April 10–Sums of squares

We prove that all integers can be written as the sum of four squares.

Sum of three squares

We finish out the sums of squares section by classifying which integers can be written as the sum of three squares and sum of four squares. These cases are more difficult than the sum of two squares since there is no formula analogous to the April 8 participation assignment.

Theorem 1 (Sum of three squares necessary condition)**.** Let $m, n \in \mathbb{Z}$ with $m, n \geq 0$. If $N = 4^m(8n+7)$, then N can not be written as the sum of 3 squares.

Proof We start by proving the $m = 0$ case. In order to get a contradiction, assume that $N = 8n+7$ can be written as the sum of three squares. Thus, there exists $x, y, z \in \mathbb{Z}$ such that

$$8n + 7 = x^2 + y^2 + z^2.$$

Now, $8n + 7 \equiv 7 \pmod 8$ and $x^2 + y^2 + z^2 \not\equiv 7 \pmod 8$ (by participation assignment), which gives the contradiction we are looking for.

Now we assume $m > 0$. and again assume $N = 4^m(8n+7)$ can be written as the sum of three squares. As before, there exist $x, y, z \in \mathbb{Z}$ such that

$$4^m(8n+7) = x^2 + y^2 + z^2$$

and x, y, z are even (by participation assignment). So there exists x', y' and z' such that $x = 2x', y = 2y'$, and $z = 2z'$. Substituting into our definition of N, we get

$$4^{m-1}(8n+7) = (x')^2 + (y')^2 + (z')^2.$$

Repeating this process $m-1$ times, we find $8n+7$ is expressible as a sum of three squares, a contradiction. Thus, $N = 4^m(8n+7)$ cannot be written as the sum of three squares. ■

Now, the converse is true. Legendre proved this in 1798, but is much harder to prove, due to the lack of formula like the one from April 8 participation assignment. Note that any integer that cannot be written as the sum of three squares cannot be written as the sum of two squares.

Learning outcomes:
Author(s):

Example 1. Determine whether 1584 is expressible as the sum of three squares.

The highest power of 4 that divides 1584 evenly is 16, leaving $99 \equiv 3 \pmod 8$). Thus, 1584 can be written as the sum of three squares:

Multiple Choice:

(a) True ✓

(b) False

(c) Not enough information

Since this also allows us to factor 1584, we also know 1584 can be written as the sum of two squares:

Multiple Choice:

(a) True

(b) False ✓

(c) Not enough information

Sum of four squares

We now prove that all positive integers can be written as the sum of four squares. The new few results are similar to the proof of the sum of two squares. Some of these calculations are even more involved, but still use multiplication and factoring. I will upload a scan of the sums of squares section from *Elementary Number Theory* by James K. Strayer. All of the missing calculations are expanding and refactoring polynomial expression.

Theorem 2 (Euler)**.** Let $n_1, n_2 \in \mathbb{Z}$ with $n_1, n_2 > 0$. If n_1 and n_2 are expressible as the sum of four squares, then so is $n_1 n_2$.

Proof Let $a, b, c, d, w, x, y, u \in \mathbb{Z}$ such that

$$n_1 = a^2 + b^2 + c^2 + d^2$$

and

$$n_1 = w^2 + x^2 + y^2 + z^2.$$

Then

$$n_1 n_2 = (aw+bx+cy+dz)^2+(-ax+bw-cz+dy)^2+(-ay+bz+cw-dx)^2+(-az-by+cx+dw)^2$$

as desired. ■

Theorem 3 (Also Euler)**.** If p is an odd prime number, then there exist $x, y \in \mathbb{Z}$ such that $x^2 + y^2 + 1 = kp$ for some $k \in \mathbb{Z}$ with $0 < k < p$.

Proof We consider two cases.

Case 1: $p \equiv 1 \pmod 4$. Then $\left(\frac{-1}{p}\right) = 1$, so 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 $y = 0$. Since $x^2 + 1$ and p are positive, so is k. Also,

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

implies $k < p$.

Case 2: $p \equiv 3 \pmod 4$. Let a be the least positive quadratic nonresidue modulo p. Note that $a \geq 2$. Then

$$\left(\frac{-a}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{a}{p}\right) = (-1)(-1) = 1$$

and so there exists $x \in \mathbb{Z}$ with $0 < x \leq \frac{p-1}{2}$ such that $x^2 \equiv -a \pmod p$. Now, $a - 1$ is positive and less than a, then $a - 1$ is a quadratic residue modulo p. Thus, there exists $y \in \mathbb{Z}$ with $0 < y \leq \frac{p-1}{2}$ such that $y^2 \equiv a - 1 \pmod p$. Thus,

$$x^2 + y^2 + 1 \equiv (-a) + (a - 1) + 1 \equiv 0 \pmod p$$

or, equivalently, $x^2 + y^2 + 1 = kp$ for some $k \in \mathbb{Z}$. Again, $k > 0$. Furthermore,

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

implies $k < p$. ■

We will prove that every prime number can be written as the sum of four squares.

Theorem 4 (Lagrange, 1770)**.** All prime numbers can be written as the sum of four squares.

Proof When $p = 2 = 1^2 + 1^2 + 0^2 + 0^2$, we are done. In fact, we can also writes a prime p where $p \equiv 1 \pmod 4$ as $p = x^2 + y^2 + 0^2 + 0^2$, but the following method works for all odd primes.

Let m be the least positive integer where $x^2 + y^2 + z^2 + w^2 = mp$ and $0 < m < p$. We want to show that $m = 1$. To get a contradiction, assume $m > 1$. We consider two cases.

Case 1: m even. There are three posibilities: w, x, y, z are all even; w, x, y, z are all odd; two of w, x, y, z are odd and the other two are even. In all three cases, we can assume $w \equiv x \pmod 2$ and $y \equiv z \pmod 2$. Then $\frac{w+x}{2}, \frac{w-x}{2}, \frac{y+z}{2}, \frac{y-z}{2}$ are integers and

$$\left(\frac{w+x}{2}\right)^2 + \left(\frac{w-x}{2}\right)^2 + \left(\frac{y+z}{2}\right)^2 + \left(\frac{y-z}{2}\right)^2 = \frac{mp}{2}$$

which contradicts the fact that m is minimal.

Case 2: m is odd.

Then $m \geq 3$. Let $a, b, c, d \in \mathbb{Z}$ such that

$$\begin{aligned} a \equiv w &\pmod m, \frac{-m}{2} < a < \frac{m}{2} \\ b \equiv x &\pmod m, \frac{-m}{2} < b < \frac{m}{2} \\ c \equiv y &\pmod m, \frac{-m}{2} < c < \frac{m}{2} \\ d \equiv z &\pmod m, \frac{-m}{2} < d < \frac{m}{2}. \end{aligned}$$

Then $a^2 + b^2 + c^2 + d^2 \equiv w^2 + x^2 + y^2 + z^2 \equiv mp \equiv 0 \pmod m$ and so there exists $k \in \mathbb{Z}$ with $k > 0$ such that $a^2 + b^2 + c^2 + d^2 = km$. Now

$$(a^2 + b^2 + c^2 + d^2)(w^2 + x^2 + y^2 + z^2) = (km)(mp) = km^2p.$$

By theorem 2 from today, we can rewrite $a^2 + b^2 + c^2 + d^2)(w^2 + x^2 + y^2 + z^2)$ as the sum of four squares $(aw + bx + cy + dz)^2 + (-ax + bw - cz + dy)^2 + (-ay + bz + cw - dx)^2 + (-az - by + cx + dw)^2 = km^2p$. Since $a \equiv w \pmod m, b \equiv x \pmod m, c \equiv y \pmod m, \frac{-m}{2} < c < \frac{m}{2}, d \equiv z \pmod m, \frac{-m}{2} < d < \frac{m}{2}$, we have

$$\begin{aligned} aw + bx + cy + dz &\equiv w^2 + x^2 + y^2 + z^2 \equiv 0 \pmod m \\ -ax + bw - cz + dy &\equiv -wx + xw - yz + zy \equiv 0 \pmod m \\ -ay + bz + cw - dx &\equiv -wy + yw + xz - zx \equiv 0 \pmod m \\ -az - by + cx + dw &\equiv -wx + zw - xy + yx \equiv 0 \pmod m \end{aligned}$$

Let $W = \frac{w^2 + x^2 + y^2 + z^2}{m}, X = \frac{-wx + xw - yz + zy}{m}, Y = \frac{-wy + yw + xz - zx}{m}, Z = \frac{-wx + zw - xy + yx}{m}$. Then $W^2 + X^2 + Y^2 + Z^2 = \frac{km^2p}{m^2} = kp$. Since $\frac{-m}{2} < a, b, c, d < \frac{m}{2}$, then $a^2, b^2, c^2, d^2 < \frac{m^2}{4}$. Thus,

$$km = a^2 + b^2 + c^2 + d^2 < \frac{4m^2}{4}$$

and $k < m$. This contradicts that m is the smallest such integers.

Thus, $m = 1, w^2 + x^2 + y^2 + z^2 = p$. ■

Theorem 5 (Lagrange)**.** All positive integers can be written as the sum of four squares.

Proof Let $n \in \mathbb{Z}$ with $n > 1$. If $n = 1 = 1^2 + 0^2 + 0^2 + 0^2$. If $n > 1$, then n is the product of primes by the Fundamental Theorem of Arithmetic. By the previous theorem, every prime number can be written as the sum of four squares. By theorem 2 from today, n is can be written by the sum of four squares. ■

We finish this section with a few famous problems.

Example 2 (Waring's Problem, 1770)**.** Let $k \in \mathbb{Z}$ with $k > 0$. Does there exist a minimum integer $g(k)$ such that every positive integer can be written as the sum of at most $g(k)$ nonnegative integers to the k^{th} power?

For example, $g(1) = 1$. Today we showed that $g(2) = 4$. The next step would be to find if $g(3)$ exists and what it equals.

Theorem 6 (Hilbert, 1906)**.** Let $k \in \mathbb{Z}$ with $k > 0$. There exists a minimal integer $g(k)$ such that every positive integer can be written as the sum of at most $g(k)$ nonnegative integers to the k^{th} power.

The proof of Hilbert's theorem does not provide a formula for $g(k)$, merely proves it exists. Numerical evidence suggests $g(k) = \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor + 2^k - 2$. It's been proven that there are only finitely many (or 0) k where the formula does not hold, and the formula holds when $k \leq 471,600,000$. Thus, $g(3) = 9, g(4) = 19$, and $g(5) = 37$. Proofs of these facts come from analytic number theory.