Théorème des deux carrés de Fermat

On note $\Sigma_2 := \{n \in \mathbb{N} \mid \exists a, b \in \mathbb{N},\ n = a^2 + b^2\}$.

Lemme Soit $n \in \Sigma_2$.
Alors $n \equiv 0 \mod 4$, $n \equiv 1 \mod 4$ ou $n \equiv 2 \mod 4$.

Soient $m = 2k$ et $\ell = 2q + 1$ alors :

$$m^2 = 4k^2 \equiv 0 \mod 4 \quad \text{et} \quad \ell^2 = 4q^2 + 4q + 1 \equiv 1 \mod 4$$

Ainsi, un élément $n = a^2 + b^2 \in \Sigma_2$ vérifie :

$$n \equiv 0 \mod 4, \quad n \equiv 1 \mod 4 \quad \text{ou} \quad n \equiv 2 \mod 4$$

Lemme On considère $\mathbb{Z}[i]$ l'anneau des entiers de Gauss.
Alors l'anneau $\mathbb{Z}[i]$ est euclidien.

On considère l'application $N : \mathbb{C} \longrightarrow \mathbb{R}$, $z \longmapsto \bar{z}z$. Alors, $N(a + ib) = a^2 + b^2$.

Soient $\alpha = a_1 + ia_2$ et $\beta = b_1 + ib_2 \neq 0$ des éléments de $\mathbb{Z}[i]$.
Alors $\frac{\alpha}{\beta} \in \mathbb{C}$ s'écrit $x + iy$ avec $x, y \in \mathbb{R}$.

On considère k_1, k_2 les entiers vérifiant $|x - k_1| \leqslant \frac{1}{2}$ et $|y - k_2| \leqslant \frac{1}{2}$.
On note :

$$k = k_1 + ik_2 \in \mathbb{Z}[i] \quad \text{et} \quad r = \alpha - \beta k$$

On a alors :

$$N(r) = N(\alpha - \beta k) = N\left(\frac{\alpha}{\beta} - k\right) N(\beta) = \left((x - k_1)^2 + (y - k_2)^2\right) N(\beta) \leqslant \frac{1}{2} N(\beta) < N(\beta)$$

Donc $\mathbb{Z}[i]$ est euclidien de stathme N.

Théorème de Fermat Soit p un nombre premier.
Alors p est dans Σ_2 si et seulement si $p = 2$ ou $p \equiv 1 \mod 4$.

- Le sens direct est immédiat par le premier lemme.

- Si $p = 2$, $p = 1^2 + 1^2 \in \Sigma_2$.
  Supposons que $p \equiv 1 \mod 4$.

Le groupe $\mathbb{Z}_p^*$ est cyclique d'ordre $p - 1$, donc pour tout diviseur d de $p - 1$, il existe un élément d'ordre d.
Par hypothèse, 4 divise $p - 1$, il existe donc $\overline{m} \in \mathbb{Z}_p^*$ d'ordre 4. Ainsi, $\overline{m}^2$ est d'ordre 2 dans $\mathbb{Z}_p^*$.
Ainsi, $m^2 \equiv -1 \mod p$ c'est-à-dire que p divise $m^2 + 1 = (m - i)(m + i)$.

Supposons que p soit irréductible dans $\mathbb{Z}[i]$, alors p est premier dans $\mathbb{Z}[i]$ euclidien donc factoriel.
Alors,

p divise $m - i$ ou p divise $m + i$

Il existe donc $z = k_1 + ik_2 \in \mathbb{Z}[i]$ tel que $pz = m \pm i$ donc $z = \frac{m}{p} \pm i\frac{1}{p}$ dans $\mathbb{C}$.
Or p est premier donc non inversible dans $\mathbb{Z}$ ainsi $z \notin \mathbb{Z}[i]$. Absurde !

Donc p est réductible dans $\mathbb{Z}[i]$.

Il existe donc $a + ib, c + id \in \mathbb{Z}[i]^*$ tels que $p = (a + ib)(c + id)$.
On obtient ainsi $p^2 = N(a + ib)\, N(c + id)$ avec $N(a + ib), N(c + id) \neq 1$.
Alors : $p = N(a + ib) = N(c + id) = a^2 + b^2 \in \Sigma_2$.