Recasages possibles : 121, 122, 127.
Référence : Cours d'algèbre, Perrin (p. 56-58).

Développement On pose $\mathbb{Z}[i] = \{a + ib \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$ l'anneau des entiers de Gauss, $\Sigma = \{n \in \mathbb{N} \mid n = a^2 + b^2 : a, b \in \mathbb{N}\}$, et N l'application

$$N : \left| \begin{array}{ccc} \mathbb{Z}[i] & \longrightarrow & \mathbb{N} \\ a + ib & \longmapsto & a^2 + b^2 \end{array} \right.$$

Lemme 1 L'anneau $\mathbb{Z}[i]$ est euclidien, de groupe des inversibles $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$.

Lemme 2 L'ensemble Σ est stable par multiplication

Théorème 3 Si $p \in \mathbb{N}$ est premier, alors $p \in \Sigma \Leftrightarrow p = 2$ ou $p \equiv 1$ [4].

Corollaire 4 (Fermat) Soit $n \in \mathbb{N}_{\geqslant 2}$. Pour p premier, on note $v_p(n)$ sa valuation p-adique. Alors, $n \in \Sigma \Leftrightarrow$ pour tout p premier tel que $p \equiv 3$ [4], $v_p(n)$ est pair.

Corollaire 5 Les irréductibles de $\mathbb{Z}[i]$ sont (modulo association) les $p \in \mathbb{N}$ premiers tels que $p \equiv 3$ [4], et les $a + ib$ tels que $a^2 + b^2$ est premier.

- *Preuve du Lemme 1* : Montrons que l'application N rend l'anneau $\mathbb{Z}[i]$ euclidien, *i.e* que $\forall z, t \in \mathbb{Z}[i]$, $t \neq 0$, $\exists q, r \in \mathbb{Z}[i]$: $z = tq + r$ et $N(r) < N(t)$. Soient $z, t \in \mathbb{Z}[i]$ avec $t \neq 0$. On considère le nombre complexe $\frac{z}{t} = x + iy$, avec $x, y \in \mathbb{R}$. L'idée est d'approcher $\frac{z}{t}$ par l'élément de $\mathbb{Z}[i]$ le plus proche. Plus précisément, si $a, b \in \mathbb{Z}$ sont respectivement les entiers les plus proches de x et de y (il n'y a pas unicité de a et b a priori), on pose $q = a + ib \in \mathbb{Z}[i]$. On a manifestement $|x - a| \leqslant \frac{1}{2}$ et de même $|y - b| \leqslant \frac{1}{2}$. Ainsi,

$$\left|\frac{z}{t} - q\right| = \sqrt{(x-a)^2 + (y-b)^2} \leqslant \sqrt{\frac{1}{4} + \frac{1}{4}} = \frac{\sqrt{2}}{2} < 1.$$

  On pose alors $r = z - qt \in \mathbb{Z}[i]$ qui vérifie bien $z = qt + r$ et $|r| = |t| \left|\frac{z}{t} - q\right| < |t|$. On a bien construit une division euclidienne de z par t, donc $\mathbb{Z}[i]$ est euclidien pour le stathme N. Remarquons que si $z = a + ib \in \mathbb{Z}[i]$, alors $N(z) = a^2 + b^2 = z\overline{z}$. En particulier, si $z' \in \mathbb{Z}[i]$, on a $N(zz') = zz'\overline{zz'} = z\overline{z}z'\overline{z'} = N(z)N(z')$. Montrons alors que $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$. Notons déjà que $\{\pm 1, \pm i\} \subset \mathbb{Z}[i]^\times$ car $1 = (-1)^2 = i(-i)$. Réciproquement, soit $z = a + ib \in \mathbb{Z}[i]^\times$. Par définition, il existe $z' \in \mathbb{Z}[i]$ tel que $zz' = 1$. Ainsi, $N(z)N(z') = N(zz') = N(1) = 1$. En particulier, l'entier positif $N(z)$ divise 1, d'où $N(z) = 1$. Ainsi, $a^2 + b^2 = 1$, mais comme $a, b \in \mathbb{Z}$, on a nécessairement $a = \pm 1$ et $b = 0$ ou $a = 0$ et $b = \pm 1$. Ces quatre cas possibles donnent exactement $z = \pm 1$ ou $z = \pm i$, d'où $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$, ce qui conclut la preuve du **Lemme 1**.

- *Preuve du Lemme 2* : L'introduction des entiers de Gauss dans l'étude de Σ est naturelle puisque pour $n \in \mathbb{N}$, on a $n \in \Sigma \Leftrightarrow \exists z \in \mathbb{Z}[i] : N(z) = n$. En particulier, la multiplicativité de N donne directement la stabilité de Σ par produit : si $n, n' \in \Sigma$, alors il existe $z, z' \in \mathbb{Z}[i]$ tels que $n = N(z)$ et $n' = N(z')$ et alors $nn' = N(z)N(z') = N(zz') \in \Sigma$. Remarquons qu'on aurait pu directement montrer ce lemme sans passer par $\mathbb{Z}[i]$ en utilisant l'identité de Lagrange

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2.$$

- *Preuve du Théorème 3* : Soit $p \in \mathbb{N}$ premier. Remarquons tout d'abord que $p \in \Sigma$ si et seulement si p n'est pas irréductible dans $\mathbb{Z}[i]$. En effet, si $p = a^2 + b^2$ avec $a, b \in \mathbb{N}$, alors on a $p = (a+ib)(a-ib)$ et $a, b \geqslant 1$ donc $a+ib, a-ib \notin \mathbb{Z}[i]$, et donc p n'est pas irréductible. Réciproquement si $p = zz'$ avec $z, z' \in \mathbb{Z}[i] \setminus \{\pm 1, \pm i\}$, alors $N(p) = N(z)N(z') = p^2$. Ainsi, $N(z) \mid p^2$ dans $\mathbb{N}$, *i.e* $N(z) \in \{1, p, p^2\}$. Or, $N(z), N(z') \neq 1$ car $z, z' \notin \mathbb{Z}[i]^\times$, donc $N(z) = p$, d'où $p \in \Sigma$. On veut alors montrer que p n'est pas irréductible dans $\mathbb{Z}[i]$ si et seulement si $p = 2$ ou $p \equiv 1$ [4]. Comme $\mathbb{Z}[i]$ est principal d'après le **Lemme 1**, la première condition équivaut au fait que l'idéal $(p) = p\mathbb{Z}[i]$ n'est pas premier, ou encore que l'anneau quotient $\mathbb{Z}[i]/(p)$ n'est pas intègre. Or, la division euclidienne dans $\mathbb{Z}[X]$ par le polynôme unitaire $X^2 + 1$ fournit un isomorphisme d'anneaux $\mathbb{Z}[i] \simeq \mathbb{Z}[X]/(X^2 + 1)$, donc

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

  Ainsi, on obtient que p est non irréductible dans $\mathbb{Z}[i]$ si et seulement si $X^2 + \overline{1}$ est non irréductible dans l'anneau principal $\mathbb{F}_p[X]$, c'est-à-dire si et seulement s'il admet une racine (étant de degré $2 \leqslant 3$) dans $\mathbb{F}_p$. Ceci équivaut enfin au fait que $-\overline{1}$ est un carré dans $\mathbb{F}_p$, *i.e* que $p = 2$ ou $p \equiv 1$ [4].

- *Preuve du Corollaire 4* : Soit $n \in \mathbb{N}_{\geqslant 2}$. Montrons l'équivalence par double implication :
  ($\Leftarrow$) Notons $\mathcal{P}$ l'ensemble des nombres premiers dans $\mathbb{N}$. On suppose que pour tout $p \in \mathcal{P}$ tel que $p \equiv 3$ [4], on a $v_p(n)$ pair. Écrivons

$$n = \left(\prod_{\substack{p \in \mathcal{P} \\ p \equiv 3 \ [4]}} p^{\frac{v_p(n)}{2}}\right)^2 \left(\prod_{\substack{p \in \mathcal{P} \\ p \not\equiv 3 \ [4]}} p^{v_p(n)}\right) =: \omega^2 m.$$

Comme ω^2 est un carré de $\mathbb{N}$, on a clairement $\omega^2 \in \Sigma$ et d'après le **Théorème 3** et le **Lemme 2**, $m \in \Sigma$ également donc par le **Lemme 2**, on a $n \in \Sigma$.

($\Rightarrow$) Soit $p \in \mathcal{P}$ tel que $p \equiv 3$ [4]. Montrons par récurrence sur $m \in \mathbb{N}$ que si $n \in \Sigma$ est tel que $v_p(n) = m$, alors m est pair :

- Si $m = 0$, il n'y a rien à montrer.
- Soit $m \in \mathbb{N}_{\geqslant 1}$. Supposons que pour tout $k \leqslant m-1$, s'il existe $\eta \in \Sigma$ tel que $v_p(\eta) = k$, alors k est pair. Soit $n \in \Sigma$ tel que $v_p(n) = m$. Soient $a, b \in \mathbb{N}$ tels que $n = a^2 + b^2 = (a+ib)(a-ib)$. Comme $p \equiv 3$ [4], on a vu que p est irréductible dans $\mathbb{Z}[i]$, donc comme $\mathbb{Z}[i]$ est principal, p divise $a+ib$ ou $a-ib$ dans $\mathbb{Z}[i]$. Supposons par exemple qu'il existe $\alpha+i\beta \in \mathbb{Z}[i]$ tel que $a+ib = p(\alpha+i\beta)$. Alors, en identifiant parties réelles et imaginaires, on obtient $a = p\alpha$ et $b = p\beta$, d'où $p \mid a, b$ dans $\mathbb{Z}$. Le cas $p \mid a-ib$ est similaire donc dans tous les cas $p \mid a, b$ dans $\mathbb{Z}$, et donc $p^2 \mid n$ dans $\mathbb{Z}$. En écrivant $a = pa'$ et $b = pb'$, on a $\frac{n}{p^2} = a'^2 + b'^2 \in \Sigma$. Alors, $v_p\left(\frac{n}{p^2}\right) = v_p(n) - 2 = m - 2$ est pair par hypothèse de récurrence, donc $v_p(n)$ est aussi pair, ce qui conclut la récurrence.

Ceci achève la preuve du **Corollaire 4**, dit *Théorème des deux carrés de Fermat.*

- *Preuve du Corollaire 5* : Remarquons tout d'abord que les éléments de $\mathbb{Z}[i]$ donnés dans l'énoncé du corollaire sont bien irréductibles. En effet, si $p \in \mathbb{N}$ est premier congru à 3 modulo 4, le **Théorème 3** donne que $p \notin \Sigma$ et donc p est irréductible dans $\mathbb{Z}[i]$. De même, si $a+ib \in \mathbb{N}$ est tel que $N(a+ib) = a^2+b^2$ est premier (dans $\mathbb{N}$), et si on écrit $a+ib = zz'$ avec $z, z' \in \mathbb{Z}[i]$, alors $N(z)N(z') = a^2+b^2$ donc $N(z), N(z') \mid a^2+b^2$ dans $\mathbb{Z}$. Comme a^2+b^2 est premier, on a $N(z) = 1$ ou $N(z') = 1$, puis $z \in \mathbb{Z}[i]^\times$ ou $z' \in \mathbb{Z}[i]^\times$, donc $a+ib$ est irréductible dans $\mathbb{Z}[i]$.

  Réciproquement, soit $z \in \mathbb{Z}[i]$ irréductible et soit $p \in \mathbb{N}$ premier tel que p divise $N(z) = z\overline{z}$ dans $\mathbb{Z}$. On fait une disjonction de cas selon si $p \equiv 3$ [4] ou non :
  - Si $p \equiv 3$ [4], alors $p\mathbb{Z}[i]$ est premier d'après le **Théorème 3** donc $p \mid z$ ou $p \mid \overline{z}$ dans $\mathbb{Z}[i]$. Si $p \mid \overline{z}$, alors $\overline{p} = p \mid z$ donc dans tous les cas, $p \mid z$ dans $\mathbb{Z}[i]$. Par irréductibilité de z, et puisque $p \notin \mathbb{Z}[i]^\times$, on obtient que p est associé à z, donc z est de la première forme.
  - Sinon, d'après le **Théorème 3**, on a $p \in \Sigma$ donc $p = a^2+b^2$ pour $a, b \in \mathbb{N}$. On considère l'entier de Gauss $a+ib \in \mathbb{Z}$. Il est de la deuxième forme puisque $N(a+ib) = p$ est premier, donc d'après ce qui précède, $a+ib$ est irréductible dans $\mathbb{Z}[i]$, et donc $(a+ib)\mathbb{Z}[i]$ est premier. Or, $a+ib \mid p \mid z\overline{z}$ donc $a+ib \mid z$ ou $a-ib \mid z$ (toutes ces divisibilités sont dans $\mathbb{Z}[i]$). Comme z est irréductible dans $\mathbb{Z}[i]$, z est associé à $a+ib$ ou à $a-ib$, qui sont bien de la deuxième forme.