Sum of Two Squares

Reading None

Theorem 1. Let $n \in \mathbb{Z}$ with $n > 0$. Then n is expressible as the sum of two squares if and only if every prime factor congruent to 3 modulo 4 occurs to an even power in the prime factorization of n.

Proof ($\Leftarrow$) Assume that every prime factor of n congruent to 3 modulo 4 occurs to an even power in the prime factorization of n. Then n can be written as $n = m^2 p_1 p_2 \dots p_r$ where $m \in \mathbb{Z}$ and $p_1, p_2, \dots, p_r$ are distinct prime numbers equal to 2 or equivalent to 1 modulo 4. Now, $m^2 = m^2 + 0^2$, so is expressible as the sum of two squares, and each p_1 is also expressible as the sum of two squares by the theorem labeled Primes as Sums of Squares. Thus, by the first theorem of the day, n is expressible as the sum of two squares.

($\Rightarrow$) Assume that p is an odd prime number and that $p^{2i+1}, i \in \mathbb{Z}$ occurs in the prime factorization of n. We will show that $p \equiv 1 \pmod 4$. Since n is expressible as the sum of two squares of integers, there exist $x, y \in \mathbb{Z}$ such that $n = x^2 + y^2$. Let $(x, y) = d, a = \dfrac{x}{d}, b = \dfrac{y}{d}$ and $m = \dfrac{n}{d^2}$. Then $(a, b) = 1$ and $a^2 + b^2 = m$. Let $p^j, j \in \mathbb{Z}$ be the largest power of p dividing d. Then $p^{(2i-1)-2j} \mid m$; since $(2i + 1) - 2j) \geq 1$, we have $p \mid m$. Now, $p \nmid a$ since $(a, b) = 1$. Thus, there exists $z \in \mathbb{Z}$ such that $az \equiv b \pmod p$. Then $m = a^2 + b^2 \equiv a^2 + (az)^2 \equiv a^2(1 + z^2) \pmod p$.

Since $p \mid m$, we have

$$a^2(1 + z^2) \equiv 0 \pmod p$$

or $p \mid a^2(1 + z^2)$ or $z \equiv -1 \pmod p$. Thus, -1 is a quadratic residue modulo p, so $p \equiv 1 \pmod 4$. By contrapositive, any prime factor congruent to 3 modulo 4 occurs to an even power in the prime factorization of n as desired.

■

Learning outcomes:
Author(s): Claire Merriman