sur $\mathbb{Q}$.*

Définition 3.7 *Soit p un nombre premier impair. Le* symble de Legendre *de n modulo p, noté $\left(\frac{n}{p}\right)$, est défini par :*

$$\left(\frac{n}{p}\right) = \begin{cases} 0 \text{ si } a \equiv 0 \ [p] \\ 1 \text{ si } a \text{ est un carré non nul modulo } p \\ -1 \text{ si } a \text{ n'est pas un carré modulo } p \end{cases}$$

Proposition 3.8 *Le nombre de carrés dans $\mathbb{F}_p$ est $(p+1)/2$.*

Proposition 3.9 $\forall a \in \mathbb{Z}, \ \left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \ [p]$

Définition 3.10 *Soit N un entier impair, $N = \prod_i p_i^{\alpha_i}$, et a un entier. Le* symbole de Jacobi *est donné par :*

$$\left(\frac{a}{N}\right) = \prod_i \left(\frac{a}{p_i}\right)^{\alpha_i}$$

Remarque. Le symbole de Jacobi sert surtout comme un intermédiaire de calcul au symbole de Legendre.

Proposition 3.11 *(i) si $a \equiv b \ [N]$, alors $\left(\frac{a}{N}\right) = \left(\frac{b}{N}\right)$, et $\left(\frac{a}{N}\right) = 0$ ssi $a \wedge N > 1$*

(ii) $\forall a, b \in \mathbb{Z}, \ \left(\frac{ab}{N}\right) = \left(\frac{a}{N}\right)\left(\frac{b}{N}\right)$

(iii) $\left(\frac{-1}{N}\right) = (-1)^{(p-1)/2}$ *et* $\left(\frac{2}{N}\right) = (-1)^{(p^2-1)/8}$

Application(Dirichlet faible) Cf Perrin !

Théorème 3.12 (Loi de réciprocité quadratique) *Soient N, M des nombres impairs distincts. Alors on a :*

$$\left(\frac{N}{M}\right)\left(\frac{M}{N}\right) = (-1)^{\frac{N-1}{2}\frac{M-1}{2}}$$

Ce théorème associé aux propositions précédentes fournit un algorithme rapide de calcul du symbole de Legendre : on est ramené à un algorithme d'Euclide.

Exemple.(Hindry p.10) Soit p un nombre premier s'écrivant $p = x^2 - 6y^2$, avec $x, y \in \mathbb{Z}$. Alops p ne divise pas y, car sinon p diviserait aussi x et donc p^2 diviserait p. Donc $6 \equiv (xy^{-1})^2$ $[p]$, donc $\left(\frac{6}{p}\right) = 1$ i.e. $(-1)^{(p^2-1)/8}(-1)^{(p-1)/2}\left(\frac{p}{3}\right) = 1$, on en déduit des congruences de p modulo 24.

Théorème 3.13 (Frobenius-Zolotarev) *Soit p un nombre premier impair et V un $\mathbb{F}_p$-e.v. de dimension finie. Alors pour tout $u \in Gl(V)$, on peut considérer u comme un élément de $\mathfrak{S}(V)$, si bien qu'on peut lui associer sa signature. On a alors $\varepsilon(u) = \left(\frac{det(u)}{p}\right)$.*

Théorème 3.14 (Deux carrés) *Un entier $n \geq 2$, dont la décomposition en facteurs premiers s'écrit $\prod_{p\in\mathcal{P}} p^{v_p(n)}$, est la somme de deux carrés entiers ssi pour tout $p \equiv 3$ $[4]$, $v_p(n)$ est pair.*

Algorithme RSA. On se donne deux grands nombres premiers p et q tels que $n = pq$, et un entier d inversible modulo $\varphi(n)$, appelé *clef publique*. Le chiffrement d'un message $a \in \mathbb{Z}/n\mathbb{Z}$ est donné par la fonction $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $a \mapsto a^d$, et le déchiffrement par l'inverse de $f : g : a \mapsto a^e$, avec e un inverse de d dans $\mathbb{Z}/\varphi(n)\mathbb{Z}$, appelé *clef privée*. La robustesse de cet algorithme réside dans le fait que le calcul de g, i.e. celui de e, nécessite la connaissance de $\varphi(n)$, et donc de p et de q. Or la factorisation de nombres tels que n est en pratique extrèmement longue : le calcul de l'inverse est impossible en temps raisonnable. Reste à savoir comment fabriquer de tels grands nombres premiers p et q.

Théorème 3.15 (Wilson !)

Proposition 3.16 (Théorème de Fermat-Euler) *Si a est un entier premier à n, alors $a^{\varphi(n)} \equiv 1 \mod n$.*

Lemme 3.17 *Soit $H = \{a \in (\mathbb{Z}/n\mathbb{Z})^* / a^{(n-1)/2} \equiv \left(\frac{a}{n}\right)$ $[n]\}$. Alors n est premier ssi $H = (\mathbb{Z}/n\mathbb{Z})^*$.*

Le test de Solovay-Stassen consiste alors à tester l'égalité du lemme pour des nombres aléatoires. Si n passe successivement k tests, on peut dire qu'il est premier avec une probabilité supérieure à $1 - 2^{-k}$.