JOSEPH OKONOBOH/ KAVEH DADBIN
MATHEMATICS
CAL STATE LONG BEACH

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 $q \equiv 3$ 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. Let n be a positive integer. Since $\mathbb{Z}$ is a UFD, we can write

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

where $p_1, \ldots, p_r$ are distinct primes congruent to 1 modulo 4 and $q_1, \ldots, q_s$ are distinct primes congruent to 3 modulo 4. Suppose first that n has an even number of factors of primes q, where $q \equiv 3 \bmod 4$. That is, $d_1, \ldots, d_s$ are even. By Proposition 1, there exist integers a_i and b_i such that ${a_i}^2 + {b_i}^2 = p_i$ for $i = 1, \ldots, r$. Let

$$X = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}^k \begin{pmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{pmatrix}^{c_1} \cdots \begin{pmatrix} a_r & b_r \\ -b_r & a_r \end{pmatrix}^{c_r} \begin{pmatrix} q_1 & 0 \\ 0 & q_1 \end{pmatrix}^{d_1/2} \cdots \begin{pmatrix} q_s & 0 \\ 0 & q_s \end{pmatrix}^{d_s/2}.$$

Notice that $X \in \mathbb{Z}[i]$ so that $X = \begin{pmatrix} x & y \\ -y & x \end{pmatrix}$ and $x^2 + y^2 = \det(X) = n$, so that n is the sum of two integer squares. Conversely suppose that $n = a^2 + b^2$. Let $B = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$. Since

$\mathbb{Z}[i]$ is a UFD we have the following factorization of B (up to units) into irreducibles from Proposition 1:

$$B = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}^u {A_1}^{e_1} {A_1'}^{e_1'} \cdots {A_m}^{e_m} {A_m}^{e_m'} {C_1}^{f_1} \cdots {C_t}^{f_t},$$

where the A_i and A_i' are conjugate irreducibles, the determinant of A_i (which is equal to the determinant of A_i') is a prime congruent to 1 modulo 4, and the determinant of C_j is the square of a prime such that this prime is congruent to 3 modulo 4. Let

$$\det(A_i) = \pi_i \text{ and } \det(C_j) = {\alpha_j}^2.$$

Thus it follows that

$$n = a^2 + b^2 = \det(B) = 2^u {\pi_1}^{e_1+e_1'} \cdots {\pi_m}^{e_m+e_m'} {\alpha_1}^{2f_1} \cdots {\alpha_t}^{2f_t}.$$

The above equality

$$n = 2^u {\pi_1}^{e_1} \cdots {\pi_m}^{e_m} {\alpha_1}^{2f_1} \cdots {\alpha_t}^{2f_t}$$

gives us a factorization of n into primes and it is clear that there are an even number of prime factors q of n such that $q \equiv 3 \bmod 4$. To complete the proof, observe the prime factorizations of n:

$$2^k {p_1}^{c_1} \cdots {p_r}^{c_r} {q_1}^{d_1} \cdots {q_s}^{d_s} \text{ and } 2^u {\pi_1}^{e_1+e_1'} \cdots {\pi_m}^{e_m+e_m'} {\alpha_1}^{2f_1} \cdots {\alpha_t}^{2f_t}.$$

Since prime factorizations are unique (up to order and units) in $\mathbb{Z}$, it follows that $r = m$, $s = t$, and $u = k$. Also we can assume without loss that $p_i = \pi_i$, $q_j = \alpha_j$, and $c_i = e_i + e_i'$, $\alpha_j = q_j$, so that $f_j = d_j/2$. To complete the proof, notice from the equation

$$c_i = e_i + e_i'$$

that since e_i can take on values $0, \ldots, c_i$ it follows that there are $c_i + 1$ nonnegative pair of solutions for (e_i, e_i'). Thus there are at least $(c_1 + 1) \cdots (c_r + 1)$ choices for B. Since there are four units in $\mathbb{Z}[i]$, it follows that there are $4(c_1 + 1) \cdots (c_r + 1)$ choices for B.