Množenj s [2], kako izračunati $\frac{1}{2}P$?

$$E: y^2 = x^3 + ax + b$$

$2(x_P, y_P) = (x_R, y_R)$ gdje je

↑ zadano

$$x_R = \lambda^2 - 2x_P$$

$$y_R = \lambda(x_P - x_R) - y_P \quad \text{i}$$

$$\lambda = \frac{3x_P^2 + a}{2y_P} \quad . \longrightarrow y_R \cdot y_P = p(x_P)$$

$$4x_R \cdot y_P^2 = (3x_P^2 + a)^2 - 2x_P \cdot 4y_P^2$$

↗ polinom stupnja 4 u x_P ... $y_P^2 = x_P^3 + ax_P + b$

↑ kada ima racionalna rješenja?

Jedna ideja na puno načina

Kako odrediti $E(\mathbb{Q})/2E(\mathbb{Q})$?

najlakši slučaj

Neka je $E: y^2=(x-e_1)(x-e_2)(x-e_3)$

puna racionalna 2-torzija

$e_i \in \mathbb{Q}$;

Primjetimo je za $(b_1,b_2,b_3) \in \left(\mathbb{Q}^*/\mathbb{Q}^{*2}\right)^3$

t.d. je $b_1 b_2 b_3 \in \mathbb{Q}^{*2}$ pomoćnih krivulja

↖ možemo uzeti $b_3=b_1b_2$

$$H_{b_1,b_2}: \begin{cases} y_1^2 = b_1(x-e_1) \\ y_2^2 = b_2(x-e_2) \\ y_3^2 = b_3(x-e_3) = b_1b_2(x-e_3) \end{cases}$$

i.e. $b_1 y_1^2 = x-e_1$

Imamo prirodnu preslikavanje

$$\varphi: H_{b_1,b_2} \xrightarrow{4:1} E$$

$$(x,y_1,y_2,y_3) \longmapsto \left(x, \frac{y_1y_2y_3}{b_1b_2}\right)$$

Osnovna opservacija/ideja: svaka racionalna točka $P \in E(\mathbb{Q})$ se nalazi u slici $\varphi(H_{b_1,b_2}(\mathbb{Q}))$ za točno jedan par $(b_1,b_2) \in (\mathbb{Q}^*/\mathbb{Q}^{*2})^2$!

skup S

Plan: 1. Odrediti sve parove (b_1,b_2) za koje je $H_{b_1,b_2}(\mathbb{Q}) \neq \emptyset$. 2. Zatim za svaki od tih parova reći nešto o (odrediti) skupu $H_{b_1,b_2}(\mathbb{Q})$.

Tvrdnja: Ako je $H(\mathbb{Q})$ neprazan onda je $H(\mathbb{Q}_v)$ neprazan za svaki apsolutni $v = p$ i $v = \infty$.

kažemo: H je lokalno svuda rješiva (ELS)

Pretp. da $p \mid b_1$. Tada

$$b_2 y_2^2 - b_1 y_1^2 = e_1 - e_2$$

$$b_1 b_2 y_3^2 - b_1 y_1^2 = e_1 - e_3$$

rach. jednostavnosti možemo pretp. da su $e_i \in \mathbb{Z}$

S ji podskup tog

pa slijedi $p \mid e_1 - e_2$ i $p \mid e_1 - e_3$

$\Rightarrow p \mid (e_1 - e_2)(e_1 - e_3)$

Skup pa ji konačan

Propozicija: Skup parova $(b_1, b_2) \in \left(\mathbb{Q}^+ / \mathbb{Q}^{*2}\right)^2$ za koje je $H_{b_1 b_2}$ ELS je konačan.

Svi njihovi prosti faktori dijele $(e_1 - e_2)(e_1 - e_3)$

$(\, v_p(b_i) \equiv 1 \,(2)\,)$

taj skup ćemo poslije zvati Selmerova grupa

Što možemo zaključiti o skupu S analizom preslikavanja

slika je skup svih b_1-ova

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

$$P \longmapsto x(P) - e_1 \quad ?$$

prvi pristup ↓

Prethp. sveli jednostavnosti $e_1 = 0$.

misli vektor 2

Propozicija: Neka su P_1, P_2 i P_3 kolinearne racionalne točke na E. Tada je

$$x(P_1)\,x(P_2)\,x(P_3) \in \mathbb{Q}^{\times 2}$$

Dokaz: Neka se točke nalaze na pravcu $y = kx + l$. Tada su $x(P_i)$ nultočke polinoma

$E: y^2 = x(x^2 + ax + b)$

$$-(kx+l)^2 + x(x^2 + ax + b)$$

Prema Vieteovim formulama

$$-x(P_1)\,x(P_2)\,x(P_3) = l^2$$

∎

Korolar: Preslikavanj $P \mapsto x(P)$,

nakon što ga proširimo do $E(\mathbb{Q})$

s $\mathcal{O} \mapsto 1$ i $(0,0) \longmapsto b$

↑ zašto?

je homomorfizam

$$E(\mathbb{Q}) \xrightarrow{\theta} \mathbb{Q}^* / \mathbb{Q}^{*2}.$$

Dokaz: $x(P_1)x(P_2)x(P_3) \in \mathbb{Q}^{*2}$

$\Leftrightarrow$

$x(P_1)\ x(P_2) \equiv x(-(P_1+P_2)) \mod \mathbb{Q}^{*2}$

$\Leftrightarrow$

$x(P_1)\,x(P_2) \equiv x(P_1+P_2) \mod \mathbb{Q}^{*2}$.

∎

Što je $\ker\theta$? Kako izgledaju točke

iz $E(\mathbb{Q})$ čija je x-koord. potpuni kvadrat?

Jednadžba krivulje koja opisuje takve točke dobijemo supstitucijom $t = x^2$

$$y^2 = x^2(x^4 + ax^2 + b) \text{ tj.}$$

$$C : Y^2 = X^4 + aX^2 + b$$

$$C \longrightarrow E$$

$$(x, y) \overset{\alpha}{\mapsto} (x^2, y \cdot x)$$

ali nesing.

u težinskom projekt. prostoru

Uočimo $(x, y) \xrightarrow{\alpha} (x^2, yx)$

$(-x, -y) \xrightarrow{\alpha} (x^2, yx)$

preslikavanje je 2:1.

možemo primijeniti

Riemann - Hurwitzovu formulu nakon razrješenja singulariteta.

u $\mathbb{P}^2$

C je singularna krivulja genusa 1

s racionalnom točkom u beskonačnosti

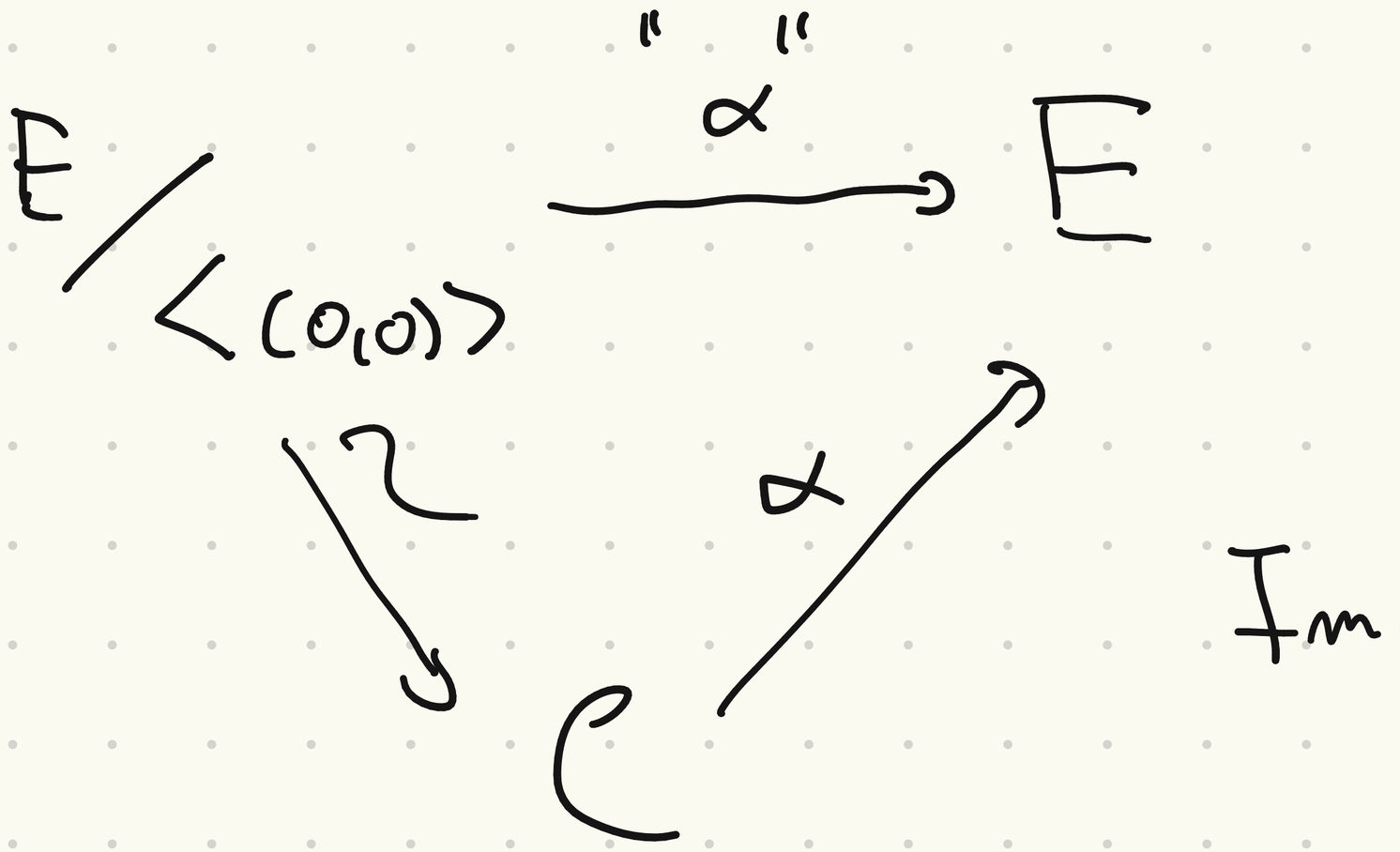
C ima dvije singularne točke u ∞.

$\Rightarrow C$ je biracionalno izomorfna s

eliptičkom krivuljom ↑

dz. izračunajte Weierst. model

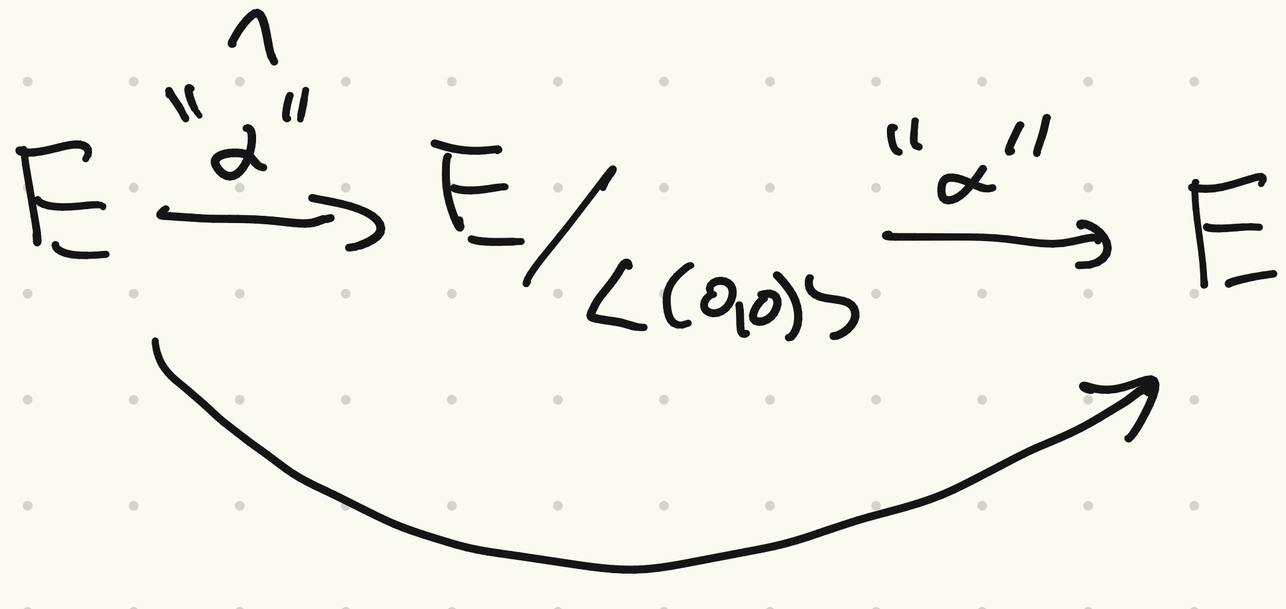
Dakle, "α" je 2- izogenija. (zašto ?)



$\mathrm{Im}\,\alpha = \mathrm{Im}\,\text{"}\alpha\text{"}$

Što možemo reći o $\mathrm{Im}\,\alpha$?

Znamo



[2]

pa $\mathrm{Im}\,\alpha$ sadrži [2] $E(\mathbb{Q})$!

$$E(\mathbb{Q}) \to \mathbb{Q}^*/\mathbb{Q}^{*2}$$
$$P \overset{\theta}{\mapsto} \chi(P)$$

$$\Rightarrow \quad E(\mathbb{Q})/\ker\theta \hookrightarrow \mathbb{Q}^*/\mathbb{Q}^{*2}$$

+ znamo da je slika od θ sadrzana u konacnom skupu

$$\Rightarrow E(\mathbb{Q})/2E(\mathbb{Q}) \text{ je konacan jer}$$

zašto? d.z.

je $[\ker\theta : 2E(\mathbb{Q})]$ konacan

$$\ker\theta = \mathrm{Im}\,\alpha$$

d.z. čemu je jednak?

drugi dokaz ove tvrdnje (koji samo zahtijeva jednu točku reda 2, $(0,0)$):

Neka je $\left(\frac{m}{e^2}, \frac{n}{e^3}\right) \in E(\mathbb{Q})$; $e, m, n \in \mathbb{Z}$. Uvrsti. dobivamo rel. prosti

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

Neka je $d = \gcd(m, m^2 + ame^2 + be^4)$. Tada

$d \mid m$ i $d \mid b e^4$. Ali $(m,e)=1 \Rightarrow d \mid b$

$\Rightarrow$ svaki p koji dijeli m se javlja s

parnom potencijom osim možda onih

koji dijele b

$\Rightarrow$ slika od Θ je konačna

Pristup preko divizora - kako možemo

vidjeti da je $x(2P)$ potpuni kvadrat za

$P \in E(\mathbb{Q})$ (gdje je $y^2 = x(x^2+ax+b)$?

Neka su $T_1, T_2 \in E[2]$ generatori

$\| \qquad\qquad$ i $f(P) = x(2P)$

$(0,0)$

$$\operatorname{div} f = \sum_{T \in E[2]} 2(R+T) - \sum_{T \in E[2]} [T]$$

jer je $\operatorname{div} x = 2(0,0) - 2\mathcal{O}$

jedn je $2R = (0,0)$.

Primijetimo da je $\sum_{T \in E[2]} (R+T) - \sum_{T \in E[2]} (T)$ divizor

neke racion. funkcije. zašto?

Neka je $g \in \mathbb{Q}(E)$, $\operatorname{div} g = \sum_T (R+T) - \sum_T (T)$

Tada je $f = c \cdot g^2$ za neka konstanta $c \in \mathbb{Q}$.

zašto 2.

Kako možemo zaključiti da je c potpun kvadrat?

Možemo ovim pristupom doći i do 2-izogenije...

Ako je $\varphi : E' \to E$ 2-izogenija s jezgrom $\langle T \rangle$

kod koje je $\varphi(R) = (0,0)$ onda je $T \in E'(\mathbb{Q})$

prekp.
$E'[2](\mathbb{Q}) = \langle T \rangle$.

$$\operatorname{div} x \circ \varphi = 2(R) + 2(R+T) - 4(O)$$

Je li $(R) + (R+T) - 2(O)$ divizor racion.

funkcije na E'? Znamo $\varphi(2R) = 2 \cdot \varphi(R) = 2 \cdot (0,0) = O$

$\Rightarrow 2R = T$ ili $2R = O$. U prvom slučaju

je odgovor pozitivan jer $R + R + T = T + T = O$

pa je $x \circ \varphi = c \cdot g^2$ kao i ranije.

Neka je $\sigma \in \operatorname{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. Tada je $\sigma(R) = R$ ili

$\sigma(R) = R + T$. Zašto? Kopi je polje definicije od R?

Odaberimo sad jedan par (b_1, b_2)

za koji je $H_{b_1 b_2}(Q) \neq \emptyset$.

Što možemo reći o $\varphi(H(Q))$?