JOSEPH OKONOBOH
Mathematics
Cal State Long Beach

MATH 444, Spring 2015
Section 1 (5562)
PROJECT, DUE: 2015, MAY 04

Proposition 1.

1. A prime p can be written as a sum of two integer squares if and only if $p = 2$ or $p \equiv 1 \mod 4$.

2. The irreducibles in $\mathbb{Z}[i]$ are:

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

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

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

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

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

Proof. Suppose first that n is an integer that has an even number of factors of primes p, where $p \equiv 3 \mod 4$. Thus we can write n as a product of primes

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

where $p_1, \ldots, p_r$ are distinct primes congruent 1 mod 4 and $q_1, \ldots, q_s$ are distinct primes congruent 3 mod 4. By Proposition 1, there exist integers a_i and b_i such that ${a_i}^2 + {b_i}^2 = {p_i}^2$ for $i = 1, \ldots, r$. Let

$$X = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}^k \begin{pmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{pmatrix}^{c_1} \cdots \begin{pmatrix} a_r & b_r \\ -b_r & a_r \end{pmatrix}^{c_r} \begin{pmatrix} q_1 & 0 \\ 0 & q_1 \end{pmatrix}^{d_1} \cdots \begin{pmatrix} q_s & 0 \\ 0 & q_s \end{pmatrix}^{d_s}.$$

Notice that $X \in \mathbb{Z}[i]$ and $\det(X) = n$, so that n is the sum of two integer squares.