2025. IV. 16

Sums of two squares

Thm If p is a prime such that $p \equiv 1 \pmod 4$, then $p = a^2 + b^2$ for some positive integers a, b.

E.g. $5 = 1^2 + 2^2$, $13 = 2^2 + 3^2$, $17 = 1^2 + 4^2$, $29 = 2^2 + 5^2$, etc.

Q What is $p \equiv 3 \pmod 4$?

$p = 2 = 1^2 + 1^2$

$p = 3 \neq a^2 + b^2$

$p = 7 \neq a^2 + b^2$

In fact, if $p \equiv 3\ (4)$, then $\forall a, b \in \mathbb{Z}_{>0}$,

$$p \neq a^2 + b^2.$$

$a^2 \equiv 0$ or $1 \pmod 4$

$\Longrightarrow a^2 + b^2 \equiv 0, 1,$ or $2 \pmod 4$.

Lemma For any prime $p \equiv 1 \pmod 4$, there exists $m \in \mathbb{Z}$ such that

$-1 \equiv m^2 \pmod p$.

Pf We are looking for a primitive 4th root of unity in $\mathbb{Z}/p\mathbb{Z}$. We have $(\mathbb{Z}/p\mathbb{Z})^\times$ cyclic of order $p-1$, and $4 \mid p-1$, so there is indeed a subgroup of order 4 in $(\mathbb{Z}/p\mathbb{Z})^\times$ and we can take m to be a generator. $\square$

$G \leq (\mathbb{Z}/p\mathbb{Z})^\times$, $G \cong C_4$

$G = \langle x \rangle = \{1, x, x^2, x^3\}$

Pf of Thm Fix a prime $p \equiv 1 \pmod 4$ and $k \in \mathbb{Z}$ such that $-1 \equiv k^2 \pmod p$. Set $\mathcal{L} = \begin{pmatrix} 1 & 0 \\ k & p \end{pmatrix} \mathbb{Z}^2$ so that $\det \mathcal{L} = p$.

Consider the convex centrally symmetric body

$$B := \{ x \in \mathbb{R}^2 \mid \|x\| \leq \sqrt{2p} \}$$

of volume $2p\pi$. Then $\operatorname{vol} B > 2^2 \det \mathcal{L}$ holds

because $2p\pi > 4p$ (indeed $2\pi > 4$).

So by Mikowski's convex body theorem,

$$B^\circ \cap (\mathcal{L} \setminus 0) \ni (a, b)$$

Then $\exists\, m, n \in \mathbb{Z}$ s.t. $\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ k & p \end{pmatrix} \begin{pmatrix} m \\ n \end{pmatrix} = \begin{pmatrix} m \\ mk + np \end{pmatrix}$

and $a^2 + b^2 = m^2 + (mk + np)^2 \equiv_p m^2(1 + k^2) \equiv 0 \pmod p$.

I.e. $p \mid a^2+b^2$. Finally, since $(a,b) \in B^\circ$, we also have $a^2+b^2 < 2p \implies p = a^2+b^2$. $\square$