Proposition : Soit $p>2$ premier et $q=p^n$. Soit $x \in \mathbb{F}_q^*$.
Alors $x \in \mathbb{F}_q^{*2} \Leftrightarrow x^{\frac{q-1}{2}} = 1$.

Considérons le morphisme de groupes (multiplicatifs) $\varphi : \begin{array}{ccc} \mathbb{F}_q^* & \longrightarrow & \mathbb{F}_q^{*2} \\ x & \longmapsto & x^2 \end{array}$. Alors $\operatorname{Ker}\varphi = \{x \in \mathbb{F}_q^* ; x^2 = 1\} = \{\pm 1\}$ (car q impair) et φ est surjectif par définition. Par le 1er théorème d'isomorphisme, $|\mathbb{F}_q^{*2}| = \frac{|\mathbb{F}_q^*|}{|\{\pm 1\}|} = \frac{q-1}{2}$.

Supposons que $x \in \mathbb{F}_q^{*2}$, alors $x = y^2$ donc $x^{\frac{q-1}{2}} = y^{q-1} = 1$ par le théorème de Lagrange.

Notons $X := \{x \in \mathbb{F}_q^* ; x^{\frac{q-1}{2}} = 1\}$. Alors $|X| \leq \frac{q-1}{2}$ (car $X^{\frac{q-1}{2}} - 1$ a au plus $\frac{q-1}{2}$ racines) et $\mathbb{F}_q^{*2} \subset X$. D'où $\mathbb{F}_q^{*2} = X$ par cardinalité.

Corollaire : Sous ces hypothèses, $-1 \in \mathbb{F}_q^{*2} \Leftrightarrow q \equiv 1 [4]$.

Par la proposition précédente, $-1 \in \mathbb{F}_q^{*2} \Leftrightarrow (-1)^{\frac{q-1}{2}} = 1 \Leftrightarrow \frac{q-1}{2} \equiv 0 [2] \Leftrightarrow q-1 \equiv 0 [4] \Leftrightarrow q \equiv 1 [4]$.

Proposition : L'anneau $\mathbb{Z}[i]$ est euclidien, donc principal.

Soit $a \in \mathbb{Z}[i]$, $b \in \mathbb{Z}[i] \setminus \{0\}$. Alors $\frac{a}{b} = x+iy \in \mathbb{Q}[i]$. Soit $(p,q) \in \mathbb{Z}[i]^2$ tel que $|x-p| \leq \frac{1}{2}$ et $|y-q| \leq \frac{1}{2}$.

Alors $N\left(\frac{a}{b} - (p+iq)\right) = \left|\frac{a}{b} - (p+iq)\right|^2 = (x-p)^2 + (y-q)^2 \leq \frac{1}{4} + \frac{1}{4} = \frac{1}{2} < 1$.

D'où $a = b(p+iq) + \underbrace{b\left(\frac{a}{b} - (p+iq)\right)}_{\in \mathbb{Z}[i]}$ avec $N\left(b\left(\frac{a}{b} - (p+iq)\right)\right) = N(b) N\left(\frac{a}{b} - (p+iq)\right) < N(b)$.

Théorème : Notons $\Sigma = \{n \in \mathbb{N} ; \exists (a,b) \in \mathbb{N}^2, n = a^2+b^2\}$. Soit $p>2$ premier.
Alors $p \in \Sigma \Leftrightarrow p \equiv 1 [4]$.

1) $p \in \Sigma \Leftrightarrow p$ est réductible dans $\mathbb{Z}[i]$:

$\Rightarrow$: Si $p = a^2+b^2$ avec $a, b \neq 0$, alors $p = (a+ib)(a-ib)$. De plus, $a \pm ib \notin \mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$. Donc p est réductible dans $\mathbb{Z}[i]$.

$\Leftarrow$: Si $p = zz'$ avec $z, z' \notin \mathbb{Z}[i]^\times$, alors $p^2 = N(p) = \underbrace{N(z)}_{\neq 1} \underbrace{N(z')}_{\neq 1}$. Donc $N(z) = N(z') = p \in \Sigma$ (car $N(z) = a^2+b^2$) (car p premier).

2) $p \in \Sigma \Leftrightarrow -1 \in \mathbb{F}_p^{*2}$: D'après 1), puisque $\mathbb{Z}[i]$ est principal, p est réductible dans $\mathbb{Z}[i]$ ssi $\frac{\mathbb{Z}[i]}{(p)}$ n'est pas intègre.

On, $\mathbb{Z}[i] \simeq \frac{\mathbb{Z}[X]}{(X^2+1)}$ par le 1er théorème d'isomorphisme appliqué à $\varphi : \begin{array}{ccc} \mathbb{Z}[X] & \to & \mathbb{Z}[i] \\ P & \mapsto & P(i) \end{array}$ et $\operatorname{Ker}\varphi = (X^2+1)$.

D'où $\frac{\mathbb{Z}[i]}{(p)} \simeq \frac{\mathbb{Z}[X]/(X^2+1)}{(p)} \overset{(**)}{\simeq} \frac{\mathbb{Z}[X]}{(p, X^2+1)} \simeq \frac{\mathbb{Z}[X]/(p)}{(X^2+1)} \overset{(*)}{\simeq} \frac{\mathbb{Z}/p\mathbb{Z}[X]}{(X^2+1)} = \frac{\mathbb{F}_p[X]}{(X^2+1)}$.

Donc $\frac{\mathbb{Z}[i]}{(p)}$ est non intègre $\Leftrightarrow \frac{\mathbb{F}_p[X]}{(X^2+1)}$ non intègre ($\mathbb{F}_p[X]$ principal (car $\mathbb{F}_p$ est un corps))
$\Leftrightarrow X^2+1$ réductible dans $\mathbb{F}_p[X]$ (car X^2+1 est de degré 2)
$\Leftrightarrow X^2+1$ a une racine dans $\mathbb{F}_p$
$\Leftrightarrow -1 \in \mathbb{F}_p^{*2}$
$\Leftrightarrow p \equiv 1 [4]$ d'après le corollaire

(*) Soit A un anneau et $p \in A$. On considère le morphisme $\pi : \begin{array}{ccc} A[X] & \twoheadrightarrow & \frac{A}{(p)}[X] \\ Q & \longmapsto & \overline{Q} \end{array}$ qui est surjectif.
On a $\operatorname{Ker}\varphi = (p)$ car $Q \in \operatorname{Ker}\varphi \Leftrightarrow p \mid Q \Leftrightarrow Q \in (p)$. D'où $\frac{A[X]}{(p)} \simeq \frac{A}{(p)}[X]$.

(**) Soit I, J deux idéaux de A. On considère le morphisme surjectif $p \circ \pi_I : A \overset{\pi_I}{\twoheadrightarrow} \frac{A}{I} \overset{p}{\twoheadrightarrow} \frac{\frac{A}{I}}{\pi_I(J)}$
où $\pi_I(J) \subset \frac{A}{I}$ désigne la réduction de J modulo I.
- Soit $Q \in \operatorname{Ker}(p \circ \pi_I)$. Alors $\pi_I(Q) \in \pi_I(J)$ i.e. il existe $j \in J$ tel que $\pi_I(Q) = \pi_I(j)$ i.e. il existe $i \in I$ tel que $Q = j+i \in (I,J)$.
- Soit $Q \in (I,J)$. Alors il existe $i \in I$, $j \in J$ tels que $Q = i+j$. D'où $\pi_I(Q) = \pi_I(j)$ et $p \circ \pi_I(Q) = p(\underbrace{\pi_I(j)}_{\in \pi_I(J)}) = 0$

Ainsi, $\operatorname{Ker}(p \circ \pi_I) = (I,J)$ et $\frac{A}{(I,J)} \simeq \frac{\frac{A}{I}}{\pi_I(J)}$.