C3.10 Additive and Combinatorial NT
Lecture 2: Sums of two squares

Joni Teräväinen

Mathematical Institute

Sums of squares

The square numbers are $\{0^2, 1^2, 2^2, 3^2, \ldots\}$.

Theorem (Fermat)

An odd prime p is a sum of two squares if and only if $p \equiv 1 \pmod 4$.

Theorem (Lagrange)

Every positive integer n is the sum of four squares.

Proof of Fermat's theorem

Necessity: Note that $x^2 \equiv 0, 1 \pmod 4$. Hence, $x^2 + y^2 \equiv 0, 1, 2 \not\equiv 3 \pmod 4$.

Sufficiency: Based on a useful principle:

Infinite descent

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 $n \in \mathbb{N}$.

Equivalent to $\mathbb{N}$ being well-ordered.

Example

We claim that if $5^a \mid\mid x^2 + 2y^2$, then a is even. Suppose a is an odd integer such that $5^a \mid\mid x^2 + 2y^2$ for some x, y. Note that $x^2 + 2y^2 \equiv 0 \pmod 5$ implies $x \equiv y \equiv 0 \pmod 5$. Hence, $5^{a-2} \mid\mid (x/5)^2 + 2(y/5)^2$ and $a - 2 \geq 1$. Now done by infinite descent.

Proof of Fermat's theorem

Let $m \geq 1$ be the smallest integer such that $mp = x^2 + y^2$ for some x, y.

Existence: Since $p \equiv 1 \pmod 4$, -1 is a quadratic residue $\pmod p$ [part A Number Theory]. Hence, $\exists x$: $x^2 \equiv -1 \pmod p$, so $x^2 + 1^2 = mp$.

Upper bound: Since the transformations $x \mapsto x \pmod p$ and $x \mapsto -x$ do not change $x^2 \pmod p$, we may assume that $|x|, |y| < p/2$. Hence, $mp = x^2 + y^2 < 2(p/2)^2 < p^2 \implies m < p$.

Descent: We claim that there exists $1 \leq r < m$ such that $rm \cdot mp = A^2 + B^2$ with $A, B \equiv 0 \pmod m$. Then, $rp = (A/m)^2 + (B/m)^2$. Done by infinite descent.

Proof of Fermat's theorem

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 multiplication.

Let a, b be such that $x \equiv a \pmod{m}$, $y \equiv b \pmod{m}$ and $|a|, |b| \leq m/2$. Then

$$a^2 + b^2 \equiv x^2 + y^2 \equiv 0 \pmod{m}$$

and $a^2 + b^2 > 0$ (since $m < p$). Now, $a^2 + b^2 = rm$ for some $1 \leq r < 2(m/2)^2/m < m$. But by the key identity,

$$rm \cdot mp = A^2 + B^2, \quad A = ax + by, \quad B = ay - bx.$$

We have $ax + by \equiv x^2 + y^2 \equiv 0 \pmod{m}$, $ay - bx \equiv xy - yx \equiv 0 \pmod{m}$, so we are done by the descent step. □

Proof of Lagrange's theorem

Key identity:

$$(x_1^2+x_2^2+x_3^2+x_4^2)(y_1^2+y_2^2+y_3^2+y_4^2) = (x_1y_1+x_2y_2+x_3y_3+x_4y_4)^2 + (x_1y_2-x_2y_1+x_3y_4-x_4y_3)^2 + (x_1y_3-x_3y_1+x_4y_2-x_2y_4)^2 + (x_1y_4-x_4y_1+x_2y_3-x_3y_2)^2.$$

Thus, the set of sums of two squares is closed under multiplication.

Since $2 = 1^2+1^2+0^2+0^2$, it suffices to show that any odd prime p is the sum of four squares.
Let $m \geq 1$ be the smallest integer such that
$mp = x_1^2+x_2^2+x_3^2+x_4^2$.

Existence: Since the set S of squares $\pmod p$ has size $(p+1)/2$, the sets S and $-1-S$ always intersect. Thus, we have a solution to $-1 \equiv x_1^2+x_2^2 \pmod p$. Then,
$0 \equiv x_1^2+x_2^2+1^2+0^2$, so m exists.

Proof of Lagrange's theorem

Upper bound: Making changes $x \mapsto x \pmod{p}$ and $x \mapsto -x$, we may assume that $|x_i| < p/2$. Thus,

$$mp = x_1^2 + x_2^2 + x_3^2 + x_4^2 < 4(p/2)^2 = p^2 \Longrightarrow m < p.$$

Case 1: If m is even, reorder x_i such that $x_1 \equiv x_2$, $x_3 \equiv x_4 \pmod{2}$. Now,

$$\frac{1}{2}mp = ((x_1 + x_2)/2)^2 + ((x_1 - x_2)/2)^2 + ((x_3 + x_4)/2)^2 + ((x_3 - x_4)/2)^2,$$

contradicting the minimality of m.

Case 2: Let m be odd.

Descent: We claim that there exists $1 \leq r < m$ such that $rm \cdot mp = A^2 + B^2 + C^2 + D^2$ with $A, B, C, D \equiv 0 \pmod{m}$. Then, $rp = (A/m)^2 + (B/m)^2 + (C/m)^2 + (D/m)^2$. Done by infinite descent.

Proof of Lagrange's theorem

Let y_i be such that $x_i \equiv y_i \pmod{m}$, $|y_i| < m/2$ (recall m is odd).

Then

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 < 4(m/2)^2 = m^2$$

and $y_1^2 + y_2^2 + y_3^2 + y_4^2 > 0$ (as $m < p$), so $y_1^2 + y_2^2 + y_3^2 + y_4^2 = rp$ for some $1 \leq r < m$.

Now

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

where $A = x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4 \equiv x_1^2 + \ldots + x_4^2 \equiv 0 \pmod{m}$ (similarly for B, C, D). We are done by the descent step. $\square$

Sums of three squares etc.

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

Theorem

An integer $n \geq 1$ is the sum of three squares if and only if n is not of the form $4^a(8m + 7)$.

Proof of necessity: Sheet 1.

We also mention the characterisation of sums of two squares:

Theorem

An integer $n \geq 1$ is the sum of two squares if and only if every prime divisor p of n that is congruent to $-1 \pmod 4$ divides n to an even power.

Proof: Sheet 1.