Lecture 2: Sums of Two Squares

§1 Sums of Squares

The square numbers are $\{0^2, 1^2, 2^2, \dots\}$.

Thm (Fermat) An odd prime p is a sum of two squares $\Leftrightarrow p \equiv 1 \mod 4$.

Thm (Lagrange) Every positive integer n is the sum of 4 squares.

§2 Proof of Fermat's Theorem

($\Rightarrow$) Necessity Note that $x^2 \equiv 0, 1 \mod 4 \Rightarrow p = x^2 + y^2 \equiv 0, 1, 2 \not\equiv 3 \mod 4$.

($\Leftarrow$) Sufficiency Based on a useful principle:

> Infinite Descent (Equivalent to $\mathbb{N}$ being well-ordered)
>
> Let $P(n)$ be a proposition. Suppose that the existence of $n_0 \in \mathbb{N}$ with $P(n_0)$ true implies the existence of a smaller $n_1 \in \mathbb{N}$ with $P(n_1)$ true. Then $P(n)$ is false for all $n \in \mathbb{N}$.

Example Claim: $5^a \| x^2 + 2y^2 \Rightarrow a$ even.

Suppose a odd s.t. $\exists x, y$, $5^a \| x^2 + 2y^2 \equiv 0 \mod 5$

$\Rightarrow x \equiv y \equiv 0 \mod 5$ as $x^2, y^2 \equiv 0, 1 \mod 5$

$\Rightarrow 5^{a-2} \| (\frac{x}{5})^2 + 2 \cdot (\frac{y}{5})^2$, $a - 2 \geq 1$

$\rightsquigarrow$ done by inf descent.

Proof (of Fermat's thm) $m \geq 1$ be the smallest int s.t. $mp = x^2 + y^2$.

① Existence: $p \equiv 1 \mod 4 \Rightarrow -1$ quadratic residue mod p. (by reciprocity).

$\Rightarrow \exists x$ s.t. $x^2 \equiv -1 \mod p \Rightarrow x^2 + 1 = mp$.

② Upper bound $x \mapsto x \bmod p$, $x \mapsto -x$ preserve $x^2 \bmod p$.

$\Rightarrow$ may assume $|x|, |y| < \frac{p}{2}$.

$\Rightarrow mp = x^2 + y^2 < 2 \cdot (\frac{p}{2})^2 = p^2 \Rightarrow m < p$.

③ Descent Claim: $\exists\, 1 \leq r < m$ s.t. $rm \cdot mp = A^2 + B^2$ with $A, B \equiv 0 \bmod m$.

$\Rightarrow rp = (\frac{A}{m})^2 + (\frac{B}{m})^2$. Done by inf descent.

Key identity $(a^2+b^2)(c^2+d^2) = (ac+bd)^2 + (ad-bc)^2$

(thus the set of sums of two squares is closed under multi.)

Let a, b be s.t. $x \equiv a \bmod m$, $y \equiv b \bmod m$, & $|a|, |b| \leq \frac{m}{2}$.

Then $a^2 + b^2 \equiv x^2 + y^2 \bmod m$, $a^2 + b^2 > 0$ (since $m < p$).

$\Rightarrow a^2 + b^2 = rm$, $1 \leq r < 2 \cdot (\frac{m}{2})^2 \cdot \frac{1}{m} = m$.

$\overset{\text{key}}{\Rightarrow} rm \cdot mp = A^2 + B^2$, $A = ax + by$, $B = ay - bx$.

we have $\left.\begin{array}{l} ax + by \equiv x^2 + y^2 \equiv 0 \bmod m, \\ ay - bx \equiv xy - yx \equiv 0 \bmod m. \end{array}\right\}$ done ☺

$\square$

§3 Proof of Lagrange's Theorem

① Key identity $(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2)$

$$= (x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2 + (x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3)^2$$
$$+ (x_1y_3 - x_3y_1 + x_4y_2 - x_2y_4)^2 + (x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2)^2.$$

$\rightsquigarrow$ thus the set of sums of 4 squares is closed under multi.

Since $2 = 1^2 + 1^2 + 0^2 + 0^2$, it suffices to prove for odd primes.

Let $m \geq 1$ be the smallest integer s.t. $mp = x_1^2 + x_2^2 + x_3^2 + x_4^2$.

② Existence Since the set of S of squares (mod p) has size $(p+1)/2$,

the set $S \cap (-1 - S) \neq \phi$.

$\Rightarrow \exists\, (x_1, x_2)$ s.t. $-1 \equiv x_1^2 + x_2^2 \bmod p$. $\Rightarrow 0 \equiv x_1^2 + x_2^2 + 1^2 + 0^2$.

$\rightsquigarrow$ m exists.

③ Upper bound Via $x \mapsto x \bmod p$ and $x \mapsto -x$, may assume $|x| < \frac{p}{2}$.

Thus, $mp = x_1^2 + x_2^2 + x_3^2 + x_4^2 < 4\left(\frac{p}{2}\right)^2 = p^2 \Rightarrow m < p$.

Case 1 m even. $\leadsto$ reorder x_i s.t. $x_1 \equiv x_2$, $x_3 \equiv x_4 \bmod 2$.

Now $\frac{1}{2}mp = \left(\frac{x_1+x_2}{2}\right)^2 + \left(\frac{x_1-x_2}{2}\right)^2 + \left(\frac{x_3+x_4}{2}\right)^2 + \left(\frac{x_3-x_4}{2}\right)^2$

contradicting the minimality of m.

Case 2 m odd.

$\boxed{\text{Descent}}$ Claim: $\exists\, 1 \leq r < m$ s.t. $rm \cdot mp = A^2 + B^2 + C^2 + D^2$

with $A, B, C, D \equiv 0 \bmod m$.

$\Rightarrow rp = \left(\frac{A}{m}\right)^2 + \left(\frac{B}{m}\right)^2 + \left(\frac{C}{m}\right)^2 + \left(\frac{D}{m}\right)^2$.

$\leadsto$ Done by inf descent.

Let y_i be s.t. $x_i \equiv y_i \bmod m$, $|y_i| < \frac{m}{2}$ (m odd).

Then $0 < \underbrace{y_1^2 + y_2^2 + y_3^2 + y_4^2}_{= rp,\ 1 \leq r < m} < 4 \cdot \left(\frac{m}{2}\right)^2 = m^2$

as $m < p$

Now $rm \cdot mp = A^2 + B^2 + C^2 + D^2$

where $A = x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4 \equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \bmod m$.

(similarly for B, C, D).

$\leadsto$ We're done by descent step. $\square$

§4 Sums of Three Squares, etc.

We mention the following theorem of Legendre (not proved on this course)

Thm (Legendre) An int $n \geq 1$:

$$n = x^2 + y^2 + z^2 \iff n \neq 4^a(8m+7)$$

Proof of necessity ($\Rightarrow$) is attainable.

We also mention the characterization of sums of two squares.

Thm $n \geq 1$, $n = x^2 + y^2 \iff \forall p \mid n$ prime divisor s.t. $p \equiv -1 \bmod 4$,

$v_p(n)$ is even.