Rang eliptičkih krivulja

Žunić, Luka

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Luka Žunić

RANG ELIPTIČKIH KRIVULJA

Diplomski rad

Voditelj rada:
prof. dr. sc. Andrej Dujella

Zagreb, veljača, 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. _____

Obitelji i prijateljima.
Posebno hvala prof. dr. sc. Andreju Dujelli na savjetima i mentorstvu.

Sadržaj

Uvod

Kroz povijest su se eliptičke krivulje pojavljivale u više navrata, bez konkretne definicije i bez svog trenutnog naziva. Diofant je u svojoj knjizi *"Aritmetika"* zapisao jednadžbu oblika $Y(a - Y) = X^3 - X$, i tako prvi zapisao jednadžbu eliptičke krivulje. Fibonacci se također susreo s takvim jednadžbama kad je tražio racionalne brojeve r takve da su $r^2 - 5$ i $r^2 + 5$ kvadrati. Zapravo, rješavao je jednadžbu $y^2 = x(x - 5)(x + 5)$, također eliptička krivulja. Francuski matematičar Bachet je 1621. objavio Diofantovu *"Aritmetiku"* na latinskom, a Fermat ju proučava od 1630. godine. Fermat je pokušavao dokazati da pravokutni trokut čije su duljine svih stranica racionalni brojevi ne može imati površinu koja je kvadrat racionalnog broja. Dokazujući to, zapravo je dokazao da eliptička krivulja $y^2 = x(x - 1)(x + 1)$ ima samo tri racionalne točke $(-1, 0), (0, 0), (1, 0)$. Eliptičke krivulje imaju važnu ulogu u više područja matematike, a s razvojem tehnologije i modernih metoda za dekriptiranje, igraju ključnu ulogu i u kriptografiji. Iako mogu biti definirane nad proizvoljnim poljima, za teoriju brojeva je najvažniji slučaj polja racionalnih brojeva $\mathbb{Q}$, dok su za primjene, uključujući i kriptografiju, najvažnija konačna polja. Rang eliptičkih krivulja je danas jako istraživan pojam, te ne postoji egzaktan način kako se to svojstvo računa za proizvoljnu eliptičku krivulju.

Kako bi postavili bolje temelje za pojmove koji su bitni za ovaj rad, u prvom poglavlju su definirane osnovne algebarske strukture i neka od njihovih svojstava. Definiramo grupe i polja te važne pojmove točaka konačnog i beskonačnog reda te izomorfizama među grupama.

U drugom poglavlju uvodimo konkretne definicije eliptičkih krivulja, nad poljem racionalnih brojeva $\mathbb{Q}$. Nad poljem realnih brojeva $\mathbb{R}$ vizualiziramo eliptičke krivulje ovisno o parametrima s kojima ih definiramo. Također ćemo definirati zbrajanje dvije točke nad eliptičkim krivuljama.

Rang eliptičke krivulje definiramo u trećem poglavlju te predstavljamo neke od metoda za računanje ranga. Dajemo i konkretnu metodu kako se ta veličina računa za eliptičke krivulje koje sadrže racionalnu točku reda 2, ali i metode s kojima možemo pronaći točke na eliptičkoj krivulji ranga ≥ 2.

Zadnje poglavlje bavi se primjenama eliptičkih krivulja u kriptografiji, gdje se upoznajemo s kriptografijom javnog ključa i razlozima zašto eliptičke krivulje igraju važnu ulogu

u modernim sustavima kriptiranja.

U svim poglavljima ovog rada koriste se termini koji obuhvaćaju algebarske strukture opisane u skripti *Algebarske strukture* autora B. Širole, te eliptičke krivulje i njihove primjene u kriptografiji, prema proučavanjima iz knjiga *"Kriptografija"* autora A. Dujelle i M. Maretića [8] te *"Teorija brojeva"* autora A. Dujelle [4].

Poglavlje 1

Algebarske strukture

Prije samog proučavanja eliptičkih krivulja, u ovom poglavlju postavljamo temelje za razumijevanje eliptičkih krivulja, uvodeći ključne algebarske strukture i njima pripadne operacije. Posebna pažnja posvećena je konceptu direktnih suma te izomorfizmu grupa, ključnim pojmovima koji će se pokazati bitnima u formulaciji Mordell-Weilovog teorema, najvažnijeg teorema u promatranju eliptičkih krivulja. Definiramo i strukture oblika $\mathbb{Z}/n\mathbb{Z}$, najčešće korištenu grupu u promatranju eliptičkih krivulja nad poljem racionalnih brojeva.

Definicija 1.0.1. *Uređeni par $(G, \cdot)$, gdje je G neprazan skup, a $\cdot : G \times G \to G$ binarna operacija zove se **grupa** ako vrijede sljedeća svojstva:*

$(x \cdot y) \cdot z = x \cdot (y \cdot z),\ \forall x, y, z \in G$ *(asocijativnost)*
$(\exists e \in G)\ e \cdot x = x \cdot e = x,\ \forall x \in G$ *(postojanje neutralnog elementa)*
$(\forall x \in G)\ (\exists!\ x^{-1} \in G)\ x \cdot x^{-1} = x^{-1} \cdot x = e$ *(postojanje inverza)*

Uz gore definirano, dodatno uvodimo i svojstvo komutativnosti:
$x \cdot y = y \cdot x, \forall x, y \in G.$
Ako vrijedi i ovo svojstvo, kažemo da je G komutativna (Abelova) grupa.

Napomena 1.0.2. *U zapisu grupe $(G, \cdot)$ se često izostavlja operacija te se grupa G poistovjećuje sa $(G, \cdot)$.*

Definicija 1.0.3. *Neka je G grupa. Podskup $H \subseteq G$ je podgrupa od G ako vrijedi:*

$$xy \in H, \forall x, y \in H$$

$$x^{-1} \in H, \forall x \in H.$$

Definicija 1.0.4. *Neka su $(G, \cdot)$, $(H, *)$ dvije grupe s binarnim operacijama $\cdot : G \times G \to G$, $* : H \times H \to H$. Preslikavanje $f : G \to H$ je homomorfizam ako vrijedi:*

$$f(x \cdot y) = f(x) * f(y), \forall x, y \in G$$

Bijektivan homomorfizam nazivamo izomorfizam, te za dvije grupe G, H kažemo da su izomorfne ako postoji neki izomorfizam f među njima i pišemo:

$$G \cong H$$

Definicija 1.0.5. *Neka je S proizvoljan podskup grupe G. Definiramo grupu generiranu sa S kao:*

$$\langle S \rangle := \bigcup_{\substack{H \leq G \\ S \subseteq H}} H$$

gdje $H \leq G$ označava činjenicu da je H podgrupa od G.

Definicija 1.0.6. *Za G kažemo da je **konačno generirana** ako postoji $S = \{x_1, ..., x_n\} \subseteq G$ takav da je $G = \langle S \rangle$. Grupa G je **ciklička** ako je moguće dobiti svaki element iz G pomoću jednog od elemenata, odnosno ako postoji $g \in G$ takav da je $G = \langle g \rangle$. Za svaki takav g kažemo da je **generator** cikličke grupe G.*

Definicija 1.0.7. *Neka su $(G, \cdot_G), (H, \cdot_H)$ grupe i $G \times H$ njihov Kartezijev produkt. Na $G \times H$ definiramo operaciju množenja po komponentama:*

$$(g_1, h_1) \cdot (g_2, h_2) = (g1 \cdot_G g2, h_1 \cdot_H h_2).$$

Time je na $G \times H$ dobivena struktura grupe koju nazivamo direktan produkt grupa G i H.

Definicija 1.0.8. *Direktan produkt grupa $\{G_i\}_I$ definiramo kao:*

$$\prod_{i \in I} G_i := \left\{ f : I \to \bigcup_{i \in I} G_i \mid f(i) \in G_i \right\}$$

uz operaciju množenja po komponentama:

$$(f \cdot g)(i) := f(i) \cdot g(i)$$

Direktna suma grupa $\{G_i\}_I$ definirana je kao podgrupa

$$\bigoplus_{i \in I} G_i := \{f \in \prod_{i \in I} G_i \mid f(i) \neq e_i \text{ za konačno mnogo } i \in I\}$$

direktnog produkta $\prod_I G_i$.

Za konačan skup indeksa $I = \{1, ..., n\}$, možemo pisati:

$$G_1 \times \cdots \times G_n = \prod_{i=1}^{n} G_i = G_1 \oplus \cdots \oplus G_n$$

Ako na nekom skupu S imamo definiranu neku relaciju ekvivalencije ρ, sa S/ρ označavamo skup svih klasa ekvivalencije.

Za potrebe sljedeće definicije, definirat ćemo jednu relaciju ekvivalencije za grupu G i podgrupu $H \leq G$. Relaciju definiramo na $G \times G$:

$$\forall x, y \in G, x \sim y \Leftrightarrow xH = yH \Leftrightarrow x^{-1}y \in H$$
$$(Hx = Hy \Leftrightarrow xy^{-1} \in H)$$

Definicija 1.0.9. *Klase grupe G dobivene s definiranom relacijom $\sim$ označavamo s xH (Hx) i zovemo lijeve (desne) klase od G po $\sim$. Skup svih klasa $G/\sim$ označavamo s G/H.*

Ako je G/H konačan skup, broj elemenata u G/H označavamo s $(G : H)$ i nazivamo indeks od G po H.

Za naše potrebe ćemo najčešće koristiti $G = \mathbb{Z}$ i $H = n\mathbb{Z}$, odnosno skup ostataka modulo n: $G/H = \mathbb{Z}/n\mathbb{Z}$. Vrijedi $(\mathbb{Z} : n\mathbb{Z}) = n$. Grupu $\mathbb{Z}/n\mathbb{Z}$ također ćemo označavati sa $\mathbb{Z}_n$

Teorem 1.0.10. *(Strukturni teorem za konačno generirane komutativne grupe)*
Neka je G konačno generirana komutativna grupa, tada postoji $k \in \mathbb{N}_0$ i postoje:

$$m_1|m_2|\cdots|m_t, m_i \in \mathbb{N} \setminus \{1\}$$

takvi da vrijedi:

$$G \cong (\mathbb{Z}/m_1\mathbb{Z} \oplus \mathbb{Z}/m_2\mathbb{Z} \cdots \mathbb{Z}/m_t\mathbb{Z}) \oplus \mathbb{Z}^k$$

*gdje je $\mathbb{Z}^k = \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$, k primjeraka od $\mathbb{Z}$. Broj k naziva se **rang** od G.*

Dokaz teorema 1.0.10 može se pronaći u [13].

Definicija 1.0.11. *Neprazan skup $R = (R, +, \cdot)$ nazivamo **prsten** ako za definirane operacije $+ : R \times R \to R$ i $\cdot : R \times R \to R$ vrijedi:*

$(R, +)$ je komutativna grupa, s neutralnim elementom $0 = 0_R$

$(R, \cdot)$ je polugrupa, odnosno množenje je asocijativno

te distributivnost množenja prema zbrajanju, tj.

$x \cdot (y + z) = x \cdot y + y \cdot z, \forall x, y, z \in R$

$(x + y) \cdot z = x \cdot z + y \cdot z, \forall x, y, z \in R$

Definicija 1.0.12. *Dodatno, ako je svaki ne-nul element u R invertibilan, tada R nazivamo* ***tijelo****. Ako vrijedi i svojstvo komutativnosti operacije ·, tada takvo tijelo nazivamo* ***polje****.*

Definicija 1.0.13. *Neka je K neko polje, i neka postoji $m \in N$ takav da je:*

$$mx = 0, \forall x \in \mathbb{R}$$

Karakteristiku polja K (označavamo sa char K) definiramo kao najmanji m, ako takav m postoji, u suprotnom kažemo da je R karakteristike nula i pišemo

$$char\ K = 0$$

Ako je karakteristika polja različita od 0, onda je ona neki prost broj.

Karakteristika polja će nam kasnije biti potrebna za proučavanje eliptičkih krivulja i krivulje nad poljima karakteristike 2 ili 3 proučavamo na drukčiji način. S rangom eliptičke krivulje se upoznajemo kroz krivulje nad poljem racionalnih brojeva $\mathbb{Q}$ koje je karakteristike 0.

Poglavlje 2

Eliptičke krivulje nad poljem racionalnih brojeva

2.1 Uvod u eliptičke krivulje

Definicija 2.1.1. *Neka je K polje. Eliptičku krivulju nad K definiramo kao nesingularnu projektivnu kubnu krivulju s barem jednom racionalnom točkom. Opisujemo je jednadžbom:*

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

gdje su $a, b, c, ..., j \in K$.

Koristeći biracionalne transformacije, odnosno racionalne transformacije čiji je inverz također racionalna transformacija, svaka takva jednadžba može se svesti na Weierstrassovu formu:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Nad poljima K karakteristike različite od 2 i 3 ($char\ \mathbb{Q} = 0$) možemo dalje pojednostaviti izraz do oblika koji nazivamo kratka Weierstrassova forma:

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

Kroz rad ćemo nadalje najčešće koristiti kratku Weierstrassova formu pa navodimo da je uvjet nesingularnosti u tom slučaju taj da kubni polinom $f(x) = x^3+ax+b$ nema višestrukih nultočaka. Koristeći diskriminantu, taj uvjet možemo zapisati kao da je diskriminanta $\Delta = -16(4a^3 + 27b^2) \neq 0$.

Uz sve točke na eliptičkoj krivulji, također je definirana i "točka u beskonačnosti" ($\mathcal{O}$). Ta točka služit će nam kao analog neutralnog elementa za operaciju koju kasnije uvodimo.

Opisat ćemo prirodan način na koji se kroz uvođenjem supstitucija u jednadžbu eliptičke krivulje dođe to točke koju možemo karakterizirati kao O.

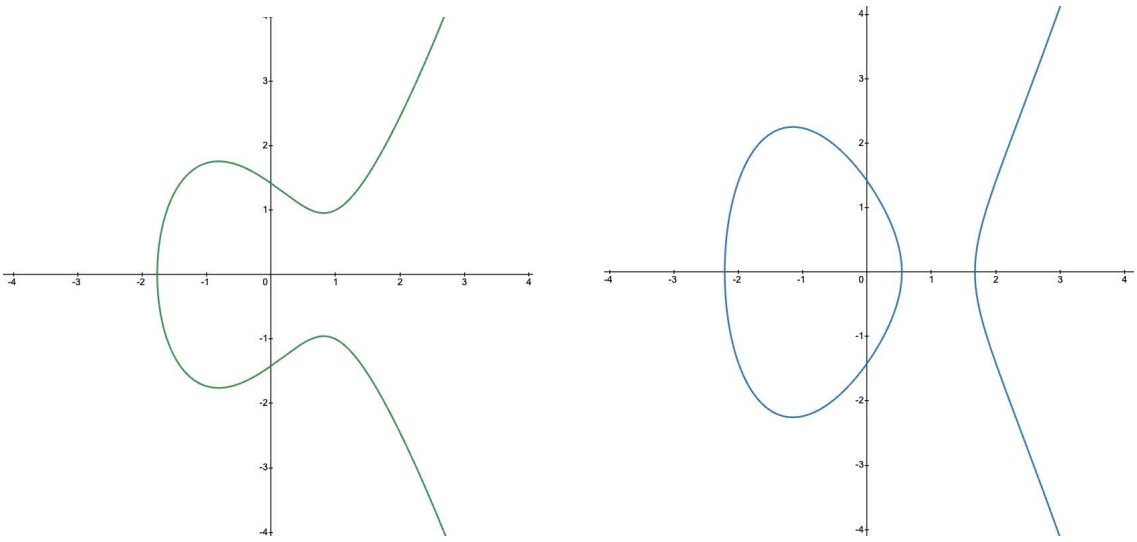
Uvest ćemo relaciju ekvivalencije $(X, Y, Z) \sim (kX, kY, KZ), k \in K, k \neq 0$ na skupu $K^3 \setminus (0, 0, 0)$. Klase ove relacije ekvivalencije obično poistovjećujemo s točkama projektivne ravnine $\mathbb{P}^2(K)$. Više detalja može se pronaći u [11, Poglavlje 1]. Sada u jednadžbu eliptičke krivulje uvedimo supstitucije $x = \frac{X}{Z}, y = \frac{Y}{Z}$, na taj način dobijemo dobijemo projektivnu jednadžbu

$$Y^2Z = X^3 + aXZ^2 + bZ^3.$$

Promatramo različite mogućnosti za Z. Za $Z \neq 0$ klasa ekvivalencije od (X, Y, Z) ima reprezentant $(x, y, 1)$ što identificiramo s afinom točkom (x, y). Reprezentant klase ekvivalencije koja sadržava točke za koje je $Z = 0$ je $(0, 1, 0)$, tu klasu identificiramo s točkom u beskonačnosti O.

Sada možemo dati kompletnu definiciju što je to zapravo eliptička krivulja. Sa $E(\mathbb{K})$ ćemo označavati skup svih točaka $(x, y) \in \mathbb{K} \times \mathbb{K}$ koje zadovoljavaju $y^2 = x^3 + ax + b$ gdje su $a, b \in K$ te vrijedi $-16(4a^3 + 27b^2) \neq 0$, zajedno s definiranom točkom u beskonačnosti O.

Eliptičku krivulju $E(\mathbb{R})$ (bez točke u beskonačnosti) možemo prikazati kao podskup ravnine. U ovisnosti o Δ, graf eliptičke krivulje može imati jednu ili dvije komponente:



(a) $E_1 : y^2 = x^3 - 2x + 2$ (b) $E_2 : y^2 = x^3 - 4x + 2$

Slika 2.1

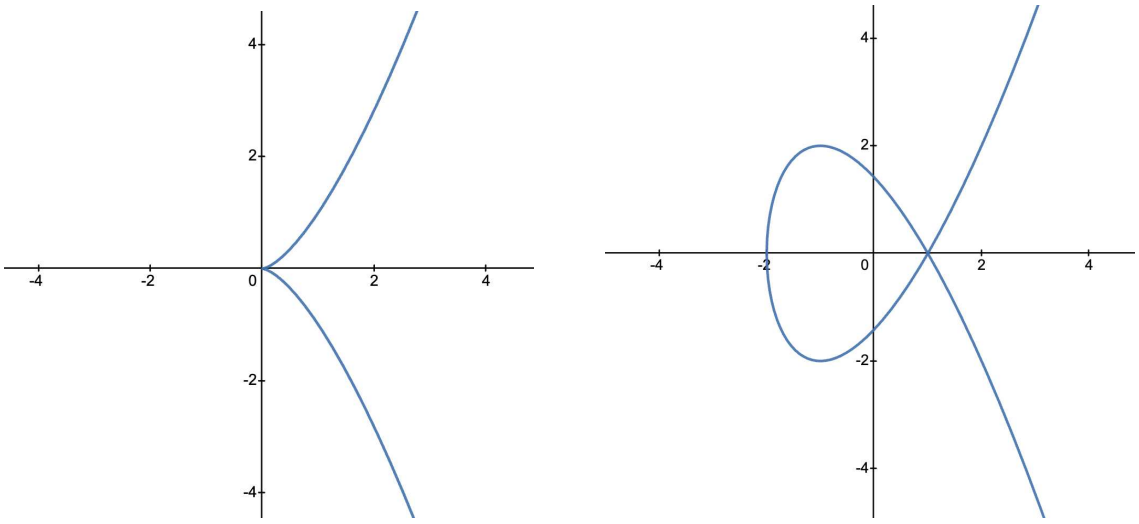
Računajući diskriminante dobijemo:

$$\Delta(E_1) = -1216$$

$$\Delta(E_2) = 12096$$

pa vidimo da za $\Delta < 0$ imamo jednu nul-točku dok za $\Delta > 0$ imamo tri nul-točke.

Gornja slika prikazuje dvije mogućnosti za krivulje koje su nesingularne, ali znamo da je uvjet kako bi krivulja bila nesingularna taj da $-16(4a^3 + 27b^2) \neq 0$, pa možemo prikazati i singularne krivulje. Kao što dobijemo dva različita prikaza eliptičkih krivulja ovisno o Δ kada je $\Delta \neq 0$, isto vrijedi i za singularne krivulje. Ako je $\Delta = 0$ i $a = 0$, tada imamo tzv. "šiljak", u slučaju kada je $\Delta = 0$ i $a \neq 0$, imamo "čvor".



(a) $y^2 = x^3$ ("šiljak") (b) $y^2 = x^3 - 3x + 2$ ("čvor")

Slika 2.2

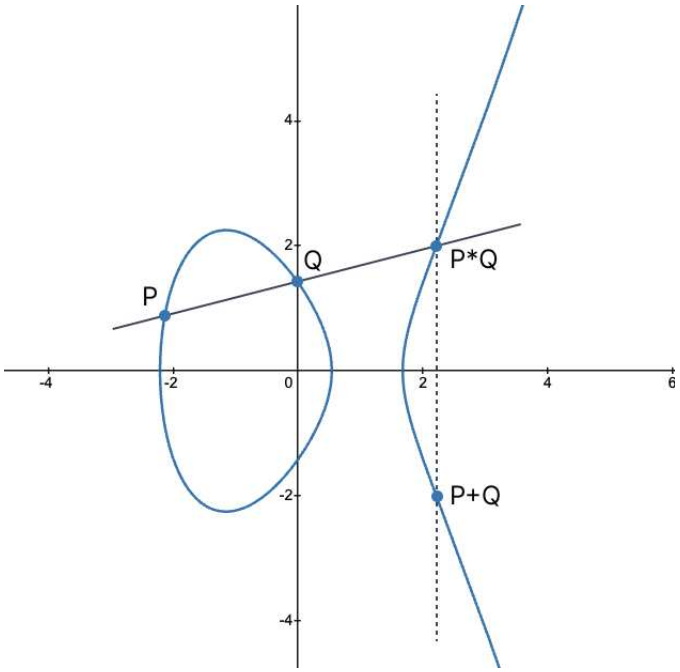
Za $\Delta \neq 0$ nemamo tri nul-točke, pa tako na lijevoj slici imamo trostruku nul-točku $x = 0$, a na desnoj slici je $x = 1$ dvostruka nul-točka.

Operacije nad eliptičkim krivuljama

Definirat ćemo operacije nad eliptičkim krivuljama za dvije točke P i $Q \in E(\mathbb{R})$. Povucimo pravac kroz P i Q. U slučaju kad $P \neq -P$, taj pravac siječe krivulju u tri točke, treću točku označimo s $P * Q$ te definiramo da je $P + Q$ točka osnosimetrična točki $P * Q$ s obzirom na os x. U slučaju kada su točke iste, odnosno $P = Q$, povlačimo tangentu kroz točku P i presjek tangente s krivuljom je upravo točka $2P$, ako je P točka infleksije, onda uzimamo $P * P = P$. Treću točku presjeka s eliptičkom krivuljom problem je pronaći kada su x-koordinate točaka iste. Pravac kroz te dvije točke je vertikalan i u tom slučaju uzimamo da je treća točka presjeka upravo točka u beskonačnosti $\mathcal{O}$. Vrijedi

$$P + \mathcal{O} = \mathcal{O} + P = P, \forall P \in E(\mathbb{R}).$$

U slikama 2.3 i 2.4 prikazan je geometrijski izvod zbrajanja točaka.



Slika 2.3: Operacije s različitim točkama

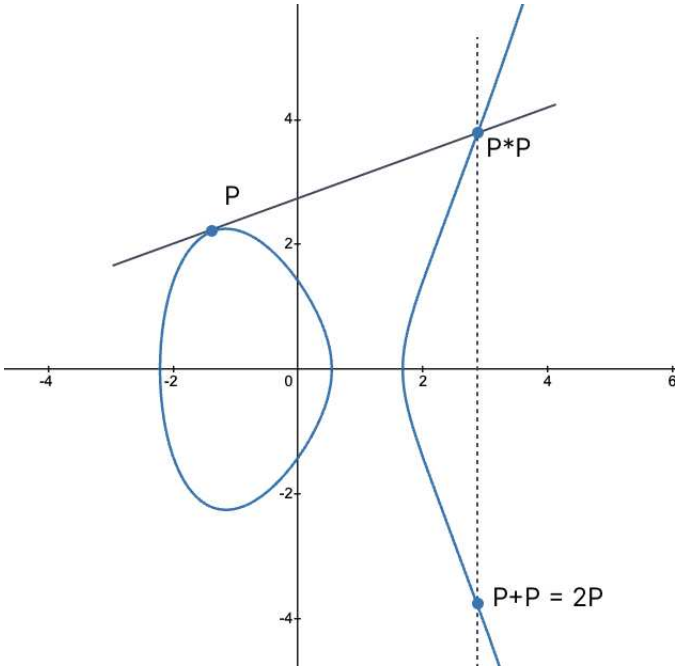
Opisan postupak može se opisati i eksplicitnim formulama za koordinate zbroja točaka. Važno je napomenuti da formule vrijede za proizvoljna polja karakteristika različitih od 2 i 3, s tim da vrijede i za takva polja uz malu modifikaciju.

Definicija 2.1.2. *Neka su $P = (x_1, y_1), Q = (x_2, y_2)$. Prva četiri slučaja opisuju "rubne slučajeve" te je peti slučaj generalno zbrajanje točaka:*

1. $-O = O$
2. $-P = (x_1, -y_1)$
3. $O + P = P$
4. *za $Q = -P$ je $P + Q = O$*
5. *za $Q \neq -P$ je $P + Q = (x_3, y_3)$ gdje je*

$$x_3 = \lambda^2 - x_1 - x_2, y_3 = -y_1 + \lambda(x_1 - x_3)$$

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & x_2 \neq x_1 \\ \frac{3x_1^2 + a}{2y_1} & x_2 = x_1 \end{cases}$$



Slika 2.4: Operacije nad jednom točkom

Definicija 2.1.3. *Kažemo da je točka $P \in E(\mathbb{Q})$ reda m ako je m najmanji prirodan broj za koji vrijedi $mP = \mathcal{O}$, ako takav m ne postoji, kažemo da je P točka beskonačnog reda.*

Pravilo *5.* iz 2.1.2 razmatra više slučajeva, pa ovdje opisujemo izvod tog pravila. Spomenuli smo da, geometrijski gledano, zbrajanje dvije točke P i Q uključuje povlačenje pravca kroz te dvije točke i pronalazak točke koja je toj točki osnosimetrična po x-osi. Neka je λ nagib pravca kroz P i Q. Ako P i Q imaju različite x koordinate, tada je λ odmah poznat:

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}.$$

Jednadžba pravca kroz P i Q je $y = \lambda x + \xi$. Vrijedi:

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1},$$
$$\xi = y_1 - \lambda x_1.$$

Tražimo treću točku presjeka ovog pravca sa krivuljom E. x-koordinate svih točaka presjeka su korijeni jednadžbe $x^3 - (\lambda x + \xi)^2 + ax + b = 0$. Dvije x-koordinate su nam već poznate, to su x_1 i x_2 iz točaka P i Q. Treću koordinatu možemo dobiti pomoću Vietéovih formula. Vrijedi $x_3 = \lambda^2 - x_1 - x_2$. Jednadžbu eliptičke krivulje možemo zapisati kao $x^3 - (\lambda x + \xi)^2 + ax + b = (x - x_1)(x - x_2)(x - x_3)$. Izjednačavanjem koeficijenata dobijemo

$\lambda^2 = x_1 + x_2 + x_3$, pa znamo da treća točka presjeka pravca sa E ima koordinate $(x_3, \lambda x + \xi)$. Sada imamo $P + Q = (x_3, -(\lambda x + \xi))$. Uvrštavanjem λ i ξ dobijemo formule za x_3 i y_3.

U slučaju $P = Q$ zapravo promatramo tangentu i tražimo presjek tangente sa eliptičkom krivuljom. Koeficijent smjera tangente λ, dobijemo derivacijom u točki P:

$$\lambda = \frac{3x_1^2 + a}{2y_1}.$$

Sada analogno kao u prošlom slučaju izvedemo formule koordinate druge točke presjeka.

Definicija 2.1.4. *Neka je E eliptička krivulja nad $\mathbb{Q}$, dana jednadžbom:*

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

gdje su $a, b \in \mathbb{Z}$. Za prost broj $p > 3$ možemo promatrati

$$y^2 = x^3 + ax + b \pmod{p}.$$

Ako ova jednadžba predstavlja eliptičku krivulju nad poljem $\mathbb{F}_p$, onda kažemo da E ima dobru redukciju modulo p. Lošu redukciju možemo dalje rastaviti, znamo da pri lošoj redukciji $x^3 + ax + b$ ima višestruke korijene modulo p, ako ima trostruki korijen, kažemo da ima aditivnu redukciju, u slučaju dvostrukog korijena kažemo da ima multiplikativnu redukciju. Dodatno, ako su koeficijenti smjera tangenata u singularnoj točki iz $\mathbb{F}_p$, kažemo da je rascjepiva, u suprotnom kažemo da je nerascjepiva.

Poglavlje 3

Rang eliptičke krivulje

Poincare je 1901. godine naslutio, a Mordell 1922. i dokazao da je grupa točkaa na eliptičkoj krivulji s racionalnim koeficijentima konačno generirana. Rješenja jednadžbe eliptičke krivulje, odnosno točke koje leže na eliptičkoj krivulji, možemo podijeliti u točke konačnog i točke beskonačnog reda. Množenjem točke beskonačnog reda s nekim $n \in \mathbb{N}$ nikada nećemo doći do točke u beskonačnosti O. Rang eliptičke krivulje povezujemo s onim točkama koje su beskonačnog reda.

Teorem 3.0.1 (Mordell-Weil)**.** *Grupa $E(\mathbb{Q})$ je konačno generirana Abelova grupa.*

Drugim riječima, svaka eliptička krivulja E nad poljem racionalnih brojeva sadrži konačan skup racionalnih točaka $P_1, ..., P_k$ iz kojih se pomoću osnovnih operacija mogu dobiti sve ostale točke na E.

Koristeći teorem 1.0.10 dobivamo sljedeću posljedicu:

Korolar 3.0.2.

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

Podgrupa $E(\mathbb{Q})_{tors}$ od $E(\mathbb{Q})$ naziva se torzijska grupa od E i sastoji se od svih točaka konačnog reda na E, a $r \in \mathbb{N}_0$, nazivamo rang eliptičke krivulje E i označavamo sa rank(E). Interpretacijom ovog korolara se vidi važnost ranga, na svakoj $E(\mathbb{Q})$ postoji r racionalnih točaka $P_1, ..., P_r$ beskonačnog reda sa svojstvom da se svaka racionalna točka P na E može prikazati u obliku:

$$P = T + m_1P_1 + ... + m_rP_r,\ m_1, ..., m_r \in \mathbb{Z}$$

gdje je T neka točka konačnog reda iz torzijske grupe $E(\mathbb{Q})_{tors}$. Suma $P + ... + P$ od m pribrojnika se često označava sa mP ili $[m]P$. Rang neke eliptičke krivulje je 0 ako i samo ako ta krivulja sadrži konačno mnogo racionalnih točaka, odnosno po pozitivnom rangu znamo da krivulja sadrži beskonačno mnogo racionalnih točaka. Ako pokušavamo naći sve moguće torzijske grupe neke eliptičke krivulje, odgovor leži u Mazurovom teoremu,

gdje je dokazano da postoji 15 mogućih torzijskih grupa. Za mogući rang nemamo teorem, imamo samo slutnju da rang može biti proizvoljno velik, odnosno da za svaki $n \in \mathbb{N}$ postoji eliptička krivulja E nad $\mathbb{Q}$ takva da je $\text{rank}(E) \geq n$. Iako je slutnja da je rang proizvoljno velik, pronaći krivulju visokog ranga je teško, 2006. godine je krivulju ranga ≥ 28 otkrio Noam Elkies. Jednadžba te krivulje je:

$y^2 + xy + y = x^3 - x^2$

$-20067762415575526585033208209338542750930230312178956502x$

$+3448161179503055646703298569039072037485594435931918036126600829629193944873224342 9$

Primjer 3.0.3. *Promotrimo eliptičku krivulju sa slike 3.1 danu jednadžbom:*

$$E : y^2 = x^3 - 357x + 2556$$

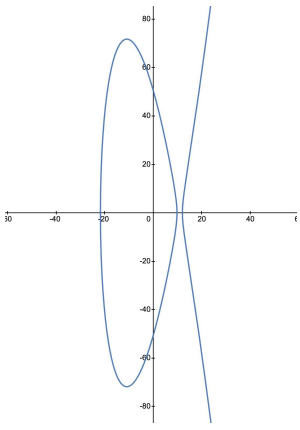
nad poljem racionalnih brojeva $\mathbb{Q}$. Eliptička krivulja E je ranga 2 sa pripadnom torzijskom grupom $\mathbb{Z}/2\mathbb{Z}$.

$$E(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}^2$$

Torzijska grupa sadržava točke konačnog reda, na ovoj krivulji je točka $(12, 0)$ reda 2. Vrijedi

$$(12, 0) + (12, 0) = \mathcal{O}.$$

S obzirom da je rang 2, znamo da krivulja sadrži dvije racionalne točke beskonačnog reda. U ovom slučaju to su točke $(7, 20), (15, 24)$.



Slika 3.1: $y^2 = x^3 - 357x + 2556$

Primjer 3.0.4. *Navodimo neke eliptičke krivulje i njihove generatore:*

E	rank(E)	
$y^2 = x^3 + 1$	0	$E_1(\mathbb{Q}) = \{n(2,3) : n = 0, 1, ..., 5\}$
$y^2 = x^3 - 2x + 2$	1	$E_1(\mathbb{Q}) = \{n(1,1) : n \in \mathbb{Z}\}$
$y^2 = x^3 - 4x + 1$	2	$E_1(\mathbb{Q}) = \{n(0,1) + n'(-1,2) : n, n' \in \mathbb{Z}\}$

Kroz godine su se pronalazile eliptičke krivulje sve većeg ranga, pa tako postoji i povijesni zapis rekordnih krivulja [7]:

rang $\geq$	godina	autori
3	1938.	Billing
4	1945.	Wiman
6	1974.	Penney, Pomerance
7	1975.	Penney, Pomerance
8	1977.	Grunewald, Zimmert
9	1977.	Brumer, Kramer
12	1982.	Mestre
14	1986.	Mestre
15	1992.	Mestre
17	1992.	Nagao
19	1992.	Fermigier
20	1993.	Nagao
21	1994.	Nagao, Kouya
22	1997.	Fermigier
23	1998.	Martin, McMillen
24	2000.	Martin, McMillen
28	**2006.**	**Elkies**

Spomenuli smo da je torzijsku grupu je lakše odrediti nego rang, štoviše 1978. godine je Mazur dokazao da ih postoji samo 15 mogućih za eliptičke krivulje nad $\mathbb{Q}$:

$$\mathbb{Z}_k \text{ za } k = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12$$

$$\mathbb{Z}_2 \times \mathbb{Z}_k \text{ za } k = 2, 4, 6, 8$$

Za svaku od tih torzijskih grupa je poznata krivulja s trenutno najvećim otkrivenim rangom. Definiramo:

$$B(G) = \sup\{\text{rank}(E(\mathbb{Q})) : E(\mathbb{Q})_{\text{tors}} = G\}$$

Možemo za svaku poznatu torzijsku grupu G odrediti $B(G)$, i iako se smatra da je za svaku grupu taj broj neograničen, zasad je tek poznato da je za svaku $B(G) \geq 3$. Sljedeća tablica [6] prikazuje rekorde i godine otkrića pripadnih eliptičkih krivulja.

G	$B(G) \geq$	autori
O	28	Elkies (2006.)
$\mathbb{Z}/2\mathbb{Z}$	20	Elkies i Klagsbrun (2020.)
$\mathbb{Z}/3\mathbb{Z}$	15	Elkies i Klagsbrun (2020.)
$\mathbb{Z}/4\mathbb{Z}$	13	Elkies i Klagsbrun (2020.)
$\mathbb{Z}/5\mathbb{Z}$	9	Klagsbrun (2020.)
$\mathbb{Z}/6\mathbb{Z}$	9	Klagsbrun (2020.), Voznyy (2020.)
$\mathbb{Z}/7\mathbb{Z}$	6	Klagsbrun (2020.)
$\mathbb{Z}/8\mathbb{Z}$	6	Elkies (2006.), Dujella - MacLeod - Peral (2013.), Voznyy (2021.)
$\mathbb{Z}/9\mathbb{Z}$	4	Fisher (2009.), van Beek (2015.), Dujella - Petričević (2021.), Dujella - Petričević - Rathbun (2022.)
$\mathbb{Z}/10\mathbb{Z}$	4	Dujella (2005., 2008.), Elkies (2006.), Fisher (2016.)
$\mathbb{Z}/12\mathbb{Z}$	4	Fisher (2008.)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	15	Elkies (2009.)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$	9	Dujella i Peral (2012.), Klagsbrun (2020.)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$	6	Elkies (2006.), Dujella - Peral - Tadic (2015.), Dujella - Peral (2020.)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$	3	Connell (2000.), Dujella (2000., 2001., 2006., 2008.), Campbell i Goins (2003.), Rathbun (2003., 2006.), Dujella i Rathbun (2006.), Flores - Jones - Rollick - Weigandt - Rathbun (2007.), Fisher (2009.), AttarBashi - Rathbun - Voznyy (2022.), AttarBashi - Fisher - Rathbun - Voznyy (2022.), AttarBashi - Fisher - Voznyy (2022.)

Postoje predviđanja o tome koliki rang može biti za zadanu torzijsku grupu. U [12] Park, Poonen, Voight i Wood predviđaju da postoji konačno mnogo eliptičkih krivulja s torzijskim grupama $\mathbb{Z}/8\mathbb{Z}$ i $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ ranga ≥ 4. Dujella i Peral dokazuju u [9] da postoji konačno mnogo eliptičkih krivulja tih istih torzijskih grupa i ranga ≥ 3.

Točke torzijske grupe i nezavisne točke konačnog reda za rekordne krivulje su vrlo veliki brojevi, čak i rang ≤ 10. Promotrimo krivulju ranga 3 sa zadanom torzijskom grupom $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ koju su 2000. godine konstruirali Connell i Dujella:

$$y^2 + xy = x^3 + 157459325308290898 80x + 240282199570959694263392784 00.$$

Nezavisne točke beskonačnog reda su:

$$\{(2188064030, -7124272297330), (-2815745040, -214568724545880), (3643261410, -122557804465830)\}.$$

Točke torzijske grupe su:

$$\{O, (-4581539664, 2290769832),$$
$$(2132310660, 12167787556920), (2452514160, 12747996298920),$$
$$(9535415580, 860741285907000), (2132310660, -12169919867580),$$

$$(-1236230160, -203971265617560), (9535415580, -860750821322580),$$
$$(2452514160, -12750448813080), (2346026160, -1173013080),$$
$$(1471049760, 63627110794920), (1471049760, -63628581844680),$$
$$(3221002560, -82025835631080), (3221002560, 82022614628520),$$
$$(8942054015/4, -8942054015/8)\}.$$

Ovako veliki brojevi, već za krivulje malog ranga, predstavljaju problem za računske operacije. Kasnije će se ta veličina pokazati jednim od glavnih razloga zašto kriptografi smatraju eliptičke krivulje važnim alatom za primjene u kriptografiji.

3.1 Metode računanja ranga

Iako ne postoji univerzalni algoritam za određivanje ranga koji bi se mogao primijeniti na svaku eliptičku krivulju, u nastavku su navedeni algoritmi koji su korisni u nekim slučajevima. Sam pronalazak krivulja ranga koji nije 0 ili 1 je težak, i slutnja je da više od pola eliptičkih krivulja ima rang 0. Međutim, kod krivulja koje nemaju nijednu racionalnu točku reda 2 te imaju velike koeficijente, postojeći algoritmi još uvijek nisu dovoljno efikasni da bi se koristili u praksi.

Krivulje s točkom reda 2

U ovom algoritmu proučavamo eliptičke krivulje E koje imaju barem jednu točku reda 2. Jedna od metoda za računanje ranga takvih krivulja naziva se "silazak pomoću 2-izogenije". Homomorfizam između dvije eliptičke krivulje dan pomoću racionalnih funkcija nazivamo izogenijom. Možemo pretpostaviti da je točka reda 2 upravo točka $(0, 0)$ te da E ima jednadžbu:

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

Definicija 3.1.1. *Neka je eliptička krivulja definirana sa*

$$E : y^2 = x^3 + ax^2 + bx$$

Za krivulju E' definiranu sa:

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

gdje su $a' = -2a,\ b' = a^2 - 4b$ kažemo da je 2-izogena krivulji E.

Definiramo preslikavanja između dvije eliptičke krivulje:

$$\phi : E \to E',\ \phi(P) = \begin{cases} \left(\frac{y^2}{x^2}, \frac{y(x^2-b)}{x^2}\right), P = (x, y) \neq O, (0, 0) \\ O, \text{inače} \end{cases}$$

$$\psi : E' \to E,\ \psi(P') = \begin{cases} \left(\frac{y'^2}{4x'^2}, \frac{y'(x'^2-b')}{8x'^2}\right), P' = (x', y') \neq \mathcal{O}, (0,0) \\ \mathcal{O}, \text{inače} \end{cases}$$

Vrijedi:

$$(\psi \circ \phi)(P) = 2P, \forall P \in E$$

$$(\phi \circ \psi)(P') = 2P', \forall P' \in E'$$

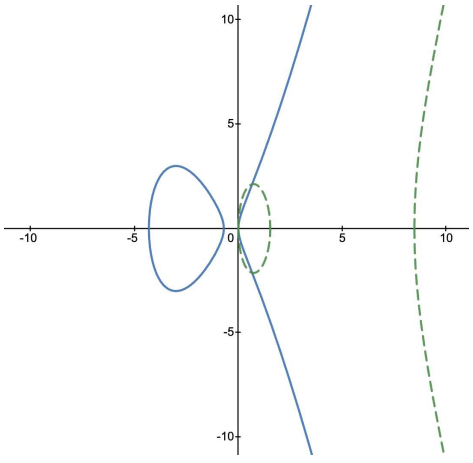
Definiramo i preslikavanja:

$$\alpha : E(\mathbb{Q}) \to \mathbb{Q}^*/\mathbb{Q}^{*2}, \alpha(x,y) = \begin{cases} x \cdot \mathbb{Q}^{*2}, P = (x,y) \neq \mathcal{O}, (0,0) \\ b \cdot \mathbb{Q}^{*2}, P = (0,0) \\ 1 \cdot \mathbb{Q}^{*2}, P = \mathcal{O} \end{cases}$$

$$\beta : E(\mathbb{Q}) \to \mathbb{Q}^*/\mathbb{Q}^{*2}, \beta(x,y) = \begin{cases} x \cdot \mathbb{Q}^{*2}, P = (x,y) \neq \mathcal{O}, (0,0) \\ b \cdot \mathbb{Q}^{*2}, P = (0,0) \\ 1 \cdot \mathbb{Q}^{*2}, P = \mathcal{O} \end{cases}$$

Želimo dobiti opis elemenata iz $Im(\alpha)$, sa $\tilde{x}$ ćemo označiti klasu od x u $\mathbb{Q}/\mathbb{Q}^{*2}$. Neka je $(x,y) \in E(\mathbb{Q})$. Ako je $x = 0$, onda je $(x,y) = (0,0)$ i $\alpha(x,y) = \tilde{b}$. Ako je $x \neq 0$, zapišimo x i y u obliku $x = \frac{m}{e^2}$, $y = \frac{n}{e^3}$, $\text{nzd}(m,e) = \text{nzd}(n,e) = 1$ te ih uvrstimo u jednadžbu od E. Dobivamo:

$$n^2 = m(m^2 + ame^2 + be^4)$$



Slika 3.2: $y^2 = x^3 + 5x^2 + 3x$ (plavo) i njoj 2-izogena $y^2 = x^3 - 10x^2 + 13x$ (zeleno)

Neka je $b_1 = \pm nzd(m, b)$ gdje je predznak odabran tako da je $mb_1 > 0$. Tada je $m = b_1m_1, b = b_1b_2, n = b_1n_1$ pa dobivamo:

$$n_1^2 = m_1(b_1m_1^2 + am_1e^2 + b_2e^4).$$

Budući da su faktori desne strane relativno prosti te $m_1 > 0$, tada postoje cijeli brojevi M, N tako da vrijedi $m_1 = M^2, b_1m_1^2 + am_1e^2 + b_2e^4 = N^2$. Dobijemo jednadžbu:

$$N^2 = b_1M^4 + aM^2e^2 + b_2e^4$$

s nepoznanicama M, e, N. Sada je $\alpha(x, y) = \left(\frac{b_1M^2}{e^2}\right) \cdot \mathbb{Q}^{*2} = \tilde{b_1}$.

Zaključujemo da se $Im(\alpha)$ sastoji od $\tilde{1}, \tilde{b}$ te od svih $\tilde{b_1}$ gdje je b_1 djelitelj broja b za kojeg jednadžba

$$N^2 = b_1M^4 + aM^2e^2 + b_2e^4$$

gdje je $b_1b_2 = b$ ima rješenja $N, M, e \in Z, e \neq 0$. Tada je $\left(\frac{b_1M^2}{e^2}, \frac{b_1MN}{e^3}\right) \in E(\mathbb{Q})$. Uočimo da ta jednadžba ima rješenje za $b_1 = 1$, a to je $(M, e, N) = (1, 0, 1)$ i za $b_1 = b$, a to je $(M, e, N) = (0, 1, 1)$.

Pomoću definiranih transformacija možemo konstruirati algoritam:
Za svaku faktorizaciju $b = b_1b_2$ gdje je b_1 kvadratno slobodan cijeli broj, napišemo jednadžbu $N^2 = b_1M^4 + aM^2e^2 + b_2e^4$ i pokušamo odrediti ima li ta jednadžba netrivijalnih cjelobrojnih rješenja. Svako rješenje (M, e, N) inducira točku na krivulji E s koordinatama $x = \frac{b_1M^2}{e^2}, y = \frac{b_1MN}{e^3}$. Neka je r_1 broj faktorizacija za koje pripadna jednadžba ima rješenja, te neka je r_2 broj koji je definiran na isti način za konstruirani krivulju E'. Tada postoje $e_1, e_2 \in \mathbb{Z}_0$ takvi da je $r_1 = 2^{e_1}, r_2 = 2^{e_2}$ i pritom vrijedi:

$$rank(E) = e_1 + e_2 - 2$$

Primjer 3.1.2. *Izračunati ćemo rang krivulje*

$$E : y^2 = x^3 - 2x.$$

Računamo koeficijente pripadne 2-izogene krivulje sa

$$a' = -2 \cdot 0 = 0$$

$$b' = 0^2 - 4 \cdot (-2) = 8,$$

pa je 2-izogena krivulja dana jednadžbom

$$E' : y^2 = x^3 + 8x.$$

Za $b = -2$ tražimo faktorizacije $b = b_1b_2$ gdje je $b_1 \in \mathbb{Z}$ kvadratno slobodan. Faktorizacije su $b = -1 \cdot 2 = 1 \cdot (-2) = -2 \cdot 1 = 2 \cdot (-1)$. Konstruiramo pripadne jednadžbe oblika $N^2 = b_1M^4 + aM^2e^2 + b_2e^4$ i za svaku od tih jednadžbi odredimo ima li netrivijalnih cjelobrojnih rješenja. Imamo jednadžbe:

[1.] $N^2 = M^4 - 2e^4$

[2.] $N^2 = -M^4 + 2e^4$

[3.] $N^2 = 2M^4 - e^4$

[4.] $N^2 = -2M^4 + e^4$

i tražimo rješenja (M, e, N)*. Jednadžba* [1.] *ima rješenje* $(M, e, N) = (1, 0, 1)$*, i jednadžba* [4.] *ima rješenje* $(0, 1, 1)$*. Ostaje provjeriti jednadžbe* [2.] *i* [3.]*. U jednadžbe* [2.] *i* [3.] *uvrstimo* $(M, e, N) = (2, 2, 4)$*.*
Sve jednadžbe [1.] − [4.] *imaju rješenja, pa je* $r_1 = 4$*. Vrijedi* $r_1 = 2^{e_1}$*, pa je* $e_1 = 2$*.*

Isti postupak ponavljamo za E'*. Faktoriziramo broj 8. Mogućnosti za* b_1' *su* $\pm 1, \pm 2, \pm 4, \pm 8$*. BSO možemo uzeti da je* b_1' *kvadratno slobodan. Znamo da* b_1 *i* b_2 *ne mogu oba biti negativni brojevi, ako je* $b_1 < 0$*, tada* b_2 *mora biti veći od nule, inače ne može bit kvadrat. Mogućnosti koje ostaju za* b_1' *su* 1 *i* 2*. Za* b_1' *već znamo da postoji rješenje pa preostaje provjeriti jednadžbu*

$$N^2 = 2M^4 + 4e^4.$$

Jednadžba ima rješenje, $(M, e, N) = (6, 3, 54)$*. Zaključujemo da je imamo* $r_2 = 2$ *i* $e_2 = 1$
Algoritam nam daje formulu za rang prema kojoj vrijedi:

$$rank(E) = e_1 + e_2 - 2 = 2 + 1 - 2 = 1.$$

Provjerom u programu PARI možemo potvrditi da je rang ispravan i da vrijedi:

$$E(\mathbb{Q}) \cong \mathbb{Z} \times \mathbb{Z}_2,$$

gdje je točka $(0, 0)$ *reda 2, te je* $(-1, 1)$ *jedna točka beskonačnog reda.*

Konstruiranje eliptičkih krivulja velikog ranga

Zaslužnost širokoj primjeni eliptičkih krivulja u modernoj kriptografiji upravo se može pripisati težini pronalaska eliptičkih krivulja velikog ranga. Ne postoji konkretan algoritam za pronaći krivulju ranga kojeg želimo, pa tako ni nekog velikog ranga. Ako na slučajan način izaberemo parametre za eliptičku krivulju, najvjerojatnije će joj torzijska grupa biti trivijalna, a rang vrlo mali, 0 ili 1. Postoje konkretni algoritmi s kojima možemo konstruirati eliptičku krivulju sa željenom torzijskom grupom, no isto ne vrijedi i za rang. Za pronaći krivulje visokog ranga koristimo metode traženja gdje pokušavamo suziti krivulja koje ćemo promatrati na one s većom šansom da imaju veliki rang, te onda među njima pokušati pronaći odgovarajuću krivulju. Sve što znamo o trenutno rekordnoj krivulji što se tiče ranga je to da joj je rang ≥ 28. Uz slutnju da rang može biti proizvoljno velik, postoje

i novija previđanja [12] da postoji samo konačno mnogo eliptičkih krivulja nad $\mathbb{Q}$ ranga ≥ 21. Ako je ta slutnja dokaže točnom, to bi značilo da je rang ipak ograničen.

Metoda s kojom se pronalaze krivulje visokog ranga sastoji se od tri dijela, konstrukcije, sita i računanja.

- **Konstrukcija**
  U razmatranje uzmemo familiju eliptičkih krivulja nad $\mathbb{Q}$ za koju je dokazano, ili samo slutimo, da sadrži eliptičke krivulje s visokim rangom.

- **Sito**
  Kako i sam naziv koraka govori, možemo filtrirati generirane krivulje po informacijama koje znamo o njihovom rangu. Donja i gornja ograda za rang se mogu izračunati brže od samog ranga ali nam zato daju uvid u to koje krivulje nam se isplati dalje promatrati.

- **Računanje ranga**
  Za suženi izbor krivulja računamo rang, ili barem što bolju donju ogradu ranga.

Mestreova polinomijalna metoda

Po tablici rekordnih rangova, između 1982. i 1992. je očito u tom polju najaktivniji bio Jean-Francois Mestre, koji je u tom razdoblju osmislio većinu metoda korištenih u koracima konstrukcije i sita.

U ovom potpoglavlju opisat ćemo jednu od Mestreovih konstrukcija iz 1991. godine s kojom je konstruirao beskonačno mnogo eliptičkih krivulja ranga ≥ 11. Ova konstrukcija poznata je pod imenom Mestreova polinomijalna metoda.

Teorem 3.1.3. *Neka je $\mathbb{K}$ polje karakteristike 0 i neka je $p \in \mathbb{K}[x]$ normirani polinom stupnja* $\deg\ p = mn$ *gdje su $m, n \geq 1$. Tada postoji normirani polinom $q \in \mathbb{K}[x]$ takav da je* $\deg\ q = n$ *i* $\deg(p - q^m) < n(m-1)$.

Dokaz. Dokaz provodimo matematičkom indukcijom po i dokazujući da za svaki $i \leq n$, postoji polinom $q_i \in \mathbb{K}[x]$ takav da je $\deg\ q_i = n$ i $\deg\ (p - q_i^m) < n(m-1)$.
Za bazni slučaj, $i = 0$ uzmimo da je $q_0 = x^n$. Vrijedi $\deg\ x^n = n$ i $\deg(p - x^{nm}) < n(m-1)$.

Pretpostavimo da tvrdnja vrijedi za svaki $i - 1$, $0 < i \leq n$. Tada postoji polinom q_{i-1} stupnja n takav da $\deg(p - q_{i-1}^m) < nm - i + 1$. Tražimo polinom q_i oblika $q_i = q_{i-1} + cx^{n-i}$.

Možemo raspisati polinom q_i^m kao:

$$q_i^m = q_{i-1}^m + mcq_{i-1}^{m-1}x^{n-i} + \binom{m}{2}c^2q_{i-1}^{m-2}x^{2(n-i)} + \cdots$$

Za stupanj trećeg člana vrijedi $\deg\left(\binom{m}{2}c^2 q_{i-1}^{m-2}x^{2(n-i)}\right) \leq n(m-2)+2(n-i) = nm-2i < nm-i$, i isto vrijedi za svaki sljedeći član. Stupanj polinoma $q_{i-1}^{m-1}x^{n-i}$ je $nm-i$ i možemo izabrati c tako da se koeficijenti od x^{nm-i} ponište. Tako dobijemo $\deg(p-q_i^m) = \deg(p-q_{i-1}^m - mcq_{i-1}^{m-1}x^{n-i}) < nm-i$. Iz normiranosti polaznog polinoma q_0 i daljne konstrukcije vrijedi da je svaki polinom q_i normiran. □

Korolar 3.1.4. *Neka je $p(x) \in \mathbb{Q}[x]$ normirani polinom stupnja $p = 2n$. Tada postoje jedinstveni polinomi $q(x), r(x) \in \mathbb{Q}[x]$ takvi da je q je normiran, $p = q^2 - r$ i $\deg\ r \leq n-1$.*

Dokaz. Za dokazati da polinomi $q(x), r(x)$ uvijek postoje, možemo iskoristiti teorem 3.1.3 za slučaj $m = 2$. $\mathbb{Q}$ je polje karakteristike 0 i p je polinom stupnja $\deg\ p = mn = 2n$ stoga je teorem primjenjiv.

Preostaje dokazati jedinstvenost polinoma $q(x)$ i $r(x)$.

Pretpostavimo da postoje $q_1(x), r_1(x) \in \mathbb{Q}[x]$ s istim svojstvima kao i $q(x), r(x)$. Tada vrijedi i $q^2 - r = q_1^2 - r_1$ pa imamo:

$$(q-q_1)(q+q_1) = r - r_1$$

Ako uzmemo da je $q \neq q_1$, tada je $\deg\ (q-q_1)(q+q_1) \geq n$ te za $r \neq r_1$ dobijemo $\deg\ (r-r_1) \leq n-1$. S obzirom na to da nemamo isti stupanj polinoma, došli smo do kontradikcije, pa je stoga $q = q_1$ i $r = r_1$. □

Polinom q iz korolara 3.1.4 možemo dobiti uzastopnim izračunima koeficijenata ili iz asimptotskog razvoja $\sqrt{p}$.
Pretpostavimo da je

$$p(x) = \prod_{i=1}^{2n}(x-a_i)$$

gdje su $a_1, ..., a_{2n}$ međusobno različiti racionalni brojevi. Tada na krivulji:

$$C : y^2 = r(x)$$

imamo točke oblika $(a_i, \pm q(a_i)), i = 1, ..., 2n$. S obzirom na uvjet nesingularnosti, za polinom r stupnja 3 ili 4 koji nema višestrukih korijena je C eliptička krivulja. Trebamo samo odrediti točku u beskonačnosti za $\deg\ r$. Za $\deg\ r = 3$ vrijedi da je C eliptička krivulja po definiciji iz 2.1. Za $\deg\ r = 4$ uzmemo jednu racionalnu točku na C, oblika $(a_1, q(a_1))$ te nju koristimo kao točku u beskonačnosti. Za $n = 5$ skoro svi izbori od a_i daju $\deg\ r = 4$, tada C sadrži 10 racionalnih točaka oblika $(a_i, q(a_i))$ i možemo očekivati eliptičku krivulju ranga ≥ 9. Mestre je konstruirao familiju eliptičkih (odnosno eliptičku krivulju nad poljem racionalnih funkcija $\mathbb{Q}(t)$) krivulja ranga ≥ 11 tako što je uzeo $n = 6$ i $a_i = b_i + t, i = 1, ..., 6$ te $a_i = b_{i-6} - t, i = 7, ..., 12$. Polinom $r(x)$ je u tom slučaju stupnja 5 i možemo uzeti $b_1, ..., b_6$ tako da koeficijenti uz x^5 budu jednaki 0. Mestre je u prvoj konstrukciji 1991. godine uzeo $b_1 = -17, b_2 = -16, b_3 = 10, b_4 = 11, b_5 = 14, b_6 = 17$.

Birch Swinnerton-Dyer slutnja

Za početak spominjemo slutnju dokazanu za rang 0 i 1, no sama slutnja nije prikladna za direktno računanje ranga i iskoristit ćemo ideju kako bismo pokazali vezu između eliptičkih krivulja nad $\mathbb{Q}$ i onih nad konačnim poljima $\mathbb{F}_p$. Više o eliptičkim krivuljama $E(\mathbb{F}_p)$ govorimo u kontekstu kriptografije u 4.2.

Početak istraživanja koje je kasnije dovelo do BSD slutnje započelo je u prvoj polovici 1960.-tih godina. Britanski matematičari Bryan Birch i Peter Swinnerton-Dyer su za svoje izračune na sveučilištu Cambridge imali pristup EDSAC-u, jednom od najranijih računala na svijetu. Uzmimo eliptičku krivulju E nad $\mathbb{Q}$. Za svaki prost broj p takav da p ne dijeli $\Delta = -16(4a^3 + 27b^2)$ možemo reducirati a i b modulo p i promatrati E kao eliptičku krivulju nad $\mathbb{F}_p$. Birch i Swinnerton-Dyer promatrali su broj rješenja eliptičke krivulje nakon redukcije ovisno o tome izboru za p.

Definicija 3.1.5. *Za svaki prost broj p takav da p ne dijeli Δ definiramo:*

$$N_p = \#E(\mathbb{F}_p) = 1 + \#\{0 \leq x, y \leq p-1 : y^2 \equiv x^3 + ax + b \pmod{p}\}$$

Teorem 3.1.6 (Hasse)**.** *Za svaki prost broj p takav da p ne dijeli Δ vrijedi:*

$$p + 1 - 2\sqrt{p} \leq N_p \leq p + 1 + 2\sqrt{p}$$

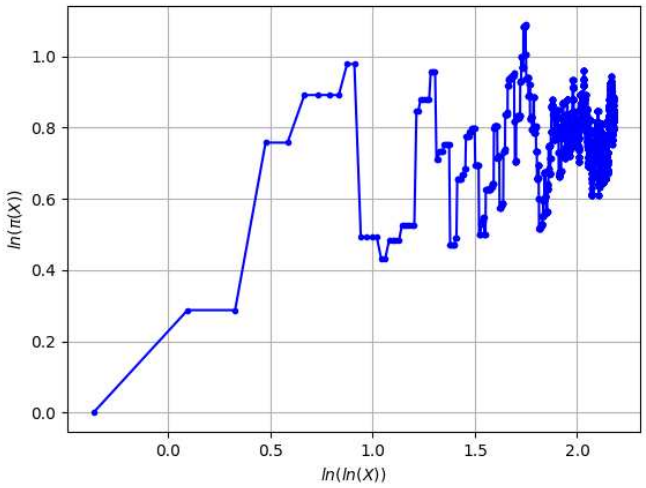
Birch i Swinnerton-Dyer započeli su svoje istraživanje računanjem vrijednosti funkcije

$$\pi_E(X) = \prod_{\substack{p \leq X \\ p \nmid \Delta}} \frac{N_p}{p}$$

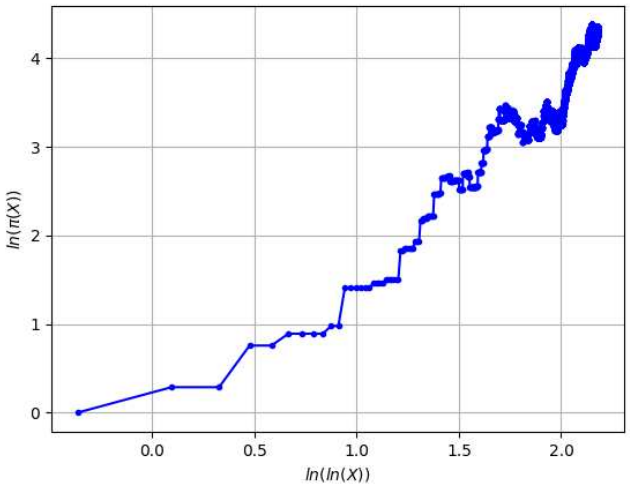
za rastuće X i proste brojeve p, nad određenim eliptičkim krivuljama. Za tri eliptičke krivulje, definirane sa

$$E_1 : y^2 = x^3 - 1^2 x$$
$$E_2 : y^2 = x^3 - 34^2 x$$
$$E_2 : y^2 = x^3 - 1254^2 x$$

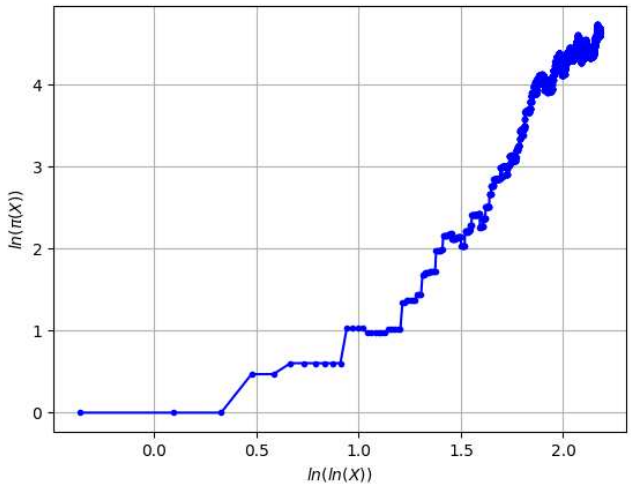
promotrimo ponašanje funkcije $\pi_{E_i}(X)$ za $0 < X \leq 7000$. Za računanje funkcije $\pi_{E_i}(X)$ korišten je kod A.1 u programu PARI, a za grafički prikaz koristimo paket programski jezik Python.



Slika 3.3: $\pi_{E_1}(X)$



Slika 3.4: $\pi_{E_2}(X)$



Slika 3.5: $\pi_{E_3}(X)$

Birch i Swinnerton-Dyer su za sve krivulje za koje su računali vrijednosti funkcije $\pi(X)$ dobili slično ponašanje. Iz takvih rezultata nastala je sljedeća slutnja:

$$\pi_E(X) \sim c \cdot (\ln(X))^{\text{rang}(E)}$$

gdje je c neka konstanta.

Sama BSD slutnja nije prikladna za direktno računanje ranga, tako da ćemo spomenuti još neke metode koje se mogu koristiti u fazi ”sijanja”.

Mestre-Nagao sume

Sljedeća metoda motivirana je BSD slutnjom i N_p je u ovoj metodi definiran na isti način. Mestre i Nago su argumentirali da bi za krivulje visokog ranga određene sume trebale poprimati velike vrijednosti. Navodimo neke od tih suma:

$$S_1(X) = \sum_{p \le X} \frac{N_p + 1 - p}{N_p} \ln p$$

$$S_2(X) = \sum_{p \le X} \frac{N_p + 1 - p}{N_p}$$

$$S_3(X) = \sum_{p \le X} (N_p - 1 - p) \ln p$$

Ovu ideju primijenimo odabirom prirodnih brojeva $X_1 < X_2 < \cdots < X_k$ i računanjem $S_i(X_1), S_i(X_2), ...$ ali tako da se u svakom koraku odbaci određeni postotak eliptičkih krivulja s najmanjom vrijednošću pripadne sume. Problem leži u računanju N_p jer za velike p nemamo efikasan algoritam, pa X_k ne smije biti prevelik. Najčešće koristimo $X \in [1000, 100000]$.

3.2 Krivulje ranga ≥ 2

Iskoristit ćemo rezultate koje su pronašli Brown i Myers 2002. godine [3] kako bismo prikazali neke familije eliptičkih krivulja za koje je poznato da nisu ranga 0 ili 1. Proučit ćemo familiju krivulja, one oblika $C_t : y^2 = x^3 - t^2x + 1$. Za $t \geq 4$ sve krivulje oblika C_t imaju trivijalnu torzijsku grupu i ranga su barem 2. Iskoristit ćemo programski paket PARI [15] za izračune vezane uz pojedine krivulje.

Krivulje oblika $C_t : y^2 = x^3 - t^2x + 1$

Koristeći PARI program možemo brzo kreirati sljedeću tablicu rangova eliptičkih krivulja C_t u ovisnosti o t:

rang $\geq$	t
2	2,3
3	4,5,6,7,9,10,11,12,15,18,21
4	8,13,14,16,19,20,22,23,26,27
5	17,25,36,41,42,46,53,59,70
6	61,107,124,128,146,148,199

Za ovu familiju krivulja pokazano je da vrijedi sljedeći teorem:

Teorem 3.2.1. *Neka je $t \in \mathbb{N}$, i neka je C_t eliptička krivulja definirana sa $y^2 = x^3 - t^2x + 1$, tada je svaka C_t ranga barem 3, za svaki $t \geq 4$.*

Koristeći metodu sijanja pomoću Mestre-Nagao suma kao u članku [14], konstruirati ćemo eliptičku krivulju ranga ≥ 8. Najveći rang pronađen za krivulje C_t gdje su $t \in \mathbb{N}$ je ≥ 9, za $t = 11416, 16228, 20529$. Te krivulje su pronađene pomoću Mestre-Nagaovih suma, i za naš primjer ćemo na isti način pokušati doći do parametara t za koje će rang krivulja C_t biti ≥ 8. Mestre-Nagao suma koju ćemo koristiti dana je formulom:

$$S(N, E) = \sum_{p \leq N, p \text{ prost}} \frac{2 - a_p}{p + 1 - a_p} \ln(p)$$

gdje je $a_p = a_p(E) = p + 1 - \#E(\mathbb{F}_p)$. Za izračunavanje vrijednosti sume koristiti ćemo PARI, koji je efikasan za N koji nisu preveliki. Pokušati ćemo pronaći parametar t takav da je krivulja C_t ranga ≥ 8. Za brojeve $1 \leq t \leq 10000$ računamo pripadnu Mestre-Nagao sumu eliptičke krivulje C_t. Spomenuli smo da je slutnja vezana za Mestre-Nagao sume da ta je ta suma velika za krivulje visokog ranga. Postavimo li donju granicu na vrijednost sume, ne moramo računati rang svake krivulje $C_t, 1 \leq t \leq 10000$, već samo onih za koje je suma dovoljno velika. Računati ćemo rang krivulja za koje je $S(523, C_t) > 23$ i $S(1979, C_t) \geq 34$. Među ovim krivuljama je cilj pronaći neku čiji je rang ≥ 8. Izračuni su dobiveni koristeći kod A.2.

Za većinu parametara t gdje pripadna eliptička krivulja ima dovoljno veliku Mestre-Nagao sumu dobijemo da je rang 5,6 ili 7. U tablici 3.1 su prikazane nezavisne točke beskonačnog reda i rang nekih od konstruiranih krivulja.

t	Rang	Nezavisne točke beskonačnog reda
25	5	$(-13, 77), (25, 1), (-23, 47), (0, 1), (-3, 43)$
124	6	$(-46, 781), (-44, 769), (0, 1), (-14, 461), (-124, 1), (-30, 659)$
3176	7	$(-822, 87955), (-1870, 111011), (0, 1), (-1, 3176),$ $(3264, 43009), (-2084, 109409), (-3080, 43009)$
4972	8	$(-822, 87955), (-1870, 111011), (0, 1), (-1, 3176), (3264, 43009),$ $(-2084, 109409), (-3080, 43009)$

Tablica 3.1: Vrijednosti za konstruirane krivulje C_t, $t \in \mathbb{N}$

Pripadna Mestre-Nagao suma sa parametrima $N = 1979$ eliptičke krivulje $y^2 = x^3 - 4972^2x + 1$ iznosi 38.636689.

PARI ima ugrađenu funkciju za računanje ranga eliptičke krivulje. Funkcija *ellrank*(E) nam uz točke konačnog reda daje donju i gornju granicu ranga. Za krivulju $y^2 = x^3 - 4972^2x + 1$ su i donja i gornja granica 8, pa tako znamo točnu vrijednost ranga. Ista donja i gornja granica se također pojavljuju i pri računanju ranga krivulja $y^2 = x^3 - 25^2x + 1$ i $y^2 = x^3 - 124^2x + 1$, pa tako znamo da je rang egzaktan.

U prethodnoj konstrukciji koristili smo $t \in \mathbb{N}$. Za sljedeće konstrukcije ćemo proširiti mogućnosti za t na racionalne brojeve. Uzmimo $t = \frac{a}{b}$, gdje su $0 < a \leq 5000, 0 < b \leq 3000$. Modificirati ćemo i filtere koje smo koristili na temelju vrijednosti Mestre-Nagao sume za danu krivulju. Računati ćemo rang samo onih krivulja za koje vrijedi $S(523, C_t) > 23$ i $S(1979, C_t) \geq 47$. Navodimo neke zanimljive rezultate u tablici 3.2.

Koristeći racionalne brojeve, postupak je dao i krivulju ranga 10. U [14] su sa većim racionalnim parametrima pronađene i krivulje ranga ≥ 11. Najveći rang koji je dobiven pomoću prirodnih brojeva je ≥ 9.

Možemo se pitati, koliko su u danim konstrukcijama zapravo rijetke krivulje ranga ≥ 8? Koristiti ćemo rezultate dobivene u [14]. Promotrimo $t \in \mathbb{N}$. U tablici su zapisani omjeri

t	Rang	Nezavisne točke beskonačnog reda
$\frac{833}{10}$	8	$\left(-\frac{833}{10}, 1\right), \left(\frac{833}{10}, 1\right), \left(-1, \frac{833}{10}\right), \left(\frac{1331}{5}, \frac{41251}{10}\right),$ $\left(-\frac{21}{5}, \frac{341}{2}\right), \left(\frac{225}{2}, 802\right), \left(\frac{436}{5}, \frac{1204}{5}\right), \left(\frac{-253}{10}, \frac{1996}{5}\right)$
$\frac{1609}{1330}$	9	$(0, 1), \left(-\frac{928}{665}, \frac{379}{665}\right), \left(\frac{127}{140}, \frac{3443}{5320}\right), \left(-\frac{3443}{9310}, \frac{39784}{32585}\right),$ $\left(\frac{361}{70}, \frac{80}{7}\right), \left(\frac{-67}{50}, \frac{12386}{16625}\right), \left(\frac{1591}{1900}, \frac{79979}{133000}\right),$ $\left(-\frac{6227}{4410}, \frac{441031}{879795}\right), \left(-\frac{12469}{25270}, \frac{303853}{240065}\right)$
$\frac{3581}{416}$	10	$\left(-\frac{189}{416}, \frac{1223}{208}\right), \left(-1, \frac{3581}{416}\right), \left(\frac{3581}{416}, 1\right), \left(\frac{-99}{32}, \frac{11785}{832}\right),$ $\left(\frac{-3335}{416}, \frac{7433}{832}\right), \left(-\frac{3399}{416}, \frac{6497}{832}\right), \left(-\frac{19275}{3328}, \frac{817823}{53248}\right),$ $\left(-\frac{3581}{416}, 1\right), \left(-\frac{27645}{5408}, \frac{2206307}{140608}\right), \left(\frac{18259}{416}, \frac{118619}{416}\right)$

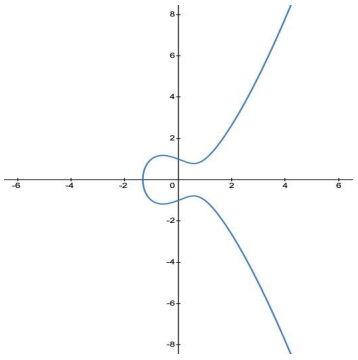
Tablica 3.2: Vrijednosti za konstruirane krivulje C_t, $t \in \mathbb{Q}$

dobivenih krivulja prema ukupnom broju krivulja za $0 < t < 21819$.

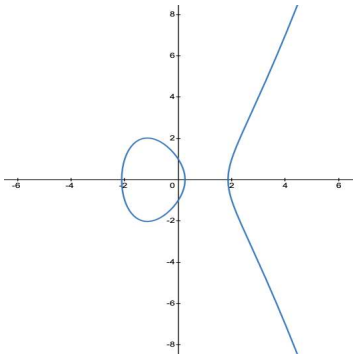
Rang	Omjer
8	25/21819 = 0.11%
9	3/21819 = 0.01%

Tablica 3.3: Broj krivulja zadanog ranga u konstrukciji sa $t \in \mathbb{N}$

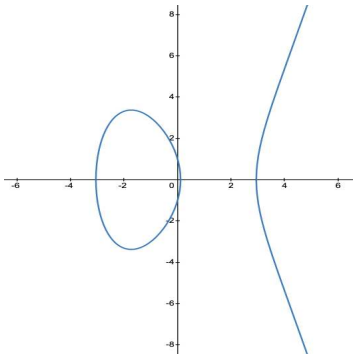
Za $1 \leq t \leq 5$ vizualiziramo C_t nad $\mathbb{R}$:



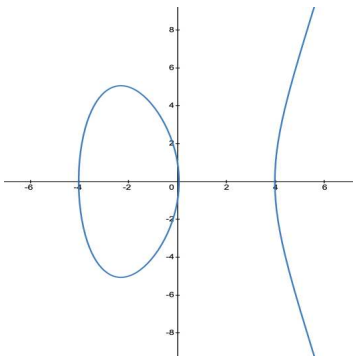
(a) $C_1 : y^2 = x^3 - x + 1$



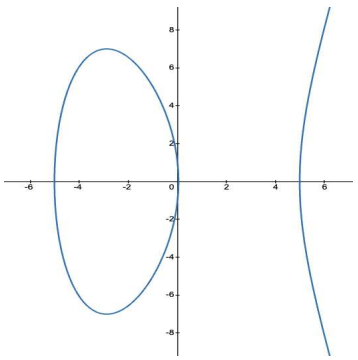
(b) $C_2 : y^2 = x^3 - 4x + 1$



(c) $C_3 : y^2 = x^3 - 9x + 1$



(d) $C_4 : y^2 = x^3 - 16x + 1$



(e) $C_5 : y^2 = x^3 - 25x + 1$

Slika 3.6: $C_t : y^2 = x^3 - t^2x + 1$

Poglavlje 4

Eliptičke krivulje nad konačnim poljima

4.1 Konačna polja

Polja iz definicije 1.0.12 koja imaju $q < \infty$ elemenata označavamo sa $\mathbb{F}_q$. Važno je napomenuti da arakteristika polja $\mathbb{F}_p$ ne može biti 0, u suprotnom broj elemenata nije konačan. Uzmimo da je p karakteristika od $\mathbb{F}_q$, tada $\mathbb{F}_q$ sadrži prosto polje $\mathbb{Z}/p\mathbb{Z}$. $\mathbb{F}_q$ je konačno dimenzionalan vektorski prostor nad $\mathbb{F}_p$. Uzmimo da je $\{e_1, ..., e_n\}$ baza od $\mathbb{F}_q$. Tada svaki element $a \in \mathbb{F}_q$ možemo prikazati kao linearnu kombinaciju elemenata baze, odnosno:

$$a = \lambda_1 e_1 + \cdots \lambda_n e_n,$$

gdje su $\lambda_i \in \mathbb{F}_p$. Svakom elementu $a \in \mathbb{F}_q$ stoga možemo bijektivno pridružiti uređenu n-torku $(\lambda_1, ..., \lambda_n) \in (\mathbb{F}_p)^n$. Zaključujemo da je $q = p^n$. S $\mathbb{F}_q^*$ označavamo multiplikativnu Abelovu grupu koju čine elementi polja $\mathbb{F}_q$ različiti od nule. Svaka grupa $\mathbb{F}_q^*$ je ciklička.

Konačna polja koja se pojavljuju u ovom radu su najčešće konačna polja $\mathbb{F}_p$. U opisivanju Birch Swinnerton-Dyer slutnje, određujemo red grupe $E(\mathbb{F}_p)$, u primjeni eliptičkih krivulja u kriptografiji, također koristimo grupu $E(\mathbb{F}_p)$. Iz tog razloga ćemo u ovom potpoglavlju detaljnije opisati konačna polja $\mathbb{F}_p$. Više detalja o $\mathbb{F}_q, q = p^k$ može se pronaći u [4].

Spomenuli smo da za konačno polje F_q, q mora biti prost broj ili neka potencija prostog broja. Glavna prepreka konstruiranja konačnih polja je uvjet postojanja inverznog elementa iz tog polja za svaki element.

Primjer 4.1.1. *Prikazati ćemo primjer konačnog polja $\mathbb{Z}_7$, i pokušati konstruirati konačno polje $\mathbb{Z}_6$. Elementi oba polja će biti cijeli brojevi. Uzmimo elemente skupa* $\{0, 1, 2, 3, 4, 5, 6\}$ *i pokušajmo konstruirati $\mathbb{Z}_7$. Rezultat operacija zbrajanja i množenja dva elementa u $\mathbb{Z}_7$ moraju biti elementi iz $\mathbb{Z}_7$. Uzmimo elemente* 2 *i* 6*, vrijedi* $2 + 6 = 8 \notin \mathbb{Z}_7$, $2 \cdot 6 = 12 \notin \mathbb{Z}_7$. *Koristeći modularnu aritmetiku gdje koristimo operaciju modulo 7, dobijemo:* $2 + 6 \equiv 1$

(mod 7), *i* $2 \cdot 6 \equiv 5 \pmod 7$.

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	0	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

Tablica 4.1: Zbrajanje u $\mathbb{Z}_7$

·	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Tablica 4.2: Množenje u $\mathbb{Z}_7$

Sa definiranim operacijama, za svaki element polja postoji inverz u tom polju. Promotrimo broj 2*, vrijedi* $2 + 5 \equiv 0 \pmod 7$ *i* $2 \cdot 4 \equiv 1 \pmod 7$. *Promotrimo sada tablicu množenja u slučaju* $\mathbb{Z}_6$.

·	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Tablica 4.3: Množenje u $\mathbb{F}_6$

Elementi $2, 3, 4$ *nemaju inverz u* $\mathbb{F}_6$*, odnosno za svaki* $x \in \{2, 3, 4\}$ *ne postoji element* $x^{-1} \in \mathbb{F}_6$ *takav da vrijedi* $2 \cdot x^{-1} \equiv 1 \pmod 7$.

4.2 Grupa $E(\mathbb{F}_q)$

Eliptičke krivulje nad konačnim poljima su se pokazale korisnima za primjene u kriptografiji. Definirati ćemo grupu $E(\mathbb{F}_q)$, i pokazati način na koji možemo odrediti strukturu i elemente te grupe. Najčešće se koriste konačna polja karakteristike $q = p^k$, gdje je p prost broj. S obzirom da su 2 i 3 prosti brojevi, dodatno ćemo opisati kako jednadžba eliptičke krivulje izgleda nad konačnim poljima karakteristike 2 ili 3. Dakle, za konačna polja $\mathbb{F}_{p^k}$, $p > 3$ možemo svesti krivulju na oblik

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

Za $\mathbb{F}_{3^k}$ jednadžbu možemo svesti do oblika $y^2 = x^3 + ax^2 + bx + c$, a za $\mathbb{F}_{2^k}$ imamo dva moguća oblika:

$$y^2 + cy = x^3 + ax + b,$$
$$y^2 + xy = x^3 + ax^2 + b.$$

Uočimo da nad poljima karakteristike 2, s lijeve strane ne možemo imati samo y^2. Uklanjanjem članova cy ili xy, krivulja će sigurno biti singularna. Naime, vrijedi $(y^2)' = 2yy'$, s obzirom na to da je polje karakteristike 2, zapravo dobijemo nulu pa ujedno i singularitet.

Primjer 4.2.1. *Neka je eliptička krivulja dana nad poljem $\mathbb{F}_7$ jednadžbom:*

$$E : y^2 = x^3 + 4x.$$

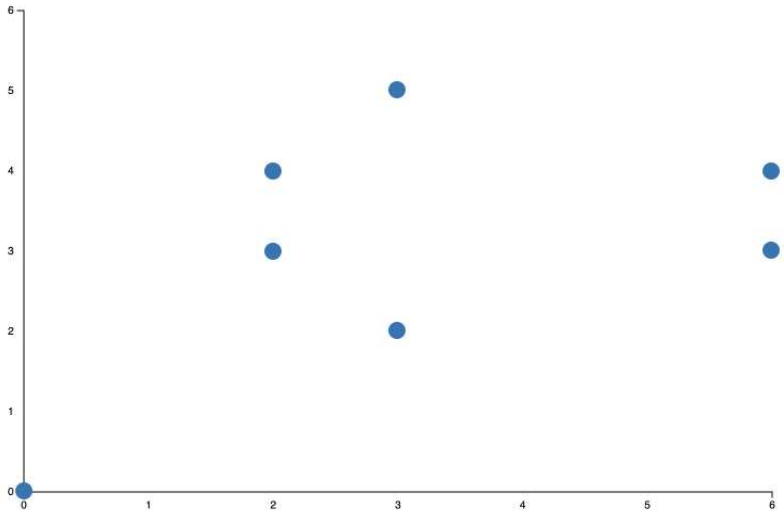
S obzirom na to da se radi u konačnom polju, moguće je odrediti sve elemente dane krivulje. Uzimamo u obzir brojeve koji su kvadrati u zadanom polju, s obzirom na to da je s lijeve strane y^2. U polju $\mathbb{F}_7$ su to brojevi 0,1,2 i 4. Uvrštavamo $x \in \{0, 1, 2, 3, 4, 5, 6\}$ u jednadžbu krivulje E i provjeravamo koji od njih daje kvadrat. Redom dobijemo $y^2 = 0, 1, 16, 39, 80, 145, 240$. U $\mathbb{F}_7$ su to brojevi $0, 1, 2, 4, 3, 5, 2$ pa znamo da $x = 0, 3, 6$ zadovoljavaju jednadžbu eliptičke krivulje u $\mathbb{F}_7$.
S pripadnim rješenjima za x dobijemo sve elemente grupe $E(\mathbb{F}_7)$:

$$E(\mathbb{F}_7) = \{O, (0, 0), (2, 3), (3, 2), (3, 5), (4, 6), (6, 3), (6, 4)\}.$$

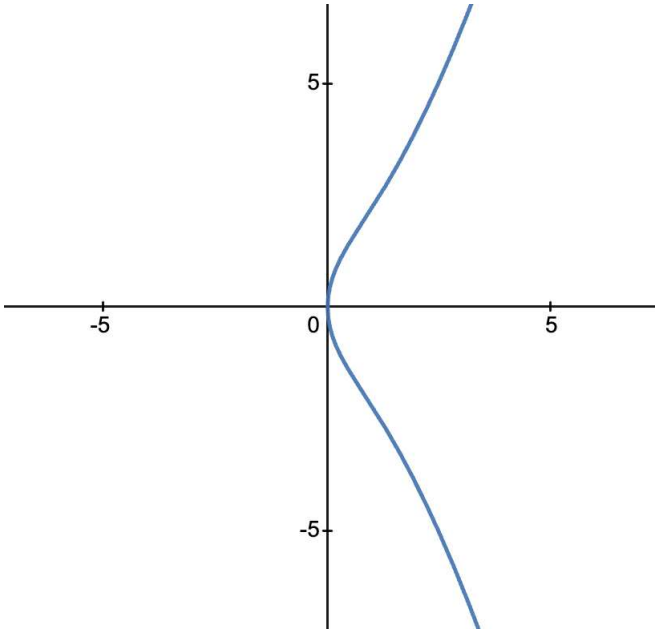
S točkom $P = (6, 3)$ možemo generirati sve ostale elemente, imamo:

$$[2]P = (2, 3)\ [3]P = (3, 5),\ [4]P = (0, 0),\ [5]P = (3, 2),\ [6]P = (2, 3),\ [7]P = (6, 4),\ [8]P = O.$$

Iz tog zaključujemo da je $E(\mathbb{F}_7)$ ciklička grupa reda 8 s generatorom $(6, 3)$.



Slika 4.1: $y^2 \equiv x^3 + 4x \pmod 7$



Slika 4.2: $y^2 = x^3 + 4x$

Poglavlje 5

Primjene eliptičkih krivulja u kriptografiji

Već 1985. godine se raspravljalo o potencijalu koristi eliptičkih krivulja u kriptografske svrhe. Američki matematičari Neal Koblitz i Victor S. Miller nagrađeni su Levchin nagradom[1] 2021. godine za uvođenje eliptičkih krivulja u kriptografiju. Moderni kriptosustavi nisu prilagođeni za jačinu kvantnih računala. Kriptografi rade na kriptosustavima koji će biti otporni na napade čak i s kvantnih računala. Jedan od kriptosustava predložen kao mogući sustav u post-kvantnoj kriptografiji koristi supersingularne eliptičke krivulje. Potencijal eliptičkih krivulja proteže se čak i u post-kvantnu kriptografiju, iz tog razloga je vrijedno razmotriti trenutne primjene, i kako točno rang eliptičke krivulje predstavlja jedan od glavnih razloga za njihovu korisnost. U prethodnim poglavljima proučili smo rang eliptičkih krivulja i težinu pronalaska eliptičkih krivulja visokog ranga. U ovom poglavlju ćemo to i iskoristiti, spomenuli smo krivulju ranga ≥ 28, no 28 nije ni blizu dovoljan rang za razbijanje kriptosustava koje ćemo kasnije definirati.

5.1 Uvod u kriptografiju javnog ključa

Glavni cilj kriptografije je očuvanje povjerljivosti informacija. Poruke, e-mailovi, podatci poput lozinki, adresa te brojeva kreditnih kartica moraju biti zaštićeni kad se šalju preko interneta. Svi podatci moraju biti enkriptirani, odnosno izmijenjeni tako da je iz njih nemoguće iščitati originalne informacije u slučaju nesigurnih komunikacijskih kanala. Metode s kojima se podatci mogu kriptirati i dekriptirati između dvije osobe (pošiljalac i primalac, u literaturi često Alice i Bob) tako da ih ne može razumijeti treća osoba (često Eve ili Oscar) proučava znanstvena disciplina kriptografija. Poruku koju pošiljalac želi poslati

[1] Levchin nagrada dodjeljuje se za iznimne doprinose u kriptografiji i primjenama kriptografije.

primaocu zovemo otvoreni tekst. Pošiljalac transformira otvoreni tekst u šifrat koristeći unaprijed dogovoreni ključ K postupkom šifriranja. Nebitno je što treća osoba može saznati šifrat, bez ključa ne može saznati otvoreni tekst. Za razliku od njega, primalac zna ključ kojim je šifrirana poruka, pa može dešifrirati šifrat i odrediti otvoreni tekst. Definirajmo neke pojmove s pomoću kojih ćemo opisivati algoritme u kriptografiji.

Definicija 5.1.1. *Kriptosustav je uređena petorka $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$, gdje je $\mathcal{P}$ konačan skup svih otvorenih tekstova, $\mathcal{C}$ konačan skup svih šifrata, $\mathcal{K}$ konačan skup svih mogućih ključeva. Za svaki ključ $K \in \mathcal{K}$ postoji funkcija šifriranja $e_K \in \mathcal{E}$, $e_K : \mathcal{P} \to \mathcal{C}$, i odgovarajući $d_K \in \mathcal{D}$, $d_K : \mathcal{C} \to \mathcal{P} \in \mathcal{D}$. Ako uzmemo neki otvoreni tekst $x \in \mathcal{P}$ te na njega primijenimo funkciju šifriranja e_K dobijemo šifrat $e_K(x)$. Pripadnom funkcijom dešifriranja d_K možemo iz šifrata dobiti originalni otvoreni tekst, odnosno $d_K(e_K(x)) = x$.*

Kriptosustav koji je opisan u uvodu ima jedan očiti problem, razmjenu ključeva, koja također mora biti sigurna. Godine 1976. Diffie i Hellman, koji se smatraju začetnicima kriptografije javnog ključa, ponudili su rješenje problema razmjene ključeva, koristeći činjenicu da je u nekim grupama potenciranje puno jednostavnije od logaritmiranja.

Fokus kriptosustava u kriptografiji javnog ključa je konstruiranje sustava u kojem je moguće da svi znaju funkciju šifriranja e_K, ali da je nemoguće u nekom razumnom vremenu dobiti funkciju dešifriranja. Tako, čak ako netko sazna šifrat i funkciju s kojom je šifrat dobiven, i dalje ne može dobiti otvoreni tekst. Pitanje je kako onda primalac dešifrira poruku. Umjesto jednog univerzalnog ključa, Alice i Bob imaju po dva ključa, jedan javni (e_K) i jedan tajni (d_K). Alice ima poruku x koju želi poslati Bobu, prvo ju šifrira s pomoću Bobovog javnog ključa e_B, tako dobije šifrat $y = e_B(x)$ koji šalje Bobu. U ovom trenu treća osoba može saznati funkciju šifriranja e_K te šifrat y ali ne zna tajni ključ e_B s kojim Bob dešifrira šifrat. Dešifriranje se odvija na sljedeći način: $d_B(y) = d_B(e_B(x)) = x$. Funkcija d_B je očito inverz funkcije e_B no kriptosustav mora biti konstruiran tako da postupak računanja tog inverza bude nemoguć ako se ne zna neki dodatan podatak o e_B, kojeg Bob zna. Za šifriranje poruka se ne koriste kriptosustavi s javnim ključem s obzirom na to da su sporiji, ali zato se koriste za razmjenu ključeva. Opisat ćemo jedan kriptosustav koji koristi činjenicu da je u grupi $(\mathbb{F}_p^*, *_p)$ teško riješiti problem računanja diskretnog logaritma.

5.2 Problem diskretnog logaritma

Neka je G konačna Abelova grupa. S obzirom na to da promatramo grupu u kontekstu kriptografije, G trebamo konstruirati tako da su ostvarena neka svojstva. Operacije množenja i potenciranja moraju biti jednostavne, odnosno brze. Još jedno bitno svojstvo je mogućnost generiranja slučajnih elemenata iz G na uniforman način. Uz operacije koje trebaju biti lake, logaritmiranje kao inverz potenciranja, bi trebalo biti vrlo teško. Grupa s ovim svojstvima je odličan kandidat za primjene u kriptografiji.

Definicija 5.2.1. *Neka je $(G, \cdot)$ konačna grupa, $g \in G, H = \{g^i : i \geq 0\} \leq G$, $\langle g \rangle = H$, te $h \in H$. Diskretni logaritam je najmanji nenegativni cijeli broj x takav da je $h = g^x$, gdje je $g^x = g \cdot g \cdot ... \cdot g$. Diskretni logaritam označavamo sa* $\log_g h$.

Diffie i Hellman su problem diskretnog logaritma iskoristili u svom rješenju za protokol s kojim je moguća sigurna razmjena ključeva.

Diffie-Hellman protokol za razmjenu ključeva
1. Alice generira slučajan prirodan broj $a \in \{1, 2, ..., |G| - 1\}$ i šalje Bobu g^a
2. Bob generira slučajan prirodan broj $b \in \{1, 2, ..., |G| - 1\}$ i šalje Bobu g^b
3. Alice računa $(g^b)^a = g^{ab}$
4. Bob računa $(g^a)^b = g^{ab}$

Njihov tajni ključ je $K = g^{ab}$.

U originalnoj definiciji Diffie-Hellmanovog protokola se za grupu G uzima multiplikativna grupa $\mathbb{Z}_p^*$ svih ne-nul ostataka modulo p, gdje je p dovoljno velik prost broj. Poznato je da je grupa $\mathbb{Z}_p^*$ ciklička. Opisat ćemo kriptosustav kojeg je 1985. godine osmislio egipatski kriptograf Taher ElGamal.

ElGamalov kriptosustav
Neka je p prost i $\alpha \in \mathbb{Z}_p^*$ primitivni korijen modulo p. Neka je $\mathcal{P} = \mathbb{Z}_p^*, C = \mathbb{Z}_p^* \times \mathbb{F}_p^*$ i

$$\mathcal{K} = \{(p, \alpha, a, \beta) : \beta \equiv \alpha^a (\text{mod } p)\}$$

Vrijednosti p, α, β su javne, a vrijednost a je tajna.
Za $K \in \mathcal{K}$ i tajni broj $k \in \{0, 1, ..., p - 1\}$ definiramo:

$$e_K(x, k) = (\alpha^k \bmod p, x\beta^k \bmod p)$$

Za $y_1, y_2 \in \mathbb{Z}_p^*$ definiramo:

$$d_K(y_1, y_2) = y_2 (y_1^a)^{-1} \bmod p$$

5.3 Eliptičke krivulje u kriptografiji

Kriptosustavi zasnivaju svoju sigurnost na teškoći pojedinih radnji, kao što je faktorizacija velikih prirodnih brojeva (RSA, Rabinov kriptosustav, ...). Eliptičke krivulje nude više razloga zašto su prikladne za kriptografiju. U našem je slučaju najbitniji razlog težina pronalaženja eliptičke krivulje visokog ranga. Konkretnu primjenu eliptičkih krivulja vidjeti ćemo kroz rješavanje problem diskretnog logaritma u grupi $E(\mathbb{F}_p)$. U toj grupi je problem diskretnog logaritma znatno teži od problema diskretnog logaritma u grupi $\mathbb{F}_p^*$.

Index calculus metoda

Index calculus metoda (diskretni logaritam se naziva i indeks) je najefikasniji algoritam kojeg trenutno imamo za rješavanje problema diskretnog logaritma u grupi $\mathbb{F}_p^*$. Spominjali smo važnost odabiranja grupe koje imaju svojstva dobra za primjene u kriptografiji. Iako se metoda može definirati za proizvoljnu grupu G, efikasnost bitno ovisi o svojstvima te grupe. Jedno od svojstava grupe je to da možemo odabrati relativno mali podskup $\mathcal{B}$ grupe G koja ima svojstvo da se velik broj elemenata iz G može efikasno prikazati kao produkt elemenata iz $\mathcal{B}$. Takav podskup $\mathcal{B}$ naziva se i faktorska baza. Upravo je teškoća nalaženja eliptičkih krivulja velikog ranga najvažniji ograničavajući faktor za primjenu ove metode na grupe eliptičkih krivulja nad konačnim poljem.

Index calculus algoritam

1. *Izbor faktorske baze*
   Izaberemo podskup $\mathcal{B} = \{p_1, ..., p_m\}$ od G sa svojstvom da se relativno velik broj elemenata iz G može prikazati kao produkt elemenata iz $\mathcal{B}$

2. *Linearne relacije u logaritmima*
   Za slučajan broj k, $0 \leq k \leq n-1$ izračunamo g^k, te ga pokušamo prikazati kao produkt elemenata iz $\mathcal{B}$:

   $$g^k = \prod_{i=1}^{m} p_i^{c_i}, c_i \geq 0$$

   Ako smo uspješni, logaritmiramo dobivenu relaciju, te tako prikažemo $k \ mod \ n$ kao linearnu kombinaciju logaritama:

   $$k \equiv \sum_{i=1}^{m} c_i \log_g p_i \pmod{n}$$

   Ponavljamo ovaj postupak sve dok ne dobijemo barem m takvih relacija. Dovoljno je $m+10$ relacija jer tada, s velikom vjerojatnošću, pripadni sustav od $m+10$ jednadžbi s m nepoznanica ima jedinstveno rješenje.

3. *Rješavanje sustava*
   Riješimo konstruirani linearni sustav te tako dobijemo vrijednosti $\log_g p_i$.

4. *Računanje* $x = \log_g h$
   Za slučajan broj k, $0 \leq k \leq n-1$ izračunamo $h * g^k$, te ga pokušamo prikazati kao produkt elemenata iz $\mathcal{B}$:

$$h * g^k = \prod_{i=1}^{m} p_i^{d_i}, d_i \geq 0$$

U slučaju da nismo uspjeli, izaberemo novi k, a ako smo uspješni, logaritmiramo dobivenu relaciju te dobijemo:

$$x = \log_g h = \left(\sum_{i=1}^{m} d_i \log_g p_i - k \right) \pmod{n}$$

Opisat ćemo način primjene *index calculus* metoda na grupu $\mathbb{F}_p^*$. Grupa $\mathbb{F}_p^*$ je ciklička reda $n = p - 1$, za $\mathcal{B}$ uzimamo prvih m prostih brojeva. Brojeve oblika $r = g^k \ mod \ p$ pokušamo prikazati preko elemenata iz $\mathcal{B}$ kao produkt potencija prvih m prostih brojeva. Veličina skupa $\mathcal{B}$ je bitna, jer što veći m izaberemo, veća je vjerojatnost da ćemo neki $r \in G$ moći prikazati. Ako pogledamo 3. korak algoritma vidimo da moramo riješiti sustav, što je veći m taj sustav će biti teže riješiti. S obzirom na ove dvije posljedice odabira m, optimalan izbor za $\mathcal{B}$ je taj da je najveći element p_m približno jednak:

$$L(p) = e^{\sqrt{\ln p \ln \ln p}}$$

S tim odabirom *index calculus* postaje subeksponencijalni algoritam za računanje diskretnog logaritma u grupi $\mathbb{F}_p^*$. Subeksponencijalni algoritmi su oni kojima za ulaz veličine x vrijeme izvršavanja iznosi $T(x)$, te vrijedi da $\forall b > 1, T(x) < b^x$ za dovoljno velike x. Polinomni algoritmi su također subeksponencijalni, međutim u kriptografiji se taj pojam najčešće odnosi na algoritme čije je izvršavanje sporije od polinomijalnog, ali brže od eksponencijalnog. [10]

Problem diskretnog logaritma na eliptičkim krivuljama (ECDLP)

Kao motivaciju za uvođenje eliptičkih krivulja u kriptografiju, naveli smo činjenicu da je problem diskretnog logaritma teži u grupi $E(\mathbb{F}_p)$ nego u grupi $\mathbb{F}_p^*$. ECDLP (Elliptic curve discrete logarithm problem) samo je poseban slučaj problema definiranog u 5.2.1. Neka je E eliptička krivulja definirana nad konačnim poljem $\mathbb{F}_p$, i neka je $P \in E(\mathbb{F}_p)$ točka reda n. Neka je $Q \in \langle P \rangle$, odnosno točka koju možemo generirati točkom P. Problem diskretnog logaritma sada postaje pronaći $0 \leq k \leq n - 1$ takav da vrijedi $Q = [k]P$.

Duljina ključa je bitan pojam u kriptografiji. Cilj je postići što veću razinu sigurnosti, a da pritom koristimo kraći ključ. Eliptičke krivulje, zbog težine problema diskretnog logaritma, omogućavaju istu razinu sigurnosti neki drugi kriptosustavi, pritom koristeći kraći ključ. Za usporedbu ćemo promotriti poznati RSA kriptosustav, o kojem se više detalja može naći u [8]. Duljinu ključa mjerimo u bitovima, te koristimo jedinicu MIPS (engl.

million-instructions-per-second) godina. Jedna MIPS godina definirana je kao količina računanja koje se može provesti u jednoj godini, na nekom računalu koje može odraditi milijun naredbi u sekundi. Sa ECC označavamo engleski naziv "elliptic curve cryptography" koji se odnosi na kriptografiju gdje se koriste eliptičke krivulje.

Godina	RSA duljina ključa	ECC duljina ključa	MIPS godina
1990.	622	117	$3.51 \cdot 10^7$
2000.	952	132	$7.13 \cdot 10^9$
2010.	1369	146	$1.45 \cdot 10^{12}$
2020.	1881	161	$2.94 \cdot 10^{14}$
2030.	2493	176	$5.98 \cdot 10^{16}$
2040.	3214	191	$1.22 \cdot 10^{19}$

Tablica 5.1: Usporedba duljine ključa RSA i ECC kriptosustava

Duljine ključeva su znatno manje u ECC, iz tablice vidimo da je u 2020. godini duljina ključa otprilike 11 puta manja. Bitna činjenica je da će se ta efikasnost nastaviti i kroz nadolazeća desetljeća, sa predviđanjem da će 2040. za ECC biti potreban skoro 17 puta manji ključ. Mali uređaji, koji nemaju veliku moć računanja, poput SIM kartica, iskorištavaju manje veličine ključeva za bolju sigurnost informacija.

U definiciji ElGamalovog kriptosustava smo koristili grupu $\mathbb{Z}_p^*$, no svi kriptosustavi koji koriste $\mathbb{Z}_p^*$ u svojoj definiciji, mogu se modificirati tako da koriste grupu $E(\mathbb{Z}_p)$. Jedna varijanta ElGamalovog kriptosustava koja koristi grupu $E(\mathbb{Z}_p)$ je *Menezes-Vastoneov kriptosustav*.

Već smo naveli da je pronalaženje eliptičkih krivulja visokog ranga jedan od glavnih faktora zašto su korisne u kriptografiji. Kad bi bilo moguće relativno brzo pronaći takve krivulje, onda bi mogli primijeniti analogon index calculus metode i sličnom brzinom riješiti problem diskretnog logaritma u grupi $E(\mathbb{Z}_p)$. Za faktorsku bazu $\mathcal{B}$, umjesto prostih brojeva, možemo uzeti generatore neke eliptičke krivulje nad $\mathbb{Q}$ velikog ranga. Postavlja se pitanje, koliko velikog ranga ta krivulja mora biti? Procjena je da bi se za $p \approx 2^{160}$ trebala upotrijebiti krivulja ranga > 180. Ova ideja je naravno danas nemoguća, s obzirom na to da je najveća krivulja koju trenutno poznajemo ranga 28.

Zamislimo da postoji neki dokaz da eliptička krivulja može biti proizvoljnog ranga, ali pitanje je, što je s njenim generatorima? Već smo spomenuli jednadžbu eliptičke krivulje ranga ≥ 28, no uzmimo neku krivulju manjeg ranga i netrivijalne torzijske grupe. Klagsburn je 2020. godine konstruirao krivulju ranga 4 s torzijskom grupom $\mathbb{Z}/5\mathbb{Z}$. Jednadžba te krivulje je:

$y^2 + xy + y = x^3 - 12713764765147881239791121283129 80x$
$+2481317177640146784233372994443880360830251424879 52.$

Već sami koeficijenti krivulje su veliki brojevi. Torzijska grupa dana je sa:

$$\{O, (81072141178321384, -260369108483587571136261 32),$$
$$(81072141178321384, 260369107672866159353047 48),$$
$$(-36657363539197856, 156677453652870280470438 28),$$
$$(-36657363539197856, -156677453286296645078459 72)\}$$

Već za rang 4 su koordinate točaka konačnog reda veliki brojevi s kojima je računanje zahtjevan proces. Nemamo slutnju da se te točke smanjuju s većim rangom, i ovo još samo doprinosi činjenici da su eliptičke krivulje koristan alat u kriptografiji.

Sad kad znamo da je modifikacija ElGamalovog algoritma mnogo lakša nego modifikacija index calculus metode, opišimo Menezes-Vastoneov kriptosustav.

Menezes-Vanstoneov kriptosustav

Neka je E eliptička krivulja nad $\mathbb{Z}_p$, gdje je $p > 3$ prost broj, i H ciklička podgrupa od E generirana s $\alpha \in E(\mathbb{F}_p)$. Definiramo:

$$\mathcal{P} = \mathbb{Z}_p^* \times \mathbb{Z}_p^*$$

$$C = E \times \mathbb{Z}_p^* \times \mathbb{Z}_p^*$$
$$\mathcal{K} = \{(E, \alpha, a, \beta) : \beta = [a]\alpha\},$$

gdje je $[a]\alpha$ oznaka za $\alpha + \cdots + \alpha$ (a puta) i $+$ je zbrajanje točaka na eliptičkoj krivulji. Vrijednosti E, α, β su javne, a vrijednost a je tajna. Za $K \in \mathcal{K}$ i tajni slučajni broj $k \in \{0, 1, ..., |H| - 1\}$, i za $x = (x_1, x_2) \in \mathbb{Z}_p^* \times \mathbb{Z}_p^*$ definiramo funkciju šifriranja:

$$e_K(x, k) = (y_0, y_1, y_2),$$

gdje je $y_0 = [k]\alpha$, $(c_1, c_2) = [k]\beta$, $y_1 = c_1 x_1 \bmod p$, $y_2 = c_2 x_2 \bmod p$. Neka je $y = (y_0, y_1, y_2)$ šifrat, definiramo funkciju dešifriranja:

$$d_K(y) = (y_1 (c_1)^{-1} \bmod p, y_2 (c_2)^{-1} \bmod p,$$

gdje je $[a]y_0 = (c_1, c_2)$.

U Menezes-Vanstoneovom kriptosustavu su otvoreni tekst i šifrat proizvoljni uređeni parovi elemenata iz polja. Šifrat je 2 puta dulji od originalnog otvorenog teksta. Menezes-Vanstoneov kriptosustav rješava par problema koji se javljaju u modifikaciji kriptosustava. Rekli smo da je šifrat 2 puta dulji od otvorenog teksta, no obično se nakon modifikacije očekuje da će šifrat biti 4 puta dulji. Otvoreni tekst i šifrat ne moraju nužno odgovarati točkama na eliptičkoj krivulji. Ne postoji deterministički algoritam za prebacivanje elemenata otvorenog teksta u točke na eliptičkoj krivulju pa je ovim dopuštenjem izbora proizvoljnih elemenata modifikacija olakšana.

Dodatak A

Programski kodovi za programski paket PARI

```
E_1 = ellinit([-1,0]);
E_2 = ellinit([-34^2, 0]);
E_3 = ellinit([-1254^2, 0]);

product = 1;

bsd(upper_limit) = {
    prodeuler(p = 2, upper_limit, if(divrem(E_1.disc,p) != 0, (ellcard(E_3,p)/p)));
}

for(X = 1, 7000, {
    product = bsd(X);
    print("(", X,"," product*1.0, ")");
})
```

Dodatak A.1: Programski kod za računanje funkcije $\pi_E(X)$

```
MestreNagaoSum(N, E) = {
    MNSum = 0;

    forprime(p=2, N,
        ap = ellap(E, p);
        MNSum += (2 - ap) / (p + 1 - ap) * log(p);
    );

    MNSum;
}

curveSum(n,m) = {
     E = ellinit([-(n^2/m^2), 1]);
     sum523 = 0;
     sum523 = MestreNagaoSum(523, E);
     sum1979 = 0;


     if(sum523 > 23,
        sum1979 = MestreNagaoSum(1979, E)
     );

     if(sum1979 >= 34, print(sum1979, ";   a3 = ", n, "/", m));
     if(sum1979 >= 34, print(ellrank(E)))
}
```

Dodatak A.2: Programski kod za računanje Mestre-Nagao sume

Bibliografija

[1] M.W. Barsagade i S. Meshram, *Overview of History of Elliptic Curves and its use in cryptography*, International Journal of Scientific and Engineering Research **5** (2014).

[2] C. Bocovich, *Elliptic Curves of High Rank*, Mathematics, Statistics, and Computer Science Honors Projects, Macalaster College, (2012).

[3] E. Brown i B.T. Myers, *Elliptic Curves from Mordell to Diophantus and back*, The American Mathematical Monthly **109(7)** (2002), 639–649.

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

[5] ———, *Algoritmi u teoriji brojeva, skripta*, Sveučilište u Zagrebu, 2021.

[6] ———, *High rank elliptic curves with prescribed torsion*, `https://web.math.pmf.unizg.hr/~duje/tors/tors.html`.

[7] ———, *History of elliptic curves rank records*, `https://web.math.pmf.unizg.hr/~duje/tors/rankhist.html`.

[8] A. Dujella i M. Maretić, *Kriptografija*, Element, Zagreb, 2007.

[9] A. Dujella i J.C. Peral, *High rank elliptic curves with torsion group* $\mathbb{Z}/8\mathbb{Z}$ *or* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, Trends in Number Theory, Contemp. Math. **649** (2015), 47–62.

[10] B. Kaliski, *Subexponential Time, Encyclopedia of Cryptography and Security*, Springer US, Boston, 2011.

[11] D. Palman, *Projektivna geometrija*, Školska knjiga, 1984.

[12] J. Park, B. Poonen, J. Voight i M.M. Wood, *A heuristic for boundedness of ranks of elliptic curves*, J. Eur. Math. Soc. (JEMS) **21** (2019), 286–295.

[13] A. Piro, *The fundamental theorem for finite Abelian groups: A brief history and proof*, `https://www.gcsu.edu/sites/files/page-assets/node-808/attachments/piro.pdf`.

[14] P. Tadić, *On the family of elliptic curves* $Y^2 = X^3 - T^2x + 1$, Glasnik Matematički **47** (2012), br. 2, 81–93.

[15] The PARI Group, Univ. Bordeaux, *PARI/GP version 2.15.1*, 2024, `http://pari.math.u-bordeaux.fr/`.

[16] B. Širola, *Algebarske strukture, skripta*, Sveučilište u Zagrebu, 2008.

Sažetak

Kroz ovaj rad su uvedeni osnovni pojmovi o eliptičkim krivuljama nad poljem racionalnih brojeva $\mathbb{Q}$ i nad konačnim poljima $\mathbb{F}_p$. Definiran je rang eliptičke krivulje, pojam koji ima veliku važnost u istraživanju eliptičkih krivulja te u njihovoj primjeni u kriptografiji. Opisane su neke od metoda za pronalazak ranga eliptičke krivulje te je pomoću Mestre-Nagaovih suma konstruirana eliptička krivulja ranga ≥ 8. Kroz proučavanje eliptičkih krivulja koristimo pojmove algebarskih struktura, koje navodimo u prvom poglavlju. Primjene eliptičkih krivulja u kriptografiji su danas jako istraživana tema, opisujemo problem diskretnog logaritma i težinu rješavanja tog problema u kontekstu eliptičkih krivulja. Opisujemo neke od kriptosustava koji koriste eliptičke krivulje te povezujemo težinu pronalaska eliptičkih krivulja visokog ranga s njihovom primjenom.

Summary

In this thesis, we introduce some of the fundamental concepts of elliptic curves over the field of rational numbers $\mathbb{Q}$ and finite fields $\mathbb{F}_p$. We define the rank of an elliptic curve, a notion of significant importance in the study of elliptic curves and their application in cryptography. Various methods for determining the rank of an elliptic curve are described, and an elliptic curve of rank ≥ 8 is constructed using the Mestre-Nagao sums. Through the study of elliptic curves, we utilize concepts of algebraic structures, which are outlined in the first chapter. The applications of elliptic curves in cryptography are a highly researched topic. We discuss the discrete logarithm problem and the difficulty of solving this problem in the context of elliptic curves. We describe some of the cryptosystems utilizing elliptic curves, and the connection between the challenge of finding elliptic curves with high rank and their practical application.

Životopis

Rođen sam 29.07.1999. u Zadru. Završio sam Osnovnu skolu “Stanovi” te zatim Gimnaziju “Vladimir Nazor”. Maturirao sam 2018. godine te zatim upisao Preddiplomski sveučilišni studij ”Matematika i računarstvo” na Sveučilistu Josip Juraj Strossmayer u Osijeku. Završio sam preddiplomski studij 2021. godine s temom završnog rada “Automatizirano trgovanje financijskom imovinom temeljem moving average convergence divergence (MACD) metode” pod mentorstvom izv. prof. dr. sc. Nenada Šuvaka. Nakon završetka preddiplomskog studija, iste godine upisujem Sveučilišni diplomski studij “Računarstvo i matematika” na PMF-u Zagreb.