MAT–KOL (Banja Luka)
ISSN 0354-6969 (p), ISSN 1986-5228 (o)
Vol. XVII (2) (2011), 17-24

ELIPTIČKE KRIVULJE

Bernadin Ibrahimpašić[1], Alma Šehanović[2]

Abstract

U ovom članku opisaćemo eliptičke krivulje i uvesti operaciju uz koju skup tačaka na njoj postaje Abelova grupa.

Ključne riječi i fraze: Eliptička krivulja, Abelova grupa.

In this paper we describe elliptic curves. One of the most important facts about elliptic curves is that the set of points on an elliptic curves forms an abelian group.

AMS Mathematics Subject Classification (2010): 11G05, 20K01

Key words and phrases: Elliptic curve, Abelian group.

1 Uvod

Jedna od grupa koja svakako privlači pažnju je grupa tačaka na eliptičkoj krivulji nad poljem. Eliptička krivulja se može definisati nad proizvoljnim poljem $\mathbb{K}$, ali su najvažniji slučajevi kada je $\mathbb{K}$ polje racionalnih, realnih ili kompleksnih brojeva, ili konačno polje $\mathbb{F}_q$ s q elemenata.

Može se postaviti pitanje odakle dolazi naziv eliptička krivulja. Veza između eliptičkih krivulja i elipse dolazi preko problema računanja obima elipse. Ako je elipsa zadana jednačinom $b^2x^2 + a^2y^2 = a^2b^2$, onda je njen obim jednak

$$O = 4a \cdot \int_0^1 \frac{1 - \left(a^2 - b^2\right) t^2}{\sqrt{\left(1 - t^2\right)\left(1 - \left(a^2 - b^2\right) t^2\right)}}\, dt.$$

Pomoću racionalne supstitucije, ovaj se integral može svesti na sličan integral u kojem se pod korijenom nalazi kubna funkcija. Integrali u kojima se javljaju drugi korijeni polinoma trećeg ili četvrtog stepena se nazivaju eliptički integrali. Oni se ne mogu izraziti pomoću elementarnih funkcija. Međutim, moguće ih je izraziti pomoću Weierstrassove $\wp$–funkcije koja zadovoljava diferencijalnu jednačinu oblika

$$\left(\frac{\wp'}{2}\right)^2 = \wp^3 + a\wp + b.$$

[1]Pedagoški fakultet Univerziteta u Bihaću, Bosna i Hercegovina, e-mail: bernadin@bih.net.ba

[2]Gimnazija "Meša Selimović", Tuzla, Bosna i Hercegovina, e-mail: alma.sehanovic@gmail.com

2 Grupa tačaka na eliptičkoj krivulji

Definicija 2.1 *Neka je polje* $\mathbb{K}$ *karakteristike različite od* 2 *i* 3. Eliptička krivulja $E(p; a, b) : y^2 = x^3 + ax + b$ *nad poljem* $\mathbb{K}$, *je skup rješenja* $(x, y) \in \mathbb{K} \times \mathbb{K}$ *jednačine*

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

gdje su $a, b \in \mathbb{K}$ *konstante takve da je* $4a^3 + 27b^2 \neq 0$, *zajedno sa specijalnom tačkom* $\mathcal{O}$ *koja se zove* tačka u beskonačnosti.

Uslov $4a^3 + 27b^2 \neq 0$ je potreban i dovoljan da jednačina $x^3 + ax + b = 0$ nema višestrukih korijena. Ako je $4a^3 + 27b^2 = 0$, tada se odgovarajuća krivulja zove *singularna kubna krivulja*.

Ukoliko je polje $\mathbb{K}$ karakteristike 2, tada je eliptička krivulja nad $\mathbb{K}$ skup rješenja jedne od jednačina oblika

$$y^2 + cy = x^3 + ax + b \qquad \text{ili} \qquad y^2 + xy = x^3 + ax^2 + b,$$

zajedno sa tačkom u beskonačnosti $\mathcal{O}$.

Ako je polje $\mathbb{K}$ karakteristike 3, tada je eliptička krivulja nad $\mathbb{K}$ skup rješenja jednačine

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

zajedno sa tačkom u beskonačnosti $\mathcal{O}$.

Opšti oblik jednačine, koji je dobar nad svim poljima, je

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{1}$$

Ovu jednačinu zovemo *Weierstrasova forma* od E.

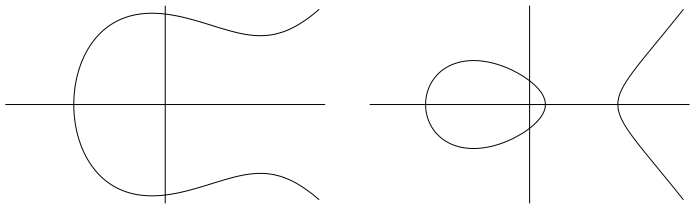
Recimo nešto o tački u beskonačnosti $\mathcal{O}$. Ona se prirodno pojavljuje ako eliptičku krivulju prikažemo u projektivnoj ravnini. Projektivnu ravninu $\mathbb{P}^2(\mathbb{K})$ dobijemo tako da na skupu $\mathbb{K}^3 \backslash \{(0,0,0)\}$ uvedemo relaciju ekvivalencije $(X, Y, Z) \sim (kX, kY, kZ)$, $k \in \mathbb{K}$, $k \neq 0$. Ako u (afinoj) jednačini eliptičke krivulje uvedemo supstituciju $x = \frac{X}{Z}$, $y = \frac{Y}{Z}$, dobijamo projektivnu jednačinu

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

Ako je $Z \neq 0$, onda klasa ekvivalencije od (X, Y, Z) ima predstavnika $(x, y, 1)$, pa tu klasu možemo poistovjetiti s (x, y). Međutim, postoji i jedna klasa ekvivalencije koja sadrži tačke za koje je $Z = 0$. Njen predstavnik je $(0, 1, 0)$ i tu klasu poistovjećujemo s tačkom u beskonačnosti $\mathcal{O}$.

Neka je E eliptička krivulja. Jedno od najvažnijih svojstava eliptičkih krivulja je da se na njima može definirati binarna operacija, tako da tačke na eliptičkoj krivulji s danom operacijom čine Abelovu grupu. Ovu operaciju obično nazivamo sabiranjem. Tačka u beskonačnosti $\mathcal{O}$ će biti neutralni element, tako da je $P + \mathcal{O} = \mathcal{O} + P = P$, $\forall P \in E$.

Da bismo to bolje objasnili, uzmimo da je $\mathbb{K} = \mathbb{R}$ polje realnih brojeva. Tada eliptičku krivulju nad poljem $\mathbb{R}$, bez tačke u beskonačnosti, možemo prikazati



Slika 1: Jednokomponentni i dvokomponentni graf

kao podskup ravnine. Polinom $f(x) = x^3 + ax^2 + bx + c$ može imati ili 1 ili 3 realna korijena. Tako imamo da graf pripadne eliptičke krivulje ima jednu ili dvije komponente, kao što je prikazano na slici.

Uvedimo operaciju sabiranja tačaka na eliptičkoj krivulji geometrijski. Neka su $P, Q \in E$, gdje je $P = (x_1, y_1)$ i $Q = (x_2, y_2)$. Razmatrat ćemo tri slučaja:

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

Razmotrimo prvi slučaj, tj. kada sabiramo tačke s različitim prvim koordinatama. Neka je l prava kroz tačke P i Q. Tada l siječe E u tačkama P i Q. Lako je vidjeti da će l presjeći E u još jednoj tački, koju ćemo označiti s R'. Neka je R osnosimetrična tačka tačke R' u odnosu na x–osu. Tada tačku R definišemo kao zbir tačaka, tj. $P + Q = R$.

Ovaj geometrijski zakon se može opisati i eksplicitnim formulama za koordinate zbira tačaka P i Q. Te formule mogu poslužiti za definiciju sabiranja tačaka na eliptičkoj krivulji nad proizvoljnim poljem, uz malu modifikaciju ako je polje karakteristike 2 ili 3.

Jednačina prave l je $y = \lambda x + \nu$, gdje je

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \qquad \text{i} \qquad \nu = y_1 - \lambda x_1 = y_2 - \lambda x_2.$$

Kako bismo našli tačke iz $E \cap l$, zamjenom $y = \lambda x + \nu$ u jednačini za E, dobijamo da je

$$(\lambda x + \nu)^2 = x^3 + ax + b,$$

odnosno

$$x^3 - \lambda^2 x^2 + (a - 2\lambda\nu)\, x + b - \nu^2 = 0. \tag{2}$$

Korijeni jednačine (2) su x koordinate tačaka iz $E \cap l$. Dvije takve tačke P i Q su nam već poznate. Stoga, x_1 i x_2 su dva korijena jednačine (2). Kako je jednačina (2) kubna i ima dva realna korijena, to i njen treći korijen također mora biti realan broj. Kako suma ova tri korijena mora biti jednaka λ^2, to je

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

Dobili smo da je x_3 upravo x koordinata tačke R'. Označimo y koordinatu tačke R' s $-y_3$. Tada, y_3 predstavlja y koordinatu tačke R. Kako je koeficijent λ u l određen s bilo koje dvije tačke kroz koje l prolazi, to možemo uzeti tačke (x_1, y_1) i (x_3, y_3), pa dobijamo da je

$$\lambda = \frac{-y_3 - y_1}{x_3 - x_1}, \qquad \text{i} \qquad y_3 = \lambda\,(x_1 - x_3) - y_1.$$

Prema tome, u prvom slučaju, kada je $x_1 \neq x_2$, tj. kada su tačke P i Q različite, formule za koordinate (x_3, y_3) zbira $P + Q$ su:

$$\begin{aligned} x_3 &= \lambda^2 - x_1 - x_2, \\ y_3 &= \lambda\,(x_1 - x_3) - y_1, \\ \lambda &= \frac{y_2 - y_1}{x_2 - x_1}. \end{aligned}$$

U drugom slučaju, kada je $x_1 = x_2$ i $y_1 = -y_2$, imamo

$$(x, y) + (x, -y) = \mathcal{O}, \quad \forall\,(x, y) \in E.$$

Iz toga zaključujemo da su (x, y) i $(x, -y)$ međusobno inverzni elementi u odnosu za operaciju sabiranja, tj. tački $P(x, y)$ je tačka $-P = (x, -y)$ inverzna tačka za operaciju sabiranja. Također imamo da vrijedi da je $P + (-P) = -P + P = \mathcal{O}$, $\forall P \in E$, pa je $\mathcal{O}$ neutralni element za operaciju sabiranja.

U trećem slučaju, kada su tačke P i Q jednake, ne govorimo o sabiranju dvije tačke nego o dupliranju tačke P, tj, računanju tačke $2P$. Kod eliptičkih krivulja, uobičajeno je da se koristi notacija $[2]P$. Sada umjesto sekante povučemo tangentu na E u tački P. Nagib od l može biti izračunat derivacijom implicitno zadane funkcije, pa je

$$2y\,\frac{dy}{dx} = 3x^2 + a.$$

Zamjenom $x = x_1$ i $y = y_1$ dobijamo da je koeficijent

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

Sabiranje tačaka na eliptičkoj krivulji je i asocijativno. To je svojstvo koje je i najkomplikovanije za dokazati. Jedna od mogućnosti za dokazivanje je da se iskoriste dobijene eksplicitne formule uz razlikovanje svih slučajeva koji mogu nastupiti, u ovisnosti da li se prilikom sabiranja u izrazu $(P + Q) + R = P + (Q + R)$ pojavljuju različite, suprotne ili jednake tačke. Osim toga, moguće je dokaz provesti pomoću Bezoutovog teorema koji govori o broju tačaka presjeka dvije krivulje (vidjeti [5]). Međutim, jedan od elegantnijih dokaza je preko svojstava spomenute Weierstrassove $\wp$ funkcije pomoću koje se sabiranje tačaka na eliptičkoj krivulji nad poljem kompleksnih brojeva $\mathbb{C}$ dovodi u vezu sa sabiranjem kompleksnih brojeva, za koje znamo da je asocijativno.

Kompleksne tačke na eliptičkoj krivulji $y^2 = x^3+ax+b$ se mogu parametrizirati pomoću $(\wp(t), \frac{1}{2}\wp'(t))$. Može se pokazati da ako je $P = (\wp(t), \frac{1}{2}\wp'(t))$ i $Q = (\wp(u), \frac{1}{2}\wp'(u))$, onda je $P + Q = (\wp(t + u), \frac{1}{2}\wp'(t + u))$. Vidimo da sabiranje tačaka na eliptičkoj krivulji nad poljem $\mathbb{C}$ odgovara sabiranju kompleksnih brojeva, a znamo da je sabiranje kompleksnih brojeva asocijativno.

Iz svega, gore navedenog, možemo zaključiti sljedeće:

1. sabiranje je zatvoreno na skupu E,
2. sabiranje je asocijativno,
3. sabiranje je komutativno,
4. tačka u beskonačnosti $\mathcal{O}$ je neutralni element za sabiranje,
5. svaka tačka P na E ima inverzni element u odnosu na sabiranje, i to je $-P$,

pa slijedi da je $(E, +)$ Abelova grupa.

Napomenimo da se eliptičke krivulje nad $\mathbb{Z}_p = \{0, 1, \ldots, p - 1\}$, gdje je p prost broj, definiraju analogno kao i nad poljem realnih brojeva, ali se operacije izvode modulo p. Također treba napomenuti da se pod dijeljenjem a/b u $\mathbb{Z}_p$ podrazumijeva množenje ab^{-1} elementa a i multiplikativnog inverza b^{-1} elementa b po modulu p. Multiplikativni inverz od b po modulu p predstavlja rješenje kongruencije $bx \equiv 1 \pmod{p}$.

3 Računske operacije na eliptičkoj krivulji

Primjer 3.1 *Odredimo eliptičku krivulju* $E\,(5; 2, 4)$*, tj. eliptičku krivulju oblika*

$$y^2 = x^3 + 2x + 4$$

nad $\mathbb{Z}_5$*.*

Rješenje: Kako je $E\,(5; 2, 4)$ to je $p = 5, a = 2, b = 4$, pa imamo

$$y^2 \equiv x^3 + 2x + 4 \pmod{5}.$$

Da bismo odredili tačke na E, možemo računati $x^3 + 2x + 4 \bmod 5$ za sve $x \in \mathbb{Z}_5$ i pokušati riješiti kongruenciju $y^2 \equiv x^3 + 2x + 4 \pmod{5}$.

x	0	1	2	3	4
$x^3 + 2x + 4 \bmod 5$	4	2	1	2	1

y	0	1	2	3	4
$y^2 \bmod 5$	0	1	4	4	1

Vidimo da je

$$E(5;2,4) = \{\mathcal{O}, (0,2), (0,3), (2,1), (2,4), (4,1), (4,4)\}.$$

Dobili smo da $E(5;2,4)$ ima 7 tačaka, tj. da je 7 red grupe $(E,+)$. Kako je svaka grupa reda prost broj ciklička, to je E izomorfna sa $\mathbb{Z}_7$ i svaka tačka na E, osim tačke u beskonačnosti, je generator od E. ♢

Primjer 3.2 *Pokažimo da je* $P = (0,2)$ *generator od* $E(5;2,4)$.

Rješenje: Kako je operacija zadana aditivno, ovdje ne govorimo o stepenu P^k, nego o $[k]P$ kao višekratniku tačke P. Da bismo odredili $[2]P = P+P$, trebamo prvo odrediti pripadni λ. Kako je $P = P$, to imamo

$$\begin{aligned}
\lambda &= \left(3x_1^2 + a\right)(2y_1)^{-1} \bmod p \\
&= \left(3 \cdot 0^2 + 2\right)(2 \cdot 2)^{-1} \bmod 5 \\
&= 2 \cdot 4^{-1} \bmod 5 \\
&= 2 \cdot 4 \bmod 5 \\
&= 3.
\end{aligned}$$

Sada računamo $[2]P = (x_3, y_3)$ gdje je

$$\begin{aligned}
x_3 &= \lambda^2 - x_1 - x_1 \bmod p \\
&= 3^2 - 0 - 0 \bmod 5 \\
&= 9 \bmod 5 \\
&= 4,
\end{aligned}$$

$$\begin{aligned}
y_3 &= \lambda(x_1 - x_3) - y_1 \bmod p \\
&= 3 \cdot (0-4) - 2 \bmod 5 \\
&= -12 - 2 \bmod 5 \\
&= -14 \bmod 5 \\
&= 1. \\
&\Rightarrow [2]P = (4,1)
\end{aligned}$$

Sada računamo $[3]P = P + [2]P$. Kako je $P \neq [2]P$, to pripadni λ računamo na sljedeći način:

$$\begin{aligned}
\lambda &= (y_2 - y_1)(x_2 - x_1)^{-1} \bmod p = (1-2)(4-0)^{-1} \bmod 5 \\
&= -1 \cdot 4^{-1} \bmod 5 = -1 \cdot 4 \bmod 5 = -4 \bmod 5 = 1.
\end{aligned}$$

Sada je $[3]P = (x_3, y_3)$, gdje je

$$\begin{aligned}
x_3 &= \lambda^2 - x_1 - x_2 \bmod p = 1^2 - 0 - 4 \bmod 5 = -3 \bmod 5 = 2, \\
y_3 &= \lambda(x_1 - x_3) - y_1 \bmod 5 = 1 \cdot (0-2) - 2 \bmod 5 = -4 \bmod 5 = 1.
\end{aligned}$$

$$\Rightarrow [3]P = (2,1)$$

Nastavimo li dalje s računanjem, dobijamo

$$[4]P = (2,4)\,, \qquad [5]P = (4,4)\,, \qquad [6]P = (0,3) \qquad [7]P = \mathcal{O}\,,$$

pa vidimo da je $P = (0,2)$ generator grupe $E\,(5;2,4)$.

Napomenimo da na isti način možemo provjeriti za svaku od tačaka iz $E(5;2,4)$ da je njen generator. $\diamondsuit$

U programskom paketu PARI/GP [4] implementiran je veliki broj važnijih funkcija vezanih uz eliptičke krivulje (i ne samo uz njih). Popis svih funkcija se može dobiti s ?*, a popis funkcija vezanih uz eliptičke krivulje se može dobiti s ?5. Ovdje ćemo navesti nekoliko funkcija koje se mogu iskoristiti za provjeru navedenih rezultata.

Pretpostavljamo da je eliptička krivulja dana u Weierstrassovoj formi (1) i u PARI–ju je reprezentiramo kao petkomponentni vektor $e = [a_1, a_2, a_3, a_4, a_6]$ i inicijaliziramo je naredbom

`E=ellinit([a1, a2, a3, a4, a6])`.

Tačke na E se reprezentiraju kao dvokomponentni vektori $[x, y]$, osim tačke u beskonačnosti, koju reprezentiramo kao jednokomponentni vektor [0].

Navedimo sada nekoliko naredbi.

- `elladd(E,P,Q)`: računa zbir tačaka P i Q na E;
- `ellsub(E,P,Q)`: računa razliku tačaka P i Q na E;
- `ellpow(E,P,k)`: računa višekratnik $[k]P$ tačke P na E;
- `ellordinate(E,x)`: daje vektor koji sadrži y koordinate tačaka na E čija je x koordinata zadana;
- `ellisoncurve(E,P)`: daje 1 ("istina") ako je tačka P na E, a 0 ("laž") inače;

4 Binarna metoda

Eliptičke krivulje su našle široku primjenu. Naročito treba istaknuti primjenu eliptičkih krivulja u testiranju prostosti i faktorizaciji, te kriptografiji javnog ključa. Glavni razlog uvođenja eliptičkih krivulja u kriptografiju javnog ključa je taj da se ista sigurnost kriptosistema zadržava i ukoliko koristimo ključ 7 puta manji, za danas standardne vrijednosti. Tako se kod kriptosistema čija se sigurnost zasniva na faktorizaciji, npr. RSA, koji su sigurni uz ključ dužine 1024 bita, upotrebom eliptičkih krivulja ista sigurnost postiže ključem dužine 160 bitova.

U grupi G, koja je interesantna za primjene u kriptografiji, operacije množenja i stepenovanja bi trebale biti jednostavno izvedive, dok bi logaritmiranje trebalo bilo znatno teže. Računanje višekratnika tačke P na eliptičkoj krivulji je

specijalan slučaj stepenovanja u Abelovoj grupi. Zato se za računanje $[k]P$, višekratnika tačke P na elipičkoj krivulji, može iskoristiti jednostavna metoda koja koristi binarni zapis broja k. Metoda je najjednostavnija od svih poznatih i ujedno i najstarija, a zove se *binarna metoda*.

To je algoritam čiji je ulaz tačka P i r bitni prirodan broj $k = \sum_{j=0}^{r} k_j 2^j$, gdje je $k_j \in \{0, 1\}$, a koji kao rezultat vraća tačku $Q = [k]P$.

$Q = P$
za $j = r - 1$ do 0 korakom -1 radi
    $Q = 2Q$
    ako je $k_j = 1$ tada $Q = Q + P$
vrati Q

Primjer 4.1 *Izračunati* $[10000]P$ *binarnom metodom.*

Rješenje: Binarni zapis broja 10000 je

$$10000 = (1\ 0\ 0\ 1\ 1\ 1\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 0)_2$$

pa je

$$[10000]P = 2(2(2(2(2(2(2(2(2(2(2P)) + P) + P) + P)))) + P)))).$$

♢

Literatura

[1] A. Dujella: *Applications of elliptic curves in public key cryptography*, Lecture notes,
`http://web.math.hr/~duje/pdf/bilbaocourse.pdf`

[2] D. Hankerson, A. Menezes, S. Vanstone: *Guide to Elliptic Curve Cryptography*, Springer–Verlag, New York, 2004.

[3] B. Ibrahimpašić: *Matematičke osnove kriptografije javnog ključa*, Magistarski rad, PMF, Sarajevo, 2004.

[4] PARI/GP, version `2.3.2`, Bordeaux, 2007,
`http://pari.math.u-bordeaux.fr`

[5] J. H. Silverman, J. Tate: *Rational Points on Elliptic Curves*, Springer–Verlag, New York, 1994.

Pristiglo u Redakciju 05.07.2011.