Théorème des deux carrés

NOTATIONS :

- $\mathbb{Z}[i] = \{a + ib \ : \ a, b \in \mathbb{Z} \}$
  $\mathbb{Z}[i]$ est un anneau euclidien (donc principal et factoriel) pour le stathme
  $$\begin{array}{rccc} N : & \mathbb{Z}[i] & \longrightarrow & \mathbb{N} \\ & z = a + ib & \longmapsto & N(z) = z\overline{z} = a^2 + b^2 \end{array}$$
  et $\mathbb{Z}[i]^\times = \{ \pm 1 , \pm i\}$.
- $\Sigma = \{n \in \mathbb{N} \ : \ \exists a, b \in \mathbb{Z} \quad n = a^2 + b^2 \}$ et Σ est stable par multiplication.
- $\mathcal{P} = \{p \in \mathbb{N} \ : \ p \textit{ premier} \}$

Lemme. $p \in \Sigma \iff p$ *non irréductible dans* $\mathbb{Z}[i]$.
Proposition. $p \in \Sigma \iff p = 2$ *ou* $p \equiv 1\,[4]$.

Théorème des deux carrés. $n = \prod_{p \in \mathcal{P}} p^{\nu_p(n)} \in \Sigma \iff 2 \,|\, \nu_p(n)$ *pour* $p \equiv 3\,[4]$

Démonstration du Lemme.
$\boxed{\Longrightarrow}$ Comme $p \in \Sigma$, $p = a^2 + b^2 = (a + ib)(a - ib)$. Or, $p \in \mathcal{P}$ donc $a, b \neq 0$. Ainsi, $a + ib, a - ib \notin \mathbb{Z}[i]^\times$.
$\boxed{\Longleftarrow}$ Si $p = zz'$ avec $z, z' \in \mathbb{Z}[i] \backslash \mathbb{Z}[i]^\times$ alors $N(p) = p^2 = N(z)N(z)$. Or, $z \notin \mathbb{Z}[i]^\times$ donc $N(z) \neq 1$. Ainsi, $N(z) = p$ et $p \in \Sigma$.

□

Démonstration de la proposition.
Soit $p \in \mathcal{P}$. Comme $\mathbb{Z}[i]$ est factoriel, on a :
$$\begin{array}{rcl} p \in \Sigma & \iff & p \textit{ non irréductible de } \mathbb{Z}[i] \\ & \iff & (p) = p\mathbb{Z}[i] \quad \textit{n'est pas premier} \\ & \iff & \mathbb{Z}[i]/(p) \quad \textit{n'est pas intègre} \end{array}$$

Or, par le théorème d'isomorphisme on a :
$$\mathbb{Z}[i]/(p) \ \simeq \ \mathbb{Z}[X]/(X^2 + 1, p) \ \simeq \ \mathbb{Z}[X]/(p)\Big/(X^2 + 1) \ \simeq \ \mathbb{F}_p[X]/(X^2 + 1)$$

D'où :
$$\begin{array}{rcl} p \in \Sigma & \iff & \mathbb{F}_p[X]/(X^2 + 1) \quad \textit{n'est pas intègre} \\ & \iff & (X^2 + 1) = (X^2 + 1)\mathbb{F}_p[X] \quad \textit{n'est pas premier} \\ & \iff & X^2 + 1 \quad \textit{admet une racine dans } \mathbb{F}_p^* \\ & \iff & (-1) \in \mathbb{F}_p^{*2} \end{array}$$

Or,
$$(-1) \in \mathbb{F}_p^{*2} \iff (-1)^{\frac{p-1}{2}} = 1$$

En effet, si $p = 2$ alors par bijectivité du morphisme de FROBENIUS : $\mathbb{F}_2^2 = \mathbb{F}_2$. Supposons donc $p > 2$. Si $(-1)^{\frac{p-1}{2}}$ alors il existe $x \in \mathbb{F}_p$ tel que $-1 = x^2$. D'où, par le théorème de LAGRANGE : $(-1)^{\frac{p-1}{2}} = x^{2\frac{p-1}{2}} = x^{p-1} = 1$.
Ainsi, $\mathbb{F}_p^{*2} \subset X = \{x \in \mathbb{F}_p \ : \ x^{\frac{p-1}{2}} = 1\}$. Or, $\mathbb{F}_p$ étant un corps, le polynôme $X^{\frac{p-1}{2}} - 1$ a au plus $\dfrac{p-1}{2}$ racines dans $\mathbb{F}_p$. Ainsi, $|X| \leqslant \dfrac{p-1}{2}$.

D'où, par le théorème d'isomorphisme on obtient : $\left|\mathbb{F}_p^* \Big/ \{\pm 1\}\right| = \left|\mathbb{F}_p^{*2}\right| = \frac{p-1}{2}$.

Finalement, par inclusion et égalité des cardinaux on obtient : $\mathbb{F}_p^{*2} = X$, *i.e.*, $x \in \mathbb{F}_p^{*2} \iff x^{\frac{p-1}{2}} = 1$.

Dans notre cas, si $p \neq 2$:

$$\begin{aligned} p \in \Sigma &\iff (-1) \in \mathbb{F}_p^{*2} \iff (-1)^{\frac{p-1}{2}} = 1 \iff \frac{p-1}{2} \text{ est pair} \\ &\iff \frac{p-1}{2} = 2k \iff p = 4k+1 \iff p \equiv 1\,[4] \end{aligned}$$

D'où le résultat.

□

Démonstration du théorème.

$\boxed{\Longleftarrow}$ Par stabilité de Σ par multiplication, il suffit que chaque $p \in \Sigma$ ou $p^{\nu_p(n)} \in \Sigma$ pour tout $p \in \mathcal{P}$. Comme p est premier ou bien $p \equiv 1\,[4]$ ou bien $p \equiv 3\,[4]$.

Or, par la proposition précédente si $p \iff 1\,[4]$ alors $p \in \Sigma$ et donc $p^{\nu_p(n)} \in \Sigma$. Si $p \equiv 3\,[4]$ alors par hypothèse $\nu_p(n) = 2k$. Or, un carré est toujours dans Σ donc $p^{2k} \in \Sigma$.

$\boxed{\Longrightarrow}$ Soit $p \in \mathcal{P}$ tel que $p \equiv 3\,[4]$. On veut montrer que $2 \big| \nu_p(n)$. Pour cela, on procède par récurrence sur $\nu_p(n)$:

$$(H_d) \quad : \quad 2 \,\big|\, \nu_p(n) \quad \textit{pour tout } \nu_p(n) \leqslant d$$

(H_0) : Évident car $\nu_p(n) = 0$.

$(H_d) \to (H_{d+1})$: Par définition de n, $p \,\big|\, n$. Or, par hypothèse $n \in \Sigma$, *i.e.*, $n = a^2 + b^2 = (a+ib)(a-ib)$. Donc $p \,\big|\, (a+ib)(a-ib)$. Mais p est premier donc par le lemme de Gauss, $p \,\big|\, a+ib$ ou $p \,\big|\, a-ib$. De plus, $a, b \in \mathbb{Z}$ ainsi dans les deux cas : $p \,\big|\, a$ ET $p \,\big|\, b$. Donc $p^2 \,\big|\, n$.

D'où : $\nu_p\left(\frac{n}{p^2}\right) = \nu_p(n) - 2 \leqslant d$ car $\nu_p(n) \leqslant d+1$.

Or par hypothèse de récurrence, $2 \,\big|\, (\nu_p(n) - 2)$ et donc $2 \,\big|\, \nu_p(n)$.

Ce qui conclut la récurrence et donc le théorème.

□