NYC Math Team 1/15/16

Lagrange's Four Squares Theorem

1. If 23 is written as the sum of the squares of 4 positive integers (not necessarily different), what is the largest square in this sum? *NYML 2015 2-1*

2. How many ways can you express 73 as the sum of the squares of 4 positive integers?

3. Are the following statements true or false? Justify your answer.
   - "All positive integers can be written as the sum of the squares of 2 integers."
     False: 3 cannot be written as the sum of 2 squares.
   - "All positive integers can be written as the sum of the squares of 3 integers."
     False: 7 cannot be written as the sum of 3 squares

     Interesting Note » Legendre proved that all integers can be written as the sum of 3 squares if and only if they are not of the form $4^k(8m+7)$ for integers k and m

What about writing them as the sum of the squares of 4 integers? It turns out this is possible!

Lagrange's Four Squares Theorem
Every positive integer is the sum of the squares of four integers.

4. Verify the theorem for the first ten integers.

History
This theorem has been known since at least the 3rd Century AD. Diophantus, the Greek mathematician was familiar with it. Much later, Fermat wrote that he had a proof, though it was never published. Lagrange, however, published the first solution in 1770.

In order to prove this theorem, we need a few tools

Theorem 1
If m and n are positive integers that are each the sum of four squares, then their product mn is also the sum of four squares.

Proof

Let $m = a^2 + b^2 + c^2 + d^2$ and $n = e^2 + f^2 + g^2 + h^2$

Consider the expression:

$(ae + bf + cg + dh)^2 + (af - be + ch - dg)^2 + (ag - bh - ce + df)^2 + (ah + bg - cf - de)^2$

Expand the expression completely and factor the result.

$a^2e^2 + b^2f^2 + c^2g^2 + d^2h^2 + 2abef + 2aceg + 2adeh + 2bcfg + 2bdfh + 2cdgh$

$$a^2f^2 + b^2e^2 + c^2h^2 + d^2g^2 - 2abef + 2acfh - 2adfg - 2bceh + 2bdeg - 2cdgh$$
$$a^2g^2 + b^2h^2 + c^2e^2 + d^2f^2 - 2abgh - 2aceg - 2adfg + 2bceh - 2bdfh - 2cdef$$
$$a^2h^2 + b^2g^2 + c^2f^2 + d^2e^2 + 2abgh - 2acfh - 2adeh - 2bcfg - 2bdeg + 2cdef$$
$$=$$
$$a^2e^2 + a^2f^2 + a^2g^2 + a^2h^2 + b^2e^2 + b^2f^2 + b^2g^2 + b^2h^2 + c^2e^2 + c^2f^2 + c^2g^2 + c^2h^2 + d^2e^2 + d^2f^2 + d^2g^2 + d^2h^2$$
$$= (a^2 + b^2 + c^2 + d^2)(e^2 + f^2 + g^2 + h^2)$$ ■

Why does this identity prove the theorem?

Euler's Four-Square Identity

$$(a^2 + b^2 + c^2 + d^2)(e^2 + f^2 + g^2 + h^2)$$
$$= (ae + bf + cg + dh)^2 + (af - be + ch - dg)^2 + (ag - bh - ce + df)^2 + (ah + bg - cf - de)^2$$

5. Use the identity we just proved to show that 70 can be written as a sum of 4 squares.

A *lemma* is a "helping theorem" that we prove and use as a stepping stone to prove a larger theorem.

Lemma 1

If $2m$ is a sum of two squares, then so is m.

Proof

Let $2m = a^2 + b^2$

Then a and b are either both even or both odd, making $\frac{a+b}{2}$ and $\frac{a-b}{2}$ both integers

$m = \left(\frac{a+b}{2}\right)^2 + \left(\frac{a-b}{2}\right)^2 = \frac{2a^2+2b^2}{4} = \frac{a^2+b^2}{2}$ ■

Lemma 2

If p is an odd prime, then there exists an integer $k < p$ such that kp can be written as the sum of four squares of integers.

In other words, there exist integers a, b, c, d such that:

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

Proof

Let $p = 2n + 1,\ n \in \mathbb{N}$

We will show that there exist $a, b \in \mathbb{Z}$ such that $a^2 + b^2 + 1 \equiv 0\ (mod\ p)$ where $0 \le a \le n$ and $0 \le b \le n$

Consider the set $S = \left\{0^2, 1^2, 2^2, \cdots, n^2\right\} = \{0, 1, 4, 9, \cdots, n^2\}$

How many elements are there? $n + 1$

Can two elements of S be congruent modulo p? No, because if $x^2, y^2 \in S$ and $x^2 \equiv y^2 (mod\ p)$, then $x \equiv y\ (mod\ p)$

Consider the set $T = \left\{-0^2-1, -1^2-1, -2^2-1, \cdots, -n^2-1\right\}$

$$T = \left\{-1, -2, -5, -10, \cdots, -n^2-1\right\}$$

How many elements in T? n

Similarly, no two of elements of T are congruent modulo p.

Clearly, $S \cap T = \varnothing$

How many distinct elements in $S \cup T$? $2n+2 = p+1$

So, by the pigeonhole principle, if we have $p+1$ elements, there must be two integers in $S \cup T$ that are congruent modulo p, where one is in S and one is in T.

$\exists\, a^2 \in S$ and $\exists\, -1-b^2 \in S$ such that $a^2 \equiv -1-b^2\ (mod\ p)$

$\therefore a^2+b^2+1 \equiv 0\ (mod\ p)$

This implies $a^2+b^2+1^2+0^2 = kp$ for some integer k

$a^2+b^2+1 \le 2n^2+1 < (2n+1)^2 = p^2$

Therefore, $kp < p^2$ and $k < p$ ■

Theorem 2

Any prime p can be written as the sum of four squares of integers.

There exist integers a, b, c, d such that $p = a^2+b^2+c^2+d^2$.

Proof

If $p = 2$, then $p = 1^2+1^2+0^2+0^2$

Suppose p is an odd prime and let m be the smallest integer that can be written as the sum of four squares: $a^2+b^2+c^2+d^2 = mp$, where $m < p$ (there exists such an m by Lemma 2)

We need to show that $m = 1$

Case 1: Suppose $m > 1$ and m is even, then we have three possibilities for a, b, c, d (all are even, all odd, or two even, two odd)

Assume the a and b have the same parity and c and d also do.

$a \equiv b\ (mod\ 2)$ and $c \equiv d$ (mod 2)

$a^2+b^2 = 2i$ and $c^2+d^2 = 2j$

$a^2+b^2+c^2+d^2 = 2i+2j = mp$

By Lemma 1, $i+j = \left(\frac{a-b}{2}\right)^2+\left(\frac{a+b}{2}\right)^2+\left(\frac{c-d}{2}\right)^2+\left(\frac{c+d}{2}\right)^2 = \left(\frac{m}{2}\right)p$

But now we have found a number smaller than m that, when multiplied by p will result in the sum of four squares. This contradicts the fact that m was the smallest. Our assumption must have been false, making $m = 1$

Case 2: Suppose $m > 1$ and m is odd.

Let q, r, s, t be integers such that $a \equiv q \pmod m,\ b \equiv r \pmod m,\ c \equiv s \pmod m,\ d \equiv t \pmod m$ and $a, b, c, d \in \left(-\frac{m}{2}, \frac{m}{2}\right)$

How many integers are in this interval? Each one corresponds to one of the m residues modulo m (For example, consider $m = 9$)

$a^2 + b^2 + c^2 + d^2 \equiv q^2 + r^2 + s^2 + t^2 \equiv 0 \pmod m$

Therefore $q^2 + r^2 + s^2 + t^2 = km$ for some $k \in \mathbb{Z}$

$q^2 + r^2 + s^2 + t^2 \in [0, 4\left(\frac{m}{2}\right)^2)$ or $q^2 + r^2 + s^2 + t^2 \in [0, m^2)$

This means $km < m^2$ and $k < m$ (remember $m > 1$)

If $k = 0$, then $q = r = s = t = 0$ making $a \equiv b \equiv c \equiv d \equiv 0 \pmod m$

$m^2 | mp$, but this is impossible because $m \in (1, p)$ and m and p clearly have no common factors.

Therefore, we can conclude $k > 0$

Consider $\left(a^2 + b^2 + c^2 + d^2\right)\left(q^2 + r^2 + s^2 + t^2\right) = mp \cdot km = m^2 kp$

By Euler's Four-Square Identity, we get

$(aq + br + cs + dt)^2 + (ar - bq + ct - ds)^2 + (as - bt - cq + dr)^2 + (at + bs - cr - dq)^2 = m^2 kp$

Each of the four terms being squared is divisible by m, because:

$aq + br + cs + dt \equiv a^2 + b^2 + c^2 + d^2 \equiv 0 \pmod m$

$ar - bq + ct - ds \equiv ab - ab + cd - cd \equiv 0 \pmod m$

$as - bt - cq + dr \equiv ac - bd - ac - bd \equiv 0 \pmod m$

$at + bs - cr - dq \equiv ad + bc - bc - ad \equiv 0 \pmod m$

Since they are each divisible by m, dividing each by m will give us four integers, w, x, y, z

$w = \frac{aq+br+cs+dt}{m},\ x = \frac{ar-bq+ct-ds}{m},\ y = \frac{as-bt-cq+dr}{m},\ z = \frac{at+bs-cr-dq}{m}$

And we have that $w^2 + x^2 + y^2 + z^2 = \frac{m^2 kp}{m^2} = kp$

But since $k < m$ we have found a smaller integer multiple of p that can be written as the sum of four squares. This contradicts the fact that m was the smallest such integer. Our assumption must have been false, making $m = 1$ ■

Proof of Lagrange's Four Squares Theorem

Suppose that n is a positive integer. If $n = 1$, we can write it as $1^2 + 0^2 + 0^2 + 0^2$. By the fundamental theorem of arithmetic, every $n > 1$ can be written as the product of prime numbers. By the Theorem 2, every prime can be written as the sum of four squares. By Theorem 1, if we have two numbers that are the sums of four squares, then their product is the sum of four squares. Therefore, the product of the prime factors of n will be the sum of four squares. ■

Sources

- Wikipedia, "Lagrange's four-square theorem."
- Rosen, *Elementary Number Theory and its Applications*, 4th Ed., p.499-501
- http://planetmath.org/proofoflagrangesfoursquaretheorem
- http://www.maths.lancs.ac.uk/~jameson/foursquares.pdf
- http://www.personal.psu.edu/rcv4/Foursq.pdf