Lecture 6 The four-squares theorem

Theorem (Lagrange, 1770) $\forall n \in \mathbb{N}_0 \; \exists x_1, \dots, x_4 \in \mathbb{N}_0 : n = x_1^2 + x_2^2 + x_3^2 + x_4^2$. - Every number is a sum of four squares. Known to Fermat and Euler but they could not give a complete proof. We begin with two auxiliary results.

Lemma For every prime number $p > 2$ there exist numbers $a, b \in \{0, 1, 2, \dots, \frac{p-1}{2}\}$ s.t. $a^2 + b^2 + 1 \equiv 0 \pmod p$. Also, both a and b are not 0.

Proof: First note that $a, b \in \mathbb{N} \;\&\; a^2 \equiv b^2 \pmod p \Rightarrow a = b$. This is because $a^2 \equiv b^2 \Leftrightarrow (a-b)(a+b) \equiv 0 \pmod p$. Now $\left| \{ a^2 \bmod p \mid a \in \mathbb{N} \} \right| + \left| \{ -b^2 - 1 \bmod p \mid b \in \mathbb{N} \} \right| = \frac{p+1}{2} + \frac{p+1}{2}$ (as $|\mathbb{N}| = \frac{p+1}{2}$) $= p + 1 > p \Rightarrow$ the two sets intersect. ☒

The second auxiliary result is a wonder-

ful identity, due to L. Euler.

Proposition In ~~$\mathbb{Z}[a,b,c,d] = \mathbb{Z}[x_1,\dots,x_4]$~~ $\mathbb{Z}[x_1,\dots,x_4,y_1,\dots,y_4]$ it is true that

$$\sum_1^4 x_i^2 \cdot \sum_1^4 y_i^2 = \left(\sum_1^4 x_i y_i\right)^2 + (x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3)^2 +$$

$$+ (-x_1y_3 + x_3y_1 + x_2y_4 - x_4y_2)^2 + (x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2)^2.$$

Proof. $\square_a^2 + \square_b^2 + \square_c^2 + \square_d^2$. $LS = \sum_{i,j=1}^4 x_i^2 y_j^2$

$x_i^2 y_i^2$, $i=1\dots4$, 1× in a and 0× in b,c,d. Every $x_i^2 y_j^2$ with $i \neq j$ appears in exactly one of a,b,c,d. We need also to show that all other terms cancel in the RS. For every $i,j \in \{1,2,3,4\}$, $i \neq j$:

$x_iy_ix_jy_j$ has coeff. $+2$ in a and -2 in exactly one of b,c,d. $x_1x_2y_3y_4$: $+d-c$, $x_3x_4y_1y_2$: $-c+d$, $x_1x_3y_2y_4$: $+b-d$, $y_1y_3x_2x_4$: $+b-d$, and similarly $x_1x_4y_2y_3$: $-b+c$, $y_1y_4x_2x_3$: $-b+c$. ☒

Now we can prove Lagrange's four-square theorem.

By Euler's identity it suffices to show that $\forall$ prime $p = \square+\square+\square+\square$. For $p=2$ it holds $2 = 0^2+0^2+1^2+1^2$. Let $p>2$. By the lemma,

$\exists m \in \mathbb{N}: mp = a^2+b^2+1^2+0^2 \rightsquigarrow 1 \le m \le \frac{\frac{p^2}{4}+\frac{p^2}{4}+1}{p}$

$< \frac{p}{2}+1 < p$. We assume that $(m>1)$ is minimum that $p = \square+\square+\square+\square$. and deduce a ~~contradiction (infinite descend!)~~

We write $mp = x_1^2+x_2^2+x_3^2+x_4^2$, $x_i \in \mathbb{N}_0$, $1<m<p$, and take $y_i \equiv x_i \pmod m$ s.t. $-\frac{m}{2} < y_i \le \frac{m}{2}$ for $i \in [4]$. $\rightsquigarrow \sum_1^4 y_i^2 \equiv \sum_1^4 x_i^2 \equiv 0 \pmod m$

$\rightsquigarrow rm = y_1^2+y_2^2+y_3^2+y_4^2$ for some $r \in \mathbb{N}_0$.

$\rightsquigarrow 0 \le r \le m$. We show that neither $r=0$ nor $r=m$ is possible. $r=0$? $\rightsquigarrow y_1=y_2=y_3=y_4=0$ and $m \mid x_i$ for every $i \rightsquigarrow m \mid p$ $\lightning$.

$r=m$? $\rightsquigarrow y_i = \frac{m}{2}$ $\forall i \in [4] \rightsquigarrow x_i \equiv \frac{m^2}{4}$ $\forall i$

$\rightsquigarrow$ again $m \mid p$ $\lightning$. So $0<r<m$. Now

there is a nice turn in the proof: we multiply $mn = y_1^2 + \dots + y_4^2$ ~~and~~ with $mp = x_1^2 + \dots + x_4^2$ and use Euler's identity

$$mm^2p = \sum_1^4 y_i^2 \cdot \sum_1^4 x_i^2 = \underset{a^2}{\square} + \underset{b^2}{\square} + \underset{c^2}{\square} + \underset{d^2}{\square}.$$

From the particular forms of $\underbrace{a, \dots, d}_{\in \mathbb{Z}}$ it follows

but $a, b, c, d \equiv 0 \pmod m$, because $\sum_1^4 x_i^2, \sum_1^4 y_i^2 \equiv 0 \pmod m$

and $x_i \equiv y_i \pmod m$.

$\rightsquigarrow np = a_0^2 + b_0^2 + c_0^2 + d_0^2$ where $a = ma_0, \dots$

$d = md_0$

and $a_0, \dots, d_0 \in \mathbb{Z}, \mathbb{N}_0$. But $1 \leq n < m$. Thus, had to have ~~minimality~~ contradiction with the minimality of $m (>1)$, $n = 1$ and $p = a_0^2 + b_0^2 + c_0^2 + d_0^2$. ☒

Part 3 - Geometry of Numbers

We begin with Gauss' circle problem.

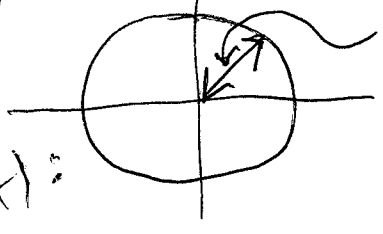
~~Let~~ For $n \in \mathbb{N}_0$ let $r_2(n) = \#\{(a,b) \in \mathbb{Z}^2 \mid a^2+b^2 = n\}$. For instance, $r_2(0) = 1$ $(0 = 0^2+0^2)$, $r_2(1) = 4$ $(1 = (\pm 1)^2 + 0^2 = 0^2 + (\pm 1)^2)$, $r_2(2) = 4$ $(2 = (\pm 1)^2 + (\pm 1)^2)$, $r_2(3) = 0$ $(\mod 4!)$, $r_2(4) = 4$ $(4 = (\pm 2)^2 + 0^2 = 0^2 + (\pm 2)^2)$, $r_2(5) = 8$ $(5 = (\pm 1)^2 + (\pm 2)^2 = (\pm 2)^2 + (\pm 1)^2)$, ... For $x \geq 0$, $\in \mathbb{R}$,

$$C(x) := \sum_{\substack{n \in \mathbb{N}_0 \\ n \leq x}} r_2(n) = ?$$

Theorem (C. F. Gauss, $\doteq$ 1800) For $x > 1$,

$$C(x) = \sum_{n \leq x} r_2(n) = \pi x + O(x^{1/2}) = \pi x + O(\sqrt{x})$$

Proof:



$\rightsquigarrow C(x) = |\mathbb{Z}^2 \cap D(x)| \doteq$

$\doteq$ area $(D(x)) = \pi(\sqrt{x})^2 = \pi x$, with the error being roughly the perimeter $2\pi\sqrt{x}$ of $D(x)$.

Suffices for a physicist (no offense) but not

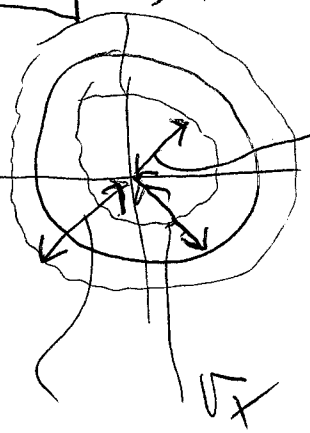
for us. For $p=(a,b)\in\mathbb{Z}^2$, let $S_p :=$ [square] and let $A := \#$ of $S_p \subset D(x)$, $B :=$ # of S_p with [circle] intersecting the boundary circle of $D(x)$ and let $E := \#$ of S_p s.t. $S_p \cap D(x) \neq \emptyset$. Then

and 1) $A \leq \underbrace{\text{area}(D(x))}_{=\pi x} \leq E$,

2) $A \leq C(x) = \#(\mathbb{Z}^2 \cap D(x)) \leq E$ and

3) $E - A = B$, $\Rightarrow |C(x) - \pi x| \leq B$. And

4) $B \leq \text{area}\left(\sqrt{x}+\sqrt{2}\right) - \left(\sqrt{x}-\sqrt{2}\right) = \pi(\sqrt{x}+\sqrt{2})^2 - \pi(\sqrt{x}-\sqrt{2})^2 = O(\sqrt{x})$.



□

*Carl Friedrich Gauss (1777–1855)

- Circle problem