Slaba Mordell-ova teorema

- Za svaku Abelovu grupu A, i $m \in \mathbb{Z}$ imamo homomorfizam 'množenje sa m':

$$A \longrightarrow A$$
$$P \longmapsto \underbrace{P+P+\ldots+P}_{m \text{ puta}} = mP$$

Njegova slika $mA \leq A$

[Slaba Mordell-ova teorema]

Teorema 1 Neka je $E/\mathbb{Q}$ eliptička kriva definisana nad $\mathbb{Q}$.

Onda je indeks

$$\boxed{[E(\mathbb{Q}) : 2E(\mathbb{Q})] < \infty}$$

$E: y^2 = f(x) = x^3 + ax^2 + bx + c$ nesingularna, $f(x) \in \mathbb{Z}[x]$

! (T.1) ćemo dokazati pod dodatnom pretpostavkom da $f(x)$ ima bar jedan racionalan koren $x_0 \in \mathbb{Q}$
($\Leftrightarrow E(\mathbb{Q})$ ima bar jednu tačku reda 2)

Primedba: Ako $f(x)$ nema korene u $\mathbb{Q}$, ako je $x_0 \notin \mathbb{Q}$ bilo koji koren $f(x)=0$, onda bi isti metod radio, ali dokaz bi morao da se izvodi nad poljem $K := \mathbb{Q}(x_0)$ i njegovim prstenom celih $\mathcal{O}_K$ - a za to je potrebno dodatno (ali standardno) znanje iz Algebarske TB.

- $f(x_0)=0$, x_0 racionalni koren $\longrightarrow x_0 \in \mathbb{Z}$

Smenom promenljivih $x \mapsto x - x_0$ možemo postići da je taj koren baš $=0$ tj. da kriva E sadrži $(0,0)$.

Dakle, radićemo sa krivama oblika

(grupa racionalnih tačaka se neće promeniti!)

$$E: \quad y^2 = f(x) = x^3 + ax^2 + bx \quad , \qquad a, b \in \mathbb{Z} \qquad (1)$$

Točka $T := (0,0)$ je reda 2: $2T = \mathcal{O}$.

- Diskriminanta kubne krivulje (1) (kubnog polinoma $f(x)$) je

$$D = b^2(a^2 - 4b) \neq 0$$

ako je $f(x) = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$, onda je

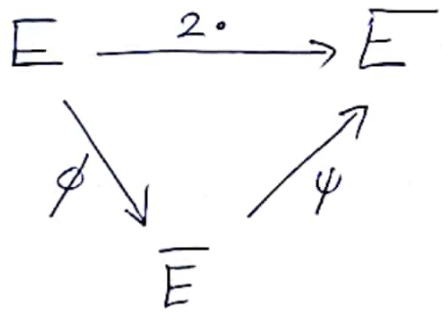
$$D = (\alpha_1 - \alpha_2)^2 (\alpha_1 - \alpha_3)^2 (\alpha_2 - \alpha_3)^2$$

i $D \neq 0 \iff$ svi korijeni $f(x)$ su različiti $\iff$ krivulja (1) je glatka

- Ideja dokaza: da homomorfizam 'množenja sa 2' razbijemo na 2 homomorfizma ψ i ϕ tj. da nađemo "homomorfizme eliptičkih krivulja" za koje je

$$\psi \circ \phi \,(P) = 2P$$

("podeli pa vladaj" – svaki od ψ, ϕ će biti jednostavniji od '2·')



$$\bar{E}: \quad y^2 = x^3 + \bar{a}x^2 + \bar{b}x \qquad (2)$$

$$\bar{a} = -2a$$
$$\bar{b} = a^2 - 4b$$

$$\bar{D} = \bar{b}^2(\bar{a}^2 - 4\bar{b}) = (a^2-4b)^2 \cdot 16b \neq 0$$

- Iteriranjem procedure dobijamo krivu

$$\bar{\bar{E}}: \quad y^2 = x^3 + \bar{\bar{a}}\, x^2 + \bar{\bar{b}}\, x = x^3 + 4a\, x^2 + 16b\, x$$

gde su

$$\bar{\bar{a}} = -2\,\bar{a} = 4a$$

$$\bar{\bar{b}} = \bar{a}^2 - 4\,\bar{b} = 4a^2 - 4a^2 + 16b$$

Smenom promenljivih: $(x, y) = (4x_1, 8y_1)$
dobijamo upravo jednačinu (1) krive E pa je

$$\bar{\bar{E}}(\mathbb{Q}) \cong E(\mathbb{Q})$$

- Definicija preslikavanja $\phi: E \to \bar{E}$ (to su sve tačke osim T i $\mathcal{O}$)

– za tačke $P = (x, y) \in E$, sa $x \neq 0$ definišemo

$\phi(x, y) = (\bar{x}, \bar{y})$ formulama

$$\boxed{\bar{x} = x + a + \frac{b}{x} = \frac{y^2}{x^2}, \qquad \bar{y} = y\left(\frac{x^2 - b}{x^2}\right)} \qquad (3)$$

ϕ je definisano racionalnim funkcijama po x, y
('morfizam varijeteta')
→ proverite da tačka $(\bar{x}, \bar{y})$ leži na krivoj $\bar{E}$

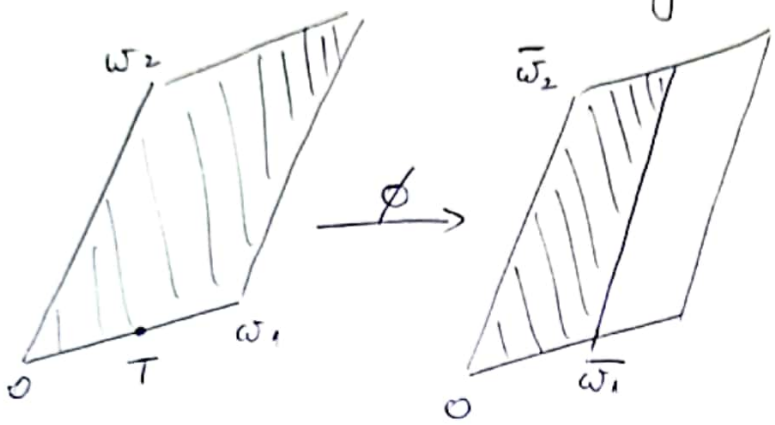
– za $T = (0, 0)$ i $\mathcal{O} = (0, 1, 0)$ definišemo

$\phi(T) = \bar{\mathcal{O}}$ — tačka u ∞ na krivoj $\bar{E}$

$\phi(\mathcal{O}) = \bar{\mathcal{O}}$

Odakle ovakvo preslikavanje ϕ ?

→ Ako el. krivoj E odgovara rešetka $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$



onda krivoj $\bar{E}$ odgovara rešetka

$$\bar{\Lambda} = \mathbb{Z}\bar{\omega}_1 + \mathbb{Z}\bar{\omega}_2$$

$$\bar{\omega}_1 = \frac{\omega_1}{2}, \quad \bar{\omega}_2 = \omega_2$$

$$E = \mathbb{C}/\Lambda \qquad \bar{E} = \mathbb{C}/\bar{\Lambda}$$

(ako izrazite $\wp(z,\bar{\Lambda})$; $\wp'(z,\bar{\Lambda})$ preko $\wp(z,\Lambda)$; $\wp'(z,\Lambda)$ dobićete racionalne fje sa desne strane u (3))

Homomorfizam $\phi : E \longrightarrow \bar{E}$

$$a\omega_1 + b\omega_2 + \Lambda \longmapsto a\omega_1 + b\omega_2 + \bar{\Lambda}$$
$$= 2a\bar{\omega}_1 + b\bar{\omega}_2 + \bar{\Lambda}$$

Vidimo da je $\ker \phi = \{\mathcal{O}, T\}$

Primedba:

$\{\mathcal{O}, T\} \leq E$ podgrupa, pa je

$\bar{E}$ u stvari količnička ~~podgr~~ grupa $E/\{\mathcal{O}, T\}$

i morfizam ϕ je prirodna projekcija $E \longrightarrow E/\{\mathcal{O}, T\}$

→ Ali ovde nije očigledno da količnička grupa $E/\{\mathcal{O}, T\}$ odgovara nekoj eliptičkoj krivoj

→ i nije očigledno da je prirodni homomorfizam grupa $E \longrightarrow E/\{\mathcal{O}, T\}$ i 'morfizam varijeteta' tj. da je zadat racionalnim funkcijama.

Lema 2 Preslikavanje $\phi : E \to \overline{E}$ je homomorfizam grupa ; $\ker \phi = \{\mathcal{O}, T\}$

▼ Kad $x \neq 0$ $\to$ $y(P) \neq 0$ $\quad$ jer je : $\bar{x} = \frac{y^2}{x^2} \neq 0 \to \phi(x,y) \neq \bar{\mathcal{O}}$
$x(P)$

tj. $\ker \phi = \{\mathcal{O}, T\}$.

Treba provesti da je $\phi(P_1 + P_2) = \phi(P_1) + \phi(P_2)$, za sve $P_1, P_2 \in E$

$+$: zbrajanje na $\overline{E}$

Slučajevi
- ako je jedna od P_1, P_2 jednaka $\mathcal{O}$ trivijalno
- ako je jedna jednaka T npr. $P_1 = T$ treba provesti

$$\phi(T+P) \overset{?}{=} \phi(P)$$

• za $P = (x,y)$ $\neq T$ je $P + T = (x,y) + (0,0) = \left(\frac{6}{x}, -\frac{6y}{x^2}\right)$

$$\phi(P+T) = \left(\bar{x}(P+T), \bar{y}(P+T)\right)$$

$$\bar{x}(P+T) = \left(\frac{y(P+T)}{x(P+T)}\right)^2 = \left(\frac{-\frac{6y}{x^2}}{\frac{6}{x}}\right)^2 = \frac{y^2}{x^2} = \bar{x}(P)$$

$$\bar{y}(P+T) = \frac{y(P+T)\left(x(P+T)^2 - 6\right)}{x(P+T)^2} = \frac{-\frac{6y}{x^2}\left(\frac{6^2}{x^2} - 6\right)}{\frac{6^2}{x^2}} =$$

$$= -y\left(\frac{6}{x^2} - 1\right) = y\left(\frac{x^2-6}{x^2}\right) = \bar{y}(P) \quad \checkmark$$

• za $P = T$ je očigledno

$$\phi(T+T) = \phi(\mathcal{O}) = \bar{\mathcal{O}} = \bar{\mathcal{O}} + \bar{\mathcal{O}} = \phi(T) + \phi(T) \quad \checkmark$$

– dalje važi $\phi(-P) = -\phi(P)$: (4)

$$\phi(-P) = \phi(x_1, -y) = \left(\left(\frac{-y}{x}\right)^2, \frac{-y(x^2-b)}{x^2} \right) = (\bar{x}(P), -\bar{y}(P))$$
$$= -(\bar{x}(P), \bar{y}(P)) = -\phi(P)$$

– sada, da bismo proverili da je ϕ homomorfizam grupa, dovoljno je proveriti implikaciju:

$$P_1 + P_2 + P_3 = \mathcal{O} \implies \phi(P_1) + \phi(P_2) + \phi(P_3) = \overline{\mathcal{O}}$$

(jer je $\phi(P_1 + P_2) = \phi(-P_3) \overset{(4)}{=} -\phi(P_3) = \phi(P_1) + \phi(P_2)$)

Pri proveri je dovoljno pretp. da nijedna od P_1, P_2, P_3 nije $\mathcal{O}$ ili T

• $P_1 + P_2 + P_3 = \mathcal{O} \iff P_1, P_2, P_3$ su na jednoj pravoj

$\boxed{y = \lambda x + \nu}$ jednačina te prave, $\nu \neq 0$ (jer su sve $\neq T$)

Računom se pokazuje da tačke $\phi(P_1), \phi(P_2), \phi(P_3)$ onda pripadaju preseku $\overline{E}$ i prave

$$\boxed{y = \bar{\lambda} x + \bar{\nu}, \quad \bar{\lambda} = \lambda - \frac{b}{\nu}, \quad \bar{\nu} = \nu - a\lambda + \frac{b\lambda^2}{\nu}}$$

Npr. za $\phi(P_1) = \phi(x_1, y_1) = (\bar{x}_1, \bar{y}_1) = \left(\frac{y_1^2}{x_1^2}, y_1 \left(\frac{x_1^2 - b}{x_1^2} \right) \right)$

$$\bar{\lambda}\bar{x}_1 + \bar{\nu} = \frac{\lambda\nu - b}{\nu} \frac{y_1^2}{x_1^2} + \frac{\nu^2 - a\lambda\nu + b\lambda^2}{\nu}$$

$$= \frac{\lambda\nu(y_1^2 - ax_1^2) - b(y_1 - \lambda x_1)(y_1 + \lambda x_1) + \nu^2 x_1^2}{\nu x_1^2}$$

$y_1^2 - a x_1^2 = x_1^3 + b x_1$, $y_1 - \lambda x_1 = \nu$

$P_1 \in E$ $\qquad$ $P_1 \in \{y = \lambda x + \nu\}$

$$= \frac{\lambda(x_1^3 + b x_1) - b(y_1 + \lambda x_1) + \nu x_1^2}{x_1^2}$$

$$= \frac{x_1^2(\lambda x_1 + \nu) - b y_1}{x_1^2} = \frac{(x_1^2 - b) y_1}{x_1^2} = \bar{y}_1$$

Ovaj račun je dobar ako su sve 3 tačke $\phi(P_1)$, $\phi(P_2)$, $\phi(P_3)$ različite. Ako nisu, treba dokazati da su $\bar{x}(P_j)$, $j=1,2,3$ zajedno 3 korena kubne jednačine $(\bar{\lambda} x + \bar{\nu})^2 = \bar{f}(x)$. U slučaju krivih nad $\mathbb{C}$, možemo iskoristiti i argument neprekidnosti. ▨

Lema 3 Primenom ove procedure na krivu $\bar{E}$ dobijamo morfizam eliptičkih krivih

$$\phi : \bar{E} \longrightarrow \bar{\bar{E}} \xrightarrow{\cong} E$$

$$(x, y) \mapsto \left(\frac{x}{4}, \frac{y}{8}\right)$$

(primedba na str. −2−)

$$\psi$$

Homomorfizam $\psi : \bar{E} \longrightarrow E$ je definisan sa

$$\psi(\bar{P}) = \begin{cases} \left(\dfrac{\bar{y}^2}{4\bar{x}^2}, \dfrac{\bar{y}(\bar{x}^2 - b)}{8\bar{x}^2}\right), & \text{ako je } \bar{P} = (\bar{x}, \bar{y}) \neq \bar{\mathcal{O}}, \bar{T}, \\ \mathcal{O}, & \text{ako je } \bar{P} \in \{\bar{\mathcal{O}}, \bar{T}\} \end{cases}$$

▨ Iz (L-2) sledi da je ψ dobro definisan homomorfizam grupa ◭

Lema 4 Kompozicija $\psi \circ \phi : E \longrightarrow E$ je 'množenje sa 2':

$$E \xrightarrow{\phi} \overline{E} \xrightarrow{\psi} E, \qquad \psi \circ \phi (P) = 2P, \qquad \forall P \in E$$

$2\cdot$

Računamo:

- formula za duplirnje tačke na E:

$$2P = 2(x,y) = \left(\frac{(x^2-b)^2}{4y^2}, \frac{(x^2-b)(x^4+2ax^3+6bx^2+2abx+b^2)}{8y^3} \right)$$

- sa druge strane (za $(x,y) \neq \mathcal{O}, T$)

$$\psi \circ \phi (x,y) = \psi \left(\frac{y^2}{x^2}, \frac{y(x^2-b)}{x^2} \right)$$

$$= \left(\frac{\left(\frac{y(x^2-b)}{x^2} \right)^2}{4\left(\frac{y^2}{x^2} \right)^2}, \frac{\frac{y(x^2-b)}{x^2}\left(\left(\frac{y^2}{x^2} \right)^2 - (a^2-4b) \right)}{8\left(\frac{y^2}{x^2} \right)^2} \right)$$

$= \ldots$ (istoristite $y^4 = x^2(x^2+ax+b)^2$) ▲

Primedba: Slično važi: $\phi \circ \psi (\bar{x}, \bar{y}) = 2(\bar{x}, \bar{y})$
tj. $\phi \circ \psi$ je 'množenje sa 2' na eliptičkoj krivoj $\overline{E}$

- Iz formula (3) se lako vidi da je preslikavanje

$$\phi : E(\mathbb{C}) \longrightarrow \overline{E}(\mathbb{C})$$

surjektivno.

Ali, nas zanimaju grupe racionalnih tačaka $E(\mathbb{Q})$ i $\overline{E}(\mathbb{Q})$

Iz (3) se vidi da ϕ slika racionalne tačke u racionalne tačke, tj. ϕ definiše i homomorfizam Mordell-Weil-ovih grupa:

$$\phi : E(\mathbb{Q}) \longrightarrow \overline{E}(\mathbb{Q})$$

Želimo da okarakterišemo sliku $\phi(E(\mathbb{Q}))$ ovog homomorfizma

Plan za dokaz (T.1) dalje sledeća

Lema 5 Neka su A, B Abelove grupe; $\phi : A \to B$, $\psi : B \to A$ homomorfizmi Abelovih grupa takvi da je

$$\psi \circ \phi (a) = 2a, \quad \forall a \in A$$
$$\phi \circ \psi (b) = 2b, \quad \forall b \in B$$

i da $[B : \phi(A)] < \infty$, $[A : \psi(B)] < \infty$.

Onda važi

$$[A : 2A] \leq [A : \psi(B)] \cdot [B : \phi(A)] < \infty$$

▽ $a_1, a_2, \ldots, a_n$ predstavnici kosete u $A/\psi(B)$

$b_1, b_2, \ldots, b_m$ predstavnici kosete u $B/\phi(A)$

- za proizvoljni $a \in A$, $\exists a_i : a - a_i \in \psi(B)$ tj.
$a - a_i = \psi(b)$, za neko $b \in B$
- za ovo $b \in B$, $\exists b_j : b - b_j \in \phi(A)$ tj.
$b - b_j = \phi(a')$, za neko $a' \in A$

Onda je

$$a = a_i + \psi(b) = a_i + \psi(b_j + \phi(a')) = a_i + \psi(b_j) + \psi(\phi(a')) = a_i + \psi(b_j) + 2a'$$

$\longrightarrow$ $\{a_i + \psi(b_j) : 1 \le i \le n,\ 1 \le j \le m\}$ sadrži se predstavnike koseta $A/2A$. ◭

• Dakle, primena (L.5) na $A = E(\mathbb{Q})$, $B = \overline{E}(\mathbb{Q})$ završava dokaz (T.1). Da bismo primenili (L.5) treba da okarakterišemo slike $\phi(E(\mathbb{Q}))$ i $\psi(\overline{E}(\mathbb{Q}))$ u $\overline{E}(\mathbb{Q})$ i $E(\mathbb{Q})$, redom, i pokažemo da su konačnog indeksa.

• Primetimo da $\overline{\mathcal{O}} \in \phi(E(\mathbb{Q}))$ jer $\phi(\mathcal{O}) = \overline{\mathcal{O}}$

Lema 6 $\quad \overline{T} = (0,0) \in \phi(E(\mathbb{Q})) \iff b = a^2 - 4b = \square$ (potpuni kvadrat)

$\uparrow$
$\overline{E}$

▽ $\overline{T} \in \phi(E(\mathbb{Q})) \iff \exists (x,y) \in E(\mathbb{Q})$ t.d. $\frac{y^2}{x^2} = 0$

($x \neq 0$, jer $x=0$ znači $(x,y) = T$, ali $\phi(T) = \overline{\mathcal{O}}$)

$$0 = y^2 = x^3 + ax^2 + bx = x(x^2 + ax + b)$$

$\nearrow$ Ima racionalan koren $\neq 0$

$\iff$

diskriminanta $a^2 - 4b = \square$ ◭

Lema 7 Neka je $\bar{P} = (\bar{x}, \bar{y}) \in \bar{E}(\mathbb{Q})$, uz $\bar{x} \neq 0$. Onda je

$$\boxed{\bar{P} \in \phi(E(\mathbb{Q})) \iff \bar{x} \in (\mathbb{Q}^\times)^2}$$

(kvadrat racionalnog broja)

($\longrightarrow$) trivijalno: ako $(x,y) \in E(\mathbb{Q})$ onda $\bar{x} = \frac{y^2}{x^2} \in (\mathbb{Q}^\times)^2$

($\longleftarrow$) neka je $\boxed{\bar{x} = w^2}$ za neko $w \in \mathbb{Q}^\times$

Kako je $\ker \phi = \{\mathcal{O}, T\}$, svaka tačka u $\phi(E(\mathbb{Q}))$ ima tačno 2 originala u $E(\mathbb{Q})$.

• Tačke

$$P_1 := (x_1, y_1) = \left(\frac{1}{2}\left(w^2 - a + \frac{\bar{y}}{w}\right),\ x_1 w \right)$$

$$P_2 := (x_2, y_2) = \left(\frac{1}{2}\left(w^2 - a - \frac{\bar{y}}{w}\right),\ -x_2 w \right)$$

(i) $\longrightarrow$ pripadaju krivoj E : grupi $E(\mathbb{Q})$

(ii) $\longrightarrow$ $\phi(P_1) = \phi(P_2) = (\bar{x}, \bar{y})$

(i): $P_i = (x_i, y_i) \in E \iff \frac{y_i^2}{x_i^2} = x_i + a + \frac{b}{x_i}$ (5)

Ali:

$$x_1 \cdot x_2 = \frac{1}{4}\left((w^2 - a)^2 - \frac{\bar{y}^2}{w^2} \right) = \frac{1}{4}\left((\bar{x} - a)^2 - \frac{\bar{y}^2}{\bar{x}} \right)$$

$$= \frac{1}{4}\left(\frac{\bar{x}^3 - 2a\bar{x}^2 + a^2\bar{x} - \bar{y}^2}{\bar{x}} \right) = b$$

jer je jednačina krive $\bar{E}$:

$$\bar{y}^2 = \bar{x}^3 - 2a\bar{x}^2 + (a^2 - 4b)\bar{x}$$

Kako je

$$\frac{y_i}{x_i} = \pm w \qquad \text{tj.} \qquad \frac{y_i^2}{x_i^2} = w^2$$

i $x_1 x_2 = b$,

Uslov (5) je za obe tačke ekvivalentan sa

$$\boxed{w^2 = x_1 + x_2 + a}$$

što odmah sledi iz f-la za x_1, x_2.

(ii): Treba proveriti da je $\frac{y_i^2}{x_i^2} = \bar{x}$; $\frac{y_i(x_i^2 - b)}{x_i^2} = \bar{y}$

$\bar{x} = w^2$; $b = x_1 x_2$

$$\frac{y_1(x_1^2 - b)}{x_1^2} = \frac{x_1 w (x_1^2 - x_1 x_2)}{x_1^2} = w(x_1 - x_2) = \bar{y}$$ iz formula za x_1, x_2

$$\frac{y_2(x_2^2 - b)}{x_2^2} = \frac{-x_2 w (x_2^2 - x_1 x_2)}{x_2^2} = w(x_1 - x_2)$$

~~Lema~~

- Da bismo pokazali da je $E(\mathbb{Q}) / \psi(\bar{E}(\mathbb{Q}))$ konačna grupa, naći ćemo injektivni homomorfizam iz ove grupe u pogodno izabranu konačnu grupu.

$(\mathbb{Q}^\times)^2 = \{ u^2 : u \in \mathbb{Q}^\times \}$ grupa racionalnih kvadrata

$\leq \mathbb{Q}^\times$

Definišemo preslikavanje

$$\alpha : E(\mathbb{Q}) \longrightarrow \mathbb{Q}^\times / (\mathbb{Q}^\times)^2$$

$$\mathcal{O} \longmapsto 1 \mod (\mathbb{Q}^\times)^2$$

$$T \longmapsto b \mod (\mathbb{Q}^\times)^2$$

$$(x, y) \longmapsto x \mod (\mathbb{Q}^\times)^2, \text{ ako je } x \neq 0$$

Primedba:
ovo preslikavanje je potpuno aritmetičko!
(sve do sada je bilo samo geometrijski definisano)
– i ono je ključno za dokaz (T.1)

Lema 8 Preslikavanje α je homomorfizam grupa.

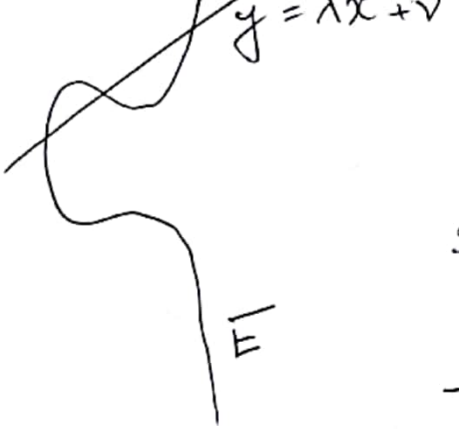
▽ α slika inverze u inverze:

$$\alpha(-P) = \alpha(x, -y) = x = \frac{1}{x} \cdot x^2 \quad \text{tj.}$$

$$\alpha(-P) \equiv \frac{1}{x} \cdot \alpha(P)^{-1} \pmod{(\mathbb{Q}^\times)^2}$$

→ dovoljno je proveriti implikaciju:

ako $P_1 + P_2 + P_3 = \mathcal{O} \longrightarrow \alpha(P_1)\,\alpha(P_2)\,\alpha(P_3) \equiv 1 \pmod{(\mathbb{Q}^\times)^2}$



x_1, x_2, x_3 x - koordinate presečnih tačaka su koreni kubne j-ne:

$$x^3 + (a - \lambda^2)x^2 + (b - 2\lambda\nu)x + \underbrace{(c - \nu^2)}_{=0} = 0$$

$$\rightarrow \quad x_1 x_2 x_3 = \nu^2 \in (\mathbb{Q}^\times)^2, \text{ ako su svi } x_i \neq 0$$

Al: $\alpha(x_j, y_j) = x_j$ za j^e

$$\alpha(P_1)\,\alpha(P_2)\,\alpha(P_3) = x_1 x_2 x_3 = \nu^2 \equiv 1 \pmod{(\mathbb{Q}^\times)^2}$$

• Dokaz za slučaj kad je neka $x_i = 0$ tj. neka od točaka $\mathcal{O}$ ili T, je domaći.

Lema 9

(i) $\ker(\alpha) = \psi\left(\bar{E}(\mathbb{Q})\right)$.

Sledstveno α indukuje injektivni homomorfizam

$$E(\mathbb{Q})/\psi\left(\bar{E}(\mathbb{Q})\right) \hookrightarrow \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$$

(ii) Neka su $p_1, p_2, \dots, p_t$ svi različiti prosti faktori koji dele b

Onda je

$$\mathrm{im}(\alpha) \leq \left\langle \left\{ \pm p_1^{E_1} p_2^{E_2} \cdots p_t^{E_t} \;\middle|\; E_j = 0, 1 \;\forall j \right\} \right\rangle \leq \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$$

podgrupa generisana ovim elementima grupe $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$

(iii) $[E(\mathbb{Q}) : \psi(\bar{E}(\mathbb{Q}))] \leq 2^{t+1}$.

(i) L.6 + L.7 primenjene na morfizam ψ.

(ii) $(x, y) \in E(\mathbb{Q})$

$$y^2 = x^3 + ax^2 + bx$$

• Ako je $x \neq 0$:

$$x = \frac{m}{M}, \quad y = \frac{n}{N}, \quad m, n \in \mathbb{Z}, \quad M, N \in \mathbb{Z}_{>0}$$
$$(m, M) = (n, N) = 1$$

$$\frac{n^2}{N^2} = \frac{m^3}{M^3} + a\frac{m^2}{M^2} + b\frac{m}{M}$$

$$M^3 n^2 = N^2 m^3 + a N^2 M m^2 + b N^2 M^2 m \qquad (*)$$

$\rightarrow$ $N^2 \mid M^3$

$\rightarrow$ $M \mid N^2$

$\rightarrow$ svi članovi jednačine osim 1. na desnoj strani su deljivi bar sa M^2 $\rightarrow$

$M^2 \mid N^2 m^3 \rightarrow M \mid N$ $\qquad$ $e := \frac{N}{M} \in \mathbb{Z}_{>0}$

$\rightarrow$ svi članovi osim 1. na desnoj str. su deljivi bar sa $M^3 \rightarrow$

$M^3 \mid N^2$

$\rightarrow$ $M^3 = N^2$

Imamo $e^2 = \frac{N^2}{M^2} = \frac{M^3}{M^2} = M$, $e^3 = \frac{N^3}{M^3} = \frac{N^3}{N^2} = N$

pa racionalna tačka $(x, y) \in E(\mathbb{Q})$ mora biti oblika

$\left(\frac{m}{e^2}, \frac{n}{e^3}\right)$, gde je još $(m, e) = (n, e) = 1$.

Posle skraćivanja j-na $(*)$ postaje

$$n^2 = m^3 + am^2e^2 + bme^4 = m\left(m^2 + ame^2 + be^4\right)$$

$d := (m, m^2 + ame^2 + be^4)$

$\rightarrow \quad d \mid be^4 \xrightarrow[(m,e)=1]{} \boxed{d \mid b}$

$$n^2 = \underset{\substack{\parallel \\ dm_1}}{m} \cdot \underbrace{(m^2 + ame^2 + be^4)}_{\substack{\parallel \\ dm_2}}$$

$(m_1, m_2) = 1$;

m_1, m_2 potpuni kvadrati

Dakle, ako je p_j prost koji se u faktorizaciji m pojavljuje sa <u>neparnim</u> stepenom, mora biti $\boxed{p_j \mid b}$ tj.

$$m = \pm \cdot \square \cdot p_1^{\varepsilon_1} p_2^{\varepsilon_2} \cdots p_t^{\varepsilon_t}, \qquad \varepsilon_j = 0, 1$$

pa je

$$\alpha(P) = x = \frac{m}{e^2} \equiv \pm p_1^{\varepsilon_1} p_2^{\varepsilon_2} \cdots p_t^{\varepsilon_t} \pmod{(\mathbb{Q}^*)^2}$$

- Ako je $x = 0$, onda je opet
  $\alpha(T) = b \pmod{(\mathbb{Q}^*)^2}$.

(iii) $|\langle \pm p_1^{\varepsilon_1} p_2^{\varepsilon_2} \cdots p_t^{\varepsilon_t} \rangle| = 2^{t+1}$.

- Potpuno analogno se pokazuje da mora biti i
  $[\bar{E}(\mathbb{Q}) : \phi(E(\mathbb{Q}))] \leq 2^{s+1}$, gde je $s = \omega(\bar{b}) = \omega(a^2 - 4b)$
- Konačno $\textcircled{L.5}$ završava dokaz $\textcircled{T.1}$.