Eliptičke krivulje:

Problem (Diofant: Aritmetika, knjiga IV Problem 24)

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

Ako Diofantov broj označimo s a, onda ji cilj pronaći pozitivne i racionalne x i y takve da ji

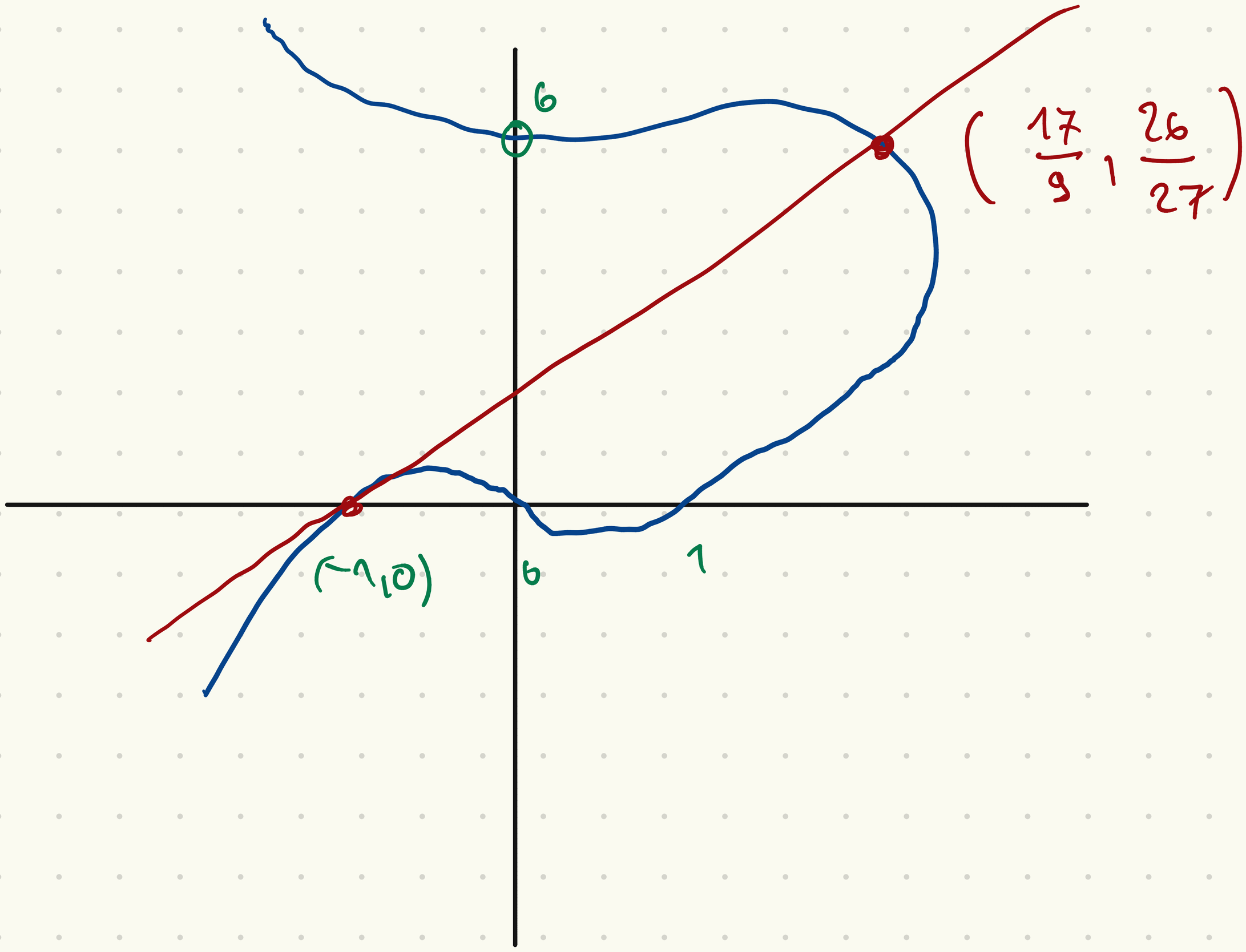
$$y(a-y) = x^3 - x.$$

Diofant ji rješio taj problem za $a=6$.

Kako?

Skicirajmo realne točke krivulje

$$C: \quad y(6-y) = x^3 - x$$



Povučemo tangento krož točko $(-1,0)$

– tretja točka presečka tangente i krivulje (različna kvatnosti) je točka $\left(\frac{17}{9}, \frac{26}{27}\right)$

– točke višje.

Definicija (apstraktna)

Eliptička krivulja nad poljem K je glatka nesing. krivulja genusa 1 definirana nad K (koef. polinoma koji ju definiraju su elementi od K) s istaknutom K-racion. točkom (točkom čiji su koordinate elementi iz K).

Svaka takva krivulja (nad poljem karakt. $\neq 2$) je izomorfna projektivnoj krivulji danoj jednadžbom

$$y^2z = x^3 + ax^2z + bxz^2 + cz^3$$

gdje su $a, b, c \in K$ i polinom

$x^3 + ax^2 + bx + c$ nema višestruke nultočke

tj. diskriminanta mu je različita od 0.

s istaknutom K-racionalnom točkom u beskonačnosti. $\mathcal{O} = [0:1:0]$.

Krivulja $y^2 = x^3 + ax^2 + bx + c$ je
afin model eliptičke krivulje.

Primjer. Pokažimo da je $C: y(6-y) = x^3 - x$
eliptička krivulja.

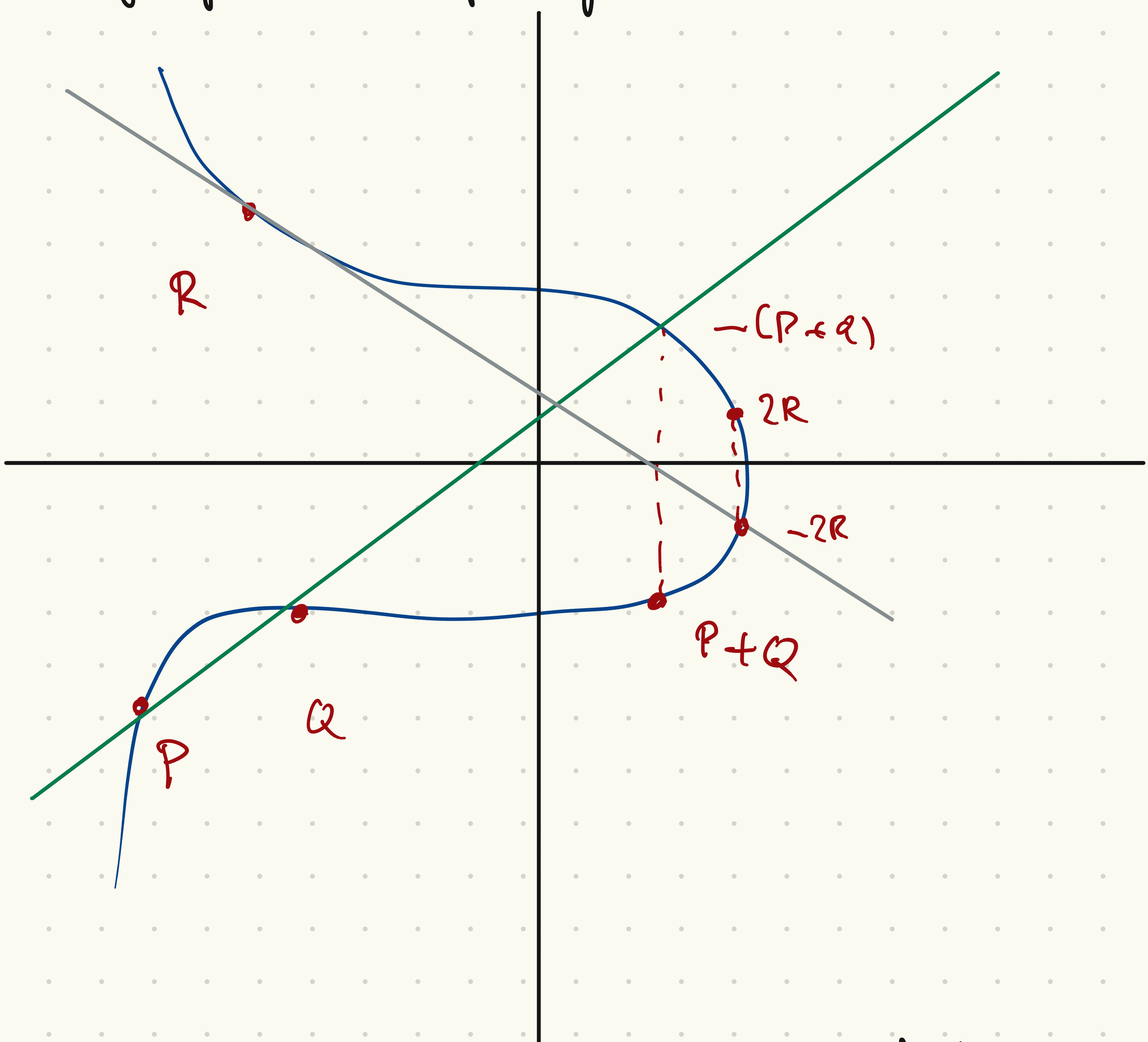
$$x - x^3 = y(y-6) = (y-3)^2 - 9$$

Definirajmo: $Y = y - 3$; $X = -x$.

U (X, Y) - koordinatama krivulja C ima
jednadžbu. $$Y^2 = X^3 - X + 9.$$

Lako se vidi da polinom $X^3 - X + 9$
ima različite nultočke.

Zbrajanje na eliptičkoj krivulji:



Ako su $P=(x_1,y_1)$ i $Q=(x_2,y_2)$ točke na krivulji $y^2=x^3+ax^2+bx+c$ onda

- $-P=(x_1,-y_1)$ $\quad a,b,c,d\in K$
- ako je $P\neq Q$ onda $\quad P+Q=(x_3,y_3)$
  i $x_1\neq x_2$
  za $\quad x_3=\lambda^2-a-x_1-x_2$,

$$y_3=\lambda(x_1-x_3)-y_1 \quad \text{gdje je } \lambda=\frac{y_2-y_1}{x_2-x_1}$$

- $P + (-P) = O$

$(x_1, x_2) + (x_1, -x_2) = O$

- $2P = ?$ [d.z.]

Označka: $E(K)$ = skup K-racionalnih točaka na E

Teorem: $(E(K), +)$ je ✓ grupa

komutativna.

jedinica ↑ asocijativnost netrivijalno [d.z.]

Zanimljiva pitanja - racionalne Diofantove m-torke

↙

Skup $\{x_1, \dots, x_m\}$ racionalnih brojeva $\neq 0$ sa svojstvom $x_i \cdot x_j + 1$ je potpuni kvadrat

Primjer: • $\{\frac{1}{16}, \frac{33}{16}, \frac{17}{4}, \frac{105}{16}\}$

je Diofantova aritmetika.

• Fermat $\{1, 3, 8, 120\}$

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

Kako je trojka $\{1, 3, 8\}$ dobili četvrti element 120?

Neka je $\{a, b, c\}$ racionalna Diofantova trojka: $ab+1 = r^2$, $ac+1 = s^2$, $bc+1 = t^2$

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

Neka je

kasnije ćemo vidjeti da je ova el. krivulja

$$E_{a,b,c}: y^2 = (ax+1)(bx+1)(cx+1)$$

eliptička krivulja pridruženu toj trojci.

Ako $d \in \mathbb{Q}$ proširuje $\{a,b,c\}$ do četvorke onda postoji racionalna točka na $E_{a,b,c}$ s x-koordinatom d. (No obrat ne mora vrijediti.)

Možemo li konstruirati neke racionalne točke na $E_{a,b,c}$ čije x-koordinate bi proširivale $\{a,b,c\}$?

Uočimo prvo neke očite točke na E_{abc}.

- $A = \left(-\frac{1}{a}, 0\right)$, $B = \left(-\frac{1}{b}, 0\right)$, $C = \left(-\frac{1}{c}, 0\right)$ su točke reda 2
- $P = (0,1)$, $S = \left(\frac{1}{abc}, \frac{rst}{abc}\right)$

Uočimo da zamjenom varijabli

$$x \mapsto \frac{x}{abc}, \quad y \mapsto y/abc$$

dobijemo izomorfnu krivulju u uobičajenom Weierstr. obliku

$$E'_{a,b,c}: y^2 = (x+bc)(x+ac)(x+ab)$$

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

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

Koristeći formule za zbrajanje računamo

koordinate točke $P' - S' \in E'_{a,b,c}$

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

odnosno $x(P-S) = \dfrac{x(P'-S')}{abc} = a+b+c+2abc$
$+2rst$

D.3. Provjerite da ni $\{a, b, c, d_+\}$

Diofantova četvorka gdje je

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

Primjer: Za $\{1, 3, 8\}$ dobije se $d_+ = 1+3+8+2\cdot 1\cdot 3\cdot 8$

$\rightsquigarrow \{1, 3, 8, 120\}$ ✓ $\quad \pm 2\cdot 2\cdot 3\cdot 5 = 60 \pm 60$

Natrag na domaću zadaću ...

Kada su dvije eliptičke krivulje izomorfne?

Trebat će nam sljedeća činjenica koju nećemo dokazati:

Propozicija: Ako je $f : E \to E'$ (definirana nad $\mathbb{C}$) nekonstantan morfizam eliptičkih krivulja koji točku a od ∞ G preslikava u točku a od ∞ krivulje E' G', tj. $f(G) = G'$ onda je f homomorfizam grupa $E(\mathbb{C}) \longrightarrow E'(\mathbb{C})$.

morfizam s tim svojstvom se zove izogenija

Neka je $E: y^2 = (x-e_1)(x-e_2)(x-e_3)$; $e_i \in \mathbb{C}$ različiti

i $E': y^2 = (x-e_1')(x-e_2')(x-e_3')$; $e_i' \in \mathbb{C}$ različiti.

Označimo s $\tilde{E}$ i $\tilde{E}'$ njihove projektivizacije.

Npr. $\tilde{E}: y^2z = (x-e_1z)(x-e_2z)(x-e_3z)$.

Neka je $f: \tilde{E} \to \tilde{E}'$ izomorf. projekt. krivulja.

Q: Kakva je veza između $\{e_i\}$ i $\{e_i'\}$?

Možemo pretp. da $f(\mathcal{O}) = \mathcal{O}'$ jer

ako je $f(\mathcal{O}) = T' \neq \mathcal{O}'$ onda umjesto f

promatramo $T_{-T'} \circ f$ gdje je $T_{-T'}$ translacija

$T_{-T'}(P) = T' + P \quad \forall P \in E'(\mathbb{C})$ koja je

izomorfizam. Izomorfizam f s ovim

svojstvom zovemo izomorfizam afinih

krivulja E i E'.

Ako malo eksperimentiramo s konstrukcijom izomorfizama f vidimo da su dobiveni izomorfizmi uvijek svojstva da

$$x(f(P)) = x(f(-P)) \quad \forall P \in E(\mathbb{C}),$$

odnosno x-koordinata točke $f(P)$ ovisi samo o $x(P)$. To možemo lako dokazati koristeći Propoziciju.

Lema: $x(f(P)) = x(f(-P)) \quad \forall P \in E(\mathbb{C})$

Dokaz: Prema Propoziciji f je izogenija (homom. grupa) pa

$$O' = f(O) = f(P + (-P)) = f(P) + f(-P)$$

$$\Rightarrow \quad f(P) = -f(-P)$$

$$\Rightarrow \quad x(f(P)) = x(f(-P))$$

točke T i $-T$ imaju isti x-koord.

$\square$

Tada svaki izomorfizam f inducira komutativni diagram

$$\begin{array}{ccc} \tilde{E} & \xrightarrow{f} & \tilde{E}' \\ \downarrow \pi & \simeq & \downarrow \pi \\ \mathbb{P}^1 & \xrightarrow{\tilde{f}} & \mathbb{P}^1 \end{array}$$

odnosno definira preslikavanje $\mathbb{P}^1 \xrightarrow{\tilde{f}} \mathbb{P}^1$ (morfizam).

Lako se vidi da je $\tilde{f}$ automorfizam od $\mathbb{P}^1$.

Također je dijagram slično da $\tilde{f}$

preslikava skup $\{e_1, e_2, e_3\}$ na skup $\{e_1', e_2', e_3'\}$.

odnosno pravilno skup

$\{[e_1:1], [e_2:1], [e_3:1]\}$ + $\tilde{f}$ fiksira točke u beskonačno

tj. $\tilde{f}([1:0]) = [1:0]$

$\Rightarrow$ točke $\{e_1, e_2, e_3\}$ i $\{e_1', e_2', e_3'\}$ su projektivno ekvivalentne. gdje proj. ekvivalencija preslikavanja $\mathbb{P}^1 \to \mathbb{P}^1$

Dakle, ako $\{e_1, e_2, e_3\}$ i $\{e_1', e_2', e_3'\}$ nisu proj. ekv. onda ne postoji izomorfizam krivulja $\tilde{E}$ i $\tilde{E}'$

Kako možemo računski provjeriti
da točke projektivne ekvival.?

Def. (križni omjer; eng. cross-ratio)

Neka su $x_1, x_2, x_3, x_4 \in \mathbb{P}^1(\mathbb{C})$ različite
točke. Njihov križni omjer je broj

$$(x_1, x_2; x_3, x_4) := \frac{(x_1 - x_3)(x_2 - x_4)}{(x_1 - x_4)(x_2 - x_3)}$$

uz konvenciju da ako je npr. $x_4 = \infty$
onda se omjer definira kao

$$\frac{x_1 - x_3}{x_2 - x_3}$$ (tj. izostavi se produkt
u kojima se nalazi x_4).

Lako se provjeri.

Lema: Ako je $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ automorfizam
(Möbiusova transf.) onda

$$(x_1, x_2; x_3, x_4) = (\phi(x_1), \phi(x_2); \phi(x_3), \phi(x_4)).$$

Vrijedi i obrat

Propozicija: Neka su $\ell_1, \ell_2, \ell_3, \ell_4 \subset \mathbb{P}^1$ i $\ell_1', \ell_2', \ell_3', \ell_4' \subset \mathbb{P}^1$ četiri u općem položaju. Tada postoji automorfizam $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ koji preslikava ℓ_i u ℓ_i' onda i samo onda

$$(\ell_1, \ell_2; \ell_3, \ell_4) = (\ell_1', \ell_2'; \ell_3', \ell_4'),$$

Dokaz: Jedan smjer slijedi iz prethodne leme.

Za drugi smjer, promatrmo automorfizam koji preslikava $(\ell_1, \ell_2, \ell_3) \mapsto (0, 1, \infty)$ (od maloprije, zbog 3-tranzitivnosti, znamo da postoji). Tvrdimo da je u tome da tj automorfizam preslikava točku ℓ_4 u $(\ell_1, \ell_2; \ell_3, \ell_4)$.

Slično, automorfizam koji preslikava $(\ell_1', \ell_2', \ell_3')$ u $(0, 1, \infty)$ preslikava ℓ_4' u tu istu točku pa kompozicija prvog automorfizma s inverzom drugog je traženi.

koji preslikava (e_1, e_2, e_3, e_4) u (e_1', e_2', e_3', e_4')

Q: Za skupove $\{e_1, e_2, e_3\}$ i $\{e_1', e_2', e_3'\}$

koji su nultočke polinoma

$f(x) = x^3 + ax^2 + bx + c = (x - e_1)(x - e_2)(x - e_3)$

i $g(x) = x^3 + a'x^2 + b'x + c = (x - e_1')(x - e_2')(x - e_3')$

kako ći koeficijenti a, b i c (ovisno a', b' i c')

provjeriti postoji li automorfizam koji preslikava

skup $\{e_1, e_2, e_3\}$ u $\{e_1', e_2', e_3'\}$?

↙

Često nemamo eksplicitnu formulu za nultočke

polinoma pa ovaj način nije baš koristan