Thm (Fermat): If $n \in \mathbb{N}$, then $n = k^2 + m^2$ for some $k, m \in \mathbb{Z}^+$ iff every prime factor $p \equiv 3 \pmod 4$ appears with an even exponent in the prime factorization of n.

Lemma 3: Every prime $p \in \mathbb{P}$ with $p = 4k+1$ (i.e.) $p \equiv 1 \pmod 4$ can be written as the sum of two squared natural numbers:

$$p = n^2 + m^2 \text{ for some } n, m \in \mathbb{N}.$$

pf (Thue): Consider the integral pairs (n,m) s.t. $0 \leq n, m \leq \lfloor\sqrt{p}\rfloor$; there are $(\lfloor\sqrt{p}\rfloor+1)^2$ such pairs. So $\forall s \in \mathbb{Z}$, it is impossible for $n - sm$ to take on distinct values mod p $\forall$ pairs (n,m) and $\exists$ at least two distinct pairs (n_1, m_1) and (n_2, m_2) s.t.

$$n_1 - sm_1 \equiv n_2 - sm_2 \pmod p.$$

Define $n := |n_1 - n_2|$, $m := |m_1 - m_2|$.

So, $n_1 - n_2 \equiv s(m_1 - m_2) \pmod p$

$\Leftrightarrow$ $n \equiv \pm sm \pmod p$ where $n, m \in \{0, 1, \ldots, \lfloor\sqrt{p}\rfloor\}$. Notice that $(n,m) \neq (0,0)$ because our pairs are distinct. Now let this s be the s in Lemma 1. Let's consider the equation,

$$n^2 \equiv s^2 m^2 \equiv -m^2 \pmod p$$

$$\Longleftrightarrow n^2 + m^2 \equiv 0 \pmod p$$

Notice that $0 < n^2 + m^2 < 2p$, thus $n^2 + m^2 = p$.

QED

Def: $n \in \mathbb{N}$ is representable iff $n = k^2 + \ell^2$ for some $k, \ell \in \mathbb{N}$.

Pf (of Fermat's Thm):

($\Leftarrow$) Notice that $1^2 = 0^2 + 1^2$, $2 = 1^2 + 1^2$.

Also by Lemma 3, if $p = 1 \pmod 4$ then p is representable. Now if n_1 and n_2 are representable, let $n_1^2 = k_1^2 + \ell_1^2$ and $n_2^2 = k_2^2 + \ell_2^2$. Consider,

$$n_1 n_2 = (k_1^2 + \ell_1^2)(k_2^2 + \ell_2^2)$$
$$= (k_1 k_2 + \ell_1 \ell_2)^2 + (k_1 \ell_2 - k_2 \ell_1)^2$$

Also if n is representable, then $\forall j \in \mathbb{N}$ $j^2 n$ is representable because:

$$j^2 n = j^2(k^2 + \ell^2) = (jk)^2 + (j\ell)^2.$$

Thus every integer is representable unless it has an odd power of $p = 3 \pmod 4$.

($\Rightarrow$) Suppose n is representable and suppose for $p = 3 \pmod 4$, that $p \mid n$. Then

$p \mid k^2 + \ell^2$. Since $k^2 + \ell^2$ has no real factors, then $p \mid k^2$ and $p \mid \ell^2$. Thus $p \mid k$ and $p \mid \ell$. So $p^2 \mid k^2$ and $p^2 \mid \ell^2$. $\blacksquare$