Sums of squares

Reading None

The first result will prove which primes can be written as the sum of two squares. Note $1^2 + 1^2 = 2$, and if a is a positive integer such that $a \equiv 3 \pmod 4$, then a cannot be written as the sum of two squares.

Proposition 1. Let $m, n \in \mathbb{Z}$ with $m, n > 0$. If m and n can be written as the sums of two squares of integers, then mn can be written as the sum of two squares of integers.

Proof Let $m, n \in \mathbb{Z}$ with $m, n > 0$ and assume that there exists $a, b, c, d \in \mathbb{Z}$ such that $m = a^2 + b^2$ and $n = c^2 + d^2$. Then

$$\begin{aligned} mn = (a^2 + b^2)(c^2 + d^2) &= a^2c^2 + b^2c^2 + a^2d^2 + b^2d^2 \\ &= a^2c^2 + 2abcd + b^2d^2 + a^2d^2 - 2abcd + b^2c^2 \\ &= (ac + bd)^2 + (ad - bc)^2. \end{aligned}$$

■

We need two lemmas to prove

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.

Lemma 1. If p is a prime such that $p \equiv 1 \pmod 4$, then there are integers x, y such that $x^2 + y^2 = kp$ for some $k \in \mathbb{Z}$ with $0 < k < p$.

Proof Since $p \equiv 1 \pmod 4$, we have that $\left(\frac{-1}{p}\right) = 1$. Thus, there exists $x \in \mathbb{Z}$ with $0 < x \leq \frac{p-1}{2}$ such that $x^2 \equiv -1 \pmod p$. Then, $p \mid x^2 + 1$, and we have that $x^2 + 1 = kp$ for some $k \in \mathbb{Z}$. Thus, we found x and $y = 1$. Since $x^2 + 1$ and p are positive, so is k. Also,

$$kp = x^2 + y^2 < \left(\frac{p}{2}\right)^2 + 1 < p^2$$

implies $k < p$. ■

Proposition 2. A prime p can be written as the sum of two squares if and only if $p = 2$ or $p \equiv 1 \pmod 4$.

Proof If $p \equiv 3 \pmod 4$, then p cannot be written as the sum of two squares. Since the squares modulo 4 are 0 and 1, the integers that can be written as a sum of two squares are congruent to $0^2 + 0^2 \equiv 0 \pmod 4$, $1^2 + 0^2 \equiv 1 \pmod 4$ or $1^2 + 1^2 \equiv 2 \pmod 4$, so no integer that is congruent to $3 \pmod 4$ can be written as the sum of two squares. Thus, if p can be written as the sum of two squares, $p \not\equiv 3 \pmod 4$. That is, $p = 2$ or $p \equiv 1 \pmod 4$.

We will prove the other direction with two cases. When $p = 2$, then $1^2 + 1^2 = 2$. It remains to show that every prime $p \equiv 1 \pmod 4$ can be written as the sum of two squares.

Let $p \equiv 1 \pmod 4$, and let m be the least integer such that there exists $x, y \in \mathbb{Z}$ with $x^2 + y^2 = mp$ and $0 < m < p$ as in the previous theorem. We show that $m = 1$. Assume, by way of contradiction, that $m > 1$. Let $a, b \in \mathbb{Z}$ such that

$$a \equiv x \pmod m, \quad \frac{-m}{2} < a \leq \frac{m}{2}$$

Learning outcomes:
Author(s): Claire Merriman

and

$$b \equiv y \pmod{m}, \quad \frac{-m}{2} < b \leq \frac{m}{2}.$$

Then

$$a^2 + b^2 \equiv x^2 + y^2 = mp \equiv 0 \pmod{m},$$

and so there exists $k \in \mathbb{Z}$ with $k > 0$ such that $a^2 + b^2 = km$. (Why?)

Now,

$$(a^2 + b^2)(x^2 + y^2) = (km)(mp) = km^2p.$$

By , $(a^2+b^2)(x^2+y^2) = (ax+by)^2 + (ay-bx)^2$, so $(ax+by)^2 + (ay-bx)^2 = km^2p$. Since $a \equiv x \pmod{m}$ and $b \equiv y \pmod{m}$,

$$ax + by \equiv x^2 + y^2 \equiv 0 \pmod{m}$$

and

$$ay - bx \equiv xy - yx \equiv 0 \pmod{m}$$

so $\dfrac{ax+by}{m}, \dfrac{ay-bx}{m} \in \mathbb{Z}$ and

$$\left(\frac{ax+by}{m}\right)^2 + \left(\frac{ay-bx}{m}\right)^2 = \frac{km^2p}{m^2} = kp.$$

Now, $\dfrac{-m}{2} < a \leq \dfrac{m}{2}$ and $\dfrac{-m}{2} < b \leq \dfrac{m}{2}$ imply that $a^2 \leq \dfrac{m^2}{4}$ and $b^2 \leq \dfrac{m^2}{4}$. Thus, $km = a^2 + b^2 \leq \dfrac{m^2}{2}$. Thus, $k \leq \dfrac{m}{2} < m$, but this contradicts that m is the smallest such integer.

Thus, $m = 1$ and p can be written as the sum of two squares of integers. ■