Théorème des deux carrés de Fermat

- Perrin, *Cours d'algèbre.* (56-58)

Lemme 1 : L'anneau $\mathbb{Z}[i] = \{a + ib,\ a, b \in \mathbb{Z}\}$ est euclidien de stathme N défini par $N(a + ib) = a^2 + b^2$ et $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$.

Démonstration.
• Soient $z, t \in \mathbb{Z}[i]\backslash\{0\}$. Pour faire la division euclidienne de z par t, on considère $\frac{z}{t} \in \mathbb{C}$. Si $\frac{z}{t} = x + iy$ alors prenons $q = a + ib$ où $a, b \in \mathbb{Z}$ sont les plus proches de x et y.
Ainsi, $\left|\frac{z}{t} - q\right| \leqslant \frac{\sqrt{2}}{2} < 1$ car $|x - a| \leqslant \frac{1}{2}$ et $|y - b| \leqslant \frac{1}{2}$.
Posons $r = z - qt$. Ainsi, $r \in \mathbb{Z}[i]$ et $|r| = \left|t\left(\frac{z}{t} - q\right)\right| < |t|$, donc $|r|^2 < |t|^2$.
Ainsi, $N(r) < N(t)$ et $z = qt + r$. Donc $\mathbb{Z}[i]$ est un anneau euclidien de stathme N.
• Si $z \in \mathbb{Z}[i]^*$, alors il existe $z' \in \mathbb{Z}[i]$ tel que $zz' = 1$ d'où $N(z)N(z') = N(zz') = 1$.
Comme N est à valeurs dans $\mathbb{N}$, alors $N(z) = N(z') = 1$. Si $z = a + ib$ alors $a^2 + b^2 = 1$ avec $a, b \in \mathbb{Z}$, donc l'un est nul et l'autre vaut ± 1. □

Lemme 2 : On pose $\Sigma = \{n \in \mathbb{N},\ n = a^2 + b^2 \text{ avec } a, b \in \mathbb{N}\}$. Soit p premier.
On a $p \in \Sigma$ ssi p est réductible dans $\mathbb{Z}[i]$.

Démonstration.
($\Rightarrow$) Si $p = a^2 + b^2 = (a + ib)(a - ib)$ et si $a, b \neq 0$ alors $a + ib, a - ib \notin \mathbb{Z}[i]^*$ d'après le lemme 1. Ainsi, p est réductible dans $\mathbb{Z}[i]$.
($\Leftarrow$) Si $p = zz'$ avec $z, z' \in \mathbb{Z}[i]^*$ et $p^2 = N(p) = N(z)N(z')$. Comme $z, z' \in \mathbb{Z}[i]^*$ alors $N(z), N(z') \neq 1$ alors $N(z) = p$. D'où $p = a^2 + b^2$. □

Théorème des deux carrés de Fermat (cas n premier) :
Soit p premier. $p \in \Sigma$ ssi $p = 2$ ou $p \equiv 1\ [4]$.

Démonstration. Comme $\mathbb{Z}[i]$ est principal (alors factoriel) dire que p est non irréductible dans $\mathbb{Z}[i]$ revient à dire que $(p) = p\mathbb{Z}[i]$ est un idéal principal non premier donc $\mathbb{Z}[i]/(p)$ n'est pas intègre.
• Étudions l'isomorphisme $\mathbb{Z}[i] \simeq \mathbb{Z}[X]/(X^2 + 1)$.
En effet, par propriété universelle de l'anneau des polynômes, on a un morphisme surjectif $\varphi : \mathbb{Z}[X] \to \mathbb{Z}[i]$ défini de manière unique par $\varphi(X) = i$. Son noyau contient clairement l'idéal $(X^2 + 1)$.
Réciproquement, si $P \in \mathrm{Ker}\varphi$, alors par division euclidienne unitaire dans $\mathbb{Z}[X]$, il existe Q, R tels que $P = (X^2 + 1)Q + R$ avec $\deg(R) \leqslant 1$. Et $R(i) = 0 \Rightarrow R = 0$ car R est de degré $\leqslant 1$. Le théorème d'isomorphisme donne alors l'isomorphisme souhaité.
Ce même théorème permet d'intervertir l'ordre des quotients :

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

$\mathbb{F}_p[X]/(X^2 + 1)$ est intègre ssi $X^2 + 1$ est irréductible dans $\mathbb{F}_p[X]$
ssi $X^2 + 1$ est sans racine dans $\mathbb{F}_p[X]$
Ainsi, p est réductible dans $\mathbb{Z}[i]$ ssi $X^2 + 1$ a une racine dans $\mathbb{F}_p[X]$
ssi $-1 \in (\mathbb{F}_p^*)^2$

• Si $p = 2$ alors tous les éléments sont des carrés car $x \mapsto x^2$ est le morphisme de Frobenius qui est injectif (donc bijectif par cardinalité).

• Si $p > 2$ alors x est un carré de $\mathbb{F}_p^*$ ssi $x^{\frac{p-1}{2}} = 1$.

En effet, posons $X = \{x \in \mathbb{F}_p,\ x^{\frac{p-1}{2}} = 1\}$. On a $|X| \leqslant \dfrac{p-1}{2}$ (car le nombre maximal de racines de $X^{\frac{p-1}{2}} - 1$). De plus, si $x \in (\mathbb{F}_p)^*$, alors $\exists y \in \mathbb{F}_p^*,\ x = y^2$ donc $x^{\frac{p-1}{2}} = y^{p-1} = 1$. Donc, $(\mathbb{F}_p^*)^2 \subset X$ et par cardinalité, on a égalité.

Ainsi, $-1 \in (\mathbb{F}_p^*)^2 \iff (-1)^{\frac{p-1}{2}} = 1 \iff \dfrac{p-1}{2}$ est pair $\iff p \equiv 1\ [4]$. □

Théorème des deux carrés de Fermat :
Soit $n \in \mathbb{N}\backslash\{0,1\}$ dont la décomposition en facteurs premiers est $\prod_{p\in\mathcal{P}} p^{v_p(n)}$.
Alors, $n \in \Sigma$ ssi $v_p(n)$ est pair pour $p \equiv 3\ [4]$.

Démonstration. ($\Leftarrow$) Il suffit de voir que Σ est stable par multiplication.
En effet, par les entiers de Gauss, on a $n \in \Sigma \iff \exists z \in \mathbb{Z}[i],\ n = N(z)$.
Par conséquent, pour $n, n' \in \Sigma,\ \exists z, z' \in \mathbb{Z}[i],\ n = N(z)$ et $n' = N(z')$. Donc par l'égalité de Lagrange, pour $z = a + ib$ et $z' = c + id$, on a

$$nn' = N(z)N(z') = (a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad - bc)^2 \in \Sigma$$

Soit $p \in \mathcal{P}$.
• Si $p = 2$ ou $p \equiv 1\ [4]$ alors par le théorème précédent, c'est un élément de Σ et donc $p^{v_p(n)} \in \Sigma$ par stabilité par produit.
• Si $p \equiv 3\ [4]$ alors par hypothèse $v_p(n)$ est pair et $p^{v_p(n)}$ est alors un carré donc il appartient à Σ.
Au final, n est un produit d'éléments de Σ donc $n \in \Sigma$.

($\Rightarrow$) Supposons $n \in \Sigma$. Soit $p \equiv 3\ [4]$. On veut montrer que $v_p(n)$ est pair.
$\forall k \in \mathbb{N}$, on pose H_k : si $v_p(n) \leqslant k$ alors $v_p(n)$ est pair.

Pour H_0, on a $v_p(n) = 0$ donc c'est clair.
Soit $k \in \mathbb{N}$ tel que H_k soit vraie. On suppose $v_p(n) \leqslant k + 1$.
Par définition de n, on a $p \,|\, n = a^2 + b^2 = (a + ib)(a - ib)$.
Or p est premier donc par le lemme de Gauss, $p \,|\, (a + ib)$ ou $p \,|\, (a - ib)$.
Donc $p \,|\, a$ et $p \,|\, b$. Ainsi, $p^2 \,|\, n$.
Par conséquent, $v_p\left(\dfrac{n}{p^2}\right) = v_p(n) - 2 \leqslant k$ car $v_p(n) \leqslant k + 1$.
D'après H_k, on a alors $v_p\left(\dfrac{n}{p^2}\right)$ pair et donc que $v_p(n)$ est pair. D'où H_{k+1}. □

Remarque. Ce théorème permet de déterminer les éléments irréductibles de $\mathbb{Z}[i]$ (aux éléments inversibles près) : les $p \in \mathcal{P}$ avec $p \equiv 3\ [4]$ et les entiers de Gauss $a + ib$ dont la norme $a^2 + b^2$ est premier.

Lemme : Soit A un anneau. Soient $a, b \in A$. Alors, $\big(A/(a)\big)/(b) \simeq A/(a, b)$.

Démonstration. On pose les injections canoniques $\pi_a : A \to A/(a)$ et $\pi_{a,b} : A \to A/(a, b)$.
Comme $(a) \subset (a, b)$, par la propriété universelle des quotients, il existe un morphisme d'anneaux $\overline{\pi_{a,b}} : A/(a) \to A/(a, b)$ tel que $\overline{\pi_{a,b}} \circ \pi_a = \pi_{a,b}$.
D'après le 1^e théorème d'isomorphisme, $\mathrm{Im}(\overline{\pi_{a,b}}) \simeq \big(A/(a)\big)/\mathrm{Ker}(\overline{\pi_{a,b}})$. Or $\mathrm{Im}(\overline{\pi_{a,b}}) = \mathrm{Im}(\pi_{a,b}) = A/(a, b)$ et $\bar{x} \in \mathrm{Ker}(\overline{\pi_{a,b}}) \Leftrightarrow \pi_{a,b}(x) = 0 \Leftrightarrow x \in (a, b) \Leftrightarrow \bar{x} \in (b)$. □

Lemme de Gauss : Soient $a, b, c \in \mathbb{N}^*$. Si $a \mid bc$ et si $\mathrm{pgcd}(a, b) = 1$ alors $a \mid c$.

Démonstration. Comme $\mathrm{pgcd}(a, b) = 1$ alors par le théorème de Bézout, il existe $u, v \in \mathbb{Z}$ tels que $au + bv = 1$. Donc $(ac)u + (bc)v = c$. Or $a \mid ac$ et $a \mid bc$ donc $a \mid c$. □