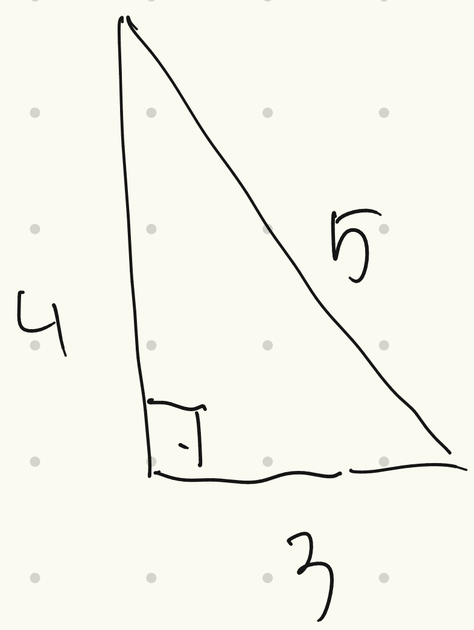
Fermatov beskonačan spust i eliptičke krivulje

Motivacijski problem:

Racionalan broj je kongruentan ako je jednak površini nekog pravokutnog trokuta s racionalnim stranicama.

6 je kongruentan broj

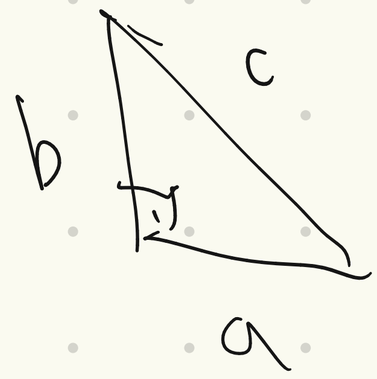


Teorem (Fermat)

1 nije kongruentan broj 'ih'

ekvivalentno, ne postoji pravokutan trokut s cjelobrojnim stranicama čija je površina potpun kvadrat.

Dokaz: Pretp. suprotno, neka je



$a,b,c \in \mathbb{Z}$ t.d. $P = \frac{1}{2}ab$ potpun kvadrat.

Možemo pretp. da su a, b, c u parovima relativno prosti (zašto?). Tada postoji (Pitagorina trojka) $m, n \in \mathbb{N}$ relativno prosti t.d.

$$a = m^2 - n^2, \quad b = 2mn, \quad c = m^2 + n^2$$

gdje $m > n$ i m, n nisu oboji neparni.

Tada, po pretpostavci, postoji $d \in \mathbb{N}$ t.d.

$$P(\Delta) = d^2 = \frac{1}{2}ab = mn(m^2 - n^2)$$

$\exists\, p, q, r \in \mathbb{N}$ $\Longleftarrow$ faktori su relat. prosti.

t.d. $m = p^2$, $n = q^2$, $m^2 - n^2 = r^2$

$\Rightarrow$ $\boxed{p^4 - q^4 = r^2}$

p, q su relativno prosti + različite parnosti

pokazat ćemo da ova jednadžba ne može imati netrivijalna rješenja.

↑ ona za koju je $pqr \neq 0$.

Propozicija (Fermat): Jednadžba

primitivno rješenje

$$x^4 - y^4 = z^2$$

nema rješenja u $\mathbb{N}$

što ako nisu?

t.d. $(x,y) = 1$ i x i y su različite parnosti.

Dokaz: Pretp. suprotno. Neka je (p,q,r) takvo rješenje. Tada $(p^2 - q^2)(p^2 + q^2) = r^2$.

← relativno prosti

$\exists$ sit relativno prosti t.d.

$$p^2 - q^2 = s^2$$

$$p^2 + q^2 = t^2$$

$\Rightarrow$ s,t su neparni.

$$t^2 = s^2 + 2q^2$$

$$\left(\frac{t+s}{2}\right)\left(\frac{t-s}{2}\right) = \frac{1}{2}q^2$$

↑ relativno prosti → ↑ parnog broja

$\Rightarrow$ jedan od faktora s lijeve strane je parnog

$$\Rightarrow \left(\frac{t \pm s}{2}\right)\left(\frac{t \mp s}{u}\right) = \left(\frac{q}{2}\right)^2$$ ← kvadrat u $\mathbb{N}$!

zašto?

$$\Rightarrow \pm s = u^2 - 2v^2 \qquad q = 2uv$$

$$t = u^2 + 2v^2$$

$$\Rightarrow p^2 = q^2 + s^2 = (2uv)^2 + (u^2 - 2v^2)^2$$

$$= u^4 + 4v^4$$

↑ →

važan međukorak, dobili smo rješenja (u, v, p) jednadžbe $x^4 + 4y^4 = z^2$ (iz rješenja jednadžbe $x^4 - y^4 = z^2$)

$\Rightarrow (u^2, 2v^2, p)$ je primitivna Pitagorina trojka s površinom $(uv)^2$ ← kvadrat!

Kao na početku, takva trojka daje još jedno primitivno rješenje (p', q', r') jednadžbe $x^4 - y^4 = z^2$.

No, $p' < p'^4 + q'^4 = m'^2 + n'^2 = p$.

↑ → →

proširite se formula.

Dakle, novo rješenje ima x - koordinatu (koja je prirodan broj) manju od prethodnog rješenja. Ako ovaj postupak ponavljamo dobit ćemo u jednom trenutku kontradikciju jer postoji konačno mnogo prirodnih brojeva manjih od p. ∎

Možemo li bolje razumjeti ovaj dokaz? Što se ovdje dešava?

Kvadrati su od primitivnog rješenja (p,q,r) jednadžbe $C: x^4 - y^4 = z^2$ i iz njega konstruirali rješenje (u,v,p) jednadžbe $\tilde{C}: x^4 + 4y^4 = z^2$ dok smo iz tog rješenja opet konstruirali rješenje (p',q',r') jednadžbe C.

Promotrimo pravo $C \hookrightarrow \hat{C}$, $(p,q,r) \mapsto (u,v,p)$.

Koja je veza između ovih rješenja? Ako pogledamo formule vidimo da (p,q,r) možemo prikazati kao polinome u u,v i p

odnosno možemo definirati preslikavanje koje

$\psi : \hat{C}(\mathbb{Q}) \hookrightarrow C(\mathbb{Q})$ pridružuje rješenju (u,v,p) od $\hat{C}$ pripadno rješenje od C.

↑ skup rješenja jednadžbe iz $\mathbb{Q}$

↑ nije bitno u kojem polju gledamo rješenje.

$$\psi((u,v,p)) = (p, 2uv, (u^2-2v^2)(u^2+2v^2))$$ ↑ najpripadniji $\mathbb{Q}$

Fermatov argument pokazuje da za svaki primitivno rješenje (p,q,z) od C postoji primitivno rješenje (u,v,p) od $\hat{C}$ t.d. $\psi(u,v,p) = (p,q,r)$.

Sličnu, primitivnom rješenju (u, v, p) od $\hat{C}$ smo u dokazu pridružili rješenje (p', q', r') od C što (ako pogledamo formule) pokazuje da možemo definirati preslikavanje

$$\hat{\varphi} : C(\mathbb{C}) \to \hat{C}(\mathbb{C})$$

$$(P, Q, R) \longmapsto (R, PQ, P^4 + Q^4)$$

od $\hat{C}$

takvo da za rješenje (u, v, p) dobivamo u pretkoraku korak poslije rješenje (p', q', r') od C t.d. $\hat{\varphi}(p', q', r') = (u, v, p)$.

Vidjet ćemo, C i $\hat{C}$ su

eliptičke krivulje dok su φ i $\hat{\varphi}$

izogenije između njih!

Eliptičke krivulje

Za nas će eliptičke krivulje biti skup rješenja jednadžbe

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

Weierstrassov model

općenitije: $y^2 = x^3 + ax^2 + bx + c$

, gdje su $a, b \in \mathbb{Q}$

takvi da polinom $x^3 + ax + b$ nema višestrukih nultočki nad $\mathbb{C}$ (odnosno diskr. $\neq 0$).

Zašto "su" C i $\hat{C}$ eliptičke krivulje?

$$C: \quad x^4 - y^4 = z^2 \quad / : y^4$$

$$\left(\frac{x}{y}\right)^4 - 1 = \left(\frac{z}{y^2}\right)^2$$

$$s^4 - 1 = t^2$$

gdje je $s = \frac{x}{y}$, $t = \frac{z}{y^2}$

Očnosno $\hat{C}: x^4 + 4y^4 = z^2 \quad / : y^4$

$\downarrow$

$$s^4 + 4 = t^2$$

Ako sada uvrstimo $t := w + s^2$ u obje jednadžbe dobit ćemo za C

$$s^4 - t = (w + s^2)^2 = w^2 + 2ws^2 + s^4 \quad / \cdot w$$

$$-w = w^3 + 2(ws)^2 \; ; \quad ws = \alpha$$

$$2\alpha^2 = w^3 + w \quad / 8 \qquad \tilde{w} = 2w$$

$$\tilde{\alpha} = 4\alpha$$

$$E: \; \tilde{\alpha}^2 = \tilde{w}^3 + 4\tilde{w}$$

↑ eliptička krivulja!

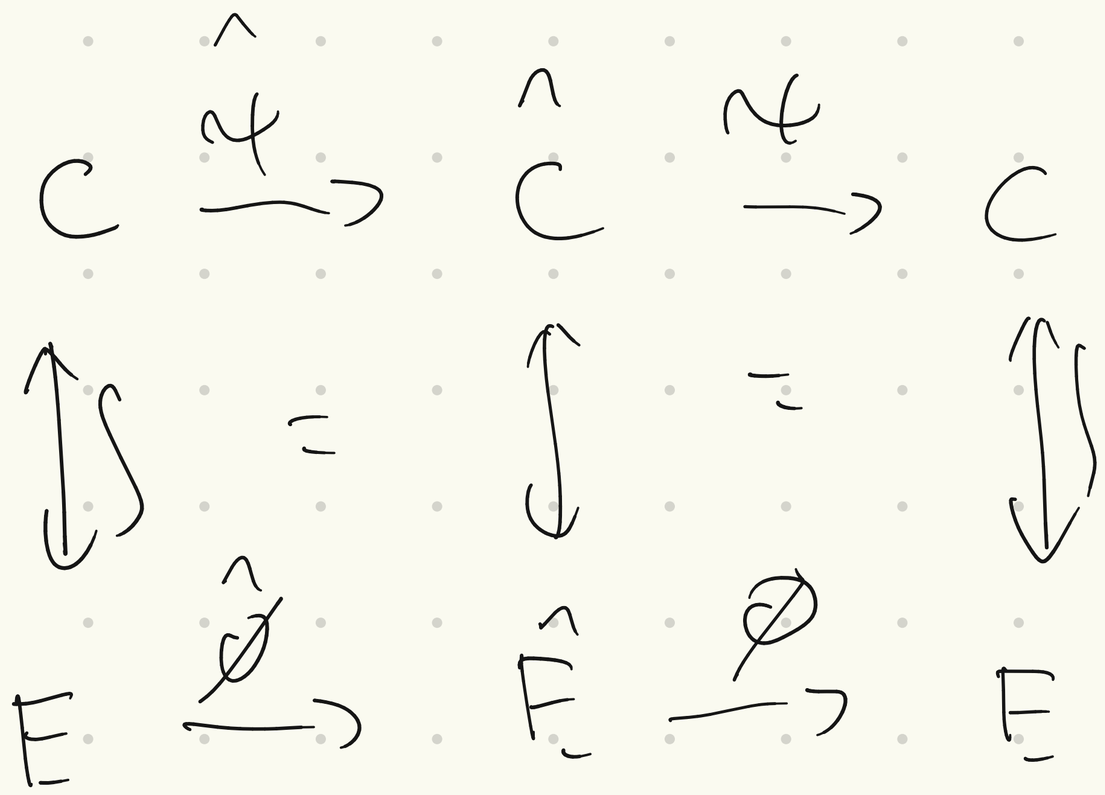
Slično i za $\hat{C}$, dobije se

$$\hat{E}: \; \tilde{\alpha}^2 = \tilde{w}^3 - \tilde{w}$$

Zadatak 1: Prikažite $\tilde{x}, \tilde{w}$ pomoću x, y, z u oba slučaja (C i $\hat{C}$).

Preslikavanja ψ i $\hat{\psi}$ sada inducirana preslikavanja ϕ i $\hat{\phi}$ između E i $\hat{E}$ t.d.

sljedeći dijagram komutira:



Lako se vidi da su ϕ i $\hat{\phi}$ definirani

preko racionalnih funkcija.

Zadatak 2: U gornjem dijagramu

$(a_1, a_2) \in E \rightsquigarrow (p', q', r') \in C$

$(a_1', a_2') \in \hat{E}$ gdje $(u, v, p) \in \hat{C}$

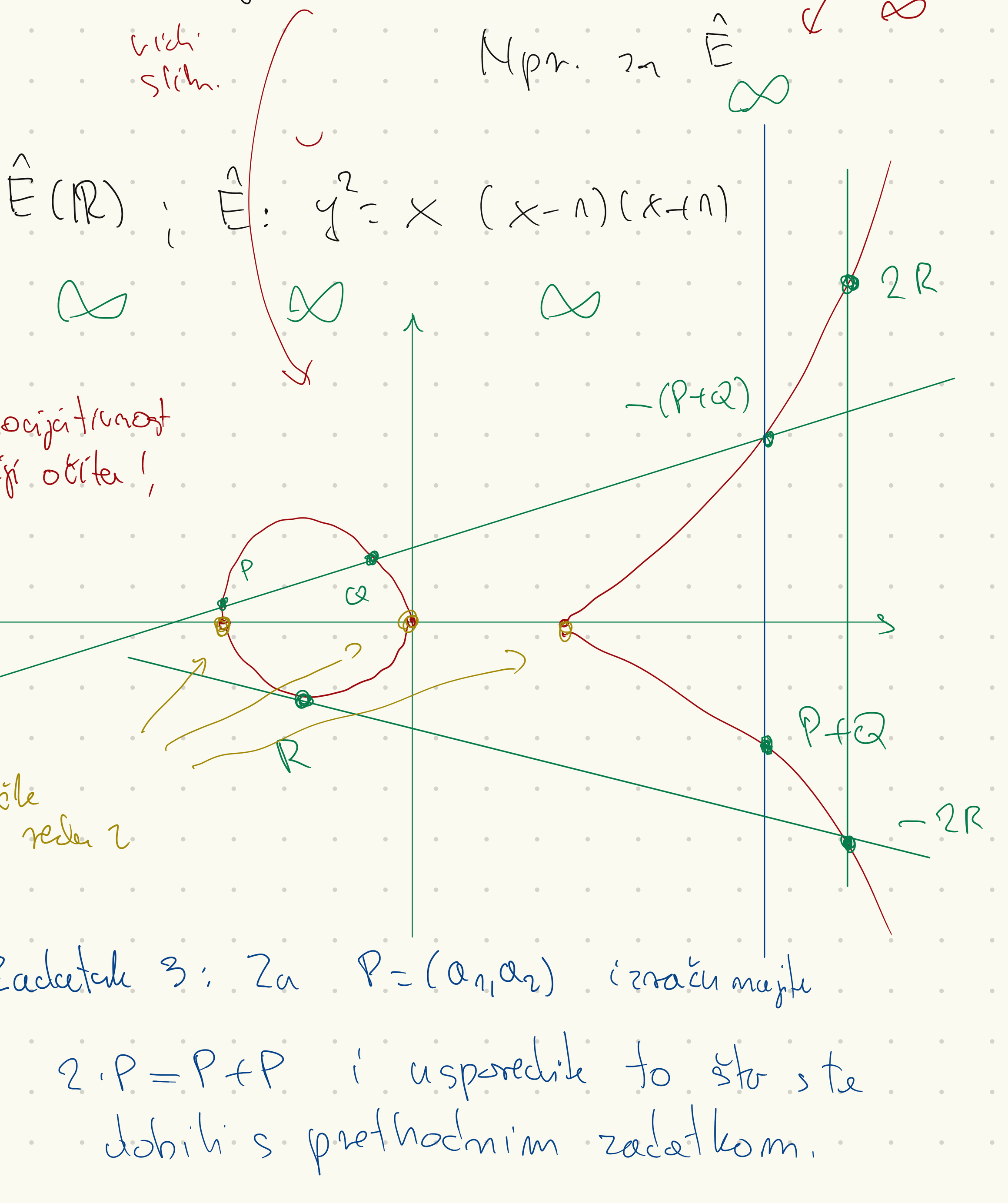
izrazite a_1' kao racionalnu funkciju od a_1 (ovisnost o b_1 će nestati)

Što ji tu zanimljivo?

nad bilo kojim polje (pa i konačnim)

Općenito, na skupu rješenja eliptičke krivulje (na skupu točaka) možemo definirati grupovnu operaciju koristeći algebarsku geometriju:

Npr. za $\hat{E}$



asocijativnost mi otiđe!

točke reda 2

Zadatak 3: Za $P = (a_1, a_2)$ izračunajte

$2 \cdot P = P + P$ i usporedite to što ste dobili s prethodnim zadatkom.

Opčenito imamo ovaj teorem.

Teorem: Neka su

$$E: y^2 = x^3 + ax^2 + bx \quad ; \quad \hat{E}: Y^2 = X^3 - 2aX^2 + (a^2 - b)X$$

eliptičke krivulje. Tada je

$$\phi : E \to \hat{E} \qquad \phi(x,y) = \left(\frac{y^2}{x^2}, \frac{y(b-x^2)}{x^2} \right)$$

dobro definirano preslikavanje (zovemo ga **izogenija**).

na skupu točaka izogenija

definira homomorfizam (za preth. def. grupovnu operaciju)

$$\phi : E(K) \to \hat{E}(K)$$ ← nije očito!

Jezgra preslikavanja ϕ je podgrupa reda 2:

$$E[\phi] = \{ \infty, (0,0) \}$$ → kažemo izogenija stupnja 2

Istom formalom možemo definirati

izogeniju $\hat{\phi}: E' \to E'' \simeq E$ jer je

E'' izomorfna s E pa kompozicija

definira izogeniju $E \xrightarrow{\phi} E' \xrightarrow{\hat{\phi}} E$.

Vrijedi $\hat{\phi}' \circ \phi = [2]_E$ ← množenje s 2.

Zaključak: Fermatov argument ← objasnit čemu ovo služi

implicira (uz malo truda) da je ← skup racionalnih rješenja.

grupa $E(\mathbb{Q})$ konačna (generirana

s točkom $(4,2)$ reda 4 – provjerite to!).

Općenito imamo **Mordell-Weilov teorem**

koji kaže da je za svaku eliptičku krivulju E

s racionalnim koef. grupa $E(\mathbb{Q})$

konačno generirana, tj.

$$E(\mathbb{Q}) \simeq E_{tor} \oplus \mathbb{Z}^r$$

ovako izgledaju konačno generirane grupe

podgrupa točaka konačnog reda

rang el. krivulje

Birch - Swinnerton Dyerova slutnja!

Što ji zapravo Fermat pokazao?

Za svaku točku $P \in E(\mathbb{Q})$ (koja nije točka konačnog reda) postoji $R \in E(\mathbb{Q})$ t.d. $2R = R+R = P$! Točka R ji preciznom smislu jednostavnija od točke P (njezine koordinate imaju "manji" brojnik i nazivnik) tako da ponavljanjem ovog postupka u jednom trenutku moramo "stati" i tako dobiti kontradikciju.

Ovaj argument se generalizira i na sve druge eliptičke krivulje E i računa ji korak u dokazu Mordell-Weilovog teorema (tj. kao prvi korak se metodu 2-spusta (2-descent)

pokaže da je grupa $E(\mathbb{Q})/2E(\mathbb{Q})$ konačna).

Zadatak 3: Sličnim argumentom dokažite da $x^4 + y^4 = z^4$ nema rješenja $xyz \neq 0$ u $\mathbb{Z}$. Koje se sve eliptičke krivulje javljaju i koja preslikavanja između njih?

Više o svemu ovome:

Silverman, Tate: Rational Points on Elliptic Curves

Programski paketi: kao što su SageMath i Magma znatno olakšavaju rad s eliptičkim krivuljama.