P. Maurer

ENS Rennes

Recasages : 121, 122, 126.

Référence : Perrin, Cours d'Algèbre & Duverney, Théorie des nombres

Théorème des deux carrés

1 Définitions et notations

On note $\mathbb{Z}[i] := \{a + ib \ : \ a \in \mathbb{Z} \text{ et } b \in \mathbb{Z}\}$ l'anneau des entiers de Gauss. On définit sur $\mathbb{Z}[i]$ l'application $N : \mathbb{Z}[i] \to \mathbb{N}$, $a + ib \mapsto a^2 + b^2$. Pour $z \in \mathbb{Z}[i]$, $N(z)$ est appelé la norme de l'entier de Gauss z. On remarque que N est multiplicative : $\forall z, z' \in \mathbb{Z}[i]$, $N(zz') = N(z)N(z')$.

On note $\Sigma := \{n \in \mathbb{Z} \ : \ \exists a, b \in \mathbb{Z} \quad n = a^2 + b^2\}$ l'ensemble des entiers qui s'écrivent comme somme de deux carrés.

2 Préliminaires

Proposition 1. *$\mathbb{Z}[i]$ est euclidien pour l'application N, donc principal.*

Démonstration. Soit $x, t \in \mathbb{Z}[i]$, avec t non nul. On écrit $z/t = x + iy$ avec $x, y \in \mathbb{C}$, et on note $q = a + ib$, où a et b sont les entiers les plus proches de x et y. On a alors $|x - a| \leq \frac{1}{2}$ et $|y - b| \leq \frac{1}{2}$, donc $\left|\frac{z}{t} - q\right| \leq \frac{1}{\sqrt{2}} < 1$. Posons $r = z - qt$. Alors $r \in \mathbb{Z}[i]$, et on a $r = t\,(z/t - q)$, donc :

$$|r| \leq |t| \cdot |z/t - q| < |t|$$

On en déduit $N(r) < N(t)$. □

Lemme 2. *L'anneau $\mathbb{Z}[i]^\times$ des inversibles de $\mathbb{Z}[i]$ est $\{\pm 1, \pm i\}$.*

Démonstration. Soit $z = a + ib \in \mathbb{Z}[i]^\times$, et z' son inverse. Alors $N(z)\,N(z') = 1$, donc $N(z)$ est inversible dans $\mathbb{N}$: ce ne peut être que 1. On en déduit $a^2 + b^2 = 1$, et les seuls entiers de Gauss solution sont donc ± 1 et $\pm i$. Réciproquement, il est clair que ces derniers sont inversibles. □

Lemme 3. *Soit p un nombre premier impair.*

On a l'équivalence $p \in \Sigma \iff p$ est réductible dans $\mathbb{Z}[i]$.

Démonstration.

$\boxed{\Longrightarrow}$ Soit $p = a^2 + b^2$. Alors $p = (a + ib)(a - ib)$ dans $\mathbb{Z}[i]$. De plus, $N(a + ib) = N(a - ib) = p > 1$, donc $a + ib$ et $a - ib$ ne sont pas inversibles. On en déduit que p est réductible dans $\mathbb{Z}[i]$.

$\boxed{\Longleftarrow}$ Soit $p = xy$ avec $x, y \in \mathbb{Z}[i]$ non inversibles. Alors $p^2 = N(p) = N(x)\,N(y)$. Comme p est premier et que $N(x), N(y) > 1$, on en déduit que $p = N(x)$, donc $p \in \Sigma$. □

Lemme 4. *Σ est stable par multiplication.*

Démonstration. Soit $x, y \in \Sigma$. Alors il existe $z, z' \in \mathbb{Z}[i]$ tels que $x = N(z)$ et $y = N(z')$. On en déduit que $xy = N(z)\,N(z') = N(zz')$, donc $xy \in \Sigma$. □

3 Théorème(s) des deux carrés

Théorème 5. *Soit p un nombre premier impair. Alors $p \in \Sigma \iff p \equiv 1[4]$.*

Démonstration.

D'après ce qui précède, on a $p \in \Sigma$ si et seulement si p est réductible dans $\mathbb{Z}[i]$. Ce dernier étant factoriel (car principal), p est réductible dans $\mathbb{Z}[i]$ si et seulement si $\mathbb{Z}[i]/(p)$ est non intègre.

Par ailleurs, de l'isomorphisme $\mathbb{Z}[i] \simeq \mathbb{Z}[X]/(X^2+1)$ on déduit :

$$\mathbb{Z}[i]/(p) \simeq \mathbb{Z}[X]/(X^2+1, p) \simeq (\mathbb{Z}[X]/(p))/(\overline{X^2+1}) \simeq \mathbb{F}_p[X]/(X^2+1)$$

Donc :

$$\begin{aligned} p \text{ est réductible dans } \mathbb{Z}[i] &\iff \mathbb{F}_p[X]/(X^2+1) \text{ est non intègre} \\ &\iff X^2+1 \text{ est réductible dans } \mathbb{F}_p[X] \\ &\iff X^2+1 \text{ a une racine dans } \mathbb{F}_p \\ &\iff -1 \text{ est un carré modulo } p \\ &\iff (-1)^{\frac{p-1}{2}} = 1 \\ &\iff p \equiv 1[4] \end{aligned}$$

□

Corollaire 6. *Soit $n \in \mathbb{Z}$, écrit sous forme factorisée $n = \prod_{p \in \mathbb{P}} p^{v_p(n)}$, où $\mathbb{P}$ désigne l'ensemble des nombres premiers. On a l'équivalence :*

$$n \in \Sigma \iff \forall p \in \mathbb{P} \quad (p \equiv 3[4] \implies v_p(n) \equiv 0[2])$$

Démonstration.

$\boxed{\Longleftarrow}$ On écrit $n = \left(\prod_{p \equiv 3[4]} p^{\frac{v_p(n)}{2}} \right)^2 \cdot \prod_{p \not\equiv 3[4]} p^{v_p(n)}$. D'après le théorème précédent (et comme $2 = 1^2+1^2$), pour tout $p \equiv 1[4]$, $p \in \Sigma$, donc comme Σ est stable par multiplication, le produit de droite est un élément de Σ, et le produit de gauche s'écrit comme un carré : on en déduit que $n \in \Sigma$.

$\boxed{\Longrightarrow}$ Soit $n \in \Sigma$, avec $n = a^2+b^2$. On écrit $n = \delta^2(a'^2+b'^2)$ avec $\delta = a \wedge b$, de sorte que $a' \wedge b' = 1$.

Soit p un diviseur premier impair de $a'^2+b'^2$. On va démontrer, en raisonnant par l'absurde, que p est réductible dans $\mathbb{Z}[i]$: ainsi, on aura $p \equiv 1[4]$. Dans ce cas, tout diviseur premier de p congru à 3 modulo 4 vérifiera $p | \delta^2$, donc $v_p(n) \equiv 0[2]$.

Supposons donc que p est irréductible dans $\mathbb{Z}[i]$. Comme p divise $(a'+ib')(a'-ib')$, d'après le lemme de Gauss, p divise $a'+ib'$ ou $a'-ib'$. Or, pour $z \in \mathbb{Z}[i]$, on a :

$$p|z \iff \exists z' \in \mathbb{Z}[i] \quad p = zz' \iff \exists z' \in \mathbb{Z}[i] \quad \overline{p} = \overline{z}\,\overline{z'} \iff p|\overline{z}$$

Donc si p divise $a'+ib'$, il divise aussi $a'-ib'$, et inversement : p divise donc ces deux éléments. Dès lors, on peut en déduire que p divise $2a'$ et $2ib'$. Comme p est impair, on en déduit que p divise a' et b' : ceci contredit que $a' \wedge b' = 1$. □