Théorème des deux carrés

Théorème . Soit $p \geq 3$ un nombre premier. On pose $\Sigma := \{a^2+b^2 \ ; \ a,b \in \mathbb{N}\}$. Alors

$$\Big(p \in \Sigma\Big) \quad \iff \quad \Big(p \equiv 1 \quad [4]\Big).$$

Preuve :
On va travailler dans l'anneau des entiers de Gauss $\mathbb{Z}[i]$, sur lequel on définit

$$\begin{array}{rccc} N: & \mathbb{Z}[i] & \to & \mathbb{N} \\ & a+ib & \mapsto & a^2+b^2 \end{array}$$

Elle vérifie en particulier $\forall z,z' \in \mathbb{Z}[i], N(zz') = N(z)N(z')$.

On a alors $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$. En effet, pour $z = a+ib \in \mathbb{Z}[i]^\times$, on a

$$N(zz^{-1}) = N(z)N(z^{-1}) = 1,$$

donc $a^2+b^2 = N(z) = N(z^{-1}) = 1$. Les seules solutions sont $(a^2,b^2) \in \{(1,0),(0,1)\}$ ce qui donne la première inclusion. Réciproquement, on a bien $\pm 1, \pm i \in \mathbb{Z}[i]^\times$.
On sait ensuite que $\mathbb{Z}[i]$ est factoriel, on peut en fait montrer qu'il est euclidien pour N. On a donc

$$\begin{aligned} p \text{ est réductible dans } \mathbb{Z}[i] &\iff (p) \text{ n'est pas un idéal premier de } \mathbb{Z}[i] \\ &\iff {}^{\mathbb{Z}[i]}\!/_{(p)} \text{ n'est pas intègre.} \end{aligned}$$

On sait que $\mathbb{Z}[i] \simeq {}^{\mathbb{Z}[X]}\!/_{(X^2+1)}$, donc

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

On a alors

$$p \text{ est réductible dans } \mathbb{Z}[i] \iff X^2+1 \text{ est réductible dans } \mathbb{F}_p[X].$$

Or X^2+1 est réductible dans $\mathbb{F}_p[X]$ si et seulement si -1 est un carré dans $\mathbb{F}_p$, c'est-à-dire si $(-1)^{\frac{p-1}{2}} = 1$, ou encore $p \equiv 1 \quad [4]$.

Pour conclure, on montre que $p \in \Sigma$ si et seulement si p est réductible dans $\mathbb{Z}[i]$.

Si $p = a^2+b^2 \in \Sigma$, alors $p = (a+ib)(a-ib)$. Or $N(a+ib) = N(a-ib) = p > 1$, on a décomposé p comme produit de deux éléments non inversibles donc p est réductible.
Réciproquement, soit $p = zz' \in \mathbb{Z}[i]$ avec $z,z' \notin \mathbb{Z}[i]^\times$. On a $N(z)N(z') = N(p) = p^2$ avec $N(z) \neq 1$ et $N(z') \neq 1$, donc $N(z) = p$ et ainsi $p \in \Sigma$.

□

Corollaire . Pour un entier n non nul, on a

$$\Big(n \in \Sigma\Big) \quad \iff \quad \Big(v_p(n) \text{ impair} \implies p \equiv 1 \quad [4]\Big).$$

Preuve :
Tout d'abord, Σ est stable par multiplication. En effet, $n \in \Sigma$ si et seulement s'il existe $z \in \mathbb{Z}[i]$ tel que $n = N(z)$ donc

$$\Big(n, n' \in \Sigma\Big) \implies \Big(n = N(z) \text{ et } n' = N(z')\Big) \implies \Big(nn' = N(z)N(z') = N(zz') \in \Sigma\Big).$$

Si $n \in \mathbb{N}^*$ tel que $v_p(n) \equiv 1 \quad [2] \implies p \equiv 1 \quad [4]$. Alors

$$n = \left(\prod_{\substack{p \in \mathscr{P} \\ v_p(n) \text{ pair}}} p^{\frac{v_p(n)}{2}} \right) \left(\prod_{\substack{p \in \mathscr{P} \\ v_p(n) \text{ impair}}} p^{v_p(n)} \right),$$

on conclut alors par le théorème l'implication réciproque.

Réciproquement, soit $n = a^2 + b^2 \in \Sigma$.
On note $d = a \wedge b$ et $a', b' \in \mathbb{N}$ tels que $a = a'd$ et $b = b'd$. Donc $a' \wedge b' = 1$ et $n = d^2(a^2 + b^2)$.
Soit $p \in \mathscr{P}$ un facteur premier de n tel que $v_n(p)$ soit impair. Comme $v_n(p)$ est impair, on a $p | a'^2 + b'^2$. Ainsi $p \nmid a'$ et $p \nmid b'$ car $a' \wedge b' = 1$. Donc a' est inversible dans $\mathbb{Z}/p\mathbb{Z}$.
On a $a'^2 + b'^2 = 0$ donc $\left(a'^{-1} b'\right)^2 = -1$. Donc -1 est un carré dans $\mathbb{F}_p$, donc $p \equiv 1 \quad [4]$.

□