Th: p premier, $\Sigma = \{ a^2+b^2,\ a,b \in \mathbb{N} \}$

$p \in \Sigma \iff p = 2$ ou $p \equiv 1\ [4]$

Lemme: $(\mathbb{Z}[i]; N)$ est euclidien où $N(a+ib) = a^2+b^2$

et $\mathbb{Z}[i]^* = \{ \pm 1; \pm i \}$

preuve: comme $N(zz') = N(z)N(z')$

si $z \in \mathbb{Z}[i]^*$ $\exists z' \in \mathbb{Z}[i]$ / $zz' = 1$ d'où $N(z)N(z') = 1$

avec $N(z)$ et $N(z') \in \mathbb{N}$ d'où $N(z) = 1$

ainsi $\mathbb{Z}[i]^* \subset \{ \pm 1; \pm i \}$. l'inclusion réciproque étant vraie on a alors $\mathbb{Z}[i]^* = \{ \pm 1; \pm i \}$

$(\mathbb{Z}[i]; N)$ euclidien: Soient $z, t \in \mathbb{Z}[i] \setminus \{0\}$ on souhaite diviser z par t. Pour cela on considère $\frac{z}{t} \in \mathbb{C}$ que l'on écrit $\frac{z}{t} := x+iy$ avec $x, y \in \mathbb{R}$. Soient a, b les entiers les plus proches de respectivement x, y, on pose $q = a+ib$. On a alors $|\frac{z}{t} - q| \leq \frac{\sqrt{2}}{2} < 1$ (car $|x-a|$ et $|y-b| \leq \frac{1}{2}$)

Il reste à poser $r = z - qt$, $r \in \mathbb{Z}[i]$ et $r = t(\frac{z}{t} - q)$

donc $|r| = |t||\frac{z}{t} - q| < |t|$ d'où $N(r) < N(t)$

on a alors $z = qt + r$ avec $N(r) < N(t)$

Et donc $(\mathbb{Z}[i], N)$ euclidien.

Lemme: $p \in \Sigma \iff p$ pas inductible dans $\mathbb{Z}[i]$

preuve: $\Rightarrow$ $p = a^2+b^2$, on a $p = (a+ib)(a-ib)\ (= N(a+ib))$

avec a et $b \neq 0$ (car p premier) donc $a+ib$ et $a-ib \notin \mathbb{Z}[i]^*$

et donc p pas inductible dans $\mathbb{Z}[i]$

⊂ on a $p = zz'$ avec $z, z' \notin \mathbb{Z}[i]^*$

$N(p) = N(z)N(z') = p^2$ et comme $N(z), N(z') \neq 1$

par lemme d'Euclide on en déduit $N(z) = p$

c'est à dire $p \in \Sigma$

preuve du th: D'après le lemme précédent il suffit de montrer p pas irréductible dans $\mathbb{Z}[i] \Leftrightarrow p = 2$ ou $p \equiv 1 [4]$

Or on a montré que $\mathbb{Z}[i]$ est euclidien, il est donc principal et factoriel. En particulier p non irréductible $\Leftrightarrow \langle p \rangle$ non premier ou encore p non irréductible $\Leftrightarrow \mathbb{Z}[i]/\langle p \rangle$ non intègre

Or on a $\mathbb{Z}[i]/\langle p \rangle \simeq \mathbb{Z}[X]/\langle X^2+1, p \rangle \simeq \mathbb{Z}/p\mathbb{Z}[X]/\langle X^2+1 \rangle$

$\mathbb{Z}/p\mathbb{Z}$ étant le corps à p éléments on a montré (car $\mathbb{Z}/p\mathbb{Z}[X]$ principal)

p non irréductible $\Leftrightarrow X^2+1$ non irréductible dans $\mathbb{Z}/p\mathbb{Z}[X]$

$\Leftrightarrow X^2+1$ a une racine dans $\mathbb{Z}/p\mathbb{Z}$

d'où $p \in \Sigma \Leftrightarrow -1$ est un carré dans $\mathbb{Z}/p\mathbb{Z}$

c'est à dire $p = 2$ ou $p \equiv 1 [4]$

En effet -1 est un carré dans $\mathbb{Z}/p\mathbb{Z} \Leftrightarrow p = 2$ ou $(-1)^{\frac{p-1}{2}} = 1$

$\Leftrightarrow p = 2$ ou $\frac{p-1}{2} \equiv 0 [2]$

$\Leftrightarrow p = 2$ ou $p \equiv 1 [4]$