Metoda beskonačnog spusta (Fermat)

↗

prapovijest Mordell-Weilovog teorema

Teorem: Jednadžba $X^4+y^4=z^2$ nema netrivijalnih rješenja u $\mathbb{Z}$.

Dokaz: Pretp. $(x,y,z)\in\mathbb{Z}^3$, $xyz\neq 0$, rješenje za koje je $\max\{|x|,|y|\}$ minimalan (pa su x,y,z u parovima relativno prosti).

Možemo pretp. da je x paran, a y i z neparni.

Imamo [16] $x^4=(z-y^2)(z+y^2)$.

Lako se vidi $GCD(z+y^2, z-y^2)\in\{1,2\}$ odnosno

$GCD=2$. $\Rightarrow$ dvije mogućnosti

a) $\exists u,v\in\mathbb{N}$ t.d. $z+y^2=8u^4$ i $z-y^2=2v^4$

ili

V neparan

b) $\exists u,v\in\mathbb{N}$ t.d. $z^2+y^2=2u^4$ i $z-y^2=8v^4$

u neparan

a) $\Rightarrow$ $y^2 = 4u^4 - v^4 \Rightarrow y^2 \equiv 3 \ (4) \Rightarrow \Leftarrow$

neparni

b) $\Rightarrow$ $y^2 = u^4 - 4v^4 \Rightarrow 4v^4 = u^4 - y^2 = (u^2 - y)(u^2 + y)$

$\Rightarrow \exists s, r \in \mathbb{N}$ t.d. $u^2 + y = 2r^4$

$u^2 - y = 2s^4$

tj. $v^4 = (rs)^4$

$v = \pm rs$

$r, s, v > 0$

$\Rightarrow v = rs$

$$\Rightarrow \boxed{r^4 + s^4 = u^2}$$

Našli smo novo rješenje (r, s, u) za koje vrijedi

$$x^4 = (z - y^2)(z + y^2) = 16u^4v^4 = 4u^4(u^2 + y)(u^2 - y)$$

$$= 16u^4r^4s^4$$

$\Rightarrow rs \neq 0$ i $|r| < |x| \Rightarrow \Leftarrow$

$\square$

Malo moderniji pogled na Fakar

Uočimo druge krivulje (u $\mathbb{P}(1,1,2)$ nad $\mathbb{Q}$)

$$C: X^4+Y^4=Z^2 \quad ; \quad C': U^4-4V^4=W^2$$

i dva racionalna preslikavanja

$$\varphi: C \to C' ; \quad [X:Y:Z] \mapsto [Z:-XY:X^4-Y^4]$$

$$\hat{\varphi}: C' \to C ; \quad [U:V:W] \mapsto [2UV:W:U^4+4V^4]$$

$a=(a_0,\dots,a_n)$

$$\mathbb{P}(a_0,\dots,a_n) := \mathbb{A}^{n+1}\setminus\{0\} \Big/ \mathbb{G}_m^{(a)}$$

gdje $\lambda \in \mathbb{G}_m^{(a)}$ djeluje na $(x_0,\dots,x_n)\in \mathbb{A}^{n+1}\setminus\{0\}$

$$\lambda(x_0,\dots,x_n) = (\lambda^{a_0}x_0,\dots,\lambda^{a_n}x_n)$$

Naloga na dokaz:

$(x,y,z) \in C \rightsquigarrow (u,v,y) \in C'$

$\downarrow$

$(r,s,u) \in C$

bolj:

$(r,s,u) \in C \mapsto (u, -rs, 2r^4 - u^2) \mapsto (u, rs, 2r^4 - u^2)$

$(u,v,y) \mapsto (2uv, y, 2v^4 + y^2)$

$2r^4 - r^4 - s^4 = r^4 - s^4$

$x = 4u^4 + v^4 = z$

$(x:y:z) = \varphi'(u:v:y)$

$(u:v:y) = \varphi(r:s:u)$

Kriti preslikavi!

C i C' su eliptičke krivulje

općenito, krivulje

$$C_t : X^4 + Y^4 = Z^2$$ je izomorfna s

$$E_t : v^2 = u^3 - 4tu$$

$$[X:Y:Z] \xmapsto{\tau_t} [2Y(Z+X^2) : 4(ZX+X^3) : Y^3]$$

$$\Rightarrow \quad C \simeq \quad E_1 : v^2 = u^3 - 4u$$

$$C' \simeq \quad E_{-4} : \quad v^2 = u^3 + 16u$$

pa dijagram

$$\begin{array}{ccccc} C & \xrightarrow{\varphi} & C' & \longrightarrow & C \\ \downarrow \tau & & \downarrow \tau' & & \downarrow \tau \\ E_1 & \xrightarrow{\phi} & E_{-4} & \xrightarrow{\hat{\phi}} & E_1 \end{array}$$ komutira gdje je

$$\phi : E_1 \to E_{-4}$$

$$(u,v) \longmapsto \begin{cases} \left(u - \frac{4}{u}, v + \frac{4v}{u^2}\right) & \text{za } u \neq 0 \\ O & \text{za } u = 0 \end{cases}$$

odnosno

$$\hat{\phi} : E_{-4} \to E_1 ;\ (u,v) \mapsto \begin{cases} \left(\frac{1}{4}\left(u+\frac{16}{u}\right), \frac{1}{8}\left(v-\frac{16v}{u^2}\right)\right) & \text{za } u \neq 0 \\ O & \text{za } u = 0 \end{cases}$$

$$\phi \circ \hat{\phi} = [2]$$

Kako popraviti lemin predznak?

krivulje $C_f : X^4 + fY^4 = Z^2$ imaju

očite automorfizme reda 2:

$$(X:Y:Z) \mapsto (\pm X : \pm Y : \pm Z)$$

D.Z. "Identificirajte" te automorfizme.

Što je Fermat pokazao?

Svaka racionalna točka, do na translaciju za točku reda dva, se nalazi u slici

$[2](E_{-1}(\mathbb{Q}))$, odnosno

$$E_{-1}(\mathbb{Q}) \Big/ 2E_{-1}(\mathbb{Q}) \simeq \left(\mathbb{Z}/2\mathbb{Z}\right)^2$$

Fermat ji naravno pokazao i da postupak spusta u jednom trenutku stane pa vrijedi

$$E_{-n}(\mathbb{Q}) \simeq E_{-n}[2],$$ odnosno rang konike je 0.

Kako generalizirati Fermatov rad na proizvoljne eliptičke krivulje?

Teorem 1. (slabi Mordell-Weil)

Za svaku $E/\mathbb{Q}$ vrijedi da je

$$E(\mathbb{Q}) \Big/ 2E(\mathbb{Q})$$ konačan skup.

Teorija visina koja nam garantira da će postupak spusta u jednom trenutku stati.

Samo kratko o visinama na $\mathbb{Q}$

$$E: y^2 = x^3 + Ax + B, \quad A, B \in \mathbb{Z}$$

Def: Neka je $t \in \mathbb{Q}$, $t = \frac{p}{q}$, $\gcd(p, q) = 1$. Tada

$$H(t) = \max\{|p|, |q|\}$$

↗

visina od t

Def. (logaritamska visina na $E(\mathbb{Q})$ u odnosu na Weiers. model)

$$h_x : E(\mathbb{Q}) \to \mathbb{R}, \quad h_x(P) = \begin{cases} \log H(x(P)) & P \neq \mathcal{O} \\ 0 & P = \mathcal{O} \end{cases}$$

Napomena: $h_x(P) \geq 0 \quad \forall P \in E(\mathbb{Q})$

Lema.

a) Neka je $P_0 \in E(\mathbb{Q})$. Postoji konstanta C_1 koja ovisi o P_0, A i B t.d.

$$h_x(P + P_0) \leq 2 h_x(P) + C_1 \quad \forall P \in E(\mathbb{Q}).$$

b) Postoji konstanta C_2 koja ovisi o A i B t.d.

$$h_x([2]P) \geq 4h_x(P) - C_2 \quad \forall P \in E(\mathbb{Q})$$

c) Za svaki C_3 skup

$$\{P \in E(\mathbb{Q}) : h_x(P) \leq C_3\}$$

je konačan.

zašto?

Sad se lako vidi da Lema zajedno

sa slabim Mordell-Weilovim teorem

implicira

Teorem (Mordell) Neka je $E/\mathbb{Q}$.

Tada je $E(\mathbb{Q})$ konačno generirana.

Teorija visina nad proizvoljnim poljem

brojeva K je kompliciranija (i zanimljivija)

jer nad G_K nemamo jedinstvena faktorizacija.