Théorème des deux carrés par les entiers de Gauss

Théo Jaudon

On note Σ l'ensemble $\{\ n \in \mathbb{N} \quad | \quad \exists (a,b) \in \mathbb{Z}^2 \text{ tel que } n = a^2 + b^2\ \}$
et $\mathbb{Z}[i] = \{\ a + ib \quad | \quad (a,b) \in \mathbb{Z}^2\ \}$ l'anneau des entiers de Gauss. L'objectif de ce développement est de prouver le théorème suivant.

Théorème 1. *Soit p un nombre premier. On a l'équivalence*

$$p \in \Sigma \iff p = 2 \text{ ou } p \text{ est congru à } 1 \text{ modulo } 4.$$

Définition 2. *Pour $z \in \mathbb{C}$ on définit $N(z) = z\overline{z} = |z|^2$. On remarque alors que $N(\mathbb{Z}[i]) \subset \mathbb{N}$ et que N est multiplicative. On en déduit facilement les inversibles de $\mathbb{Z}[i]$.*

Lemme 3. *On a*

$$\mathbb{Z}[i]^\times = \{\ z \in \mathbb{Z}[i] \quad | \quad N(z) = 1\ \} = \{\pm 1,\ \pm i\}.$$

Preuve. On montre les inclusions successives.
Soit $z \in \mathbb{Z}[i]^\times$. Alors $N(z)N(z^{-1}) = N(zz^{-1}) = N(1) = 1$ et comme $N(z)$ et $N(z^{-1})$ sont des entiers positifs on en déduit en particulier $N(z) = 1$.
Les seuls entiers de Gauss de norme 1 sont ± 1 et $\pm i$.
Enfin on vérifie que les éléments $1, -1, i$ et $-i$ sont inversibles et ont respectivement pour inverse $1, -1, -i$ et i.

Théorème 4. *L'anneau $\mathbb{Z}[i]$ est euclidien relativement à N.*

Preuve. On se donne $z \in \mathbb{Z}[i]$ et $w \in \mathbb{Z}[i]$ non nul et on écrit $\frac{z}{w} = x + iy$ avec $x, y \in \mathbb{Q}$. Soient a, b deux entiers tels que $|a - x| \leq \frac{1}{2}$ et $|b - y| \leq \frac{1}{2}$. On pose alors $q = a + ib \in \mathbb{Z}[i]$ et $r = z - wq \in \mathbb{Z}[i]$ de sorte que $z = wq + r$ et on trouve que
$N(r) = N(w(\frac{z}{w} - q)) = N(w)N(\frac{z}{w} - q) = N(w)((x-a)^2 + (y-b)^2) \leq N(w)(\frac{1}{4} + \frac{1}{4}) = \frac{N(w)}{2}$.

Proposition 5. *Soit p un nombre premier. On a l'équivalence*

$$p \in \Sigma \iff p \text{ n'est pas irréductible dans } \mathbb{Z}[i].$$

Preuve. Supposons qu'il existe $(a,b) \in \mathbb{Z}^2$ tels que $p = a^2 + b^2$. Alors a et b sont tous deux non nuls car p est premier et $p = (a + ib)(a - ib)$ où $a + ib$ et $a - ib$ ne sont donc pas inversibles dans $\mathbb{Z}[i]$. Ainsi p n'est pas irréductible dans $\mathbb{Z}[i]$.
Réciproquement, supposons que p n'est pas irréductible dans $\mathbb{Z}[i]$ c'est-à-dire qu'il existe $z, w \in \mathbb{Z}[i]$ non inversibles tels que $p = zw$. On trouve $N(p) = p^2 = N(z)N(w)$ et comme $N(z)$ et $N(w)$ sont différents de 1 on en déduit $N(z) = N(w) = p$, en particulier $p \in \Sigma$.

On peut alors prouver le théorème 1.

Preuve. L'anneau $\mathbb{Z}[i]$ est principal car euclidien, de sorte que p n'est pas irréductible dans $\mathbb{Z}[i]$ si et seulement si l'idéal $\langle p \rangle$ n'est pas maximal, si et seulement si l'anneau

quotient $\mathbb{Z}[i]/\langle p\rangle$ n'est pas un corps. Comme $\mathbb{Z}[i]$ est isomorphe à $\mathbb{Z}[X]/\langle X^2+1\rangle$, l'anneau $\mathbb{Z}[i]/\langle p\rangle$ est isomorphe à $\mathbb{Z}[X]/\langle X^2+1, p\rangle$.
Le morphisme d'anneaux

$$\begin{array}{rccc} g: & \mathbb{Z}[X] & \to & \mathbb{Z}/p\mathbb{Z}[X] \\ & Q=\sum a_k X^k & \mapsto & \overline{Q}=\sum \overline{a_k} X^k \end{array}$$

qui réduit les coefficients modulo p est surjectif de noyau $\langle p\rangle$.
On note $\pi : \mathbb{Z}/p\mathbb{Z}[X] \to \mathbb{Z}/p\mathbb{Z}[X]/\langle X^2+\overline{1}\rangle$ la projection sur le quotient qui est surjective de noyau $\langle X^2+\overline{1}\rangle$. Par composition, on obtient un morphisme d'anneaux surjectif $f = \pi \circ g : \mathbb{Z}[X] \to \mathbb{Z}/p\mathbb{Z}[X]/\langle X^2+\overline{1}\rangle$. Pour $Q \in \mathbb{Z}[X]$, on a les équivalences suivantes :

$$\begin{aligned} Q \in \ker(f) &\iff g(Q) \in \ker(\pi) = \langle X^2+\overline{1}\rangle \\ &\iff Q \in \langle X^2+1, p\rangle \end{aligned}$$

d'où l'isomorphisme $\mathbb{Z}[X]/\langle X^2+1, p\rangle \simeq \mathbb{Z}/p\mathbb{Z}[X]/\langle X^2+\overline{1}\rangle$. On en déduit que

$$\begin{aligned} p \in \Sigma &\iff \mathbb{Z}/p\mathbb{Z}[X]/\langle X^2+\overline{1}\rangle \text{ n'est pas un corps} \\ &\iff X^2+\overline{1} \text{ n'est pas irréductible dans } \mathbb{Z}/p\mathbb{Z}[X] \\ &\iff X^2+\overline{1} \text{ possède une racine dans } \mathbb{Z}/p\mathbb{Z} \\ &\iff -1 \text{ est un carré modulo } p \\ &\iff p=2 \text{ ou } p \text{ est congru à 1 modulo 4.} \end{aligned}$$

Quelques remarques et compléments sur ce développement :

Pour motiver la démarche de la preuve on peut d'abord présenter une autre équation diophantienne voisine telle que $p = a^2 - b^2$ avec p premier et $a, b \in \mathbb{Z}$. Le terme de droite se factorise dans $\mathbb{Z}$ en $(a-b)(a+b)$ et comme p est premier on trouve que l'un de ces termes vaut ± 1 et que l'autre vaut $\pm p$ et on en déduit facilement les solutions. On utilise ici que p est irréductible dans $\mathbb{Z}$, que les inversibles de $\mathbb{Z}$ sont ± 1 et que $\mathbb{Z}$ est factoriel.
L'équation qui nous intéresse est $p = a^2 + b^2$. Ici le terme de droite ne se factorise pas dans $\mathbb{Z}$ mais se factorise dans un anneau plus grand qui est l'anneau des entiers de Gauss en $a^2 + b^2 = (a+ib)(a-ib)$. Il nous faut maintenant étudier les propriétés de l'anneau $\mathbb{Z}[i]$, décrire ses inversibles et savoir si p est irréductible dans $\mathbb{Z}[i]$.

C'est toujours sympa de faire un dessin représentant le réseau $\mathbb{Z}[i]$ ainsi que le quotient de la division euclidienne dans la preuve du théorème 4.
De façon similaire, les anneaux $\mathbb{Z}[e^{i\frac{2\pi}{3}}]$ (entiers d'Eisenstein) et $\mathbb{Z}[i\sqrt{2}]$ sont euclidiens pour la norme N. En revanche, l'anneau $\mathbb{Z}[i\sqrt{5}]$ n'est pas factoriel et l'anneau $\mathbb{Z}[\frac{1+i\sqrt{19}}{2}]$ est un exemple d'anneau principal non euclidien.

Quelques détails sur les isomorphismes mentionnés. L'application

$$\begin{array}{rcl} \mathbb{Z}[X] & \to & \mathbb{Z}[i] \\ P & \mapsto & P(i) \end{array}$$

est un morphisme d'anneaux surjectif. En utilisant la division euclidienne, on montre que son noyau est l'idéal $\langle X^2+1\rangle$ d'où l'isomorphisme $\mathbb{Z}[i] \simeq \mathbb{Z}[X]/\langle X^2+1\rangle$. De façon similaire, la composition des flèches $\mathbb{Z}[X] \to \mathbb{Z}[i] \to \mathbb{Z}[i]/\langle p\rangle$ donne un morphisme surjectif de noyau $\langle X^2+1, p\rangle$ d'où l'isomorphisme $\mathbb{Z}[i]/\langle p\rangle \simeq \mathbb{Z}[X]/\langle X^2+1, p\rangle$.

Le théorème suivant, qu'il est bon de connaitre lorsqu'on présente ce développement, décrit exactement les entiers qui sont somme de deux carrés.

Théorème 6. *Soit $n \geq 2$. Alors $n \in \Sigma$ si et seulement si $\nu_p(n)$ est pair pour tout nombre premier p congru à 3 modulo 4.*

Preuve. Comme $\Sigma = \{\ N(z) \quad | \quad z \in \mathbb{Z}[i]\ \}$ et N est multiplicative, l'ensemble Σ est stable par multiplication. De ce qui précède on en déduit que si $\nu_p(n)$ est pair pour tout nombre premier p congru à 3 modulo 4 alors $n \in \Sigma$.
Pour la réciproque, on peut utiliser un argument de descente. En effet supposons par l'absurde qu'il existe $n \in \Sigma$ tel que $\nu_p(n)$ soit impair pour un certain nombre premier p congru à 3 modulo 4, et considérons n minimal parmi les entiers de cette forme. Alors p divise n qui est de la forme $a^2+b^2 = (a+ib)(a-ib)$ avec $a, b \in \mathbb{Z}$ et comme p est irréductible dans $\mathbb{Z}[i]$ car congru 3 modulo 4, p divise $a+ib$ ou $a-ib$ dans $\mathbb{Z}[i]$. Comme p est entier on en déduit que p divise a et b dans $\mathbb{Z}$. On écrit $a = pk$ et $b = pl$ avec $k, l \in \mathbb{Z}$ et on a $n = p^2(k^2+l^2)$ de sorte que $\frac{n}{p^2} = k^2+l^2 \in \Sigma$ et a pour valuation $\nu_p(\frac{n}{p^2}) = \nu_p(n) - 2$ qui est impair. Or $\frac{n}{p^2} < n$ ce qui contredit la minimalité de n.

Recasages : 121, 122, 126 etc ?
Références : Algèbre, Perrin.