NUMBER THEORY LECTURE, APRIL 21: LAGRANGE'S FOUR SQUARE THEOREM

Larry Rolen

LAGRANGE'S FOUR SQUARE THEOREM

THEOREM (LAGRANGE)

All positive integers are the sum of four squares.

LAGRANGE'S FOUR SQUARE THEOREM

THEOREM (LAGRANGE)

All positive integers are the sum of four squares.

LEMMA

If m, n *are sums of 4 squares, then so is* $m \cdot n$.

LAGRANGE'S FOUR SQUARE THEOREM

THEOREM (LAGRANGE)

All positive integers are the sum of four squares.

LEMMA

If m, n are sums of 4 squares, then so is $m \cdot n$.

PROOF.

$$m = a^2 + b^2 + c^2 + d^2, \quad n = e^2 + f^2 + g^2 + h^2$$

LAGRANGE'S FOUR SQUARE THEOREM

THEOREM (LAGRANGE)

All positive integers are the sum of four squares.

LEMMA

If m, n are sums of 4 squares, then so is $m \cdot n$.

PROOF.

$$\begin{aligned} m =& a^2 + b^2 + c^2 + d^2, \quad n = e^2 + f^2 + g^2 + h^2 \\ \implies mn =& (ae + bd + cg + dh)^2 + (af - be + ch - dg)^2 \\ &+ (ag - bh - ce + df)^2 + (ah + bg - cf - de)^2. \end{aligned}$$

☐

LAGRANGE'S FOUR SQUARE THEOREM

THEOREM (LAGRANGE)

All positive integers are the sum of four squares.

LEMMA

If m, n are sums of 4 squares, then so is $m \cdot n$.

PROOF.

$$\begin{aligned} m =& a^2+b^2+c^2+d^2, \quad n = e^2+f^2+g^2+h^2 \\ \Longrightarrow \; mn =& (ae+bd+cg+dh)^2+(af-be+ch-dg)^2 \\ &+(ag-bh-ce+df)^2+(ah+bg-cf-de)^2. \end{aligned}$$

☐

- Thus, it suffices to show the theorem for odd primes p.

PRIMES ARE "ALMOST" SUMS OF FOUR SQUARES

PROPOSITION

If p is an odd prime, then there is a $0 < k < p$ for which $kp = x^2 + y^2 + z^2 + w^2$ is a sum of four squares.

PRIMES ARE "ALMOST" SUMS OF FOUR SQUARES

PROPOSITION

If p is an odd prime, then there is a $0 < k < p$ for which $kp = x^2 + y^2 + z^2 + w^2$ is a sum of four squares.

PROOF.

Consider

$$S := \{0^2, 1^2, \ldots, ((p-1)/2)^2\}, \quad T := -1 - S = \{-1 - j^2\}_{j=0}^{\frac{p-1}{2}}.$$

PRIMES ARE "ALMOST" SUMS OF FOUR SQUARES

PROPOSITION

If p is an odd prime, then there is a $0 < k < p$ for which $kp = x^2 + y^2 + z^2 + w^2$ is a sum of four squares.

PROOF.

Consider

$$S := \{0^2, 1^2, \ldots, ((p-1)/2)^2\}, \quad T := -1 - S = \{-1 - j^2\}_{j=0}^{\frac{p-1}{2}}.$$

All elts. of S (resp. T) are **distinct mod** p, as $x^2 \equiv y^2 \pmod{p} \implies x \equiv \pm y \pmod{p}$.

PRIMES ARE "ALMOST" SUMS OF FOUR SQUARES

PROPOSITION

If p is an odd prime, then there is a $0 < k < p$ for which $kp = x^2 + y^2 + z^2 + w^2$ is a sum of four squares.

PROOF.

Consider

$$S := \{0^2, 1^2, \ldots, ((p-1)/2)^2\}, \quad T := -1 - S = \{-1 - j^2\}_{j=0}^{\frac{p-1}{2}}.$$

All elts. of S (resp. T) are **distinct mod** p, as $x^2 \equiv y^2 \pmod{p} \implies x \equiv \pm y \pmod{p}$.There are $p+1$ integers in $S \cup T$, so there are two numbers in $S \cup T$ which are equivalent mod p.

PRIMES ARE "ALMOST" SUMS OF FOUR SQUARES

PROPOSITION

If p is an odd prime, then there is a $0 < k < p$ for which $kp = x^2 + y^2 + z^2 + w^2$ is a sum of four squares.

PROOF.

Consider

$$S := \{0^2, 1^2, \ldots, ((p-1)/2)^2\}, \quad T := -1 - S = \{-1 - j^2\}_{j=0}^{\frac{p-1}{2}}.$$

All elts. of S (resp. T) are **distinct mod** p, as $x^2 \equiv y^2 \pmod{p} \implies x \equiv \pm y \pmod{p}$.There are $p+1$ integers in $S \cup T$, so there are two numbers in $S \cup T$ which are equivalent mod p. Thus, some elt. of S is congruent to some elt. of T, say

$$x^2 \equiv -1 - y^2 \pmod{p}, \quad 0 \leq x, y \leq \frac{p-1}{2}.$$

PRIMES ARE "ALMOST" SUMS OF FOUR SQUARES (CONT.)

PROOF.

Thus, we have $x^2 + y^2 + 1 \equiv x^2 + y^2 + 1^2 + 0^2 \equiv 0 \pmod{p}$ and so

PRIMES ARE "ALMOST" SUMS OF FOUR SQUARES (CONT.)

PROOF.

Thus, we have $x^2 + y^2 + 1 \equiv x^2 + y^2 + 1^2 + 0^2 \equiv 0 \pmod{p}$ and so $kp = x^2 + y^2 + 1^2 + 0^2$ for some $0 < k$.

PRIMES ARE "ALMOST" SUMS OF FOUR SQUARES (CONT.)

PROOF.

Thus, we have $x^2+y^2+1 \equiv x^2+y^2+1^2+0^2 \equiv 0 \pmod{p}$ and so $kp = x^2+y^2+1^2+0^2$ for some $0 < k$. We bound k by:

$$kp = x^2+y^2+1^2+0^2 \leq 2 \cdot \left(\frac{p-1}{2}\right)^2 + 1 < p^2$$

PRIMES ARE "ALMOST" SUMS OF FOUR SQUARES (CONT.)

PROOF.

Thus, we have $x^2 + y^2 + 1 \equiv x^2 + y^2 + 1^2 + 0^2 \equiv 0 \pmod{p}$ and so $kp = x^2 + y^2 + 1^2 + 0^2$ for some $0 < k$. We bound k by:

$$kp = x^2 + y^2 + 1^2 + 0^2 \leq 2 \cdot \left(\frac{p-1}{2}\right)^2 + 1 < p^2 \implies k < p.$$

□

PROOF OF LAGRANGE'S THEOREM

- For a prime $p > 2$, let m be the smallest pos. int. such that $mp = x^2 + y^2 + z^2 + w^2$ has a solution in $\mathbb{Z}$.

PROOF OF LAGRANGE'S THEOREM

- For a prime $p > 2$, let m be the smallest pos. int. such that $mp = x^2 + y^2 + z^2 + w^2$ has a solution in $\mathbb{Z}$. WNTS: $m = 1$.

PROOF OF LAGRANGE'S THEOREM

- For a prime $p > 2$, let m be the smallest pos. int. such that $mp = x^2 + y^2 + z^2 + w^2$ has a solution in $\mathbb{Z}$. WNTS: $m = 1$.
- Assume for sake of contradiction $m > 1$, find a smaller m that works.

CASE 1: m IS EVEN

- If m is even, then

$$0 \equiv mp \equiv x^2 + y^2 + z^2 + w^2 \equiv x + y + z + w \pmod 2,$$

CASE 1: m IS EVEN

- If m is even, then

  $$0 \equiv mp \equiv x^2 + y^2 + z^2 + w^2 \equiv x + y + z + w \pmod 2,$$

  so the number of x, y, z, w which are even is 0, 2, or 4.

CASE 1: m IS EVEN

- If m is even, then

  $$0 \equiv mp \equiv x^2 + y^2 + z^2 + w^2 \equiv x + y + z + w \pmod 2,$$

  so the number of x, y, z, w which are even is 0, 2, or 4.
- In each case, we rearrange: $x \equiv y \pmod 2$, $z \equiv w \pmod 2$.

CASE 1: m IS EVEN

- If m is even, then

$$0 \equiv mp \equiv x^2 + y^2 + z^2 + w^2 \equiv x + y + z + w \pmod{2},$$

  so the number of x, y, z, w which are even is 0, 2, or 4.
- In each case, we rearrange: $x \equiv y \pmod{2}$, $z \equiv w \pmod{2}$.
- But then

$$\left(\frac{x-y}{2}\right)^2 + \left(\frac{x+y}{2}\right)^2 + \left(\frac{z-w}{2}\right)^2 + \left(\frac{z+w}{2}\right)^2 = \left(\frac{m}{2}\right) \cdot p.$$

CASE 1: m IS EVEN

- If m is even, then

  $$0 \equiv mp \equiv x^2 + y^2 + z^2 + w^2 \equiv x + y + z + w \pmod{2},$$

  so the number of x, y, z, w which are even is 0, 2, or 4.
- In each case, we rearrange: $x \equiv y \pmod{2}$, $z \equiv w \pmod{2}$.
- But then

  $$\left(\frac{x-y}{2}\right)^2 + \left(\frac{x+y}{2}\right)^2 + \left(\frac{z-w}{2}\right)^2 + \left(\frac{z+w}{2}\right)^2 = \left(\frac{m}{2}\right) \cdot p.$$

- This contradicts the minimality of m.

CASE 2: m IS ODD, $m > 1$

- Set $a \equiv x \pmod{m}$, $b \equiv y \pmod{m}$, $c \equiv z \pmod{m}$, $d \equiv w \pmod{m}$ with $|a|, |b|, |c|, |d| < m/2$ (i.e., take the reduced reps. of smallest abs. value).

CASE 2: m IS ODD, $m > 1$

- Set $a \equiv x \pmod{m}$, $b \equiv y \pmod{m}$, $c \equiv z \pmod{m}$, $d \equiv w \pmod{m}$ with $|a|, |b|, |c|, |d| < m/2$ (i.e., take the reduced reps. of smallest abs. value).
- Then

$$a^2 + b^2 + c^2 + d^2 \equiv x^2 + y^2 + z^2 + w^2 \equiv 0 \pmod{m},$$

CASE 2: m IS ODD, $m > 1$

- Set $a \equiv x \pmod{m}$, $b \equiv y \pmod{m}$, $c \equiv z \pmod{m}$, $d \equiv w \pmod{m}$ with $|a|, |b|, |c|, |d| < m/2$ (i.e., take the reduced reps. of smallest abs. value).
- Then

  $$a^2 + b^2 + c^2 + d^2 \equiv x^2 + y^2 + z^2 + w^2 \equiv 0 \pmod{m},$$

  and so $a^2 + b^2 + c^2 + d^2 = km$ for some k.
- We bound

  $$0 \leq a^2 + b^2 + c^2 + d^2 < 4 \cdot \left(\frac{m}{2}\right)^2 = m^2 \implies 0 \leq k < m.$$

PENULTIMATE STEP

- Case a: If $k = 0$, then $a = b = c = d = 0$, and so $x \equiv y \equiv z \equiv w \equiv 0 \pmod{m}$.

PENULTIMATE STEP

- Case a: If $k = 0$, then $a = b = c = d = 0$, and so $x \equiv y \equiv z \equiv w \equiv 0 \pmod{m}$. But then $m^2 | mp \implies m|p$.

PENULTIMATE STEP

- Case a: If $k = 0$, then $a = b = c = d = 0$, and so $x \equiv y \equiv z \equiv w \equiv 0 \pmod{m}$. But then $m^2 | mp \implies m|p$. This contradicts $1 < m < p$.

PENULTIMATE STEP

- Case a: If $k = 0$, then $a = b = c = d = 0$, and so $x \equiv y \equiv z \equiv w \equiv 0 \pmod{m}$. But then $m^2 | mp \implies m|p$. This contradicts $1 < m < p$.
- Case b: Suppose $1 \leq k < m$. Consider $(x^2 + y^2 + z^2 + w^2)(a^2 + b^2 + c^2 + d^2) = m^2kp$.

PENULTIMATE STEP

- Case a: If $k = 0$, then $a = b = c = d = 0$, and so $x \equiv y \equiv z \equiv w \equiv 0 \pmod{m}$. But then $m^2 | mp \implies m|p$. This contradicts $1 < m < p$.
- Case b: Suppose $1 \leq k < m$. Consider $(x^2 + y^2 + z^2 + w^2)(a^2 + b^2 + c^2 + d^2) = m^2 kp$. We do the "horrible" algebra from the lemma:

$$\begin{aligned} &(ax + by + cz + dw)^2 + (bx - ay + dz - cw)^2 \\ &+ (cx - dy - az + bw)^2 + (dx + cy - bz - aw)^2 = m^2 kp. \end{aligned}$$

FINISHING THE PROOF

- We analyze the colored pieces mod m:

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

FINISHING THE PROOF

- We analyze the colored pieces mod m:

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

- Dividing each colored term by m and plugging in, we have

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

FINISHING THE PROOF

- We analyze the colored pieces mod m:

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

- Dividing each colored term by m and plugging in, we have

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

- But then $0<k<m$, kp is a sum of squares, which contradicts minimality of m.

FINISHING THE PROOF

- We analyze the colored pieces mod m:

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

- Dividing each colored term by m and plugging in, we have

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

- But then $0<k<m$, kp is a sum of squares, which contradicts minimality of m. Thus, $m=1$, and Lagrange's Theorem is true!

WHAT IS GOING ON?

- There's got to be a better way!

WHAT IS GOING ON?

- There's got to be a better way!
- Using the theory of *modular forms*, there's a way to prove things like Lagrange, and *improve it*, for free.

WHAT IS GOING ON?

- There's got to be a better way!
- Using the theory of *modular forms*, there's a way to prove things like Lagrange, and *improve it*, for free.
- Just as congruences are a tool for showing infinitely many statements with a finite check, modular forms give a way to check infinitely many identities in a finite check.

WHAT IS GOING ON?

- There's got to be a better way!
- Using the theory of *modular forms*, there's a way to prove things like Lagrange, and *improve it*, for free.
- Just as congruences are a tool for showing infinitely many statements with a finite check, modular forms give a way to check infinitely many identities in a finite check.
- Rough idea: Let $r_k(n)$ be the number of ways that n can be written as a sum of k squares. The **Jacobi theta function** $\vartheta(q) = \sum_{n\in\mathbb{Z}} q^{n^2}$ has infinitely many symmetries, and as generating functions:

$$\sum_{n\geq 0} r_k(n)q^n = \vartheta^k(q).$$

FUN IDENTITIES

- Thus, the gen. fun. $\sum_{n\geq 0} r_k(n)q^n$ has many symmetries, which force it into a **finite dimensional vector space.**

FUN IDENTITIES

- Thus, the gen. fun. $\sum_{n\geq 0} r_k(n)q^n$ has many symmetries, which force it into a **finite dimensional vector space.**

EXAMPLE

For $k=2$, it lives in the same vector space as the **Eisenstein series**: $G_{1,\chi_{-4}}(q) := 1 + 4\sum_{n\geq 1}\left(\sum_{d|n}\left(\frac{-4}{n}\right)\right)q^n$.

FUN IDENTITIES

- Thus, the gen. fun. $\sum_{n\geq 0} r_k(n)q^n$ has many symmetries, which force it into a **finite dimensional vector space.**

EXAMPLE

For $k=2$, it lives in the same vector space as the **Eisenstein series**: $G_{1,\chi_{-4}}(q) := 1 + 4\sum_{n\geq 1}\left(\sum_{d|n}\left(\frac{-4}{n}\right)\right)q^n$. This is a one-dimensional space, and they both start with $1\cdot q^0$, so they are **equal.**

FUN IDENTITIES

- Thus, the gen. fun. $\sum_{n\geq 0} r_k(n)q^n$ has many symmetries, which force it into a **finite dimensional vector space.**

EXAMPLE

For $k=2$, it lives in the same vector space as the **Eisenstein series**: $G_{1,\chi_{-4}}(q) := 1 + 4\sum_{n\geq 1}\left(\sum_{d|n}\left(\frac{-4}{n}\right)\right)q^n$. This is a one-dimensional space, and they both start with $1\cdot q^0$, so they are **equal.** Thus, we get a stronger version of Fermat's Theorem **for free:** $r_2(n) = 4\sum_{d|n}\left(\frac{-4}{n}\right)$, where $\left(\frac{-4}{n}\right)$ is 0 is n is even, $\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}$ if n is odd.

FUN IDENTITIES

- Thus, the gen. fun. $\sum_{n\geq 0} r_k(n)q^n$ has many symmetries, which force it into a **finite dimensional vector space.**

EXAMPLE

For $k=2$, it lives in the same vector space as the **Eisenstein series**: $G_{1,\chi_{-4}}(q) := 1 + 4\sum_{n\geq 1}\left(\sum_{d|n}\left(\frac{-4}{n}\right)\right)q^n$. This is a one-dimensional space, and they both start with $1\cdot q^0$, so they are **equal.** Thus, we get a stronger version of Fermat's Theorem **for free:** $r_2(n) = 4\sum_{d|n}\left(\frac{-4}{n}\right)$, where $\left(\frac{-4}{n}\right)$ is 0 is n is even, $\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}$ if n is odd. This is a summatory function of a multiplicative function, so is multiplicative.

FUN IDENTITIES (CONT.)

EXAMPLE (CONT.)

At an odd prime power p^n, if $p \equiv 1 \pmod 4$, we get $\sum_{j=0}^{n} \left(\frac{-1}{p^j}\right) = (n+1)$,

FUN IDENTITIES (CONT.)

EXAMPLE (CONT.)

At an odd prime power p^n, if $p \equiv 1 \pmod 4$, we get $\sum_{j=0}^{n} \left(\frac{-1}{p^j}\right) = (n+1)$, and if $p \equiv 3 \pmod 4$, we get $\sum_{j=0}^{n} \left(\frac{-1}{p^j}\right) = (1 + (-1) + \ldots + (-1)^n)$, which is 1 is n is even, and 0 if n is odd.

FUN IDENTITIES (CONT.)

EXAMPLE (CONT.)

At an odd prime power p^n, if $p \equiv 1 \pmod{4}$, we get $\sum_{j=0}^{n} \left(\frac{-1}{p^j}\right) = (n+1)$, and if $p \equiv 3 \pmod{4}$, we get $\sum_{j=0}^{n} \left(\frac{-1}{p^j}\right) = (1 + (-1) + \ldots + (-1)^n)$, which is 1 is n is even, and 0 if n is odd. Thus, if $n = \prod_{i=1}^{k} p_i^{a_i} \cdot \prod_{j=1}^{\ell} q_j^{b_i}$ is a prime fact. of n where $p_i \equiv 1 \pmod{4}$, $q_j \equiv 3 \pmod{4}$, then $r_2(n) > 0$ exactly when all b_i are even, and then

FUN IDENTITIES (CONT.)

EXAMPLE (CONT.)

At an odd prime power p^n, if $p \equiv 1 \pmod 4$, we get $\sum_{j=0}^{n} \left(\frac{-1}{p^j}\right) = (n+1)$, and if $p \equiv 3 \pmod 4$, we get $\sum_{j=0}^{n} \left(\frac{-1}{p^j}\right) = (1 + (-1) + \ldots + (-1)^n)$, which is 1 is n is even, and 0 if n is odd. Thus, if $n = \prod_{i=1}^{k} p_i^{a_i} \cdot \prod_{j=1}^{\ell} q_j^{b_i}$ is a prime fact. of n where $p_i \equiv 1 \pmod 4$, $q_j \equiv 3 \pmod 4$, then $r_2(n) > 0$ exactly when all b_i are even, and then $r_2(n) = 4 \prod_{i=1}^{k}(1 + a_i)$.

FUN IDENTITIES (CONT.)

EXAMPLE (CONT.)

At an odd prime power p^n, if $p \equiv 1 \pmod 4$, we get $\sum_{j=0}^{n} \left(\frac{-1}{p^j}\right) = (n+1)$, and if $p \equiv 3 \pmod 4$, we get $\sum_{j=0}^{n} \left(\frac{-1}{p^j}\right) = (1 + (-1) + \ldots + (-1)^n)$, which is 1 is n is even, and 0 if n is odd. Thus, if $n = \prod_{i=1}^{k} p_i^{a_i} \cdot \prod_{j=1}^{\ell} q_j^{b_i}$ is a prime fact. of n where $p_i \equiv 1 \pmod 4$, $q_j \equiv 3 \pmod 4$, then $r_2(n) > 0$ exactly when all b_i are even, and then $r_2(n) = 4\prod_{i=1}^{k}(1 + a_i)$.

EXAMPLE

For $k = 4$, we have a two-dimensional space, and one can compute that $r_4(n) = 8\sum_{\substack{d|n \\ 4\nmid d}} d$.

FUN IDENTITIES (CONT.)

EXAMPLE (CONT.)

At an odd prime power p^n, if $p \equiv 1 \pmod 4$, we get $\sum_{j=0}^{n} \left(\frac{-1}{p^j}\right) = (n+1)$, and if $p \equiv 3 \pmod 4$, we get $\sum_{j=0}^{n} \left(\frac{-1}{p^j}\right) = (1 + (-1) + \ldots + (-1)^n)$, which is 1 is n is even, and 0 if n is odd. Thus, if $n = \prod_{i=1}^{k} p_i^{a_i} \cdot \prod_{j=1}^{\ell} q_j^{b_i}$ is a prime fact. of n where $p_i \equiv 1 \pmod 4$, $q_j \equiv 3 \pmod 4$, then $r_2(n) > 0$ exactly when all b_i are even, and then $r_2(n) = 4 \prod_{i=1}^{k}(1 + a_i)$.

EXAMPLE

For $k = 4$, we have a two-dimensional space, and one can compute that $r_4(n) = 8 \sum_{\substack{d \mid n \\ 4 \nmid d}} d$. For $k = 8$, we have $r_8(n) = 16 \sum_{d \mid n} (-1)^{n+d} d^3$.