[1] Grupna operacija na eliptičkim krivama

"Weierstrass-ova uniformizacija" daje bijekciju

$$\mathbb{C}/L \longleftrightarrow \underbrace{\{[(x;y;z)] \in \mathbb{P}^2_{\mathbb{C}} \mid zy^2 = 4x^3 - g_2(L)xz^2 - g_3(L)z^3\}}_{E_L \subseteq \mathbb{P}^2_{\mathbb{C}}}$$

ali ovo je već očitma grupa!

$$(z_1 + L) + (z_2 + L) = (z_1 + z_2) + L$$

- Ovu bijekciju možemo iskoristiti za 'prenošenje' grupnog zakona sa torusa $\mathbb{C}/L$ na eliptičku krivu E_L:
  - za dve date tačke $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ na E_L
    $$y_i^2 = 4x_i^3 - g_2 x_i - g_3, \quad i = 1, 2$$
    nađemo originale $z_1, z_2 \in \mathbb{C}$ za koje je
    $$P_1 = (\wp(z_1), \wp'(z_1)) \quad ; \quad P_2 = (\wp(z_2), \wp'(z_2))$$
    i definišemo
    $$\boxed{P_1 + P_2 := (\wp(z_1 + z_2), \wp'(z_1 + z_2))}$$

- Ali dodatno
  1) postoji geometrijska interpretacija ove operacije 'sabiranja tačaka'!
  2) koordinate tačke $P_1 + P_2$ se mogu izraziti kao racionalne funkcije po x_1, y_1, x_2, y_2
  (ovo omogućava rad nad proizvoljnim poljima K, a ne samo nad $\mathbb{C}$!)

$\boxed{2}$ Koristiću kraći zapis:

za $z \in \mathbb{C}$ (tj. $\mathbb{C}/L$) sa $P_z = (\wp(z), \wp'(z), 1) \in E_L \subseteq \mathbb{P}^2_{\mathbb{C}}$

$P_0 = (0, 1, 0)$

- Dakle za $P_{z_1} = (x_1, y_1)$ i $P_{z_2} = (x_2, y_2)$ želimo da odredimo $P_{z_1+z_2} = (x_3, y_3)$ direktno na E_L (bez vraćanja na $\mathbb{C}/L$)

(i) <u>aditivni neutral</u> je slika neutrala $z=0$ (tj. koseta $L \in \mathbb{C}/L$) a to je baš tačka u beskonačnosti:

$$\mathcal{O} := (0, 1, 0) \in E_L$$

$$\mathcal{O} + P_{z_1} = P_0 + P_{z_1} = P_{0+z_1} = P_{z_1} \quad \text{za} \quad \forall P_{z_1} \in E_L$$

(ii) U slučaju da P_{z_1}, P_{z_2} imaju istu x-koordinatu, ali su različite tačke:

$$(x_2, y_2) = (x_1, -y_1)$$

$$\wp(z_1) = x_1 = \wp(z_2)$$

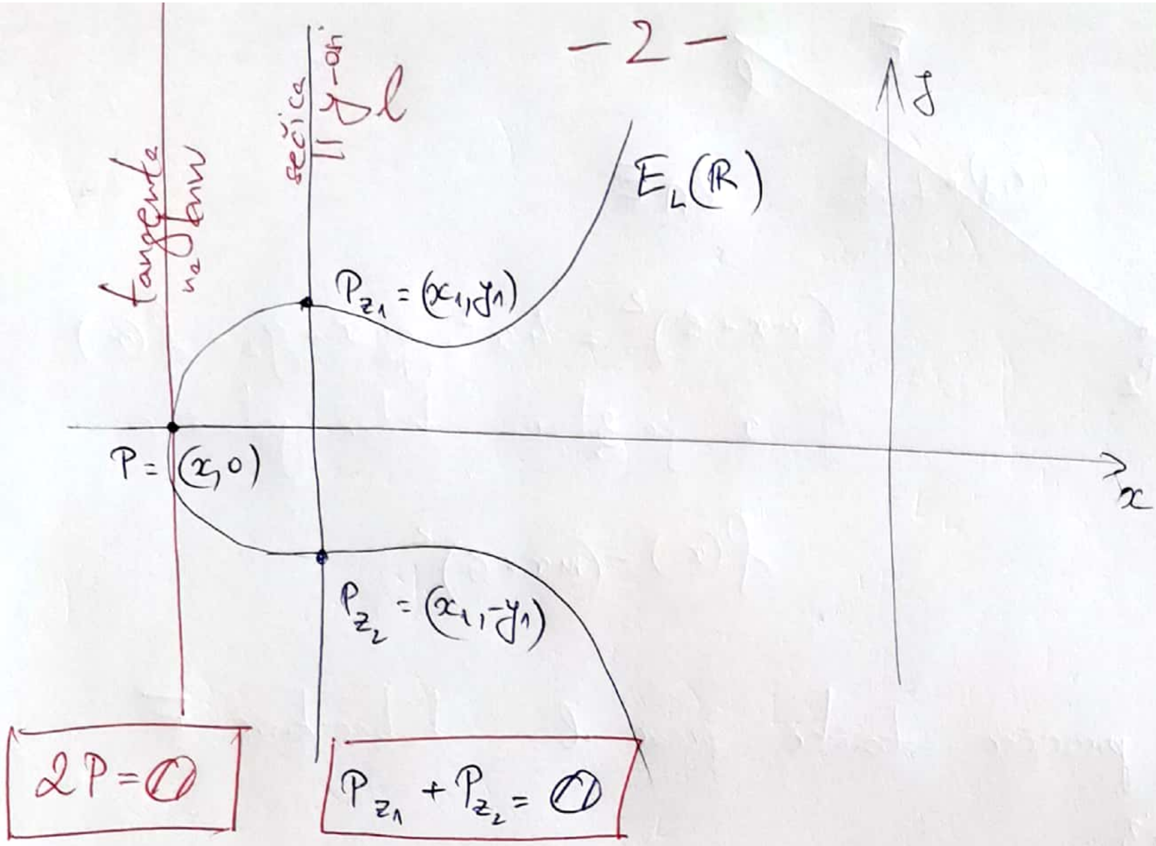
Ovo smo već rešavali ranije! - ima 2 rešenja z_1 i $z_2 = z_1^*$ koja su 'simetrična' na fund. domenu (tj. aditivna inverzna modulo rešetka L) i tada je zaista i

$$y_2 = \wp'(z_2) = \wp'(z_1^*) = -\wp'(z_1) = -y_1$$

Dakle $z_2 = -z_1$ (tj. koset $-z_1 + L \ldots$), pa je

$$P_{z_1} + P_{z_2} = P_{z_1+z_2} = P_{z_1+(-z_1)} = P_0 = \mathcal{O}$$

tj. ovakve dve tačke su međusobno inverzne!



Specijalno ako je $P \in E_L$ na x-osi, tj. u slučaju $P_{z_1} = P_{z_2} = (x, 0)$ $(y_2 = -y_1 = 0)$ dobijamo da je

$$2P = P + P = P_{z_1} + P_{-z_1} = P_0 = \mathcal{O}$$

Dakle:

(L.1) Ako je $P = (x, y) \in E$, onda je $-P = (x, -y)$.

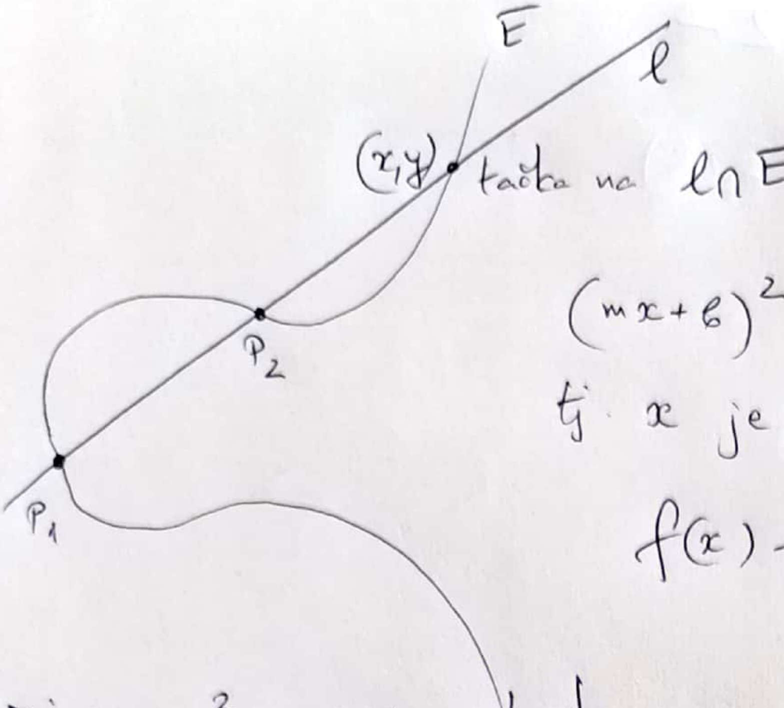
(iii) $l = \overline{P_1 P_2}$ sečica kroz $P_1 = (x_1, y_1)$; $P_2 = (x_2, y_2)$ $(\neq \mathcal{O})$ tačka u beskonačnosti

(ili tangenta na E, ako su $P_1 = P_2$)

Neka sada l "nije vertikalna". Hoćemo da nađemo koordinate tačke $P_3 = P_1 + P_2$

$$\overset{\shortparallel}{(x_3, y_3)}$$

$l = \overline{P_1 P_2}$: $y = mx + b$



$$(mx+b)^2 = 4x^3 - g_2 x - g_3 = f(x)$$

tj. x je 3. koren kubne jednačine

$$f(x) - (mx+b)^2$$

→ imamo $\underset{1\cdot 3}{\overset{\|}{3}}$ presečne tačke prave l i kubne krive E

→ U slučaju (ii), kada je prava l vertikalna, takođe imamo 3 presečne tačke: P_{z_1}, P_{z_2} i $\mathcal{O}$ – tačka u beskonačnosti.

→ U slučaju da je prava l prava u beskonačnosti $\{z=0\}$ presek prave l i projektivizacije eliptičke krive E je:

$$\begin{array}{l} l: \\ E: \end{array}\left\{\begin{array}{l} z=0 \\ zy^2 = 4x^3 - g_2 x z^2 - g_3 z^3 \end{array}\right\} \longrightarrow \boxed{4x^3=0}$$

višestrukost nule je 3,

pa je i višestrukost preseka l i E takođe 3!

Ovo sve su specijalni slučajevi sledeće teoreme:

T.2 [<u>Bezout-ova teorema</u>] K - algebarski zatvoreno polje

Neka su $\tilde{F}(x,y,z)$ i $\tilde{G}(x,y,z)$ homogeni polinomi iz $K[x,y,z]$ stepena m, odnosno n, pri čemu $\tilde{F}$ i $\tilde{G}$ nemaju zajednički polinomni faktor (=nekonstantan).

Onda projektivne krive $\{\tilde{F}=0\}$ i $\{\tilde{G}=0\}$ u projektivnoj ravni $\mathbb{P}^2_K$ imaju $\boxed{\text{tačno } m \cdot n}$ presečnih tačaka, ako ih računamo sa višestrukostima.

Tvrđenje.3 Ako su P_1 i P_2 tačke na eliptičkoj krivoj E i ako je $P_1+P_2=P_3$, onda je $-P_3$ treća presečna tačka prave $l=\overline{P_1P_2}$ i E. Pritom, ako je $P_1=P_2$ prava l je tangenta na krivu E u tački P_1 (a tangenta uvek postoji u svakoj tački, jer zahtevamo da je kriva glatka)

▽. Specijalni slučajevi kad je jedna od P_1 ili P_2 u beskonačnosti, ili kad je $P_2=-P_1$, zadovoljavaju Tvrđenje.

- zato, neka je $l=\overline{P_1P_2}$ oblika $y=mx+b$,
  $P_1=P_{z_1}$, $P_2=P_{z_2}$

Tačka $P_z=(\wp(z),\wp'(z))$ je na l $\Longleftrightarrow$ $\boxed{\wp'(z)=m\wp(z)+b}$

Eliptička f-ja $\wp'(z)-m\wp(z)-b$ ima 3 pola, pa prema "L3" ima 3 nule u $\mathbb{C}/L$.

$\boxed{\text{Lema 4}}$ $f(z) \in \mathcal{E}_L$; Π – (zatvoreni) fundamentalni paralelogram za L; $\alpha \in \mathbb{C}$ takav da $f(z)$ nema ni nule ni polove na $\partial(\alpha + \Pi)$.

Neka su:

$\{a_i\}$ sve nule od $f(z)$ u $\alpha+\Pi$, svaka ubrojana sa svojom višestrukošću

$\{b_j\}$ svi polovi $f(z)$ u $\alpha+\Pi$, svaki računat sa svojom višestrukošću.

Onda je

$$\boxed{\sum_i a_i - \sum_j b_j \in L}$$

Primenimo (L4) na $\wp'(z) - m\wp(z) - b$:

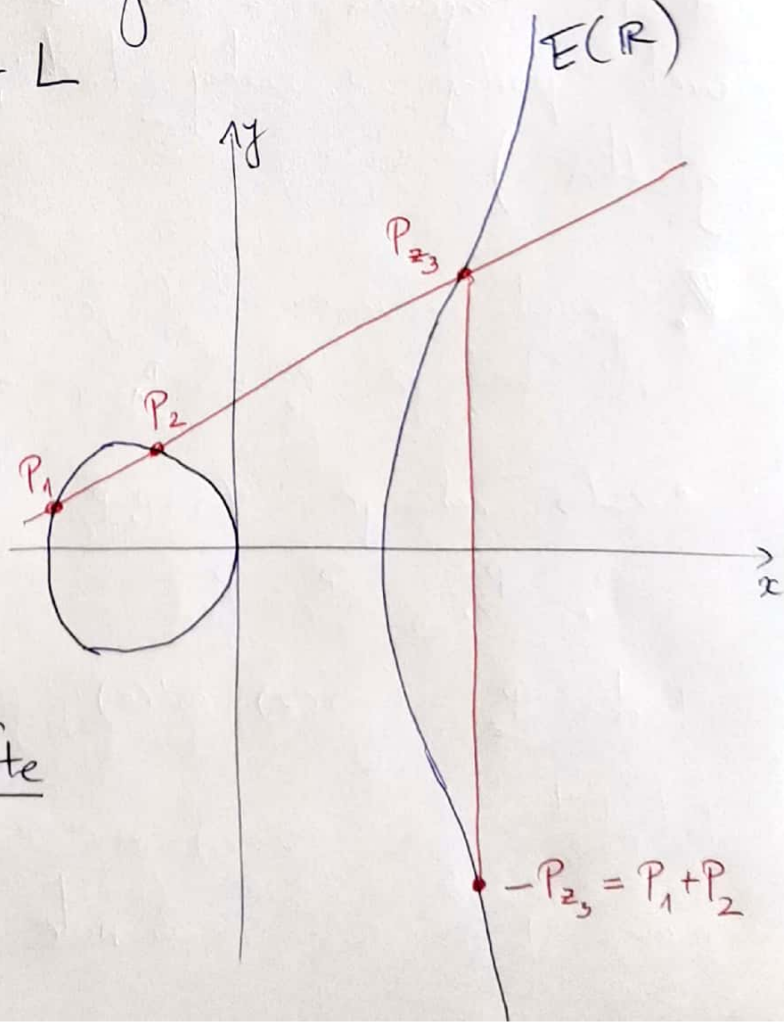
$$z_1 + z_2 + z_3 - 3 \cdot 0 \in L$$

3. nula

pol reda 3 u 0

$\rightarrow \quad z_3 = -(z_1+z_2) + L$

$\rightarrow \quad P_{z_1+z_2} = -P_{z_3}$



- Prethodni argument je korektan ako ℓ preseca E u 3 <u>različite</u> tačke.

- Inače, moramo još dokazati da dvostruka ili trostruka nula eliptičke fje $\wp'(z) - m\wp(z) - b$ odgovara preseku l sa E koji je višestrukosti 2 ili 3.

- Neka su z_1, z_2, z_3 tri nule jednačine

$$\wp'(z) - m\wp(z) - b = 0 \qquad (1)$$

izlistane sa višestrukostima (dakle dozvoljavamo i ponavljanje...)

l nije 'vertikalna' prava, pa $z_i \neq -z_j$ za sve $i \neq j$

- Onda su $z_1, -z_1, z_2, -z_2, z_3, -z_3$ svih 6 nula eliptičke funkcije

$$\wp'(z)^2 - (m\wp(z)+b)^2 = f(\wp(z)) - (m\wp(z)+b)^2$$
$$= 4(\wp(z) - v_1)(\wp(z) - v_2)(\wp(z) - v_3)$$

gde su v_1, v_2, v_3 tri kompleksna korena polinomne kubne jednačine

$$f(v) - (mv+b)^2 = 0$$

- ako su ovde npr. $v_1 = v_2 \neq v_3$,

to znači da prava l ima sa E dvostruku presečnu tačku (sa x-koordinatom v_1)

Ako je z_1 koren npr. $\wp(z) - v_1 = 0$, onda je i $-z_1 (= z_1^*)$ drugi koren ove jednačine.

Ali onda se među $z_2, -z_2, z_3, -z_3$ nalaze 2 nule 2. faktora $\wp(z) - v_2 = \wp(z) - v_1$, što znači da je $z_1 = z_2$ ili $z_1 = z_3$ (ako bi sve 3 bile $=$, kontradikcija...)

Dakle tačno 2 nule f-je (1) su iste, 3. je različita

• Slično, ako je $v_1 = v_2 = v_3$, mora biti $z_1 = z_2 = z_3$.

Ostaje dokaz (L4):

$\dfrac{f'(z)}{f(z)}$ ima polove u nulama & polovima $f(z)$

$$= \frac{m}{z-a} + \dots \quad (\text{oko nule } a \text{ reda } m \text{ f-je } f(z))$$

$$= \frac{-n}{z-b} + \dots \quad (\text{oko pola } b \text{ reda } n \text{ f-je } f(z))$$

Funkcija $\dfrac{z \cdot f'(z)}{f(z)}$ ima polove (proste) u istim tačkama

kao : $\dfrac{f'(z)}{f(z)}$, (osim ako je neko a_i ili b_j jednako 0; ali $0 \in L$ pa je O.K. za tvrđenje!)

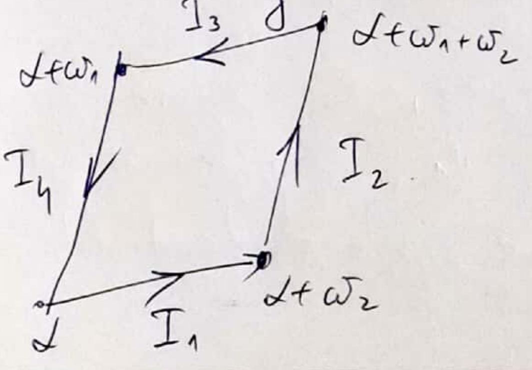
$$\frac{zf'(z)}{f(z)} = \frac{mz}{z-a} + \dots = \frac{m(a+(z-a))}{z-a} + \dots = \frac{ma}{z-a} + \dots \quad (\text{oko nule } a)$$

$$= \frac{-nz}{z-b} + \dots = \frac{-n(b+(z-b))}{z-b} + \dots = \frac{-nb}{z-b} + \dots \quad (\text{oko pola } b)$$

rezidumi

Dakle

$$\sum_i a_i - \sum_j b_j = \sum_{\text{unutar } \alpha+\Pi} \operatorname{res} \frac{zf'(z)}{f(z)} = \frac{1}{2\pi i} \int_{\partial(\alpha+\Pi)} \frac{zf'(z)}{f(z)} dz$$



Cauchy-jeva T.

$= I_1 + I_2 + I_3 + I_4$, oznake sa slike

$$I_1 + I_3 = \frac{1}{2\pi i}\int_{\alpha}^{\alpha+\omega_2} z\frac{f'(z)}{f(z)}\,dz + \frac{1}{2\pi i}\int_{\alpha+\omega_1+\omega_2}^{\alpha+\omega_1} z\frac{f'(z)}{f(z)}\,dz$$

$$= \frac{1}{2\pi i}\int_{\alpha}^{\alpha+\omega_2} z\frac{f'(z)}{f(z)}\,dz \underbrace{- \frac{1}{2\pi i}\int_{\alpha+\omega_1}^{\alpha+\omega_1+\omega_2} z\frac{f'(z)}{f(z)}\,dz}_{}$$

smena: (novo z) = (staro $z - \omega_1$)

$$\underbrace{-\frac{1}{2\pi i}\int_{\alpha}^{\alpha+\omega_2} (z+\omega_1)\frac{f'(z+\omega_1)}{f(z+\omega_1)}\,dz}_{\boxed{f \text{ eliptička}}}$$

$$-\frac{1}{2\pi i}\int_{\alpha}^{\alpha+\omega_2} (z+\omega_1)\frac{f'(z)}{f(z)}\,dz$$

$$= -\frac{\omega_1}{2\pi i}\int_{\alpha}^{\alpha+\omega_2} \frac{f'(z)}{f(z)}\,dz = -\omega_1 \cdot \boxed{\frac{1}{2\pi i}\int_{\mathcal{C}} \frac{du}{u}} = -n\omega_1$$

Smena promenljivih: $u = f(z)$, $\frac{du}{u} = \frac{f'(z)\,dz}{f(z)}$

$\mathcal{C}$ = put od $f(\alpha)$ do $f(\alpha+\omega_2) = f(\alpha)$ (zatvoren put!)

koji prođe $u = f(z)$ ↑eliptička

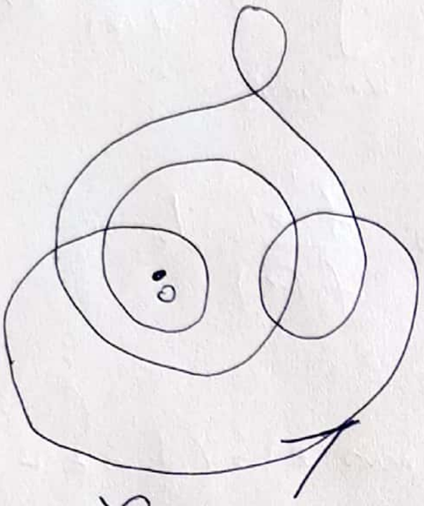
kad z prolazi od α do $\alpha+\omega_2$

$$\frac{1}{2\pi i}\int_{\mathcal{C}} \frac{du}{u} = n = \text{"winding number"}$$

neki ceo broj

$= $ broj puta koliko zatvoreni put $\mathcal{C}$ obiđe 0 (ako za pozitivno usmerenje uzmemo – suprotno kazaljki na satu)

(pogledajte npr. Ahlfors-ovu knjigu)



$\mathcal{C}$

Potpuno analogno, $I_2 + I_4 = -\omega_2 m$, za neko $m \in \mathbb{Z}$

Zajedno,

$$\sum a_i - \sum b_j = -n\omega_1 - m\omega_2 \in L$$

$\boxed{3}$ Sada ovu geometrijsku proceduru možemo da sprovedemo i nad opštijim krivama

(ne moraju biti oblika $y^2 = 4x^3 - g_2(L)x - g_3(L)$, za neku rešetku $L \leq \mathbb{C}$)

– koje su dodatno i definisane nad proizvoljnim poljem K

Npr.

$$E: \; y^2 = f(x) = ax^3 + bx^2 + cx + d \in \mathbb{C}[x]$$

pri čemu f ima sve korene različite

- P_1, P_2 obe $\neq \mathcal{O}$; $P_1 \neq -P_2$; onda: $P_i = (x_i; y_i)$, $i = 1, 2$
- prava $\overline{P_1 P_2}$: $y = mx + b$

$$m = \frac{y_2 - y_1}{x_2 - x_1}, \quad \text{ako} \quad P_1 \neq P_2$$

$$m = \left.\frac{dy}{dx}\right|_{(x_1, y_1)} \quad \text{ako} \quad P_1 = P_2$$

$$= \frac{f'(x_1)}{2y_1}$$

(implicitnim diferenciranjem
$y^2 = f(x)$
$2y\,dy = f'(x)\,dx$)

U oba slučaja $b = y_1 - m x_1$

- $x_3 =$ x-koordinata $P_1 + P_2$ = 3. koren kubne jednačine $f(x) - (mx + b)^2$

$$x_1 + x_2 + x_3 = -\frac{b - m^2}{a}$$

(2)

$$x_3 = -x_1 - x_2 - \frac{b}{a} + \frac{1}{a}\left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2, \quad \text{ako} \quad P_1 \neq P_2$$

$$x_3 = -2x_1 - \frac{b}{a} + \frac{1}{a}\left(\frac{f'(x_1)}{2y_1}\right)^2, \quad \text{ako} \quad P_1 = P_2$$

- $$y_3 = -(m x_3 + b) = -y_1 + m(x_1 - x_3), \quad m = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1}, & P_1 \neq P_2 \\ \frac{f'(x_1)}{2y_1}, & P = P_2 \end{cases}$$

Dakle, x_3, y_3 su racionalne f-je po x_1, x_2, y_1, y_2

Primedba Grupni zakon smo mogli da definišemo direktno ovim formulama.

Onda bi posao bio da se verifikuju aksiome Abelove grupe. Najteži bi bio dokaz asocijativnosti

$$(P+Q)+R = P+(Q+R)$$

za bilo koje 3 tačke P, Q, R na eliptičkoj krivoj.

- Dakle, ako je K polje $\operatorname{char} K \neq 2$,

$$y^2 = f(x) = ax^3 + bx^2 + cx + d \in K[x],$$

i definišemo $f'(x) = 3ax^2 + 2bx + c$,

onda za bilo koje raširenje $K' \supseteq K$, dve tačke $P_1, P_2 \in E(K')$ možemo sabrati formulama (2).