Le théorème des deux carrés

Leçons :

121 Nombres premiers

122 Anneaux principaux

Référence : Francinou, Gianella, Nicolas [FGN14, Algèbre 1] ou Jean-Pierre Serre, *Compléments d'arithmétique* (notes polycopiées, sans ISBN).

Avertissement La version précise (expression de $r_2(n)$) ne rentre pas dans le temps imparti. Dans la leçon « Anneau principaux » il ne faut pas dissimuler qu'en réalité seule la factorialité de $\mathbb{Z}[i]$ compte.

Théorème 1. *L'anneau $A = \mathbb{Z}[i]$ des entiers de Gauss est euclidien pour le stathme $N(z) = z\overline{z}$. En outre, les irréductibles de A sont (à association près)*
- *Les nombres premiers p congrus à 3 modulo 4*
- *Les $z \in A$ tels que $N(z)$ est premier.*

Corollaire 2 (Théorème des deux carrés). *L'entier $n \in \mathbb{N}$ est somme de deux carrés si et seulement si pour tout $p \in \mathcal{P}$ congru à 3 modulo 4, $\nu_p(n)$ est pair. Plus précisément, le nombre de décompositions de n en sommes de deux carrés de $\mathbb{Z}$ est donné par*

$$r_2(n) = 4(d_1(n) - d_3(n)) \tag{1}$$

où $d_i(n)$ est le nombre de diviseurs de n congrus à i mod 4.

(a) Preuve du théorème On prouve à l'aide du plongement $\mathbb{Z}[i] \hookrightarrow \mathbb{C}$ et de la nature géométrique de N que A est euclidien [1] : Soient a et b dans A avec $b \neq 0$, alors on écrit

$$a/b = x + iy = x_0 + iy_0 + (x - x_0) + i(y - y_0)$$

1. La même preuve s'adapte pour $\mathbb{Z}[j]$, $\mathbb{Z}\left[i\sqrt{2}\right]$ par exemple mais attention, pas pour n'importe quel anneau d'entiers quadratiques imaginaires ; ceux-ci ne sont d'ailleurs pas principaux en général, voir [Che14, chapitre 4].

avec $x_0, y_0 \in \mathbb{Z}$ et $|x - x_0| \leqslant 1/2$, $|y - y_0| \leqslant 1/2$. Posons $q = x_0 + iy_0$, il vient $a = qb + r$ avec

$$N(r) = N(b)\left(|x - x_0|^2 + |y - y_0|^2\right) \leqslant N(b)/2 < N(b)$$

Lemme 3. *Soit $p \in \mathcal{P}$. S'équivalent*
(i) p est irréductible dans A
(ii) $p \equiv 3$ modulo 4
(iii) p n'est pas somme de deux carrés.

Démonstration. (ii) $\Longrightarrow$ (iii) s'obtient par congruence modulo 4, les uniques carrés dans $\mathbb{Z}/4\mathbb{Z}$ étant $\overline{0}$ et $\overline{1}$. Montrons (iii) $\Longrightarrow$ (i) par contraposition : si $p = zz'$ avec $z, z' \notin A^\times$ alors en notant $z = a + ib$ nous avons

$$N(p) = p^2 = N(z)\, N(z').$$

Ceci impose $N(z) = N(z') = p$, d'où $a^2 + b^2 = p$, soit $\neg$(iii).

(i) $\Longrightarrow$ (ii) demande un peu plus de travail. A est euclidien donc principal, et p est irréductible dans A ssi $A/(p)$ est un corps. Or il y a un isomorphisme d'anneaux astucieux (aussi utilisé dans le cours de Perrin) lié au double quotient :

$$A/(p) \simeq \mathbb{Z}[X]/\left(p, X^2+1\right) \simeq \mathbb{F}_p[X]/\left(X^2+1\right). \tag{2}$$

Comme $\mathbb{F}_p[X]$ est principal, $\mathbb{F}_p[X]/\left(X^2+1\right)$ est un corps ssi X^2+1 est irréductible, autrement dit si X^2+1 n'a pas de racine dans $\mathbb{F}_p$. Il reste à voir que si $p \equiv 1$ modulo 4 alors -1 est un carré dans $\mathbb{F}_p$. Observons alors que[2] $(p-1)! \equiv -1\,[p]$ (regrouper les éléments avec leurs inverses) puis que

$$((p-1)/2)!^2 \equiv (-1)^{\frac{p-1}{2}}(p-1)! \equiv -1\,[p]$$

si p est congru à 1 modulo 4. □

Remarque 4. Pour (i) $\Longleftrightarrow$ (ii) on peut aussi utiliser la factorialité de A et de $\mathbb{F}_p[X]$ (notion plus faible) et observer que d'après les isomorphismes (2), $A/(p)$ est intègre ssi $\mathbb{F}_p[X]/\left(X^2+1\right)$ est intègre, ce qui donne en définitive la même chose.

Démontrons à présent le théorème :

1. Nombres premiers. D'après le lemme, si $p \equiv 3 \bmod 4$ il est irréductible dans A ; mais par ailleurs, si $p \equiv 1 \bmod 4$ il est somme de deux carrés, d'où $p = a^2 + b^2 = (a+ib)(a-ib)$ et p n'est pas irréductible dans A.
2. Si $N(z)$ est premier alors z est irréductible (vue la multiplicativité de N). Réciproquement, soit z un irréductible de A et $p \in \mathcal{P}$ divisant $N(z)$. Alors $p \mid z\overline{z}$. Si $p \in \mathcal{P}_3$ alors p est irréductible, donc $p \mid z$ ou $p \mid \overline{z}$; mais alors $p \mid z$ et $p = z$. On peut donc supposer $p \in \mathcal{P}_1$ mais alors $p = y\overline{y}$ d'après ce qui précède, ce qui contredit l'irréductibilité de z.

2. Ce fait caractérise les nombres premiers ; il est parfois connu sous le nom de théorème de Wilson

(b) Preuve du théorème des deux carrés Soit n un entier naturel. On écrira

$$n = 2^{\alpha} p_1^{\beta_1} \cdots p_r^{\beta_r} q_1^{\gamma_1} \cdots q_s^{\gamma_s} \tag{3}$$

sa décomposition en facteurs premiers avec les $p_i \equiv 1 \bmod 4$ et les $q_i \equiv 3 \bmod 4$. On notera $n \in \Sigma_2$ si n est somme de deux carrés.

(b.1) Si $n \in \Sigma_2$ alors γ_i est pair pour tout $i \in \{1, \ldots, s\}$ Ecrivons $n = a^2 + b^2$ et soit $q \in \mathcal{P}_3$ divisant n. Alors en posant $z = a + ib$, $n = N(z) = z\overline{z}$ est divisible par q, donc (puisque q est irréductible dans A) $q \mid z$, ie $q \mid a$ et $q \mid b$. Donc $q^2 \mid a^2 + b^2 = n$, et $n/q^2 = (a/q)^2 + (b/q)^2$ de sorte que $n/q^2 \in \Sigma_2$. Par une réccurence immédiate, $\nu_q(n)$ est pair.

(b.2) Si γ_i est pair pour tout $i \in \{1, \ldots, s\}$ alors $n \in \Sigma_2$ D'après la multiplicativité de N, Σ_2 est stable par multiplication ; il suffit donc d'écrire n comme un produit d'éléments de Σ_2. D'après le lemme, tous les p_i sont sommes de deux carrés. Ecrivons $p_i = a_i^2 + b_i^2 = z_i\overline{z_i}$ avec $z_i = a_i + b_i$.

— Si α est pair alors

$$n = \left(2^{\alpha/2}\right)^2 \left(a_1^2 + b_1^2\right)^{\beta_1} \cdots \left(a_r^2 + b_r^2\right)^{\beta_r} \left(q_1^2\right)^{\gamma_1/2} \cdots \left(q_s^2\right)^{\gamma_s/2}.$$

— Si α est impair alors $n = \left(1^2 + 1^2\right) n/2$ et $n/2 \in \Sigma_2$ d'après ce qui précède.

(c) Le nombre de décompositions en sommes de deux carrés. D'après ce qui précède, décomposer n en somme de deux carrés, c'est décomposer n en produit de deux termes conjugués dans l'anneau $\mathbb{Z}[i]$. Par exemple,

$$65 = 5 \times 13 = (2+i)(2-i)(3+2i)(3-2i).$$

Les éléments $2 \pm i$ et $3 \pm 2i$ étant irréductibles (car de norme première). On peut décomposer ce produit de deux manières :

$$\begin{aligned}
65 &= [(2+i)(3+2i)][(2-i)(3-2i)] \\
&= [4+7i][4-7i] \\
&= 4^2 + 7^2 \\
&= [(2+i)(3-2i)][(2-i)(3+2i)] \\
&= [8-i][8+i] \\
&= 8^2 + 1^2.
\end{aligned}$$

Soit $n \in \mathbb{N}^\star$ impair et écrivons la décomposition de n dans $\mathbb{Z}[i]$:

$$\begin{aligned}
n &= p_1^{\beta_1} \cdots p_r^{\beta_r} q_1^{\gamma_1} \cdots q_s^{\gamma_s} \\
&= (1+i)^{\alpha} (1-i)^{\alpha} (a_1 + ib_1)^{\beta_1} \cdots (a_r + ib_r)^{\beta_r} \\
&\quad (a_1 - ib_1)^{\beta_1} \cdots (a_r - ib_r)^{\beta_r} q_1^{\gamma_1} \cdots q_r^{\gamma_r}
\end{aligned}$$

Si maintenant $n = z\overline{z}$ alors pour tout irréductible π de A, $\nu_\pi(z) = \nu_{\overline{\pi}}(\overline{z})$ et $\nu_\pi(z) + \nu_\pi(\overline{z}) = \nu_\pi(n)$, donc nous pouvons écrire :

$$\begin{aligned} z &= (a_1 + ib_1)^{\beta_1'} \cdots (a_r + ib_r)^{\beta_r'} \\ &\quad (a_1 + ib_1)^{\beta_1 - \beta_1'} \cdots (a_r + ib_r)^{\beta_r - \beta_r'} q_1^{\gamma_1/2} \cdots q_s^{\gamma_s/2} \end{aligned}$$

avec $0 \leqslant \alpha' \leqslant \alpha$ et $0 \leqslant \beta_i' \leqslant \beta_i$ pour tout $i \in \{1, \ldots, r\}$. Finalement donc,

$$r_2(n) = (1 + \beta_1) \cdots (1 + \beta_r). \tag{4}$$

Remarque 5. Il existe un argument combinatoire pour démontrer le lemme 3 dû à D. Zagier, [Zag90]. Il consiste à se donner p un nombre premier congru à 1 modulo 4. ; puis on introduit l'ensemble

$$S = \{(x, y, z) \in \mathbb{N}^3 \mid x^2 + 4yz = p\}.$$

On vérifie que S est fini [3], et non vide (il contient $\left(1, 1, \frac{p-1}{4}\right)$). Soit f la fonction de S dans S défine par

$$(x, y, z) \mapsto \begin{cases} (x + 2z, z, y - x - z) & \text{si} \quad x < y - z \\ (2y - x, y, x - y + z) & \text{si} \quad y - z < x < 2y \\ (x - 2y, x - y + z, y) & \text{si} \quad x > 2y. \end{cases}$$

Alors on peut montrer que f est involutive et possède exactement un point fixe ; de telle sorte que l'on a une action de $\mathbb{Z}/2\mathbb{Z} \simeq \{\mathrm{id}, f\}$ sur S, et d'après l'équation aux classes le cardinal de S est impair. Finalement g l'involution de S donnée par

$$(x, y, z) \mapsto (x, z, y).$$

admet un point fixe ; donc p est somme de deux carrés. Cette preuve est proche de l'esprit des arguments de non-annulation de caractéristique d'Euler consistant à se ramener à un comptage de points fixe (modulo 2), en topologie différentielle.

Remarque 6 (Le problème du disque de Gauss). Si la fonction $r_2(n)$ est localement erratique, sa moyenne de Cesaro converge. En effet

$$R_2(N) = 1 + \sum_{n=1}^{N} r_2(n)$$

est exactement le nombre de points à coordonnées entières dans le disque fermé de rayon $\sqrt{N}$. On en déduit que $R_2(N) = \pi N + \mathcal{O}\left(\sqrt{N}\right)$, puis

$$\frac{1}{N} \sum_{n=1}^{N} r_2(n) = \pi + \mathcal{O}\left(N^{-1/2}\right). \tag{5}$$

3. Si $(x, y, z) \in S$ alors $xyz \neq 0$ (p est premier), donc $x, y, z \geqslant 1$. Il s'ensuit que $p = x^2 + 4yz \geqslant \max(x, y, z)$, d'où $S \subset \{1, \ldots p\}^3$ et c'est donc un ensemble fini.

L'amélioration de l'exposant $-1/2$ dans le terme de reste de (5) est un problème au long cours. Il est connu qu'on ne pourra pas faire mieux que $N^{-3/4+\epsilon}$ (Hardy, Landau).

Remarque 7 (Densités supérieures des sommes de carrés). A partir du théorème et moyennant le cas particulier [Che14, Exercice 9.9] [4] suivant du théorème de densité de Cebotarev affirmant que les nombres premiers s'équirépartissent entre 1 et 3 modulo 4, on montre que l'ensemble des sommes de deux carrés a densité naturelle nulle dans $\mathbb{N}$:

$$\limsup_{N\to+\infty} \frac{1}{N} \left|\Sigma_2 \cap \{1, \ldots N\}\right| = 0. \tag{6}$$

Remarque 8 (Trois carrés). Soit Σ_3 l'ensemble des sommes de trois carrés. Gauss a montré [Ser70, IV, appendice] que pour tout $n \in \mathbf{N}$, $n \in \Sigma_3$ si et seulement si n n'est pas la forme $4^a(8b-1)$ où a et b sont des entiers naturels.

Remarque 9. Tout nombre entier est somme de quatre carrés (voir [Sam67, 5.7] – ceci découle aussi du théorème de la remarque précédente), et il existe également une formule donnant le nombre de décomposition en somme de quatre carrés.

Remarque 10. A quoi ressemble $A/(p)$ quand $p \equiv 1$ modulo 4 ? Le polynôme X^2+1 est scindé, disons

$$X^2 + 1 = (X-u)(X+u),$$

avec $u \in \mathbb{F}_p$ et d'après le lemme des restes chinois $A \simeq \mathbb{F}_p \times \mathbb{F}_p$. C'est un anneau non intègre.

Références

[Che14] Gaëtan Chenevier. Théorie algébrique des nombres – cours de m1, ecole polytechnique, 2013–2014.

[FGN14] Serge Francinou, Hervé Gianella, and Serge Nicolas. *Exercices de mathématiques des oraux de l'École polytechnique et des Écoles normales supérieures*. Enseignement des mathématiques. Cassini, 2008–2014.

[Sam67] Pierre Samuel. *Théorie algébrique des nombres*. Hermann, Paris, 1967.

[Ser70] Jean-Pierre Serre. *Cours d'arithmétique : par Jean-Pierre Serre*. SUP. Le mathématicien. Presses universitaires de France, 1970.

[Zag90] Don Zagier. A one-sentence proof that every prime $p \equiv 1 \pmod 4$ is a sum of two squares. *Amer. Math. Monthly*, 97(2) :144, 1990.

4. Cela donne une densité de Dirichlet mais c'est tout aussi bien (même mieux) pour ce que nous voulons faire.