O aritmetici eliptičkih krivulja

Žgela, Filip

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Filip Žgela

O ARITMETICI ELIPTIČKIH KRIVULJA

Diplomski rad

Voditelj rada:
izv. prof. dr. sc. Zrinka Franušić

Zagreb, srpanj 2024.

Ovaj diplomski rad obranjen je dana _____ pred ispitnim povjerenstvom u sastavu:

1. _____, predsjednik
2. _____, član
3. _____, član

Povjerenstvo je rad ocijenilo ocjenom _____.

Potpisi članova povjerenstva:

1. _____
2. _____
3. _____

Ovaj diplomski rad posvećujem:
Mojim roditeljima koji nisu odustali od mojeg fakulteta ni nakon svih ovih godina.
Djevojci Ani, koja je vjerovala unatoč svim neuspjesima i bez koje ovaj diplomski rad nebi nikada bio gotov.
Bakama koje nisu izgubile vjeru u moje uspjehe.
Prijateljima čije su neprestane šale na moj račun o trajanju studiranja napokon urodile plodom.
Mentorici izv. prof. dr. sc. Zrinka Franušić na neizmjernoj pomoći pri pisanju ovog rada.
Svima koji su mi pomogli za vrijeme studiranja.

Diplomski rad napravljen je u sklopu aktivnosti Projekta PK.1.1.02.0004 - Znanstveni centar izvrsnosti za kvantne i kompleksne sustave te reprezentacije Liejevih algebri.

Sadržaj

Uvod

Aritmetika i krivulje, dva toliko naizgled različita pojma, a zapravo duboko isprepleteni kroz matematičke teorije i primjene. U dosadašnjem fakultetskom obrazovanju rijetko su se ta dva velika poglavlja u matematici koristila u istoj temi. Međutim, kao što će se pokazati u ovom radu matematičari čak i na krivuljama „vide" matematičke operacije.

Tema ovog diplomskog rada su eliptičke krivulje promatrane kao algebarska struktura. Eliptičke krivulje su glatke kubne krivulje, odnsono skup svih točaka ravnine koje zadovoljavaju jednadžbu

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0,$$

gdje su koeficijenti $a, b, \ldots, j$ racionalni brojevi, pri čemu zahtijevamo da krivulja ne siječe samu sebe i nema tzv. šiljaka. Pokazuje se da se svaka eliptička krivulja može zapisati u obliku kratke Weierstrassove forme

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

te ju se može promatrati na svakom polju $\mathbb{K}$ koje je karakteristike različite od 2 i 3 (zbog tehničkih razloga). Skup svih točaka eliptičke krivulje, općenito iz $\mathbb{K} \times \mathbb{K}$ označavamo s E($\mathbb{K}$).

Na eliptičkoj krivulji može se definirati binarna operacija, odnosno tzv. zbrajanje točaka. Operacija se definira geometrijski i zasniva na činjenici da pravac siječe eliptičku krivulju u tri točke. Dakle, ako su A i B točke eliptičke krivulje E($\mathbb{K}$), onda pravac AB siječe eliptičku krivulju u točki C. Ako je $A = B$, onda treću točku dobivamo povlačenjem tangente na krivulju. Ovako definirana $*$ operacija nije sasvim dobra jer za nju ne postoji neutralni element. Operaciju se može poboljšati na način da se eliptičkoj krivulji doda točka O koju zamišljamo kao „točku u beskonačnosti", a binarna operacija zbrajanja definira kao

$$A + B = O * (A * B).$$

Zapravo $A + B$ je točka eliptičke krivulje koja je zrcalno simetrična točki $A * B$ s obzirom na x-os. Pokazuje se da je uz ovako definiranu operaciju zbrajanja eliptička krivulja Abelova

grupa. U radu smo argumentirali svojstva Abelove grupe. Najteže je pokazati svojstvo asocijativnosti. Obrazložili smo ga geometrijski i (djelomično) analitički, jer se zbrajanje može prikazati analitički, odnosno formulama. Na primjer, ako je $A \neq B$ te $A = (x_1, y_1)$, $B = (x_2, y_2)$, onda je

$$A + B = \left(\left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2, \left(\frac{y_2 - y_1}{x_2 - x_1}\right)\left(-\left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 + 2x_1 + x_2\right) - y_1\right),$$

iz čega je odmah jasno da algebarski dokaz asocijativnosti ne može biti jednostavan.

Grupa eliptičke krivulje ima različite primjene. Moderna teorija diofantskih jednadžbi zasniva se na svojstvima grupe eliptičke krivulje nad poljem racionalnih brojeva. Eliptičke krivulje nad konačnim poljem primjenjuju se u kriptografiji, testovima prostosti i problemima faktorizacije (prirodnog broja).

Poglavlje 1

Racionalne točke na krivuljama

Postoji niz matematičkih problema u kojima se traži tzv. racionalno rješenje. Dio teorije brojeva koji se bavi rješavanjem polinomijalnih jednadžbi u skupu cijelih ili racionalnih brojeva naziva se teorija Diofantovih jednadžbi.

1.1 Konike i kubike

Za početak definirajmo što znači da su određeni geometrijski pojmovi racionalni.

Definicija 1.1.1. *Točka ravnine* $(a, b) \in \mathbb{R}^2$ *naziva se* ***racionalna točka*** *ako su a i b racionalni brojevi.*

Definicija 1.1.2. ***Racionalni pravac*** *je skup svih točaka ravnine,* $(x, y) \in \mathbb{R}^2$*, koji zadovoljavaju linearnu jednadžbu*

$$ax + by + c = 0$$

s racionalnim koeficijentima a, b i c.

Konike su krivulje koje nastaju kao presjeci stošca (konusa) s ravninom i po tome su dobile ime. Pročuvali su ih stari Grci i to pred više od 2000 godina (npr. Menehmo, Apolonije iz Perge, Euklid, Arhimed itd.). Konike se algebarski mogu opisati kao skup nultočaka polinoma drugog stupnja u dvije varijable, to jest kao skup svih točaka ravnine koji zadovoljavaju jednadžbu $ax^2 + bxy + cy^2 + dx + ey + f = 0$. Sada definirajmo što je to racionalna konika.

Definicija 1.1.3. ***Racionalna konika*** *je skup svih točaka ravnine koje zadovoljavaju jednadžbu*

$$ax^2 + bxy + cy^2 + dx + ey + f = 0, \tag{1.1}$$

pri čemu su koeficijenti racionalni brojevi, odnosno $a, b, c, d, e, f \in \mathbb{Q}$*.*

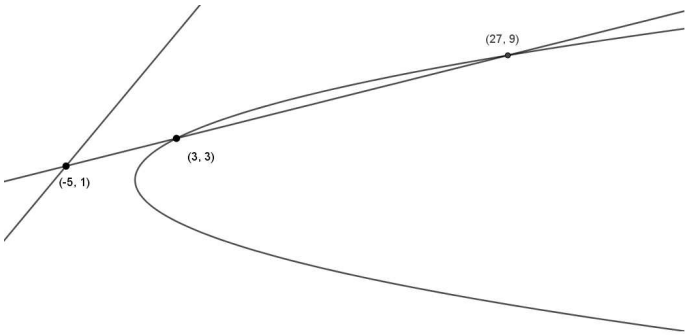
Pronaći racionalne točke racionalnog pravca je jednostavno, međutim za konike to ne vrijedi. Jedna od ideja je presjeći racionalnu koniku s racionalnim pravcem. Ako koniku (1.1) presiječemo s pravcem $y = kx + l$, $k, l \in \mathbb{Q}$ dobivamo kvadratnu jednadžbu

$$Ax^2 + Bx + C = 0,$$

pri čemu su $A, B, C \in \mathbb{Q}$ čija rješenja ne moraju biti racionalni brojevi. Ipak, ako nam je poznato da je jedno rješenje racionalno, npr. $x_1 \in \mathbb{Q}$, onda i drugo rješenje x_2 mora biti racionalan broj. Zaista, zbroj rješenja kvadratne jednadžbe, po Viéteovim formulama, možemo izračunati kao:

$$x_1 + x_2 = -\frac{B}{A} \in \mathbb{Q}.$$

Dakle ako nam je poznata jedna racionalna točka na konici, onda povlačenjem pravca kroz nju (koji nije tangenta) možemo dobiti drugu racionalu točku konike. Na slici vidimo krajnji rezultat jedne takve konstrukcije na paraboli.



Slika 1.1: Određivanje racionalne točke na konici

Budući da su eliptičke krivulje specijalni slučaj kubnih krivulja, definirajmo kubne krivulje. Kubna krivulja ili kubika je algebarska krivulja reda 3, odnosno skup svih nultočaka polinoma u dvije varijable stupnja 3.

Definicija 1.1.4. ***Racionalna kubna krivulja*** *je skup svih točaka koje zadovoljavaju jednadžbu*

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0, \tag{1.2}$$

gdje su svi koeficijenti iz jednadžbe racionalni brojevi, tj. $a, b, \ldots, j \in \mathbb{Q}$.

Pokušajmo slijediti ideju određivanja racionalnih točaka na konici te kubiku (1.2) presjeći s racionalnim pravcem kroz neku racionalnu točku (x_1, y_1) te krivulje. Tada se naš problem svodi na rješavanje kubne jednadžbe

$$Ax^3 + Bx^2 + Cx + D = 0,$$

za neke racionalne koeficijente A, B, C, D. Budući da jednadžba trećeg stupnja može imati tri rješenja za koja vrijedi

$$x_1 + x_2 + x_3 = -\frac{B}{A} \in \mathbb{Q},$$

ne možemo biti sigurni da će svako od preostalih rješenja x_2 i x_3 biti racionalno. Međutim ako na kubici možemo pronaći dvije racionalne točke, racionalni pravac kroz te dvije točke presjeći će kubiku u trećoj racionalnoj točki. U slučaju da nam je poznata samo jedna racionalna točka, kroz tu je točku moguće povući tangentu koja krivulju može sjeći u još jednoj točki i ta mora biti racionalna (jer je u tom slučaju $x_1 = x_2$). Uvođenje aritmetike na kubične, odnosno eliptičke krivulje idejno se zasniva upravo na metodi koju smo opisali.

1.2 Primjer eliptičke krivulje

Slijedi nam primjer iz stvarnog života koji nije očito rješiv eliptičkim krivuljama, a zapravo njegovo rješenje predstavlja cjelobrojnu točku na eliptičkoj krivulju koju određujemo pomoću ideje koju smo iznijeli u prethodnom odjeljku.

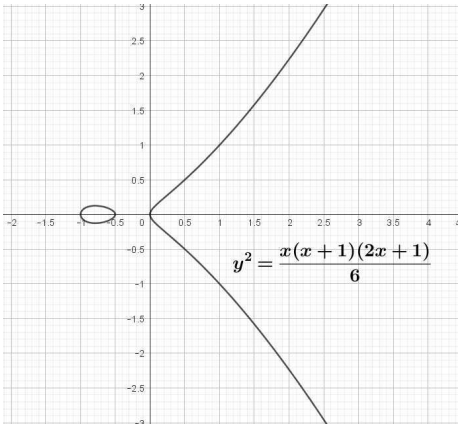
Primjer 1.2.1. *Kolekciju igraćih kocaka imamo složenu u oblik piramide tako da na vrhu imamo 1 kocku, u redu ispod vrha 4 kocke itd. Nakon igre sa njima odlučimo presložiti kolekciju u obliku kvadrata. Kolika naša kolekcija mora biti da bismo to mogli učiniti?*

Rješenje. Vidimo da kolekcija od 1 kocke čine jedan „kvadrat". Međutim, može li se to uopće nazvati kolekcija? Pretpostavimo da ih ipak imamo više od toga. Pokušamo li sa piramidom od 2 reda (5 kockica) nećemo moći složiti kvadrat jer ako ih složimo u kvadrat imati ćemo jednu kockicu viška. Vidimo da rješenje vjerojatno mora biti neki veći broj. Treba primjetiti kako kockica u piramidi ima:

$$1^2 + 2^2 + 3^2 + \ldots + x^2 = \frac{x(x+1)(2x+1)}{6},$$

gdje je x broj redova u piramidi. Ako kockice možemo presložiti u kvadrat za zaključiti je da taj broj mora biti kvadrat nekog prirodnog broja, odnosno izjednačimo:

$$y^2 = \frac{x(x+1)(2x+1)}{6} \tag{1.3}$$



Slika 1.2: Graf krivulje $y^2 = \frac{x(x+1)(2x+1)}{6}$

gdje su $x, y \in \mathbb{N}$. Uočimo da prethodna jednadžba ima dva trivijalna rješenja: $(0, 0)$ i $(1, 1)$. Međutim, koristeći te dvije točke nećemo tangentom ili pravcem kroz njih doći do druge točke s prirodnim koordinatama. Pokušajmo malo presložiti (1.3). Pomnožimo li ju s 24, možemo uz supstituciju $u = 2x$ i $v = 2y$ dobiti:

$$6v^2 = u(u + 1)(u + 2) \tag{1.4}$$

Prethodna jednadžba ima nekoliko očitih rješenja: $(0, 0)$,$(1, 1)$ i $(2, 2)$. Vidimo da su te tri točke kolinearne, pa nema smisla koristiti bilo koje dvije od tih točaka. Međutim, ono što možemo primjetiti je da je ova krivulja simetrična s obzirom na u-os pa možemo pokušati s točkama $(1, -1)$ i $(2, -2)$ koje su isto na krivulji. Odredimo pravac kroz točke $(1, -1)$ i $(2, -2)$. Dobiti ćemo pravac $v = 3u - 4$. Presjek pravca $v = 3u - 4$ i krivulje (1.4) je dan jednadžbom

$$6(3u - 4)^2 = u(u + 1)(u + 2),$$

koja nakon sređivanja glasi

$$u^3 - 51u^2 + 16u - 96 = 0.$$

Kako znamo dva rješenja ove jednadžbe $u_1 = 1$ i $u_2 = 2$, treće rješenje možemo odrediti uz pomoć Viéteove formule:

$$1 + 2 + u_3 = 51$$

pa je $u_3 = 48$. Stoga je $v_3 = 3u_3 - 4 = 140$. Vraćanjem supstitucije dobivamo novo rješenje jednadžbe u skupu prirodnih brojeva (1.3): $(x, y) = (24, 70)$. Dakle,

$$1^2 + 2^2 + 3^2 + \ldots + 24^2 = 70^2.$$

To znači da naša kolekcija mora biti veličine 4900 kockica. Je li to realna kolekcija? Jedna zanimljivost je da u Guinessovoj knjizi rekorda gospodin Kevin Cook ima kolekciju od

11097 (različitih) kockica (2004.), a on tvrdi da ih je od tada skupio i puno više. Vidimo da ipak rezultat koji smo dobili ima smisla. □

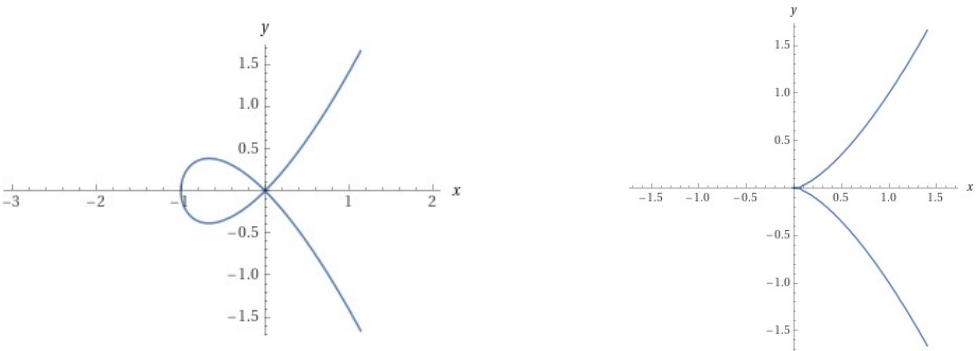
Poglavlje 2

Eliptičke krivulje

Primjer 1.2.1 riješili smo pomoću grafa kubne krivulje koju nazivamo eliptička krivulja. U ovom poglavlju ćemo reći nešto više o tim krivuljama.

2.1 Što su to eliptičke krivulje?

Eliptičke krivulje mogu se definirati na više načina. Jedna od definicija je da je eliptička krivulja nad poljem $\mathbb{K}$ *nesingularna kubična krivulja*, odnosno krivulja dana jednadžbom (1.2) s koeficijentima iz $\mathbb{K}$ i koja sadrži barem jednu točku $\mathbb{K}$. Zahtjev nesingularnost znači da krivulja ne siječe „samu sebe" i da nema „šiljaka". Na slici 2.1 su prikazane dvije singularne kubične krivulje. Obje krivulje imaju singularnu točku, odnosno *singularitet* u $(0, 0)$, to jest u točki u kojoj obje parcijalne derivacije funkcija $(x, y) \mapsto x^3 + x^2 - y^2$, $(x, y) \mapsto x^3 - y^2$ imaju vrijednost nula.



(a) $y^2 = x^3 + x^2$ (b) $y^2 = x^3$

Slika 2.1: Singularne kubične krivulje

Dakle, uvjet nesingularnosti kubične krivulje (1.2) jest da je barem jedna parcijalna derivacija funkcije $f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j$ različita od nule. U tom se slučaju jednadžba (1.2) može tzv. biracionalnim transformacijama svesti na oblik

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{2.1}$$

koji se naziva generalizirana **Weierstrassova forma** ili samo *Weierstrassova forma* krivulje.

U poljima karakteristike različite od 2 i 3 jednadžbu (2.1) možemo pojednostaviti. Najprije lijevu stranu od (2.1) nadopunimo do potpunog kvadrata i podijelimo s 2 (što je moguće jer je polje karakteristike različite od 2) te dobivamo

$$\left(y + \frac{a_1x}{2} + \frac{a_3}{2}\right)^2 = x^3 + \left(a_2 + \frac{a_1^2}{4}\right)x^2 + \left(a_4 + \frac{a_1a_3}{2}\right)x + \left(\frac{a_3^2}{4} + a_6\right). \tag{2.2}$$

Uz supstituciju

$$y' = y + \frac{a_1}{2}x + \frac{a_3}{2}$$

jednadžba (2.2) prelazi u

$$y'^2 = x^3 + a_2'x^2 + a_4'x + a_6', \tag{2.3}$$

pri čemu smo dobivene koeficijente uz x^2, x i slobodni koeficijent označili s a_2', a_4' i a_6' redom.

Konačno, budući da je polje karakteristike različite od 3 možemo u (2.3) provesti supstituciju

$$x' = x + \frac{a_2'}{3} \tag{2.4}$$

kojom eliminiramo koeficijent uz x^2, to jest dobivamo jednadžbu

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

koja se naziva *kratka Weierstrassova forma*. Napomenimo još da se uvjet nesingularnosti sada može iskazati kao uvjet da kubni polinom $x' \mapsto x'^3 + ax' + b$ nema višestrukih nultočaka (u algebarskom zatvorenju polja $\mathbb{K}$).

Zbog svega navedenog uobičajeno je eliptičku krivulju (glatku kubičnu krivulju) nad poljem $\mathbb{K}$ definirati na sljedeći način.

Definicija 2.1.1. *Neka je $\mathbb{K}$ polje karakteristike različite od 2 i 3, $a, b \in \mathbb{K}$ te $f(x) = x^3 + ax + b$ kubni polinom bez višestrukih korijena.* ***Eliptička krivulja nad poljem*** *$\mathbb{K}$ je skup svih točaka $(x, y) \in \mathbb{K} \times \mathbb{K}$ koje zadovoljavaju jednadžbu*

$$y^2 = x^3 + ax + b \tag{2.5}$$

zajedno s još jednim elementom kojeg označavamo sa $\mathcal{O}$ i zovemo „točka u beskonačnosti".

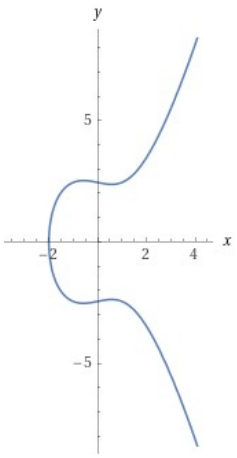
Eliptičku krivulju nad poljem $\mathbb{K}$ označavat ćemo s $\mathrm{E}(\mathbb{K})$.

Točka O je "neobičan dodatak" u definiciju, međutim koristiti ćemo ju nakon što definiramo operaciju koja eliptičku krivulju "pretvara" u algebarsku strukturu, štoviše Abelovu grupu. Zamišljamo da točku O na graf postavljamo na „vrh" i na „dno" y-osi, te zapisujemo kao (∞, ∞).

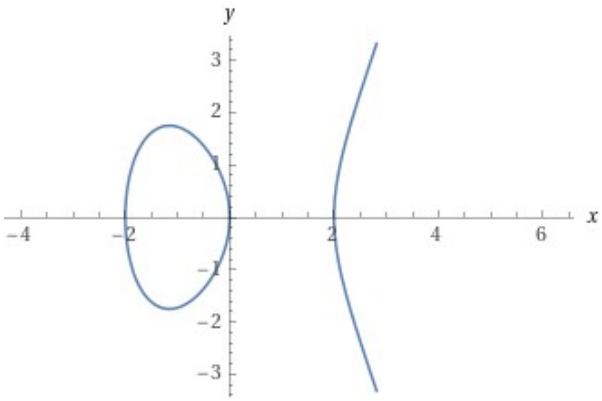
Primjer 2.1.2. *U slučaju polja realnih brojeva, tj.* $\mathbb{K} = \mathbb{R}$*, kubni polinom* $f(x) = x^3 + ax + b$ *ima ili jednu ili tri realne nultočke. Neka su zadane krivulje:*

$$\mathrm{E}_1(\mathbb{R}) \ : \ y^2 = x^3 - x + 6,$$
$$\mathrm{E}_2(\mathbb{R}) \ : \ y^2 = x^3 - 4x.$$

Bez točke O *možemo ih prikazati kao dio ravnine* $\mathbb{R}^2$ *(slika 2.2).*



(a) $y^2 = x^3 - x + 6$



(b) $y^2 = x^3 - 4x$

Slika 2.2: Eliptičke krivulje nad poljem $\mathbb{R}$

Uočimo da polinom $f(x) = x^3 - x + 6$ *ima jednu realnu nultočku* -2*, a ostale dvije nultočke su konjugirano kompleksne* $(1 \pm i\sqrt{2})$*. S druge strane polinom* $f(x) = x^3 - 4x$ *ima tri realne nultočke:* $0, \pm 2$*. Upravo o tome ovisi sastoji li se graf pripadne eliptičke krivulje od jednu ili dvije komponente, a to možemo uočiti i na slici 2.2.*

Primjer 2.1.3. *Prikažimo krivulju iz primjera 1.2.1 u kratkoj Weierstrassovoj formi.*

Rješenje. Jednadžba krivulje glasi

$$y^2 = \frac{x(x+1)(2x+1)}{6} = \frac{x^3}{3} + \frac{x^2}{2} + \frac{x}{6}.$$

Dijeljenjem jednadžbe s 9 dobivamo

$$\left(\frac{y}{3}\right)^2 = \left(\frac{x}{3}\right)^3 + \frac{1}{2}\left(\frac{x}{3}\right)^2 + \frac{1}{18}\left(\frac{x}{3}\right).$$

Uz supstituciju $x' = \frac{x}{3}$, $y' = \frac{y}{3}$ jednadžba glasi

$$y'^3 = x'^3 + \frac{1}{2}x'^2 + \frac{1}{18}x'.$$

Da bismo eliminirali koeficijent uz x^2 provodi se suptitucija (2.4), odnosno

$$x'' = x' + \frac{1}{6}.$$

Dobivamo

$$y'^2 = \left(x'' - \frac{1}{6}\right)^3 + \frac{1}{2}\left(x'' - \frac{1}{6}\right)^2 + \frac{1}{18}\left(x'' - \frac{1}{6}\right),$$

odnosno kratku Weierstrassovu formu (uz "povratak" na x i y)

$$y^2 = x^3 - \frac{x}{36}.$$

□

2.2 Transformacija kubične jednadžbe u Weierstrassovu normalnu formu

Transformacija kubične jednadžbe u Weierstrassov oblik je općenito kompliciran postupak koji ćemo djelomično objasniti. Zbog lakšeg razumijevanja započinjemo s primjerom.

Primjer 2.2.1. *Transformirajmo jednadžbu krivulje*

$$x^3 + y^3 = 1$$

u Weierstrassovu normalnu formu.

Rješenje. Postoji nekoliko prirodnih načina za pokušaj transformacije jednadžbe ove krivulje, međutim problematičan dio je naći točnu transformaciju da uz y^2 stoji koeficijent 1. Jedan od načina je pomoću suspstitucije oblika:

$$a = \frac{12}{x+y},\ b = \frac{36(x-y)}{x+y}.$$

Slijedeći korak je iz tih supstitucija dobiti izraze za x i y. Izrazimo prvo $x + y$ i $x - y$:

$$x + y = \frac{12}{a}, \quad x - y = \frac{b(x+y)}{36} = \frac{b}{3a}.$$

Rješavanjem sustava za x i y dobivamo:

$$x = \frac{b + 36}{6a}, \quad y = \frac{36 - b}{6a}.$$

Sada umjesto $x^3 + y^3 = 1$ imamo jednadžbu:

$$\left(\frac{b+36}{6a}\right)^3 + \left(\frac{36-b}{6a}\right)^3 = 1,$$

odnosno $(36 + b)^3 + (36 - b)^3 = (6a)^3$. Korištenjem izraza za zbroj kubova dobivamo

$$((36 + b) + (36 - b))\left((36 + b)^2 - (36 + b)(36 - b) + (36 - b)^2\right) = (6a)^3,$$

odnosno

$$72(3b^2 + 1296) = (6a)^3.$$

Dijeljenjem s 6^3 dobivamo traženi oblik:

$$b^2 = a^3 - 432.$$

□

Postoji i opći način za transformaciju kubike u Weierstrassovu normalnu formu, koji zahtijeva osnovno znanje iz projektivne geometrije.

Počinjemo sa kubnom krivuljom u projektivnoj ravnini. Ideja je da se odaberu koordinatne osi tako da krivulja u tim koordinatama ima jednostavnu formu. Pretpostavimo da krivulja ima racionalnu točku O. Odabiremo os $Z = 0$ tako da je ona tangenta na krivulju u O. Ova tangenta presijeca krivulju u još jednoj točki koju označimo s A. Odabiremo os $X = 0$ kao tangentu u toj novoj točki. Točka A ima koordinate $[0, 1, 0]$. Kao $Y = 0$ os uzimamo bilo koji pravac osim $Z = 0$ koji prolazi kroz točku O. Sada O ima koordinate $[1, 0, 0]$. Nakon ove (projektivne) transformacije krivulja C' ima oblik: $F'(X, Y, Z) = 0$. Također, C' sadrži O i A. Sada jednadžba krivulje i dalje ima oblik polinoma 3. stupnja, odnosno:

$$F'(X, Y, Z) = aX^3 + bX^2Y + cXY^2 + dY^3 + eZ \cdot G(X, Y, Z)$$

gdje je G polinom drugog stupnja. Pokažimo sada da su koeficijenti a, b i d jednaki nuli.

- Budući da je $O[1, 0, 0] \in C'$, slijedi $F' = (1, 0, 0) = a = 0$

- Budući da je $A[0,1,0] \in C'$, slijedi $F'(0,1,0) = d = 0$
- Promatrajmo presjek krivulje C' i $Z = 0$. Presjek se sastoji od točke O (dvaput) i točke A, a dobivamo ga kao rješenja jednadžbe $F'(X,Y,0) = 0$. Već znamo da su $a = d = 0$, pa dobivamo $bX^2Y + cXY^2 = 0$. Nakon faktoriziranja dobivamo $XY(bX + cY) = 0$. Svaki linearni faktor odgovara jednoj točki presjeka. Dakle, O zadovoljava $X = 0$, točka A zadovoljava $Y = 0$ i $bX + cY = 0$. Slijedi, $b = 0$.

Polinom F' ima oblik:

$$F'(X,Y,Z) = cXY^2 + eZ \cdot G(X,Y,Z).$$

Kada dehomogeniziramo krivulju dobivamo:

$$f(x,y) = xy^2 + ax^2 + bxy + cy^2 + dx + ey + g = 0.$$

Sada izlučivanjem dobivamo:

$$f(x,y) = (x+c)y^2 + ax^2 + bxy + dx + cy + ey + g = 0.$$

Supstituirajmo $x + c$ sa x, dobivamo:

$$xy^2 + (ax + b)y = cx^2 + dx + e.$$

Množenjem cijele jednadžbe sa x dobivamo:

$$(xy)^2 + (ax + b)xy = cx^3 + dx^2 + ex.$$

Ako zamijenimo xy s y dobivamo:

$$y^2 + (ax + b)y = cx^3 + dx^2 + ex.$$

Za kraj zamijenimo y s izrazom $y - \frac{1}{2}(ax + b)$ i dobivamo:

$$y^2 = x^3 + ax^2 + bx + c.$$

Poglavlje 3

Grupa eliptičke krivulje

Jedna od glavnih specifičnosti eliptičke krivulje jest ta što imaju zanimljivu algebarsku strukturu. Konkretno, na skupu točaka neke eliptičke krivulje može se definirati binarna operacija uz koju taj skup ima algebarsku strukturu *Abelove grupe*. Tu operaciju ćemo nazvati *zbrajanje* i uskoro ga definirati.

Prisjetimo se što je to Abelova ili komutativna grupa. Kažemo da je neprazni skup G s obzirom na operaciju + definiranu na $G \times G$ **Abelova grupa** ako vrijede sljedeća svojstva:

- Zatvorenost: $\forall a, b \in G, a + b \in G$
- Asocijativnost: $\forall a, b, c \in G, (a + b) + c = a + (b + c)$
- Postojanje neutralnog elementa: $\exists e \in G$ takav da $\forall a \in G, e + a = a + e = a$
- Postojanje inverznog/suprotnog elementa: $\forall a \in G, \exists b \in G$ za koji je $a+b = b+a = e$.
- Komutativnost: $\forall a, b \in G, a + b = b + a$

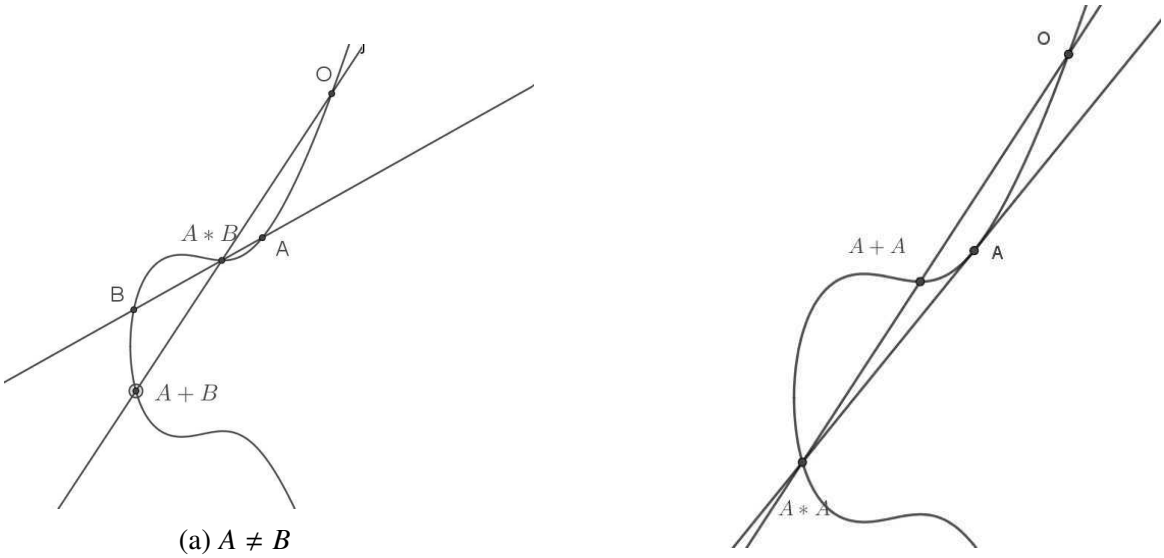
3.1 Operacija zbrajanja na eliptičkoj krivulji

Neka je zadana eliptička krivulja $\mathrm{E}(\mathbb{K})$. Zbog geometrijske ideje na kojoj se zasniva operacija zbrajanja na eliptičkoj krivulji možemo zamišljati da je $\mathbb{K} = \mathbb{R}$. Naime, za definiciju zbrajanja točaka na eliptičkoj krivulji iskoristit ćemo činjenicu da pravac siječe kubiku (a onda i eliptičku krivulju) u tri točke. Za početak, možemo definirati operaciju $*$ koja paru različitih točaka $(A, B) \in \mathrm{E}(\mathbb{K}) \times \mathrm{E}(\mathbb{K})$ pridružuje točku C dobivenu presjekom pravca AB i krivulje $\mathrm{E}(\mathbb{K})$, odnosno vrijedi da je

$$A * B = C,$$

pri čemu su $A, B, C \in \mathrm{E}(\mathbb{K})$ kolinearne točke. Ako je $A = B$, onda se pravac AB "pretvara" u tangentu, tj. točka $C = A * A$ je presjek tangente na krivulju $\mathrm{E}(\mathbb{K})$ u točki A i krivulje $\mathrm{E}(\mathbb{K})$. Međutim, ova operacija ima nedostatak jer ne postoji neutralni element operacije, pa $(\mathrm{E}(\mathbb{K}), *)$ nije grupa. Ipak, operaciju $*$ iskoristit ćemo za definiciju operacije zbrajanja na $\mathrm{E}(\mathbb{K}) \times \mathrm{E}(\mathbb{K})$, a element O za neutralni elemet. Dakle, operacija $+ : \mathrm{E}(\mathbb{K}) \times \mathrm{E}(\mathbb{K}) \to \mathrm{E}(\mathbb{K})$ se za $A, B \in \mathrm{E}(\mathbb{K})$ definira kao

$$A + B = O * (A * B).$$



(a) $A \neq B$

(b) $A = B$

Slika 3.1: Geometrijska definicija zbrajanja

Uz ovako definiranu operaciju + eliptička krivulja $\mathrm{E}(\mathbb{K})$ čini Abelovu grupu. Najprije obrazložimo da je operacija $*$, odnosno + dobro definirana. Naime, prema *Bézoutovom teoremu* algebarske krivulje stupnja d_1 i d_2 koje nemaju zajedničkih dijelova, odnosno čiji polinomi nemaju zajednički faktor, sijeku se u točno $d_1 \cdot d_2$ točaka (uključujući i njihovu kratnost). U našem slučaju eliptička krivulja i pravac se sijeku u tri točke.

Provjerimo svojstva Abelove grupe u strukturi $(\mathrm{E}(\mathbb{K}), +)$:

- *Komutativnost*: $A + B = B + A$ za sve $A, B \in \mathrm{E}(\mathbb{K})$.

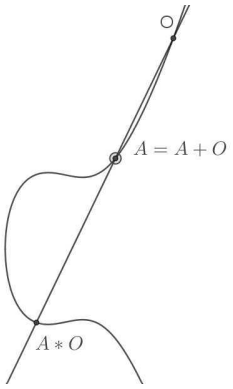
  Očito je $A * B = B * A$ jer je pravac kroz točke A i B je jednak pravcu kroz B i A. Tada je i $A + B = B + A$

- *Asocijativnost*: $(A + B) + C = A + (B + C)$ za sve $A, B, C \in \mathrm{E}(\mathbb{K})$.

  Dokaz ovog svojstva nije jednostavan i dokazat ćemo ga u zasebnom odjeljku.

- *Postojanje neutralnog elementa*: $A + O = A$ za sve $A \in \mathrm{E}(\mathbb{K})$.

  Pravac kroz A i O siječe krivulju u trećoj točki $A * O$. Kako je $A + O$ pravac kroz O i $A + O$ očito je A rezultat te operacije.



Slika 3.2: Neutralni element

- *Postojanje suprotnog elementa*: Za svaku točku $A \in \mathrm{E}(\mathbb{K})$ postoji $B \in \mathrm{E}(\mathbb{K})$ za koju je $A + B = O$.

  Najprije odredimo presjek tangente u točki O i krivulje i označimo tu točku s B', odnosno

  $$O * O = B'.$$

  Zatim presijecamo krivulju pravcem kroz točke A i B' i dobivamo

  $$A * B' = B.$$

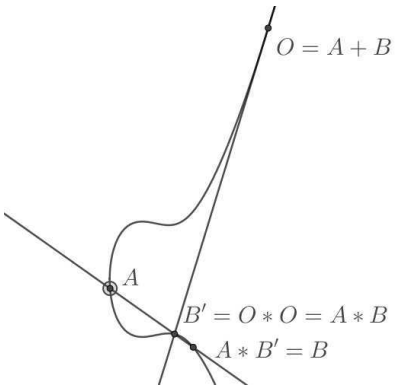
  Sada trebamo provjeriti da je

  $$A + B = O.$$

  Zaista,

  $$A + B = O * (A * B) = O * B' = O$$

  jer pravac AB siječe krivulju u B', a pravac OB' u O.



Slika 3.3: Suprotni element

Suprotni element od A na $\mathrm{E}(\mathbb{K})$ standardno označavamo s $-A$ te obično nazivamo *suprotna* ili *negativna* točka od A.

Primjer 3.1.1. *Riješimo primjer 1.2.1 pomoću zbrajanja točaka na eliptičkoj krivulji.*

Rješenje. Na eliptičkoj krivulji $y^2 = \dfrac{x(x+1)(2x+1)}{6}$ trivijalno smo uočili točke $(0,0)$ i $(1,1)$. Zbrajanjem tih točaka dobivamo točku

$$(0,0) + (1,1) = \left(\frac{1}{2}, \frac{-1}{2}\right)$$

koja ne može biti rješenje postavljenog problema. Međutim, zbroj

$$\left(\frac{1}{2}, \frac{-1}{2}\right) + (1,1) = (24, -70)$$

daje točku sa cjelobrojnim koordinatama. Budući da je krivulja simetrična s obzirom na x-os točka $(24, 70)$ leži na krivulji te predstavlja rješenje problema. (Ta točka je suprotna točka točki $(24, -70)$). □

U teoriji diofantskih jednadžbi, tj. polinomijalnih jednadžbi s racionalnim koeficijentima čija rješenja tražimo u $\mathbb{Z}$ ili $\mathbb{Q}$, grupa eliptičke krivulje nad poljem racionalnih brojeva, tj. $\mathrm{E}(\mathbb{Q})$, ima važnu ulogu. To zapravo podgrupa od $\mathrm{E}(\mathbb{R})$, a k tome je i *konačnogenerirana* Abelova grupa. Ta je važna činjenica poznata pod nazivom *Mordell-Weilov teorem*. Drugim riječima, dovoljno je konačno mnogo točaka kako bi se pronašle sve racionalne točke na eliptičkoj krivulji. To za posljedicu ima da je $\mathrm{E}(\mathbb{Q})$ izomorfna direktnom produktu torzijske grupe i konačno mnogo (r) kopija cijelih brojeva, odnosno

$$\mathrm{E}(\mathbb{Q}) \cong \mathrm{E}(\mathbb{Q})_{tors} \times \mathbb{Z}^r$$

Torzijska grupa $\mathrm{E}(\mathbb{Q})_{tors}$ je grupa svih točaka konačnog reda, a nenegativni cijeli broj r je rang od E.

Grupa eliptičke krivulje nad konačnim poljem ima važnu primjenu u kriptografiji, konkretno u kriptografiji javnog ključa. Uz to, primjenjuje se u testovima prostosti i problemima faktorizacije nekog prirodnog broja.

Primjer 3.1.2. *Neka je* $\{a, b, c\}$ *skup racionalnih brojeva, različitih od* 0*, za koje vrijedi umnožak svaka dva elementa uvećan za* 1 *jednak potpunom kvadratu u* $\mathbb{Q}$*, tj.*

$$ab + 1 = r^2,\ ac + 1 = s^2,\ bc + 1 = t^2, \tag{3.1}$$

pri čemu su $r, s, t \in \mathbb{Q}$*. Skup* $\{a, b, c\}$ *naziva se* racionalna Diofantova trojka*. Pokazuje se da se ovaj skup može proširiti do* racionalne Diofantove četvorke *sa svakim od elemenata (ako je različit od* 0*) danim izrazom*

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

U tom slučaju se $\{a, b, c, d_-\}$*, odnosno* $\{a, b, c, d_+\}$ *naziva* regularna *Diofantova četvorka.*

Pokazuje se da su racionalne Diofantove trojke povezane s eliptičkim krivuljama. Naime, množenjem uvjeta iz (3.1) *dobivamo jednadžbu eliptičke krivulje*

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

Za ovu eliptičku krivulju kažemo da je inducirana *Diofantovom trojkom* $\{a, b, c\}$*. Točke na ovoj eliptičkoj krivulji mogu se dovesti u vezu s problemom proširenja skupa* $\{a, b, c\}$*. Naime, na ovoj eliptičkoj krivulji lako možemo uočiti pet racionalnih točaka:*

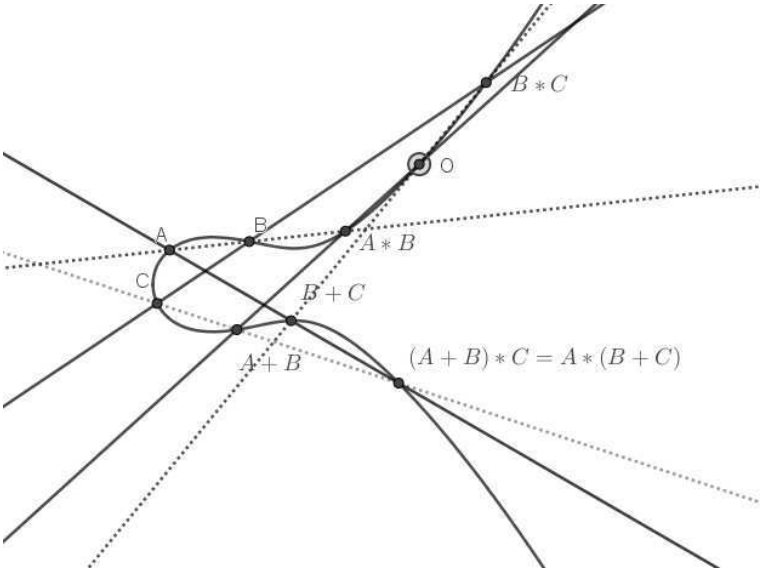
$$P_1 = \left(-\frac{1}{a}, 0\right),\ P_2 = \left(-\frac{1}{b}, 0\right),\ P_3 = \left(-\frac{1}{c}, 0\right),\ P_4 = (0, 1)\,,\ P_5 = \left(\frac{1}{abc}, \frac{rst}{abc}\right).$$

Pokazuje se da x-koordinate točaka

$$P_4 - P_5,\ P_4 + P_5$$

upravo dogovaraju regularnim proširenjima Diofantove trojke $\{a, b, c\}$*, odnosno jednake su* d_- *i* d_+*.*

3.2 Geometrijski dokaz asocijativnosti operacije zbrajanja



Slika 3.4: Asocijativnost zbrajanja

Iz slike se jasno vidi da asocijativnost vrijedi, međutim to nije dovoljan dokaz. Ipak slika će pomoći pri iznošenju dokaza. Odmah na početku možemo uočiti da ako dokažemo jednakost

$$(A + B) * C = A * (B + C),$$

tada vrijedi i svojstvo asocijativnosti jer pravac iz O kroz te „dvije točke" mora dati opet istu točku što je tvrdnja asocijativnosti.

Slika je jako „natrpana" pravcima i točkama, pa opišimo kako smo do nje došli. Prvo smo konstruirali točku $A * B$, zatim je spojili s čvrstom točkom O, a treće sjecište toga pravca s krivuljom daje točku $A + B$. Nakon toga smo nacrtali pravac kroz točke $A + B$ i C, a treća točka presjeka tog pravca s krivuljom daje $(A + B) * C$. Tri pravca pomoću kojih smo došli do točke $(A + B) * C$ su na slici označeni iscrtkano. Analogno dobivamo točku $A * (B + C)$, a tri pravca koja su nam za to potrebna BC, $(B * C)O$ i $A(B + C)$ su na slici označena punom linijom.

Problem dokaza da su te dvije točke, $(A + B) * C$ i $A * (B + C)$, jednake možemo gledati i kao slijedeći problem: sijeku li se pravci p_1 – pravac kroz točke A i $B + C$, te p_2 – pravac kroz točke C i $A+B$ u točki na krivulji? Primijetimo trivijalan slučaj ako su pravci paralelni, tada se sijeku u točki O u beskonačnosti. Dakle, pretpostavimo da se ti pravci sijeku. Na

slici 3.4 je označeno 9 točaka:

$$A, B, C, O, A * B, B * C, A + B, B + C$$

te „$(A + B) * C = A * (B + C)$" koja je za sada samo presjek dva spomenuta pravca. Na slici se one nalaze na krivulji, međutim to tek moramo dokazati. Gledajmo sada 3 iscrtkana pravca i 3 pravca punom linijom. Ti pravci čine dvije (degenerirane) kubne krivulje. To opravdavamo tako što kada bi izmnožili jednadžbe tih triju pravaca dobili bismo kubnu jednadžbu. Skup rješenja te kubne jednadžbe su ta tri pravca. Sada ćemo iskazati teorem o presjecima tri kubne krivulje:

Teorem 3.2.1. *Neka su C, C_1, C_2 kubne krivulje. Pretpostavimo da krivulja C prolazi kroz osam od devet točaka presjeka krivulja C_1 i C_2. Tada C prolazi i kroz devetu točku presjeka.*

Označimo krivulju koja odgovara icrtkanim pravcima sa C_1, a krivulju koja odgovara pravcima punom linijom sa C_2. Svih devet navedenih točaka se nalazi i na C_1 i na C_2 (iz slike). Istovremeno, prvih osam točaka se nalazi na nedegeneriranoj krivulji. Sada nam prethodni teorem kaže da se i deveta točka nalazi na toj krivulji. Tako smo dokazali asocijativnost ove operacije.
Riješimo sada jedan primjer:

Primjer 3.2.2. *Neka su C_1 i C_2 kubike zadane sljedećim jednadžbama:*

$$C_1 : x^3 + 2y^3 - x - 2y = 0, \qquad C_2 : 2x^3 - y^3 - 2x + y = 0.$$

a) Pronađimo točke presjeka krivulja C_1 i C_2.

b) Neka su $\{P_1, \ldots, P_8\}$ točke iz a). Dokažite da kubika koja prolazi točkama $P_1, \ldots, P_8$ mora prolaziti i kroz točku $(0, 0)$ bez korištenja teorema 3.2.1.

Rješenje. a) Točke presjeka tražimo kao rješenje sustava dvije kubne jednadžbe s dvije nepoznanice.

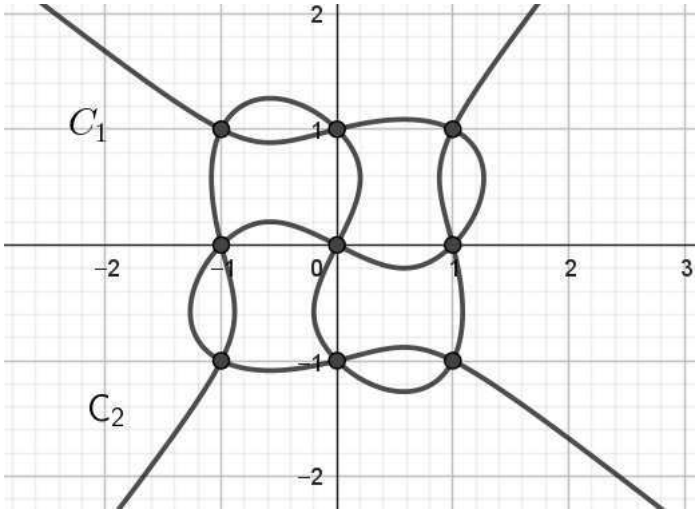
$$\begin{cases} x^3 + 2y^3 - x - 2y = 0 \\ 2x^3 - y^3 - 2x + y = 0 \end{cases}$$

Ako prvu jednadžbu podijelimo s -2 i zbrojimo ove dvije jednadžbe dobivamo vrlo jednostavnu kubnu jednadžbu:

$$\frac{3}{2}x^3 - \frac{3}{2}x = 0$$

Sada je očito da su rješenja:

$$x = 0, x = \pm 1.$$



Slika 3.5: Grafički prikaz rješenja

Uvrštavanjem prethodnih vrijednosti za x u bilo koju od jednadžbi dobiti ćemo tri rješenja za y:

$$y = 0, y = \pm 1.$$

Dakle, točke presjeka su:

$$P_0 = (0,0),\ P_1 = (1,1),\ P_2 = (1,0),\ P_3 = (1,-1),\ P_4 = (0,1)$$

$$P_5 = (0,-1),\ P_6 = (-1,1),\ P_7 = (-1,0),\ P_8 = (-1,-1)$$

b) Ovaj dio zadatka je efektivno dokaz 3.2.1 ali samo za ovih 9 točaka i ove dvije krivulje. Uvrstimo osam točaka (osim $(0,0)$) u opću jednadžbu kubike $ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0$. Dobivamo homoheni sustav od 8 linearnih jednadžbi s 10 nepoznanica $(a, b, \ldots, j)$:

$$\begin{cases} a+b+c+d+e+f+g+h+i+j=0 \\ \qquad\quad d \qquad\quad +g \qquad\quad +i+j=0 \\ -a+b-c+d+e-f+g-h+i+j=0 \\ a \qquad\quad +e \qquad\quad +h \qquad\quad +j=0 \\ -a \qquad\quad +e \qquad\quad -h \qquad\quad +j=0 \\ a-b+c-d+e-f+g+h-i+j=0 \\ -a-b-c-d+e+f+g-h-i+j=0 \\ \qquad\quad -d \qquad\quad +g \qquad\quad -i+j=0 \end{cases}$$

Rješenje prethodnog sustava je dvoparametarsko:

$$(a, b, c, d, e, f, g, h, i, j) = (a, 0, 0, d, 0, 0, 0, -a, -d, 0),\ a, d \in \mathbb{R}.$$

Dakle, kubike na kojima leži osam navedenih točaka oblika su

$$ax^3 + dy^3 - ax - dy = 0.$$

Očito je da svakoj od kubika pripada i točka $(0, 0)$. □

3.3 Analitički zapis zbrajanja

Metodu koju smo koristili na primjeru 1.2.1 možemo koristiti za traženje racionalnih točaka na bilo kojoj eliptičkoj krivulji, te generalizacijom od racionalnih na sve točke možemo dobiti zanimljivu operaciju sa točkama na eliptičkoj krivulji.

Zadana je eliptička krivulja

$$\mathrm{E}(\mathbb{K}) \ :\ y^2 = x^3 + ax + b \tag{3.2}$$

te dvije (ne nužno različite) točke te krivulje: $T_1 = (x_1, y_1)$ i $T_2 = (x_2, y_2)$. Pravac p točkama T_1 i T_2 siječe krivulju u točki $T_0 = (x_0, y_0)$. Zbroj točaka T_1 i T_2 je osnosimetrična slika točke T_0 s obzirom na os x, to jest točka $T_3 = (x_3, y_3) = (x_0, -y_0)$. Sada definiramo operaciju zbrajanja na krivulji 2.5 kao:

$$T_1 + T_2 = T_3$$

Važno je primjetiti da rezultat ovog zbrajanja nije zbrajanje koordinata točaka T_1 i T_2 kako bi zapis mogao sugerirati, ali kako ne bismo morali upotrebljavati novi znak ćemo ju ipak označavati tako.

Želimo odrediti koordinate točke $T_3 = T_1 + T_2$ pomoću koordinata točaka T_1 i T_2. Uz uvjet $x_1 \neq x_2$, koeficijent smjera pravca p (točkama T_1 i T_2) dan je s

$$k = \frac{y_2 - y_1}{x_2 - x_1}, \tag{3.3}$$

a jednadžba pravca p glasi

$$y = k(x - x_1) + y_1. \tag{3.4}$$

U slučaju $x_1 = x_2$, iz (3.2) slijedi da je $y_1 = y_2$ ili $y_1 = -y_2$.

Razmotrimo $T_1 + T_2$ u sljedeća tri slučaja:

1. $x_1 = x_2 \wedge y_1 \neq y_2$,
2. $x_1 = x_2 \wedge y_1 = y_2$,
3. $x_1 \neq x_2$.

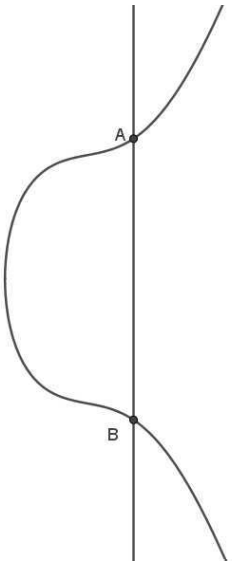
1. slučaj: $x_1 = x_2 \wedge y_1 \neq y_2$

Ovdje je p okomit na x-os i $y_2 = -y_1$. To sada znači da će p sjeći E u $\mathcal{O}$. To znamo iz dva razloga. Prvo, na grafu vidimo da ne postoje tri točke koje se nalaze na jednom pravcu okomitom na x-os. Drugo, za proizvoljan $x = x_0$ iz (3.2) dobit ćemo

$$y_0 = \pm\sqrt{x_0^3 + ax_0 + b}$$

što znači da pravac $x = x_0$ siječe krivulju u najviše dvije točke. Preslikavanjem $\mathcal{O}$ s obzirom na os x dobivamo opet $\mathcal{O}$, pa je rješenje $T_1 + T_2 = \mathcal{O}$. Nadalje, iz ovoga zaključujemo da je T_2 suprotna točka od T_1, odnosno

$$-T_1 = -(x_1, y_1) = (x_1, -y_1).$$



Slika 3.6: $x_1 = x_2 \wedge y_1 \neq y_2$

2. slučaj: $x_1 = x_2 \wedge y_1 = y_2$

Ovdje je $T_1 = T_2$, a pravac p tangenta na krivulju u točki T_1. Koeficijent smjera k pronalazimo derivacijom u toj točki:

$$2yy' = 3x^2 + a \;\Rightarrow\; k = y' = \frac{3x_1^2 + a}{2y_1}$$

Ako je $y_1 = 0$, onda imamo prvi slučaj (”tangenta” u $(0, 0)$ je zapravo okomica na x-os u toj točki) pa je $T_1 + T_2 = \mathcal{O}$. Dakle, pretpostavimo $y_1 \neq 0$. Izjednačimo jednadžbu pravca (3.4) i krivulje (3.2):

$$(k(x - x_1) + y_1)^2 = x^3 + ax + b.$$

Preslagivanjem ove jednadžbe dobivamo kubnu jednadžbu:

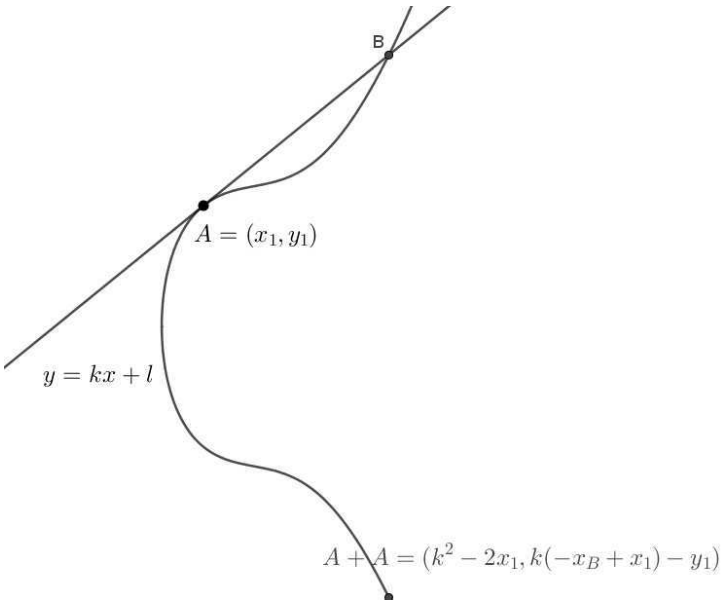
$$0 = x^3 - k^2x^2 + \cdots \tag{3.5}$$

Ostatak ove jednadžbe nam zapravo nije bitan jer možemo koristiti činjenice koje poznajemo o rješenjima ali i o rješavanju kubne jednadžbe. Budući da je točka T_1 na pravcu i krivulji te da je pravac tangenta te krivulje, zaključujemo da je x_1 dvostruko rješenje jednadžbe (3.5). Prema Viéteovoj formuli je $2x_1 + x_0 = k^2$, odnosno

$$x_0 = k^2 - 2x_1,$$

a y_0 dobijemo uvrštavanjem prethodnog izraza za x_0 u jednadžbu pravca (3.4). Iz toga slijedi:

$$T_3 = 2T_1 = (x_0, -y_0) = (k^2 - 2x_1, k(-x_0 + x_1) - y_1).$$



Slika 3.7: $x_1 = x_2 \wedge y_1 = y_2$

3. slučaj: $x_1 \neq x_2$

Ovaj slučaj se rješava kao drugi, samo što je koeficijent smjera k pravaca p dan izrazom (3.3). Nakon što dobijemo kubnu jednadžbu (3.5), možemo iskoristiti istu Viéteovu formulu samo što sada imamo dva različita rješenja x_1 i x_2. Iz toga slijedi da je $x_1+x_2+x_0 = k^2$, odnosno

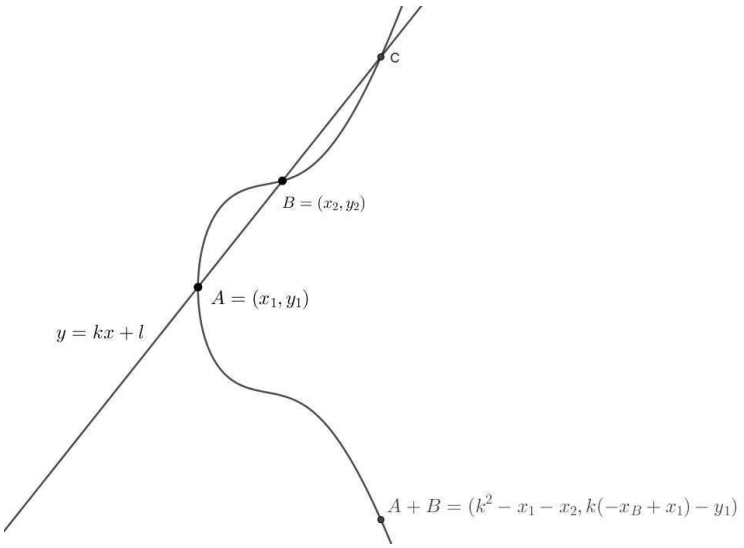
$$x_0 = k^2 - x_1 - x_2.$$

Iz jednadžbe pravca (3.4) odredimo pripadni y_0. Dakle, točka zbroja je

$$T_3 = (x_0, -y_0) = (k^2 - x_1 - x_2, k(-x_0 + x_1) - y_1),$$

odnosno

$$T_3 = (k^2 - x_1 - x_2, -k^3 + k(2x_1 + x_2) - y_1).$$



Slika 3.8: $x_1 \neq x_2$

Na kraju rezimirajmo. Neka su $T_1 = (x_1, y_1)$, $T_2 = (x_2, y_2)$ te $T_1 + T_2 = (x_3, y_3)$. Ako je $T_2 \neq -T_1$, onda je

$$(x_3, y_3) = (k^2 - x_1 - x_2, k(x_1 - x_3) - y_1),$$

pri čemu je

$$k = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1}, & \text{ako je } x_2 \neq x_1, \\ \dfrac{3x_1^2 + a}{2y_1}, & \text{ako je } x_2 = x_1. \end{cases}$$

Ako je $T_2 = -T_1$, to jest $x_2 = x_1$ i $y_2 = -y_1$, onda je $T_1 + T_2 = \mathcal{O}$.

Primjer 3.3.1. *Eliptička krivulja*

$$y^2 = x^3 + 17$$

ima sljedećih pet racionalnih točaka

$$P_1 = (-2, 3), P_2 = (2, 5), P_3 = (-1, 4), P_4 = (4, 9), P_5 = (8, 23).$$

a) Pokažite da se točke P_3, P_4 i P_5 mogu prikazati kao

$$mP_1 + nP_2,$$

za neke cijele brojeve m i n.

b) Izračunajte točke

$$P_6 = -P_1 + 2P_2,\ P_7 = 3P_1 - P_2.$$

c) Točke $P_1, \ldots, P_7$ i njima inverzne točke imaju cjelobrojne koordinate. Postoji još točno jedna racionalna točka s cjelobrojnim koordinatama za koju je $y > 0$. Odredite tu točku.

Rješenje. Za rješenje zadatka koristiti ćemo formule:

$$2T_1 = (k^2 - 2x_1, k(-(k^2 - 2x_1) + x_1) - y_1),$$

gdje je

$$k = \frac{3x_1^2}{2y_1}$$

iz 2. slučaja i

$$T_1 + T_2 = (k^2 - x_1 - x_2, k(x_1 - (k^2 - x_1 - x_2)) - y_1),$$

gdje je

$$k = \frac{y_2 - y_1}{x_2 - x_1}$$

iz 3. slučaja. Još koristimo da je

$$-T = (x, -y)$$

za $T = (x, y)$.

a) Dobivamo redom:

$$2P_1 = (8, -23) \Rightarrow P_5 = -2P_1,$$
$$P_2 + P_5 = P_3 \Rightarrow P_3 = P_2 - 2P_1,$$
$$P_1 - P_2 = P_4.$$

b)

$$P_6 = -P_1 + 2P_2 = -(P_1 - P_2) + P_2 = P_2 - P_4 = (43, 282),$$
$$P_7 = 3P_1 - P_2 = 2P_1 + P_1 - P_3 = P_4 - P_5 = (52, 375).$$

c) Zbrajanjem točaka P_6 i $-P_7$ dobivamo:

$$P_6 - P_7 = (5234, 378661) = P_8.$$

Napominjemo da na ovoj eliptičkoj krivulji postoji točno 8 točaka s cjelobrojnim koordinatama (x, y) i $y > 0$. To je nešto što nije lako za pokazati. Prema Siegelovom teoremu svaka eliptička krivulja $y^2 = x^3 + ax + b$, $a, b \in \mathbb{Z}$, ima konačno mnogo točaka s cjelobrojnim koordinatama. □

3.4 Aritmetički dokaz asocijativnosti operacije zbrajanja

U prethodnom odjeljku dali smo formule za zbrajanje točaka na eliptičkoj krivulji. Iako bi mogli pomisliti da se asocijativnost jednostavno može pokazati "uvrštavanjem u formule", algebarski dokaz asocijativnosti je prilično kompliciran. Opisat ćemo dokaz koji su proveli Fujii i Oike u [5] uz pomoć programskog paketa *Mathematica*.

Dakle, treba pokazati:

$$(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3),$$

gdje su P_1, P_2, P_3 točke eliptičke krivulje $y^2 = x^3 + Ax + B$. Nadalje, pretpostavit ćemo tzv. "generički" slučaj u kojemu je

$$P_1 \neq \pm P_2,\ P_2 \neq \pm P_3,\ P_1 + P_2 \neq \pm P_3.$$

To znači da za svaki par točaka (x_1, y_1) i (x_2, y_2) i

$$(x_1, y_1 + (x_2, y_2) = (x_3, y_3)$$

primjenjujemo formule

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2,\ y_3 = -\left(\frac{y_2 - y_1}{x_2 - x_1}\right)^3 + \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(2x_1 + x_2) - y_1,$$

odnosno za y_3 koristan je oblik

$$y_3 = -\left(\frac{y_2 - y_1}{x_2 - x_1}\right)^3 + \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 + x_2) + \frac{y_2 x_1 - x_2 y_1}{x_2 - x_1}.$$

Uočimo da je prethodna formula antisimetrična u indeksima 1 i 2.

Zapišemo $(P_1 + P_2) + P_3 = C - F$, gdje su

$$C = \left(\frac{y_3 - b}{x_3 - a}\right)^2 - (a + x_3), \quad F = \left(\frac{d - y_1}{c - x_1}\right)^2 - (x_1 + c),$$

dok su a, b, c i d izrazi dani s

$$\begin{aligned}
a &= \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - (x_1 + x_2), \\
b &= -\left(\frac{y_2 - y_1}{x_2 - x_1}\right)^3 + \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 + x_2) + \frac{x_1 y_2 - x_2 y_1}{x_2 - x_1} \\
&= -\left(\frac{y_2 - y_1}{x_2 - x_1}\right)^3 + \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 + x_2) + \frac{\begin{vmatrix} x_1 & x_2 \\ y_1 & y_2 \end{vmatrix}}{x_2 - x_1}, \\
c &= \left(\frac{y_3 - y_2}{x_3 - x_2}\right)^2 - (x_2 + x_3), \\
d &= -\left(\frac{y_3 - y_2}{x_3 - x_2}\right)^3 + \left(\frac{y_3 - y_2}{x_3 - x_2}\right)(x_2 + x_3) + \frac{x_2 y_3 - x_3 y_2}{x_3 - x_2} \\
&= -\left(\frac{y_3 - y_2}{x_3 - x_2}\right)^3 + \left(\frac{y_3 - y_2}{x_3 - x_2}\right)(x_2 + x_3) + \frac{\begin{vmatrix} x_2 & x_3 \\ y_2 & y_3 \end{vmatrix}}{x_3 - x_2}.
\end{aligned}$$

Pokazuje da je $P_1 + (P_2 + P_3) = D - G$ pri čemu se D i G također mogu zapisati pomoću a, b, c i d:

$$D = -\left(\frac{y_3 - b}{x_3 - a}\right)^3 + \left(\frac{y_3 - b}{x_3 - a}\right)(a + x_3) + \frac{\begin{vmatrix} a & x_3 \\ b & y_3 \end{vmatrix}}{x_3 - a},$$

$$G = -\left(\frac{d - y_1}{c - x_1}\right)^3 + \left(\frac{d - y_1}{c - x_1}\right)(x_1 + c) + \frac{\begin{vmatrix} x_1 & c \\ y_1 & d \end{vmatrix}}{c - x_1}.$$

Koristeći programski paket *Mathematica* autori Fujii i Oike ([5]) su uspjeli $C - F$ i $D - G$ faktorizirati, odnosno zapisati u obliku

$$C - F = \frac{R \cdot AA}{P^2 Q^2}, \quad D - G = \frac{R \cdot BB}{P^3 Q^3},$$

gdje su

$$P = (y_1 - y_2)^2 - (x_1 - x_2)^2(x_1 + x_2 + x_3),$$

$$Q = (y_2 - y_3)^2 - (x_2 - x_3)^2(x_1 + x_2 + x_3),$$
$$R = (x_2 - x_3)y_1^2 + (x_3 - x_1)y_2^2 + (x_1 - x_2)y_3^2 + (x_1 - x_2)(x_2 - x_3)(x_3 - x_1)(x_1 + x_2 + x_3).$$

Sada se problem svodi da to da treba pokazati da je zadnički faktor izraza $C - F$ i $D - G$ jednak 0, odnosno $R = 0$ pod uvjetom

$$\begin{cases} y_1^2 = x_1^3 + Ax_1 + B \\ y_2^2 = x_2^3 + Ax_2 + B \\ y_3^2 = x_2^3 + Ax_3 + B \end{cases}, \tag{3.6}$$

to jest da točke leže na eliptičkoj krivulji. Označimo,

$$R = R_1 + R_2,$$

gdje su

$$R_1 = (x_2 - x_3)y_1^2 + (x_3 - x_1)y_2^2 + (x_1 - x_2)y_3^2,$$
$$R_2 = (x_1 - x_2)(x_2 - x_3)(x_3 - x_1)(x_1 + x_2 + x_3).$$

Izraz za R_1 je upravo jednak determinanti koju smo razvili po prvom retku,

$$X = \begin{vmatrix} y_1^2 & y_2^2 & y_3^2 \\ x_1 & x_2 & x_3 \\ 1 & 1 & 1 \end{vmatrix}.$$

Budući da za točke vrijedi (3.6), slijedi da je

$$X = \begin{vmatrix} x_1^3 + Ax_1 + B & x_2^3 + Ax_2 + B & x_2^3 + Ax_3 + B \\ x_1 & x_2 & x_3 \\ 1 & 1 & 1 \end{vmatrix}.$$

Dvjema transformacijama po redcima dolazimo do

$$X = \begin{vmatrix} x_1^3 & x_2^3 & x_2^3 \\ x_1 & x_2 & x_3 \\ 1 & 1 & 1 \end{vmatrix}.$$

Zamjenom prvog i trećeg retka te svođenjem na donji trokut (elementarnim trasformacijama po stupcima) dobivamo

$$X = -(x_2 - x_1)(x_3 - x_1) \begin{vmatrix} 1 & 0 & 0 \\ x_1 & 1 & 0 \\ x_1^3 & x_2^2 + x_2x_1 + x_1^2 & (x_3 - x_2)(x_3 + x_2 + x_1) \end{vmatrix}.$$

Stoga je

$$R = X - X = 0,$$

što je i trebalo pokazati.

Bibliografija

[1] A. Dujella, *Teorija brojeva*, Školska knjiga, 2019.

[2] A. Dujella, *Eliptičke krivulje i njihova primjena u kriptografiji*, https://web.math.pmf.unizg.hr/~duje/ecc/elipdef.html

[3] A. Dujella, *Diophantine m-tuples and Elliptic Curves*, Springer, 2024.

[4] E. Dummit, *Cubic Curves and Elliptic Curves*, https://bit.ly/3JVIklF

[5] K. Fujii, H. Oike, *An Algebraic Proof of the Associative Law of Elliptic Curves*, Advances in Pure Mathematics, 7 (2017), 649–659.

[6] J. H. Silverman, J. T. Tate, *Rational Points on Elliptic Curves*, Springer, 2015.

[7] L. C. Washington, *Elliptic Curves: number theory and cryptography*, Chapman & Hall/CRC, 2008.

[8] *How to Transform a Cubic (With a Rational Point) into Weierstrass Normal Form*, https://ctnt-summer.math.uconn.edu/wp-content/uploads/sites/1632/2016/02/Matsuura-projective_transformation.pdf

[9] *An Algebraic Proof of the Associative Law of Elliptic Curves* https://www.scirp.org/journal/paperinformation?paperid=80983

[10] *Senior Math Circles - Elliptic Curves - Solutions - November 4, 2015* https://www.cemc.uwaterloo.ca/events/mathcircles/2015-16/Fall/Senior_Nov4-Solns.pdf

[11] *Diofantove m-torke i eliptičke krivulje* https://web.math.pmf.unizg.hr/~duje/diofelip/diofelip.pdf

Sažetak

Kako pronaći racionalne točke na krivulji ako su nam neke već poznate? Što su to eliptičke krivulje? Kako se zbrajaju točke na eliptičkoj krivulji? Čini li eliptička krivulja uz operaciju zbrajanja točaka neku algebarsku strukturu? Time i još nekim temama bavili smo se u ovom diplomskom radu. Niz riješenih primjera trebao bi pomoći u razumijevanju ove teme.

Summary

How does one find another rational points on curves if we know a few? How do you add points on an elliptic curve? Is that additon a group law? These and a few others are questions that we answered in this paper. We have shown a few examples which should help understanding this topic.

Životopis

Rođen sam 1. siječnja 1996. u Zagrebu, gdje sam i odrastao u kvartu Rudeš. Pohađao sam Osnovnu školu Rudeš od 2002. do 2010. Po završetku sam upisao Gimnaziju Lucijana Vranjanina u Zagrebu prirodoslovno matematički smjer. Nakon Državne Mature upisao sam 2014. sveučilišni studij Matematika na Prirodoslovno matematičkom fakultetu, a onda 2016. smjer nastavnički. 2021. godine sam završio preddiplomski te upisao diplomski nastavnički studij kojega ću 2024. godine i završiti.