110 – Nombres Premiers. Applications.

1 Généralités sur les nombres premiers

Définition 1.1 (Nombre premier) *Un entier $p \in \mathbb{N}^*$ est premier si $\mathbb{Z}/p\mathbb{Z}$ est intègre. L'ensemble des nombres premiers peut se noter $\mathbb{P}$.*

Théorème 1.2 (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.*

Remarque. $\mathbb{P} \neq \emptyset$, car $2, 3, 5 \in \mathbb{P}$ par exemple. En fait, $\mathbb{P}$ est infini : un diviseur premier de $2^p - 1$, pour p premier, est strictement supérieur à p.

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).

Applications. Équations diophantiennes (équation de Fermat pour $n = 2$ ou $n = 4$) ; irréductibilité des polynômes modulo p.

2 Répartition des nombres premiers

Définition 2.1 (Fonction dzêta de Riemann) *Soit $s \in \mathbb{C}$, $\Re(s) > 1$. On note $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$ la fonction dzêta de Riemann.*

Remarque. Cette fonction synthétise le théorème fondamental de l'arithmétique : $\zeta(s) = \prod_{p\in\mathbb{P}} \left(1 - \frac{1}{p^s}\right)^{-1}$ pour $\Re(s) > 1$.

Proposition 2.2 *La fonction ζ s'écrit comme somme de $\frac{1}{s-1}$ et d'une fonction holomorphe sur $\Re(s) > 0$. Elle se prolonge donc en une fonction méromorphe sur $\Re(s) > 0$ avec un pôle simple en $s = 1$.*

Corollaire 2.3 *La série $\sum_{p\in\mathbb{P}} \frac{1}{p}$ diverge. On a également $\sum_{p\in\mathbb{P}} \frac{1}{p^s} \sim -\ln(s-1)$ quand $s \to 1^+$.*

Définition 2.4 *Pour tout $x \in \mathbb{R}_+$, on note $\pi(x)$ le cardinal de $\mathbb{P} \cap [0, x]$.*

Théorème 2.5 (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 ; pour $t \neq 0$, on a $\zeta(1 + it) \neq 0$.

Corollaire 2.6 *Si p_n désigne le n-ième nombre premier, on a $p_n \sim n\ln(n)$ quand $n \to \infty$.*

Remarque. On peut établir une version plus faible, pour x assez grand, grâce à de l'analyse réelle : $A\frac{x}{\ln(x)} \leq \pi(x) \leq B\frac{x}{\ln(x)}$, où $2A - B > 0$.

Corollaire 2.7 (Postulat de Bertrand) *Il existe au moins un nombre premier entre un entier et son double.*

Théorème 2.8 (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 $\mathbb{Z}$.

3 Applications algébriques

3.1 Théorie des groupes, éléments de cryptographie

Définition 3.1 (Symbole de Legendre) *Pour $a \in \mathbb{Z}$ et p impair, on définit le symbole de Legendre, noté $\left(\frac{a}{p}\right)$, comme étant 0 si p divise a, et 1 ou -1 selon que a soit un carré ou non mod p (respectivement).*

Définition 3.2 (Sommes de Gauss) *Si $\chi : \mathbb{F}_p^* \to \mathbb{C}^*$ est un morphisme, prolongé par convention à $\mathbb{F}_p$ en posant $\chi(0) = 0$ si $\chi \not\equiv 1$, $\chi(0) = 1$ sinon, alors la somme $G(\chi, a) = \sum_{x\in\mathbb{F}_p} \chi(x) \exp\left(\frac{2i\pi ax}{p}\right)$ est appelée somme de Gauss.*

Applications. Loi de réciprocité quadratique : on a $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{(p-1)(q-1)/2}$ pour p et q premiers impairs ; théorème de Chevalley-Warning ; formes quadratiques sur $\mathbb{F}_p$.

Proposition 3.3 (Lemme des restes chinois) *Deux entiers m et n sont premiers entre eux si, et seulement si, $\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.*

Applications. Classification des groupes abéliens finis ; automorphismes de $\mathbb{Z}/n\mathbb{Z}$; résolution de systèmes de congruence ; calcul de l'indicatrice d'Euler $\varphi(n) = \text{card}((\mathbb{Z}/n\mathbb{Z})^*)$.

Théorème 3.4 (Théorème de Fermat-Euler) *Si a est un entier premier à n, alors $a^{\varphi(n)} \equiv 1 \mod n$.*

Applications. Cryptographie (codage RSA) ; tests de primalité.

Théorème 3.5 (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 ; écriture d'un groupe abélien comme produit de ses p-Sylow ; sous-groupes d'un p-groupe.

3.2 Théorie des corps

Proposition 3.6 *La caractéristique d'un corps est 0 ou un nombre premier.*

Applications. Invariant dans une classe d'isomorphisme ; morphisme de Frobenius.

Proposition 3.7 *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.

Théorème 3.8 (Théorème de Gauss-Wantzel) *Un polygone régulier à n côtés est constructible si, et seulement si $n = 2^k F_{i_1} \cdots F_{i_r}$ où $r \geq 0$, $k \geq 0$ et les F_i sont les nombres premiers de Fermat.*

4 Les corps p-adiques

Proposition 4.1 (Théorème d'Ostrowski) *Les seules valeurs absolues sur $\mathbb{Q}$ sont, à équivalence près, la valeur absolue archimédienne et ses valeurs absolues p-adiques. On note V l'ensemble de ces classes d'équivalence de valeurs absolues (qu'on appelle* places*) sur $\mathbb{Q}$.*

Corollaire 4.2 *Pour tout p premier, il existe un corps ultramétrique complet $\mathbb{Q}_p$, dont la valeur absolue prolonge la valeur absolue p-adique de $\mathbb{Q}$, et dans lequel $\mathbb{Q}$ est dense.*

Remarque. Un élément a de $\mathbb{Q}_p$ peut s'écrire $a = \sum_{n=-m}^{\infty} a_n p^n$, où $m \geq 0$ (la convergence est au sens de la valeur absolue p-adique). On note $v_p(a)$ le plus petit entier relatif n tel que $a_n \neq 0$ (et $v_p(0) = \infty$). Alors, $\mathbb{Z}_p = \{a \in \mathbb{Q}_p | v_p(a) \geq 0\}$ l'anneau des entiers p-adiques, et $\mathbb{Q}_p = \mathbb{Z}_p\left[\frac{1}{p}\right]$.

Remarque. Un élément a de $\mathbb{Q}$ appartient $\mathbb{Z}_p$ pour presque tout $p \in \mathbb{P}$.

Proposition 4.3 *L'anneau $\mathbb{Z}_p$ est compact, et $\mathbb{N}$ est dense dans $\mathbb{Z}_p$. L'espace $\mathbb{Q}_p$ est localement compact et totalement discontinu ; $\mathbb{Z}_p$ en est un sous-anneau ouvert.*

Proposition 4.4 *Soit $S \subseteq V$ un sous-ensemble fini de places. L'image de $\mathbb{Q}$ dans $\prod_{v \in S} \mathbb{Q}_v$ par l'application $x \mapsto (x)_{v \in S}$ est dense ($\mathbb{Q}_\infty = \mathbb{R}$).*

Remarque. Grâce à cette proposition, on peut montrer que malgré ces points communs entre les $\mathbb{Q}_p$, ils ne sont pas homéomorphes.

Proposition 4.5 *Si $p \neq 2$, un élément $x = p^n u \in \mathbb{Q}_p^*$ avec $v_p(u) = 0$ et $n \in \mathbb{Z}$ est un carré si, et seulement si n est pair, et u est un carré dans $\mathbb{Z}_p^*/(1 + p\mathbb{Z}_p) \simeq \mathbb{F}_p^*$. Un élément $x = 2^n u \in \mathbb{Q}_2^*$ est un carré dans $\mathbb{Q}_2$ si, et seulement si n est pair et $u \equiv 1 \mod 8$.*

Remarque. En particulier, $\mathbb{Q}_p^{*2}$ est un sous-groupe ouvert de $\mathbb{Q}_p^*$.

Exemple. Un entier négatif $-n$ est un carré dans $\mathbb{Q}_2$ si, et seulement si n est de la forme $4^a(8b-1)$ avec $a, b \in \mathbb{Z}$.

Lemme 4.6 (Méthode de Newton) *Soit $f \in \mathbb{Z}_p[X]$, et f' sa dérivée. Si $x \in \mathbb{Z}_p$ et $n, k \in \mathbb{Z}$ sont tels que $0 \leq 2k < n$, $f(x) \equiv 0 \mod p^n$ et $v_p(f'(x)) = k$, alors il existe $y \in \mathbb{Z}_p$ tel que*

$$f(y) \equiv 0 \mod p^{n+1}, \quad v_p(f'(y)) = k, \quad y \equiv x \mod p^{n-k}.$$

Corollaire 4.7 *Soit $f \in \mathbb{Z}_p[X_1, \dots, X_m]$, $x = (x_i)_i \in (\mathbb{Z}_p)^m$, n, k des entiers, et $j \in [\![1, m]\!]$. Si $0 \leq 2k < n$, $f(x) \equiv 0 \mod p^n$ et $v_p\left(\frac{\partial f}{\partial X_j}(x)\right) = k$, alors il existe un zéro y de f dans $(\mathbb{Z}_p)^m$ congru à x modulo p^{n-k}.*

Exemple. On a $i \in \mathbb{Q}_p$ si $p \equiv 1 \mod 4$, car -1 est un carré mod p dans ce cas (disons a^2), et la dérivée de $X^2 + 1$ en a ne s'annule pas mod p, donc est de valuation nulle.

Applications. Relèvement en solutions exactes pour des formes quadratiques ; existence de racines $(p-1)$-ièmes de l'unité dans $\mathbb{Q}_p$.

Théorème 4.8 (Théorème de Hasse-Minkowski) *Une forme quadratique sur $\mathbb{Q}$ représente 0 dans $\mathbb{Q}$ si, et seulement si elle représente 0 dans $\mathbb{Q}_v$ pour tout $v \in V$.*

Applications. Somme de deux carrés ; de trois carrés ; de quatre carrés ; de trois nombres triangulaires.

Remarque. La structure de l'ensemble des entiers écrits comme somme de deux carrés peut aussi s'étudier *via* la décomposition des éléments de $\mathbb{P}$ en irréductibles dans $\mathbb{Z}[i]$.

Définition 4.9 (Symbole de Hilbert) *Soient $(a, b) \in (\mathbb{Q}_p^*)^2$. On définit le symbole de Hilbert $(a, b)_p$ comme étant 1 si $Z^2 - aX^2 - bY^2 = 0$ a une solution non triviale dans $\mathbb{Q}_p^3$, -1 sinon.*

Application. Si q est une forme quadratique sur $\mathbb{Q}_p$ équivalente à $\sum_i a_i X_i^2$, $\varepsilon_p(q) = \prod_{i<j}(a_i, a_j)_p$ est un invariant de la classe d'équivalence de q.

Théorème 4.10 *Deux formes quadratiques sur $\mathbb{Q}_p$ sont équivalentes si, et seulement si elles ont même rang, même discriminant et même invariant ϵ_p.*

Théorème 4.11 *Deux formes quadratiques sur $\mathbb{Q}$ sont équivalentes si, et seulement si elles sont équivalentes sur chaque $\mathbb{Q}_v$, $v \in V$.*

Corollaire 4.12 *Soient (r, s), (r', s') les signatures de deux formes quadratiques q et q'. Elles sont équivalentes si, et seulement si $(r, s) = (r', s')$, $\Delta(q) = \Delta(q')$ et $\epsilon_v(q) = \epsilon_v(q')$ pour tout $v \in V$.*

5 Développements et références

Développements

(i) Théorème de Hasse-Minkowski (pour $n = 2$ et $n = 3$) ([Ser]).
(ii) Théorème d'Ostrowski ([Kat]).
(iii) Lemme de Newton et son corollaire ([Ser]).
(iv) Complétés p-adiques de $\mathbb{Q}$ ([Kat]).
(v) Théorèmes de Sylow ([Per]).
(vi) Théorème de Gauss-Wantzel ([FGN]).
(vii) Théorème de la progression arithmétique pour $a = 1$ ([Per]).
(ix) Méthode algébrique pour la structure de l'ensemble des sommes de deux carrés ([Per]).
(x) Démonstration analytique (réelle) du postulat de Bertrand ([Ell]). Pour une démonstration algébrique, voir [Rai].
(xi) Loi de réciprocité quadratique ([Hd1]).

Références

[Ell] William John Ellison, *Les nombres premiers*, 442 pages, Hermann, 1975.

[FGN] Serge Francinou, Hervé Gianella, Serge Nicolas, *Exercices de mathématiques des oraux de l'Ecole polytechnique et des Ecoles normales supérieures : Algèbre Tome 1*, 371 pages, Cassini, 2008.

[Hd1] Marc Hindry, *Arithmétique*, 327 pages, Calvage & Mounet, 2008.

[Kat] Svetlana Katok, *p-adic analysis compared with real*, 152 pages, American Mathematical Society, 2007.

[Per] Daniel Perrin, *Cours d'algèbre*, 208 pages, Ellipses, 1998.

[Rai] *Raisonnements divins*, 270 pages, Springer, 2006.

[Sam] Pierre Samuel, *Théorie algébrique des nombres*, 132 pages, Hermann, 1997.

[Ser] Jean-Pierre Serre, *Cours d'arithmétique*, 192 pages, PUF, 1994.

Aparté

- Une autre façon d'utiliser les complétés de $\mathbb{Q}$ pour résoudre un problème sur $\mathbb{Q}$ passe par la détermination du groupe des caractères de $\mathbb{Q}$, c'est-à-dire l'ensemble des morphismes continus de $\mathbb{Q}$ dans $\mathbb{U}$, qu'on note $\hat{\mathbb{Q}}$. À l'aide des isomorphismes $\hat{\mathbb{R}} \simeq \mathbb{R}$, $\hat{\mathbb{Q}}_p \simeq \mathbb{Q}_p$ et $\mathbb{Q}^\perp \simeq \mathbb{Q}$ (qui utilisent de manière décisive le fait que les espaces soient complets), on peut montrer que $\hat{\mathbb{Q}} \simeq \mathbb{A}/\mathbb{Q}$, où $\mathbb{A}$ est l'anneau des adèles, défini comme le sous-anneau de $\mathbb{R} \times \prod_{p\in\mathbb{P}} \mathbb{Q}_p$ formé des éléments $(x_v)_{v\in S}$ tels que x_p est un entier p-adique pour presque tout p. Les caractères peuvent même être explicités grâce à cet isomorphisme. La seule difficulté pour traiter ceci concerne les topologies de $\mathbb{Q}_p$ et de $\mathbb{A}$, peu naturelles.
- De nouveau concernant les formes quadratiques, on peut s'intéresser à celles qui représentent un certain nombre premier p ; par exemple, $p = ax^2 + bxy + cy^2$ a une solution dans $\mathbb{Z}^2$ si, et seulement si $\left(\frac{D}{p}\right) = 1$, où $D = b^2 - 4ac$ est le discriminant de la forme quadratique du membre de droite (à coefficients entiers).
- Heuristiquement, une des raisons pour lesquelles il est difficile de contrôler la distribution des nombres premiers est qu'on n'a pas beaucoup d'outils pour se débarrasser des «complots» entre nombres premiers, dans lesquels les nombres premiers décident d'être en corrélation avec un certain objet (en particulier, une fonction totalement multiplicative) qui, visiblement, altère la distribution des nombres premiers. Par exemple, imaginons que la probabilité que la probabilité qu'un entier n assez grand soit premier ne soit pas proche de $\frac{1}{\log n}$ (comme le dirait le théorème des nombres premiers), mais dépende plutôt de l'argument du nombre complexe n^{it} pour un certain réel t fixé. Alors, la probabilité serait sensiblement moins que $1/\log n$ quand $t \log n$ est proche d'une valeur entière, et sensiblement plus que $1/\log n$ quand $t \log n$ est proche d'un demi-entier. Ceci contredirait le théorème des nombres premiers, si bien que ce scénario aurait été éradiqué à un moment ou un autre en voulant prouver le théorème. En termes de séries de Dirichlet, ce complot se traduit par un zéro de la fonction ζ de Riemann en $1 + it$. Ceci permet de justifier l'apport des fonctions L en théorie des nombres. Le livre de Davenport, *Multiplicative number theory*, est excellent pour étudier ce sujet.
- Si on a le courage d'établir l'équation fonctionnelle de la fonction ζ (rapide à faire si on admet la formule de Poisson), appliquer la formule des résidus à $-\frac{\zeta'(s)}{\zeta(s)}\frac{x^s}{s}$ pour $x > 1$ sur un contour bien choisi permet d'obtenir la formule explicite suivante :

$$\pi(x) = \int_2^x \frac{\psi(t)}{t \cdot \ln(t)^2}\mathrm{d}t + \frac{\psi(x)}{\ln(x)} + O(\sqrt{x}),$$

où :

$$\psi(x) = x - \sum_\rho \frac{x^\rho}{\rho} - \frac{\zeta'(0)}{\zeta(0)} - \frac{1}{2}\ln(1 - x^{-2}),$$

où ρ parcourt les zéros non réels de ζ (conjecturalement de partie réelle $1/2$). C'est démontré dans le livre de Davenport, également.
- C'est peut-être un peu dangereux, mais on peut faire une très courte escale dans l'analyse p-adique. Exemple : si (u_n) est une suite récurrence linéaire d'un certain ordre, on peut prouver par des méthodes d'analyse p-adique que l'ensemble des valeurs est réunion d'au plus un nombre fini de progressions arithmétiques. La méthode classique revient à considérer une fonction analytique p-adique qui s'annule précisément en les valeurs de (u_n). Comme on ne peut avoir qu'un nombre fini de zéros dans $\mathbb{Z}_p$ (par le principe des zéros isolés, $\mathbb{Z}_p$ étant compact), on peut en déduire le résultat annoncé.
- Les polygones de Newton sont une bonne méthode géométrique pour montrer l'irréductibilité des polynômes, et utilisent les nombres p-adiques. Ils généralisent le critère d'Eisenstein. Applications : irréductibilité des exponentielles tronquées ($P_n = \sum_{k=0}^n \frac{X^k}{k!}$) sur $\mathbb{Q}$.
- Si p est un nombre premier divisant le numérateur d'aucun des nombres de Bernoulli B_k, pour k allant de 2 à $p - 3$, alors un idéal de $\mathbb{Z}[\exp(2i\pi/p)]$ est principal si, seulement si, son élévation à la puissance p est principale. Cela peut paraître un peu inutile, mais ça permet de démontrer le dernier théorème de Fermat (l'inexistence de solutions non triviales à l'équation $x^p + y^p = z^p$) pour tout nombre premier inférieur à 100 et différent de 37, 59 et 67. Les preuves de ces deux affirmations sont dans le livre de Borevitch et Shafarevich, *Théorie des nombres*.
- On peut bien sûr traiter les critères de primalité, ou encore les questions de cryptographie. Tout ceci fait l'affaire du chapitre II de [Hd1].