Théorème des deux carrés

On note $\Sigma = \left\{a^2+b^2 \in \mathbb{N} \;\middle|\; a,b \in \mathbb{N}\right\}$ l'ensembles des entiers s'écrivant comme somme de deux carrés.
On note également $\mathbb{Z}[i] = \left\{a+ib \in \mathbb{C} \;\middle|\; a,b \in \mathbb{Z}\right\}$ l'ensemble des entiers de Gauss.
Soit $N : \left|\begin{array}{ccc} \mathbb{Z}[\alpha] & \longrightarrow & \mathbb{N} \\ z=a+ib & \longmapsto & z\overline{z}=a^2+b^2 \end{array}\right.$.
On remarque que $\mathbb{Z}[i]$ est un anneau intègre car inclus dans $\mathbb{C}$.

Proposition 1. $(\mathbb{Z}[i])^\star = \{\pm 1, \pm i\}$

Démonstration de la proposition.

Montrons que $(\mathbb{Z}[i])^\times = \{\pm 1, \pm i\}$.
Soit $z = a+ib \in (\mathbb{Z}[i])^\times$. On a $N(z)N(z^{-1}) = N(zz^{-1}) = 1$. Comme $N(z), N(z^{-1}) \in \mathbb{N}$, on a $N(z) = 1$.
On en déduit que $a^2+b^2 = 1$, et donc que si $a = 0$ alors $b = \pm 1$, et inversement. Donc $(\mathbb{Z}[i])^\times = \{\pm 1, \pm i\}$. □

Théorème 2. *$\mathbb{Z}[i]$ est euclidien relativement à N, donc principal.*

Démonstration du théorème.

Soient $z, t\mathbb{Z}[i] \setminus \{0\}$. Pour faire la division euclidienne de z par t, on considère $\frac{z}{t} \in \mathbb{C}$ que l'on approxime par un entier de Gauss q : si $\frac{z}{t} = x+iy$, on prend $q = a+ib$ où a et b sont les entiers les plus proches de x et y, alors :

$$\left|\frac{z}{t} - q\right| = |(x-a)+i(y-b)| = \sqrt{(x-a)^2+(y-b)^2} \leqslant \sqrt{\frac{1}{4}+\frac{1}{4}} = \frac{\sqrt{2}}{2} < 1$$

On pose alors $r = z - qt \in \mathbb{Z}[i]$. On a $r = t\left(\frac{z}{t} - q\right)$, d'où $|r| = |t|\left|\frac{z}{t} - q\right| < |t|$, donc $N(r) < N(t)$.
On a donc bien écrit $z = qt + r$ avec $N(r) < N(t)$. □

Lemme 3. *Soit p un nombre premier impair. Alors : $p \in \Sigma \Leftrightarrow p$ est réductible dans $\mathbb{Z}[i]$.*

Démonstration du lemme.

($\Rightarrow$) Soit p un nombre premier dans Σ. On remarque que $p = a^2+b^2 = (a+ib)(a-ib)$.
Or $N(a+ib) = N(a-ib) = p > 1$, donc $a+ib$ et $a-ib$ ne sont pas inversibles, et p est réductible.

($\Leftarrow$) Soit $p = zz'$ avec z et z' non inversibles. Alors $p^2 = N(p) = N(zz') = N(z)N(z')$.
On en déduit que $N(z) = N(z') = p$, car $N(z) \neq 1 \neq N(z')$.
Comme $z = a+ib$ avec $a,b \in \mathbb{Z}$, on a $p = N(z) = a^2+b^2 \in \Sigma$.

□

Théorème 4. *Soit p un nombre premier. Alors : $p \in \Sigma \Leftrightarrow p = 2$ ou $p \equiv 1[4]$.*

Démonstration du théorème.

(i) Dire que $q \equiv 1[4]$ revient à dire que $\operatorname{Card} \mathbb{F}q^{\star 2} = \frac{q-1}{2}$ est pair. Or, par ..., ceci revient à dire qu'il y a un élément d'ordre 2 dans $\mathbb{F}q^{\star 2}$. Cet élément vérifie $x^2 = 1 \Leftrightarrow (x-1)(x+1) = 0$ et $x \neq 1$, c'est donc nécesairement -1. On a donc $q \equiv 1[4] \Leftrightarrow -1 \in \mathbb{F}q^{\star 2}$.

(ii) $\mathbb{Z}[i]$ est principal, donc p est réductible dans $\mathbb{Z}[i]$ si, et seulement si, (p) n'est pas premier.
De plus, par le lemme précédent, et ce qu'on vient de voir :

$$\begin{aligned} p \in \Sigma &\Leftrightarrow p \text{ réductible dans } \mathbb{Z}[i] \\ &\Leftrightarrow (p) \text{ n'est pas premier} \\ &\Leftrightarrow \mathbb{Z}[i]/(p) \text{ n'est pas intègre} \\ &\Leftrightarrow \mathbb{Z}[X]/(p, X^2+1) \text{ n'est pas intègre} \\ &\Leftrightarrow (\mathbb{Z}/p\mathbb{Z})[X]/(X^2+1) \text{ n'est pas intègre} \\ &\Leftrightarrow X^2+1 \text{ réductible dans } \mathbb{Z}/p\mathbb{Z}[X] \\ &\Leftrightarrow -1 \text{ est un carré dans } \mathbb{Z}/p\mathbb{Z} \\ &\Leftrightarrow p \equiv 1[4] \end{aligned}$$

□

Corollaire 5. *Soit $n \in \mathbb{N}^\star \setminus \{1\}$. On décompose n en facteurs premiers : $n = \prod_{p \in \mathbb{P}} p^{v_p(n)}$.*
Alors on a $n \in \Sigma \Leftrightarrow (p \equiv 3[4] \Rightarrow v_p(n) \equiv 0[2])$.

Démonstration du corollaire.

($\Leftarrow$) Soit $n \in \mathbb{N}^\star \setminus \{1\}$ tel que $p \equiv 3[4] \Rightarrow v_p(n) \equiv 0[2]$, alors :

$$n = \underbrace{\left(\prod_{\substack{p \in \mathbb{P} \\ p \equiv 3[4]}} p^{\frac{v_p(n)}{2}} \right)^2}_{\text{Carré parfait}} \underbrace{\left(\prod_{\substack{p \in \mathbb{P} \\ p \not\equiv 3[4]}} p^{v_p(n)} \right)}_{\text{Somme de deux carrés}}$$

($\Rightarrow$) Soit $n = a^2 + b^2 \in \Sigma$.
Soit $\delta = a \wedge b$, on pose $a = a'\delta$ et $b = b'\delta$ avec $a' \wedge b' = 1$. Alors $n = \delta^2(a'^2 + b'^2)$.
Soit p un nombre premier impair diviseur de $a'^2 + b'^2 = (a' + ib')(a' - ib')$.
— Par l'absurde, supposons p irréductible.
$p|(a'^2 + b'^2) = (a' + ib')(a' - ib')$, donc $p|(a' + ib')$ ou $p|(a' - ib')$.
Par passage au conjugué, si p divise l'un alors il divise l'autre.
Par somme et différence, on a $p|2a'$ et $p|2ib'$ dans $\mathbb{Z}[i]$.
On en déduit que $p^2|4a'^2$ et $p^2|4b'^2$ dans $\mathbb{Z}$.
Comme p est impair, on a $p|a'$ et $p|b'$, contradiction.
— On peut donc écrire $p = xy$ dans $\mathbb{Z}[i]$, avec en plus $N(x) \neq 1 \neq N(y)$.
En passant à la norme, on a $p^2 = N(x)N(y)$.
p étant premier, on a $p = N(x) = N(y)$, donc $p \in \Sigma$, d'où $p \equiv 1[4]$.
Ainsi, on a montré que les facteurs premiers congrus à 3 modulo 4 sont "dans" δ^2, donc d'exposant pair.
□

Conclusion. Un entier supérieur ou égal à 1 est somme de deux carrés si, et seulement si, chacun de ses facteurs premiers de la forme $4k+3$ intervient à une puissance paire. ◁

Références

[Per] Daniel Perrin. *Cours d'Algèbre*. Ellipses