Proposition 1.

1. A prime p can be written as a sum of two integer squares, $a^2 + b^2$, if and only if $p = 2$ or $p \equiv 1 \bmod 4$. Except for changing the signs of a and b or switching a and b, the representation of p as a sum of integer squares is unique.

2. Recall that the units in $\mathbb{Z}[i]$ are

$$\pm \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \text{ and } \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Now we have that the irreducibles, up to units, in $\mathbb{Z}[i]$ are:

(a) $\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$ (with determinant 2),

(b) $\begin{pmatrix} p & 0 \\ 0 & p \end{pmatrix}$ (with determinant p^2), where p is a prime in $\mathbb{Z}$ such that $p \equiv 3 \bmod 4$,

(c) Distinct (i.e., not associates) irreducibles $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$, where $a^2 + b^2 = p$ is a prime in $\mathbb{Z}$ such that $p \equiv 1 \bmod 4$. We shall call these pair of irreducibles conjugates.

Theorem 1. *A positive integer n can be written as a sum of two integer squares if and only if it has an even number of factors of primes q, where $q \equiv 3 \bmod 4$. Moreover if we factor n into primes:*

$$n = 2^k {p_1}^{c_1} \cdots {p_r}^{c_r} {q_1}^{d_1} \cdots {q_s}^{d_s},$$

where the p_is are distinct odd primes with $p_i \equiv 1 \bmod 4$ and the q_js are distinct odd primes with $q_j \equiv 3 \bmod 4$, then the number of representations of n as a sum of squares is

$$4(c_1 + 1) \cdots (c_r + 1).$$