Lagrange's Four-Square Theorem and Generalization

Brandon Chan, Stephanie Yao

Ross Mathematics Program

July 24, 2024

Table of Contents

Theorem

Theorem

The theorem, given any integer n, there exists four numbers $a, b, c, d \in \mathbb{Z}$

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

Lemma 1

Lemma

If p is an odd prime, then $a^2 + b^2 + 1 = kp$ for some integers a, b, k with $0 < k < p$.

Lemma 1

Lemma

If p is an odd prime, then $a^2 + b^2 + 1 = kp$ for some integers a, b, k with $0 < k < p$.

Let $p = 2n + 1$. We first take a set $A; = \{a^2 \mid 0 \leq a \leq n\}$, and $B := \{-b^2 - 1 \mid 0 \leq b \leq n\}$.

Lemma 1

Lemma

If p is an odd prime, then $a^2 + b^2 + 1 = kp$ for some integers a, b, k with $0 < k < p$.

Let $p = 2n + 1$. We first take a set $A; = \{a^2 \mid 0 \leq a \leq n\}$, and $B := \{-b^2 - 1 \mid 0 \leq b \leq n\}$.
In particular, we realize that $|A \cup B| = 2n + 2$. Therefore, there exists two elements $x, y \in A \cup B$ such that $x \equiv y \pmod{p}$. In particular, x and y both most come from A and B separately. Thus, the lemma is proved.

Lemma 2

Lemma

For any integers a, b, c, d, w, x, y, z,

$$\begin{aligned}&(a^2+b^2+c^2+d^2)(w^2+x^2+y^2+z^2)\\ =&(aw+bx+cy+dz)^2+(ax-bw-cz+dy)^2\\ &+(ay+bz-cw-dx)^2+(az-by+cx-dw)^2.\end{aligned}$$

Lemma 2

Lemma

For any integers a, b, c, d, w, x, y, z,

$$\begin{aligned}&(a^2+b^2+c^2+d^2)(w^2+x^2+y^2+z^2)\\ =&(aw+bx+cy+dz)^2+(ax-bw-cz+dy)^2\\ &+(ay+bz-cw-dx)^2+(az-by+cx-dw)^2.\end{aligned}$$

We are not going to give the gory details here for the algebra. However, one might note that this is the norm for the quaternions, also known as $\mathbb{H}$.

Lemma 3

Lemma

Assume that $2m$ is the sum of two squares $x^2 + y^2$. Then, m is the sum of two squares.

Lemma 3

Lemma

Assume that $2m$ is the sum of two squares $x^2 + y^2$. Then, m is the sum of two squares.

We note that both x, y are of the same parity. Therefore, we can take $\left(\frac{x+y}{2}\right)^2 + \left(\frac{x-y}{2}\right)^2$.

Main Proof

Theorem

The theorem, given any integer n, there exists four numbers $a, b, c, d \in \mathbb{Z}$

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

Because of lemma 2, it suffices to prove the statement for all primes p, instead of a general number n. We also know that because of Lemma 1, we have

$$a^2 + b^2 + 1^2 + 0^2 = mp$$

for some numbers $0 < m < p$.

Motivation

Then, the idea on trying to get $k = 1$, so that we can prove the theorem. To do this, we show that there is a number $0 < n < m$, such that there exists $a, b, c, d \in \mathbb{Z}$, such that

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

We define the numbers as follows:

$$
\begin{aligned}
w &\equiv a \pmod{m}\\
x &\equiv b \pmod{m}\\
y &\equiv c \pmod{m}\\
z &\equiv d \pmod{m}
\end{aligned}
$$

for $\frac{-m}{2} < w, x, y, z < \frac{m}{2}$. Our main claim will be that the four integers obtained from lemma 1's $\frac{(a^2+b^2+c^2+d^2)(w^2+x^2+y^2+z^2)}{m}$ are the numbers that have this property.

We note the fact that $w^2 + x^2 + y^2 + z^2 \equiv 0 \pmod{m}$ and $w^2 + x^2 + y^2 + z^2 < 4\frac{m^2}{4} = m^2$, because of modulo reasons. Therefore, $w^2 + x^2 + y^2 + z^2 = mn$ for some integer $0 \leq n < m$.
In particular, we realize that $n \neq 0$, because this would mean that $m \mid a, b, c, d$, which shows that $a^2 + b^2 + c^2 + d^2$ can be represented as $m^2 q = mp$, showing that $m \mid p$, implying that $m = 1$, since $0 < m < p$.

Putting it All Together

We notice that $(a^2+b^2+c^2+d^2)(w^2+x^2+y^2+z^2) = pm^2n$. Additionally, in the notation of Lemma 1, we have that

$$\begin{aligned}(aw+bx+cy+dz) &\equiv (ax-bw-cz+dy)\\ &\equiv (ay+bz-cw-dx)\\ &\equiv (az-by+cx-dw) \pmod{m}\end{aligned}$$

Putting it All Together

We notice that $(a^2 + b^2 + c^2 + d^2)(w^2 + x^2 + y^2 + z^2) = pm^2 n$.
Additionally, in the notation of Lemma 1, we have that

$$\begin{aligned}(aw + bx + cy + dz) \equiv& (ax - bw - cz + dy)\\ \equiv& (ay + bz - cw - dx)\\ \equiv& (az - by + cx - dw) \pmod{m}\end{aligned}$$

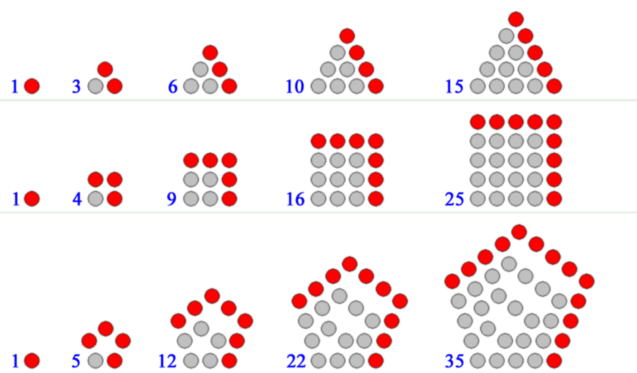
Thus, we can divide the terms by m, and get four integers that when squared and then summed, add up to pn. Hence, repeating this argument, yields the claim.

Brief Intro

Definition

A polygonal number is a number that counts dots arranged in the shape of a regular polygon.

Example



Generalization – Fermat's n-gonal Number Theorem

We only state the theorem.

Theorem

Every integer can be represented as the sum of at most n n-gonal numbers.

Reference

- Fermat Polygonal Number Theorem
- Proof of Lagraunge's Four Square Theorem
- MELVYN B. NATHANSON, A SHORT PROOF OF CAUCHY'S POLYGONAL NUMBER THEOREM