Perrin II.6. Théorème des deux carrés. 122, 126,

Théorème : Soit p premier impair.

Si $\Sigma = \{n \in \mathbb{N},\ \exists a,b \in \mathbb{N},\ n = a^2+b^2\}$, alors $p \in \Sigma \Leftrightarrow p \equiv 1\ [4]$.

Lemme : $\mathbb{Z}[i]$ est euclidien pour $N : z \in \mathbb{Z}[i] \longmapsto a^2+b^2 \in \mathbb{N}$, multiplicative.

Si $z, t \in \mathbb{Z}[i] \setminus \{0\}$, $\frac{z}{t} = x+iy \in \mathbb{C}$, alors on choisit $q = a+ib$ avec a, b entiers les plus proches de x, y : $\left|\frac{z}{t} - q\right| \leq \frac{\sqrt{2}}{2} < 1$. Soit $r = z - qt = t\left(\frac{z}{t} - q\right)$ donc $|r| < |t|$ puis $N(r) < N(t)$: $z = qt + r$

Lemme : $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$

On vérifie facilement que $\{\pm 1, \pm i\} \subset \mathbb{Z}[i]^\times$.
Si $z \in \mathbb{Z}[i]^\times$, alors $N(z)N(z^{-1}) = N(1) = 1$ donc $N(z) = 1$, puis $z \in \{\pm 1, \pm i\}$

Lemme : $p \in \Sigma \Leftrightarrow p$ réductible dans $\mathbb{Z}[i]$.

- Si $p = a^2 + b^2$, alors $p = (a+ib)(a-ib)$.
  - → Si $a = 0$ ou $b = 0$, alors $p = b^2$ ou a^2 donc réductible.
  - → Sinon $p = (a+ib)(a-ib)$ est une réduction non triviale de p.
- Si $p = zz'$ avec $z, z' \neq \pm 1, \pm i$, $N(p) = N(z)N(z') = p^2$, donc $N(z) = p$. donc $p \in \Sigma$.

p réductible dans $\mathbb{Z}[i] \Leftrightarrow (p)$ non premier dans $\mathbb{Z}[i] \Leftrightarrow \mathbb{Z}[i]/(p)$ non intègre.

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

Donc $p \in \Sigma \Leftrightarrow X^2+1$ réductible dans $\mathbb{F}_p[X]$
$\Leftrightarrow X^2+1$ a une racine dans $\mathbb{F}_p$
$\Leftrightarrow -1$ est un carré dans $\mathbb{F}_p$.

Lemme : x est un carré dans $\mathbb{F}_p \Leftrightarrow x^{\frac{p-1}{2}} = 1$.

Posons $X = \{x \in \mathbb{F}_p,\ x^{\frac{p-1}{2}} = 1\}$. $|X| \leq \frac{p-1}{2}$
Si x est un carré dans $\mathbb{F}_p$, $x = y^2$, $x^{\frac{p-1}{2}} = y^{p-1} = 1$, donc $x \in X$.
$\mathbb{F}_p^* \to \mathbb{F}_p^{*2}$, $x \mapsto x^2$ est de noyau $\{\pm 1\}$ car $p > 2$, donc $|\mathbb{F}_p^*| = \frac{p-1}{2}$
Donc $X = \mathbb{F}_p^{*2}$

De là, $p \in \Sigma \Leftrightarrow (-1)^{\frac{p-1}{2}} = 1 \Leftrightarrow p \equiv 1\ [4]$.

Corollaire : Si $n = \prod_{p \in \mathcal{P}} p^{v_p(n)}$, alors $n \in \Sigma \Leftrightarrow (\forall p \in \mathcal{P},\ p \equiv 3[4] \Rightarrow v_p(n) \equiv 0[2])$.

Lem : Σ est stable par multiplication

Si $n, n' \in \Sigma$, $n = N(z)$, $n' = N(z')$, alors $nn' = N(zz') \in \Sigma$.

$\Leftarrow$ $n = \prod_{p \in \mathcal{P}} p^{v_p(n)} = \left(\prod_{p \equiv 3(4)} p^{v_p(n)/2}\right)^2 \left(\prod_{p \not\equiv 3[4]} p^{v_p(n)}\right) \in \Sigma$.

carré — somme de deux carrés

$\Rightarrow$ Soit $p \in \mathcal{P}$, $p \equiv 3[4]$. Par lemme p est irréductible dans $\mathbb{Z}[i]$.
Raisonnons par récurrence sur $v_p(n)$.
* si $v_p(n) = 0$, c'est clair.
* si $v_p(n) > 0$, alors $p \mid n = a^2 + b^2 = (a+ib)(a-ib)$ puis $p \mid a+ib$ ou $p \mid a-ib$.
Par conjugaison, $p \mid a \pm ib$ donc $p \mid a$ et $p \mid b$ donc $p^2 \mid n$: $v_p\left(\frac{n}{p^2}\right) = v_p(n) - 2$.
et $\frac{n}{p^2} = a''^2 + b''^2 \in \Sigma$ donc par HR, $v_p(n) = v_p\left(\frac{n}{p^2}\right) + 2$ est pair.