Diofantove m-torke i eliptičke krivulje

Racionalna Diofantova m-torka je skup $\{x_1, \dots, x_m\}$ međusobno različitih racionalnih brojeva $\neq 0$ t.d. $x_i \cdot x_j + 1$ potpuni kvadrat za sve $i \neq j$.

Primjeri:

Diofantova četvorka

$$\left\{\frac{1}{16}, \frac{33}{16}, \frac{17}{4}, \frac{105}{16}\right\}$$ Diophant

$$\{1, 3, 8, 120\}$$ Fermat

$1 \cdot 3 + 1 = 2^2$ $\quad$ $3 \cdot 120 + 1 = 19^2$

$1 \cdot 8 + 1 = 3^2$ $\quad$ $8 \cdot 120 + 1 = 31^2$

$1 \cdot 120 + 1 = 11^2$

$3 \cdot 8 + 1 = 5^2$

$$\left\{\frac{11}{192}, \frac{35}{192}, \frac{155}{27}, \frac{512}{27}, \frac{1235}{48}, \frac{180873}{16}\right\}$$

Gibbs

Postoji beskonačno mnogo šestorki

koji sadrže trojku $\left\{\frac{15}{14}, -\frac{16}{21}, \frac{7}{6}\right\}$

DKMS

Kako se konstruiraju ovi skupovi?

Pomoću eliptičkih krivulja.

Eliptične krivulje:

Definicija: Eliptična krivulja nad $\mathbb{Q}$ je algebarska krivulja oblika

$E: \; y^2 = x^3 + ax^2 + bx + c \; ; \; a, b, c \in \mathbb{Q}$

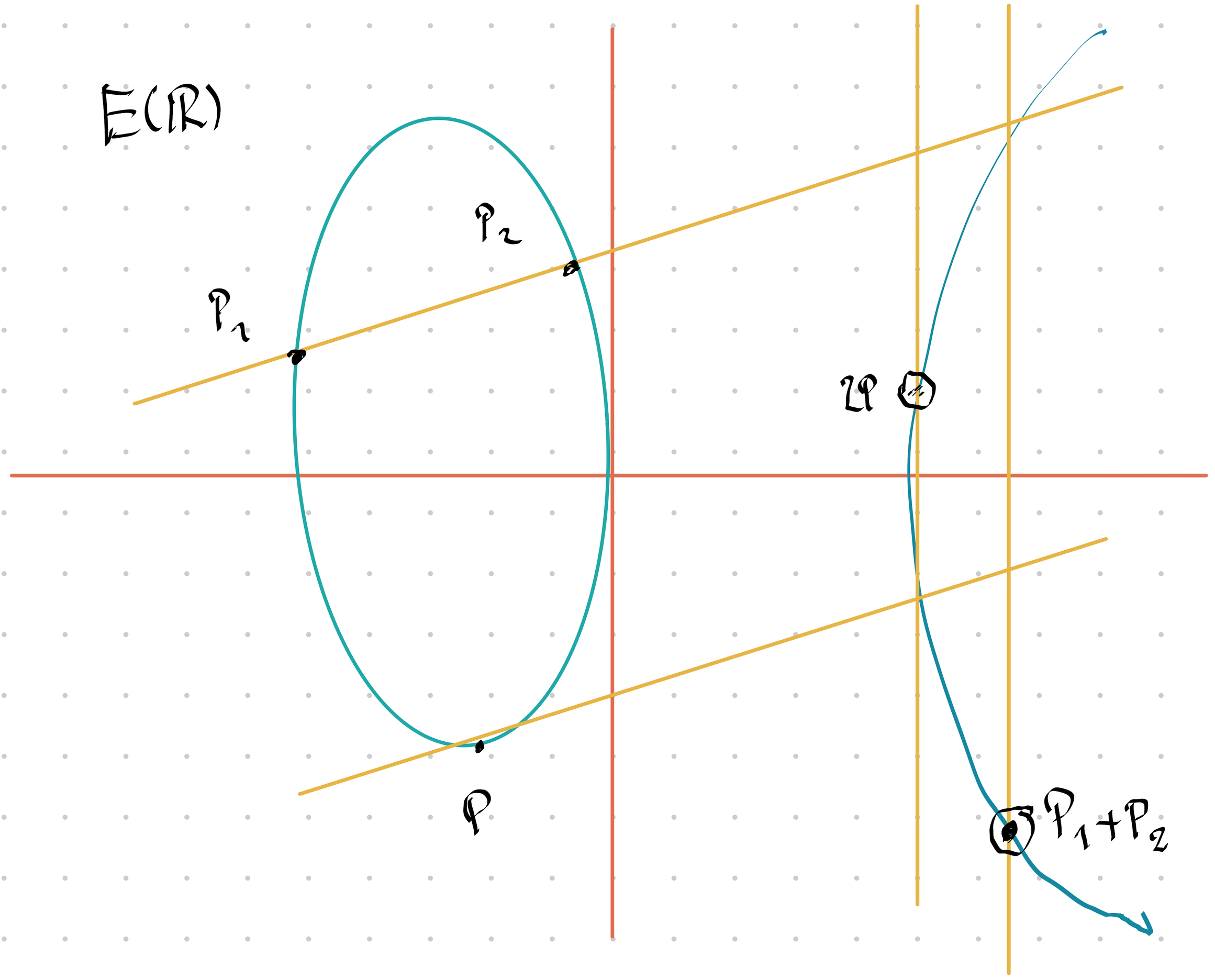
gdje polinom $f(x) = x^3 + ax^2 + bx + c$ nema višestrukih nultočaka, tj. diskriminanta mu je različita od 0.

Nas će zanimati racionalne točke na krivulji, odnosno racionalna rješenja gornje jednadžbe. Oznaka $E(\mathbb{Q})$.

Točka u beskonačnosti $\mathcal{O}$ je element toga skupa.

Primjer: $E: y^2 = x^3 - 9x = x(x-3)(x+3)$

$$E(\mathbb{Q}) = \{\mathcal{O}, (0,0), (3,0), (-3,0)\}$$



Na skupu točaka možemo definirati grupovnu operaciju. Uz tako definiranu zbrajanje $(E(\mathbb{Q}), +)$ je abelova grupa.

N.Z. Koristeći analitičku geometriju izvedite formule za zbrajanje.

Ako su $P=(x_1,y_1)$ i $Q=(x_2,y_2)$ točke na E onda

a) ako je $P \neq Q$ onda je $P+Q=(x_3,y_3)$ gdje je

$$x_3 = \lambda^2 - a - x_1 - x_2$$

$$y_3 = \lambda(x_1 - x_3) - y_1$$

gdje je $\lambda = \dfrac{y_2 - y_1}{x_2 - x_1}$

b) ako je $P=Q$, onda $2P=(x_3,y_3)$

gdje je $x_3 = \lambda^2 - a - 2x_1$

$$y_3 = \lambda(x_1 - x_3) - y_1$$

gdje je $\lambda = \dfrac{3x_1^2 + 2ax_1 + b}{2y_1}$.

D.Z. Pokažite da vrijedi asocijativnost

$$P+(Q+R) \simeq (P+Q)+R$$

Teorem (Mordell-Weil)

Neka je $E/\mathbb{Q}$ eliptička krivulja.

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

To znači da počevši od konačno mnogo točaka, povlačeći sekante i tangente

kroz postojeće točke, možemo dobiti sve racionalne točke na E.

Primjena na Diofantove metode:

Eliptičke krivulje pridružene trojkama

Neka je $\{a,b,c\}$ Diofantova trojka, tj.

$$ab+1=r^2 \quad ; \quad ac+1=s^2 \quad ; \quad bc+1=t^2$$

za neke $r,s,t \in \mathbb{Q}_{>0}$.

Možemo li tu trojku proširiti do četvorke?

Neka je

$$E: y^2=(ax+1)(bx+1)(cx+1)$$

eliptička krivulja

↑ eliptička krivulja pridružena trojci $\{a,b,c\}$.

Ako $d \in \mathbb{Q}$ proširuje $\{a,b,c\}$ do četvorke

onda postoji racionalna točka na E

s x-koordinatom d.

Na $\mathcal{E}$ se nalaze neke očite točke

točke reda 2: $A=(-\frac{1}{a},0)$, $B=(-\frac{1}{b},0)$

$C=(-\frac{1}{c},0)$.

Kao i točke $P=(0,1)$ i $S=\left(\frac{1}{abs},\frac{rst}{abc}\right)$

Možemo li kombinacijom ovih

točaka dobiti (preko x-koordinata)

proširenje 4 od 8?

Budući da polinom u definiciji od $\mathcal{E}$

nije normiran zamjenom varijabli

$x\mapsto x/abc$, $y\mapsto y/abc$ dobijemo

izomorfnu krivulju

$$\mathcal{E}': y^2=(x+bc)(x+ac)(x+ab)$$

s točkama $A'=(-bc,0)$, $B'=(-ac,0)$, $C'=(-ab,0)$.

$P' = (0, abc)$ i $S' = (1, rst)$

koristeći formule za zbrajanje računamo

koordinate točke $P' - S' \in \xi'(\mathbb{Q})$.

$$x(P' - S') = \dots = abc(a+b+c+2abc+2rst)$$

Odnosno, $x(P-S) = \dfrac{x(P'-S')}{abc}$

$$= a+b+c+2abc+2rst$$

D.Z. Provjerite da je $\{a,b,c,d_+\}$

Dio fantom četvorke gdje je

$$d_+ = a+b+c+2abc+2rst$$

To proširenje se zove regularno proširenje.

Odnosno ta četvorka se zove regularna četvorka.

Uočimo da $(x_0, y_0) \in E(\mathbb{Q})$

ne implicira da su ax_0+1, bx_0+1

i cx_0+1 kvadrati, nego samo da si

njihov produkt kvadrat.

Možemo li okarakterizirati točke na $E(\mathbb{Q})$ za koje su svi ti faktori kvadrati?

Propozicija. Neka je $T \in E(\mathbb{Q})$ i $x_0 = x(T)$. Tada su ax_0+1, bx_0+1 i cx_0+1 potpuni kvadrati ako i samo ako je $T - P \in 2E(\mathbb{Q})$

Napomena: $T - P \in 2E(\mathbb{Q})$

$\Leftrightarrow$

$T' - P' \in 2E'(\mathbb{Q})$

↗

"dvostruke" točke u $E'(\mathbb{Q})$, oblika $2R$ za $R \in E'(\mathbb{Q})$

Kod konstrukcije regularnog proširenja smo konstruirali točku $T^1 = P^1 - S^1$

Propozicija implicira da je $T^1 - P^1 = -S^1$

dvostruka točka što nju teško provjeriti:

$$S^1 = 2R^1 \quad \text{gdje je}$$

$$R^1 = (r_1 s_1 + r_1 t_1 + s_1 t_1 + \lambda_1 (r_1 + s_1)(r_1 + t_1)(s_1 + t_1)).$$

(pa je $-S^1 = 2(-R^1)$).

Možemo li gornju četvorku proširiti do petorke?

Kako je S^1 dvostruka točka u prethodnoj slici i da su

$\{a, b, c, x(T+S)\}$ odnosno $\{a, b, c, x(T-S)\}$

četvorke. No ono što je neočekivano je da je $x(T) = x(T \pm S) + 1$ unija

potpun kvadrat (n.z.) pa

ji $\{a, b, c, x(\tau), x(\tau \pm s)\}$

racionalna Diofantova petorka.

Ova petorka se zove regularna

petorka.

Napomena: Ako ji $x(\tau+s)\, x(\tau-s)+1$

potpun kvadrat onda ji

$\{a, b, c, x(\tau), x(\tau-s), x(\tau+s)\}$

racionalna Diofantova šestorka

(uz uvjet da su svi elementi međusobno različiti

i različiti od nule).

Literatura: Andrej Dujella:

Diophantine m-tuples and

Elliptic Curves

Domaća zadaća: Rješite barem 4 zadatka.

Za računanja se preporuča korištenji Sage Math ili sličnog softwara.

1. Neka su Q, T i $(0,0)$ tri racionalne točke na eliptičkoj krivulji E nad $\mathbb{Q}$ koje ji damo jidnadžbom $y^2 = f(x)$ gdje je f normirani polinom stupnja 3. Pretpostavimo $O \notin \{Q, T, Q+T\}$. Tada je $x(Q)\,x(T)\,x(Q+T) + q^2$ potpun kvadrat. Dokažite!

Pokažite tvrdnju iz predavanja: $x(T)\,x(T+S) = 1$ je potpun kvadrat.

2. Zadatak iz Diofantove aritmetike:

Podijeli dani broj a na dva broja tako da ji njihov produkt volumen kocke minus njezina stranica a.

Diofant ji nijeso ovaj problem za $a = 6$. Jel možete i vi?

Napomena: Diofant ji priznavao samo pozitivne racionalne brojeve.

3. Neka ji $\{a, b, c, d\}$ racionalna Diofantova četvorka s $abcd = 1$.

Pokažite da ji produkt bilo kojih dva elementa te četvorke potpuno kvadrat.

(Možete li parametrizirati takve četvorke?*)

4. Geometrijski okarakterizirajte
točke reda 3 na eliptičkoj krivulji
$y^2 = x^3 + ax^2 + bx + c$. Konstruirajte
neku krivulju nad $\mathbb{Q}$ koja ima
racionalnu točku reda 3.
(Za one koji znaju malo alg. geometrije,
zaključite i geometrijski karakterizaciju
eliptičkih krivulja nad $\mathbb{Q}$ čija je najviše 9
točaka reda 3.)

5. Neka je $\{a_i, b_i\}$ Diofantov par.
Pokažite da se on uvijek može
proširiti do Diofantove trojke.

6. Pronađite racionalan Diofantov
trojke $\{a, b, c\}$ za koje vrijedi da su
$a^2 + 1$ i $b^2 + 1$ potpuni kvadrati.