Eliptičke krivulje u kriptografiji

Kokanović, Anamarija

Master's thesis / Diplomski rad

2021

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **Josip Juraj Strossmayer University of Osijek, Department of Mathematics / Sveučilište Josipa Jurja Strossmayera u Osijeku, Odjel za matematiku**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:126:563752

Sveučilište J. J. Strossmayera u Osijeku
Odjel za matematiku

Anamarija Kokanović

ELIPTIČKE KRIVULJE U KRIPTOGRAFIJI

Diplomski rad

Osijek, 2021.

Sveučilište J. J. Strossmayera u Osijeku
Odjel za matematiku

Anamarija Kokanović

ELIPTIČKE KRIVULJE U KRIPTOGRAFIJI

Diplomski rad

Mentor: izv. prof. dr. sc. Ivan Matić

Osijek, 2021.

Roditeljima.
Hvala!

Sadržaj

1 Uvod

U ovom radu bavit ćemo se eliptičkim krivuljama u kriptografiji. Takav pristup kriptografiji s javnim ključem zasnovan je na algebarskoj strukturi eliptičkih krivulja nad konačnim poljima. Ovakva kriptografija jedna je od najsnažnijih, ali najmanje razumljivih vrsta kriptografije koja se danas široko koristi. Eliptičke krivulje primjenjive su u protokolima s dogovorenim ključem, za digitalne potpise, pseudo-slučajne generatore i drugo. Jedna od najpoznatijih metoda za generiranje digitalnih potpisa je upravo Elliptic Curve Digital Signature Algorithm (ECDSA). Takav algoritam je zasnovan na problemu diskretnog logaritma u multiplikativnoj grupi konačnog polja koristeći eliptičke krivulje.

U osnovi, važno je razumjeti tehnologiju koja stoji iza bilo kojeg sigurnosnog sustava kako bismo mu mogli vjerovati. U tu svrhu napisan je ovaj rad.

Godine 1985. prvi put su predloženi kriptografski algoritmi temeljeni na eliptičnim krivuljama. Njihova široka primjena počinje 2004. godine.

Problem diskretnog logaritma eliptičke krivulje težak je problem koji stoji u osnovi kriptografije koja koristi eliptičke krivulje. Unatoč gotovo tri desetljeća istraživanja, matematičari još uvijek nisu pronašli algoritam za rješavanje ovog problema koji poboljšava naivni pristup. Drugim riječima, za brojeve iste veličine rješavanje problema diskretnog logaritma za eliptičke krivulje je znatno teže od faktorizacije. Budući da računalno intenzivniji problem znači jači kriptografski sustav iz toga proizlazi da je, kriptosustav koji koristi eliptičke krivulje, teže razbiti od primjerice RSA kriptosustava i Diffie-Hellman protokola. Kako bi predočio koliko je teže slomiti ovakav kriptosustav, Lenstra[1] je predstavio sljedeći koncept. Možemo izračunati koliko je energije potrebno za razbijanje kriptografskog algoritma i usporediti to s istom količinom energije potrebne da bi prokljućala voda. Ovom mjerom za razbijanje 228-bitnog RSA ključa potrebno je manje energije nego što je potrebno za prokljućavanje žličice vode. Usporedno, razbijanje 228-bitnog ključa s eliptičkim krivuljama zahtijeva energiju potrebnu za prokljućavanje sve vode na zemlji. To znači da se ista sigurnost može postići s manjim ključem. Tako je npr. umjesto ključa duljine duljine 1024 bita, dovoljan ključ duljine 160 bitova. Ovo je izuzetno važno kod onih primjena kod kojih je prostor za pohranu ključeva vrlo ograničen (npr. čip-kartice).

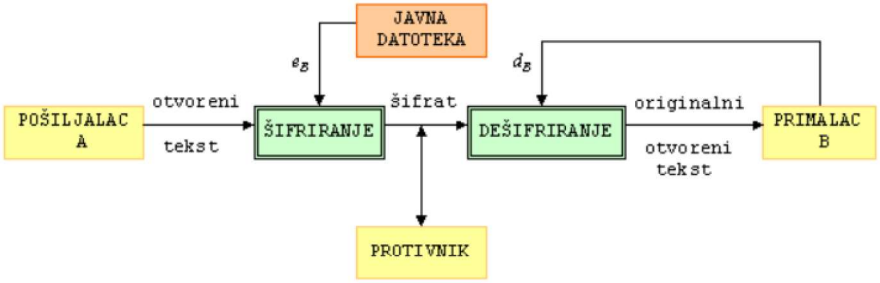
Nakon sporog starta, algoritmi temeljeni na eliptičkim krivuljama postaju sve popularniji. Kriptografija koja koristi eliptičke krivulje sada se koristi u širokom spektru aplikacija. Primjerice, američka vlada ju koristi za zaštitu internih komunikacija, a projekt Tor ju koristi za osiguravanje anonimnosti. Isto tako, to je mehanizam koji se koristi za dokazivanje vlasništva nad Bitcoinima, osigurava potpise u Appleovoj usluzi iMessage, koristi se za šifriranje DNS podataka pomoću DNSCurve, a preferirana je metoda za provjeru autentičnosti za sigurno pregledavanje weba preko SSL/TLS. CloudFlare koristi ovakvu kriptografiju kako bi pružio savršenu tajnost za privatnost na mreži. Kriptografski algoritmi prve generacije poput RSA i Diffie-Hellman i dalje su norma, ali kriptografija koja koristi eliptičke krivulje sve brže postaje rješenje za privatnost i sigurnost na mreži.

[1] Hendrik Willem Lenstra Jr., nizozemski matematičar.

2 Osnovni pojmovi u kriptografiji

Kriptografija (grč.\kryptos+grafo), u doslovnom prijevodu tajnopis, je znanstvena disciplina koja se bavi proučavanjem metoda za slanje poruka u obliku takvom da ih može pročitati samo onaj kome su namijenjene. Zadatak je omogućiti dvama subjektima Alice i Bobu **(pošiljalac i primalac)** tajnu i nesmetanu komunikaciju u nesigurnom komunikacijskom kanalu tako da treći subjekt Eve **(protivnik)** ne razumije poruke.

Otvoren tekst (eng. plaintext) je tajna pouka koju Alice želi poslati Bobu, a koju je Alice unaprijed transformirala pomoću obojma poznatog ključa. Takav postupak se naziva **šifriranje**. Poruka koja putuje komunikacijskim kanalom do Boba zove se **šifrat** (eng.ciphertext). Eva ne zna ključ i ne može dešifrirati poruku, ali Bob ga zna i u mogućnosti je dešifrirati poruku i tako dobiti otvoreni tekst.



Slika 1: Shema simetričnog kriptosustava

Definicija 2.1. *Kriptosustav je uredena petorka* $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ *za koju vrijedi*

- $\mathcal{P}$ *je konačan skup svih mogućih osnovnih elemanata otvorenog teksta,*
- $\mathcal{C}$ *je konačan skup svih mogućih osnovnih elemenata šifrata,*
- $\mathcal{K}$ *je prostor ključeva, tj. konačan skup svih mogućih ključeva.*
- *Za svaki* $K \in \mathcal{K}$ *postoji funkcija šifriranja* $e_K \in \mathcal{E}$ *i odgovarajuća funkcija dešifriranja* $d_K \in \mathcal{D}$. *Pritom su* $e_K : \mathcal{P} \to \mathcal{C}$ *i* $d_K : \mathcal{C} \to \mathcal{P}$ *funkcije sa svojstvom da*

$$d_K(e_K(x)) = x,$$

za svaki otvoren tekst $x \in \mathcal{P}$.

Ključ e_K zovemo javni ključ, a d_K zovemo tajni ili vlastiti ključ.

Klasifkacija kriptosustava prema vrsti ključa:

- Kriptosustavi s tajnim ključem ili simetrični kriptosustavi - pošiljalac i primalac izabiru tajni ključ i pomoću njega generiraju funkcije šifriranja i dešifriranja. Kako je poznat ključ za šifriranje lako je pronaći ključ za dešifriranje i obrnuto.
- Kriptosustavi s javnim ključem ili asimetrični kriptosustavi - poznat je ključ za šifriranje, ali ne i ključ za dešifriranje. Njega nije moguće lako otkriti u kratkom vremenu.

3 Eliptičke krivulje

Neka je K polje. Pojam eliptičke krivulje se može definirati nad proizvoljnim poljem K, međutim najvažniji slučajevi su kad je K polje racionalnih brojeva $\mathbb{Q}$, polje realnih brojeva $\mathbb{R}$, polje kompleksnih brojeva $\mathbb{C}$, te konačno polje $\mathbb{F}_q$ od q elemenata.

Opći oblik jednadžbe eliptičke krivulje, nad bilo kojim poljem, je

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

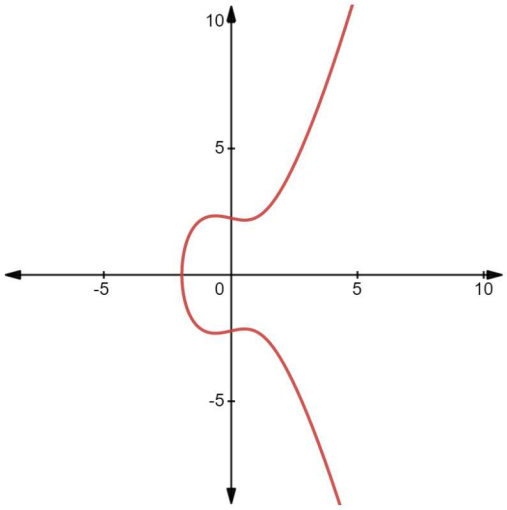
Ovakva se jednadžba naziva Weierstrassova forma od E. Uvjet je da u svakoj točki krivulje postoji tangenta, tj. da je u svakoj točki barem jedna od parcijalnih derivacija različita od 0. Ukoliko se ovu jednadžbu transformira supstitucijom varijabli nadopunom na potpuni kvadrat i potpun kub dobije se jednadžba oblika

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

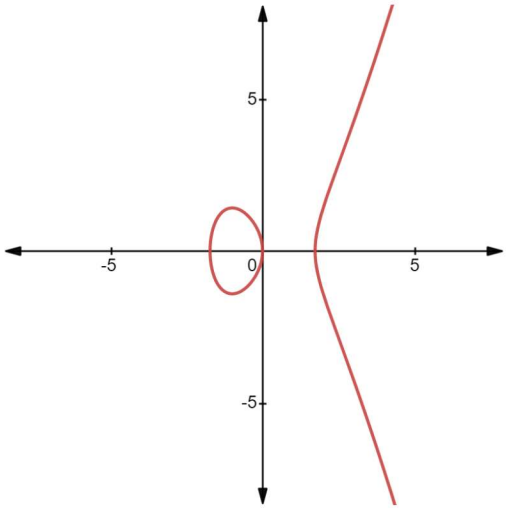
Takva jednadžba se naziva skraćena Weierstrassova forma. Uvjet je da polinom $f(x) = x^3 + ax + b$ nema višestrukih korijena. U ovom diplomskom radu bavit ćemo se eliptičkim krivuljama u skraćenoj Weierstrassovoj formi.

Jedno od najvažnijih svojstava eliptičkih krivulja jest da se na njima može uvesti operacija uz koju točke na eliptičkoj krivulji čine Abelovu grupu.

Promatrajmo polje realnih brojeva. Tada eliptičku krivulju možemo prikazati kao podskup ravnine. Polinom trećeg stupnja može imati jedan ili tri realna korijena. U ovisnosti o tome, graf eliptičke krivulje ima jednu ili dvije komponente, kao što je prikazano na Slici 2 i Slici 3.



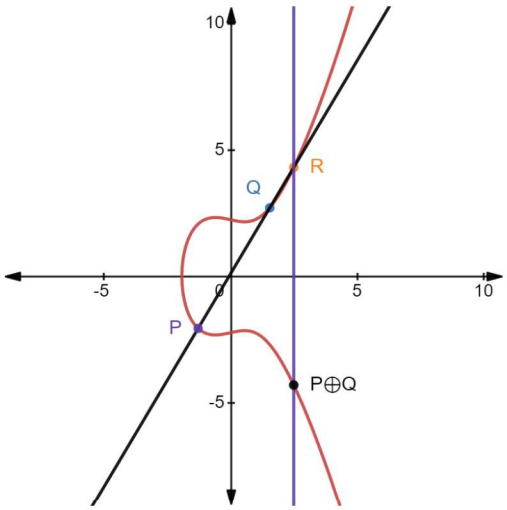
Slika 2: $E_1 : y^2 = x^3 - x + 5$ *



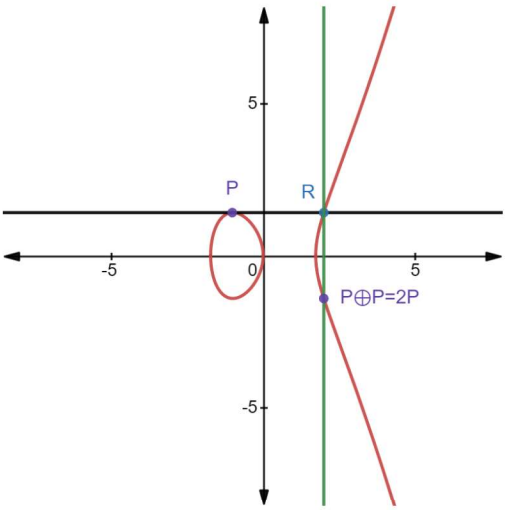
Slika 3: $E_2 : y^2 = x^3 - 3x$ *

Bitna značajka eliptičkih krivulja je da na prirodan način kojim se, krenuvši s dvije točke na eliptičnoj krivulji i njihovim "zbrajanjem", dobije treća točka. Navodnike stavljamo jer se pozivamo na operaciju sličnu operaciji zbrajanja (postojanje neutralnog elementa, komutativnost i asocijativnost), međutim u svemu ostalom različite od zbrajanja. Najprirodniji način za uočavanje navedenog je korištenje geometrije.

Uočimo navedeno primjenjujući postupak na eliptičke krivulje na Slici 2 i Slici 3. Dakle, neka su P i Q dvije točke na eliptičnoj krivulji E, kao što je prikazano na Slici 2 i Slici 3. Povucimo pravac kroz točke P i Q. On siječe krivulju E u trima točkama. Treću točku u kojoj pravac siječe krivulju označimo s R. Osnosimetričnu točku točki R s obzirom na os x označimo s $P \oplus Q$. Ako je $P = Q$, onda umjesto sekante povlačimo tangentu kroz točku P i na analogan način dobivamo točku R, a zatim $P \oplus P$. Dobiveni rezultati prikazani su na Slici 4 i Slici 5.



Slika 4: Sekanta *



Slika 5: Tangenta *

Primjer 3.1. *Neka je E eliptička krivulja*

$$y^2 = x^3 - 4x + 4. \tag{1}$$

Točke $P = (0, -2)$ i $Q = (-2, 2)$ se nalaze na krivulji E. Pravac l prolazi točkama P i Q i dan je izrazom

$$l : y = -2x - 2. \tag{2}$$

Kako bismo pronašli točke u kojima se krivulja E i pravac l sijeku uvrstimo (2) u jednadžbu (1).

$$(-2x - 2)^2 = x^3 - 4x + 4$$
$$4x^2 + 8x + 4 = x^3 - 4x + 4$$
$$0 = x^3 - 4x^2 - 12x.$$

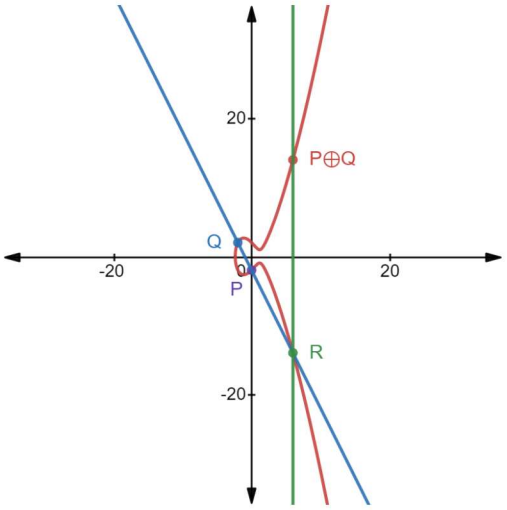
Želimo pronaći rješenja ove jednadžbe. Budući da su točke P i Q sjecište eliptičke krivulje E i pravca l znamo dva korijena $x = 0$ i $x = -2$.

$$x^3 - 4x^2 - 12x = x(x + 2)(x - 6)$$

Treći korijen polinoma je $x = 6$. Uvrštavajući $x = 6$ u (2) dobijemo $y = -14$. Dakle, $R = (6, -14)$, a osnosimetrična točka točke R je

$$P \oplus Q = (6, 14).$$

Geometrijski prikaz dan je na Slici 6.



Slika 6: $E : y^2 = x^3 - 4x + 4$ *

Izračunajmo $P \oplus P$. Koeficijent smjera tangente u točki P dobijemo koristeći pravilo za deriviranje kompozicije funkcija

$$2y\frac{dy}{dx} = 3x^2 - 4.$$

$$\frac{dy}{dx} = \frac{3x^2 - 4}{2y}.$$

i uvrštavanjem koordinata točke $P = (0, -2)$. Tada dobijemo nagib $\lambda = 1$ pa je tangenta na krivulju E u točki P dana s

$$l : y = x - 2. \tag{3}$$

Nakon što (3) uvrstimo u (1) dobijemo

$$(x-2)^2 = x^3 - 4x + 4$$

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

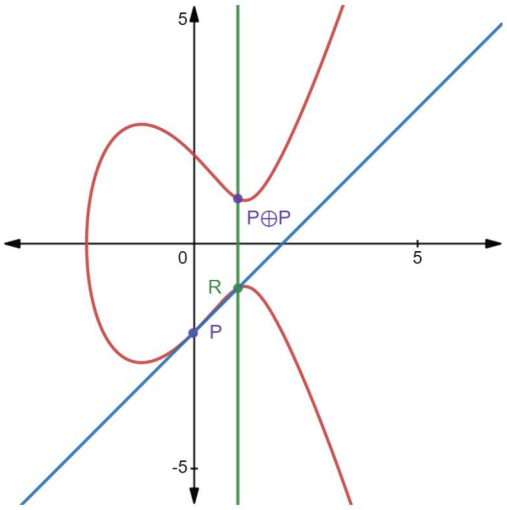
$$x^3 - x^2 = 0$$

$$x^2(x-1) = 0.$$

Uvrštavanjem $x = 1$ u (3) dobijemo $y = -1$. Dakle, osnosimetrična točka je

$$P \oplus P = (1, 1).$$

Geometrijski prikaz dan je na Slici 7.



Slika 7: $E : y^2 = x^3 - 4x + 4$ *

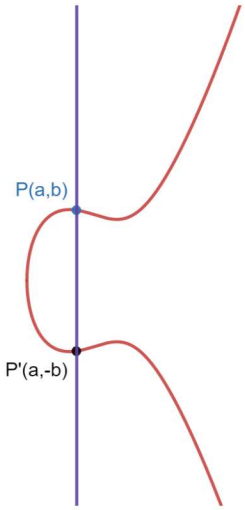
Promotrimo Sliku 8. Potencijalni problem pojavljuje se ako promatramo točku $P = (a, b)$ i njoj osnosimetričnu točku $P' = (a, -b)$, a pravac l je okomica $x = a$ takva da siječe krivulju E u te dvije točke. Ne postoji treća točka, ali rješenje je "stvoriti" dodatnu točku $\mathcal{O}$ koja živi u beskonačnosti. Preciznije, točka $\mathcal{O}$ ne postoji u xy - ravnini, ali se pretvaramo da leži na svakom okomitom pravcu. Tada stavimo

$$P \oplus P' = \mathcal{O}.$$

Pitamo se kako "zbrojiti" točku $\mathcal{O}$ i točku $P = (a, b)$ na krivulji E. Pravac l koji povezuje P i $\mathcal{O}$ je okomica kroz točku P na kojoj leži $\mathcal{O}$, a koja siječe krivulju E u točkama $P, \mathcal{O}, P' = (a, -b)$. Da bismo "zbrojili" P i $\mathcal{O}$ potrebna nam je osnosimetrična točka točke P'. To je ponovno točka P. Dakle,

$$P \oplus \mathcal{O} = P,$$

pa je $\mathcal{O}$ neutralni element za operaciju $\oplus$.



Slika 8: Okomit pravac bez treće točke na eliptičkoj krivulji E *

Primjer 3.2. *Promatrajući eliptičku krivulju E iz Primjera 3.1. primjetimo da se točka $T(-2.383, 0)$ nalazi na krivulji te da ta je tangenta na krivulju E u točki T pravac $x = -2.383$. Dakle, $T \oplus T = \mathcal{O}$.*

Primjedba 3.1. *Karakteristika polja K je najmanji prirodni broj n takav da je $1 + 1 + \cdots + 1 = n \cdot 1 = 0$, gdje su 0 i 1 neutralni elementi za zbrajanje, odnosno množenje u K, ukoliko takav n postoji. Ako je $n \cdot 1 \neq 0$ za svaki prirodan broj n, onda se kaže da je K polje karakteristike 0.*

Definicija 3.1. *Neka je K polje karakteristike različite od 2 i 3. Eliptička krivulja E je skup svih točaka $(x, y) \in K \times K$ koje zadovoljavaju jednadžbu*

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

zajedno s točkom "u beskonačnosti" $\mathcal{O}$, gdje konstante a i b moraju zadovoljavati

$$4a^3 + 27b^2 \neq 0.$$

Primjedba 3.2. *Diskriminanta kubne jednadžbe $f(x) = ax^3 + bx^2 + cx + d$ dana je s*

$$D = -4b^3d + b^2c^2 - 4ac^3 + 18abcd - 27a^2d^2.$$

Za kubne jednadžbe vrijedi:

- *ako je $D < 0$, onda jednadžba ima jedno realno i dva kompleksna rješenja.*
- *ako je $D > 0$, onda jednadžba ima tri različita realna rješenja.*
- *ako je $D = 0$, onda jednadžba ima tri realna rješenja, od kojih su barem dva međusobno jednaka (dvostruko ili trostruko rješenje).*

Primjedba 3.3. *Uvjet u Definiciji 3.1. je da kubni polinom $f(x) = x^3 + ax + b$ nema višestrukih nultočaka, tj. da je diskriminanta $D = 4a^3 + 27b^2 \neq 0$. Taj uvjet je ekvivalentan uvjetu navedenom na početku poglavlja da polinom $f(x) = x^3 + ax + b$ nema višestrukih korijena.*

Primjedba 3.4. *Polja $\mathbb{Q}, \mathbb{R}$ i $\mathbb{C}$ su karakteristike 0, dok je karakteristika od $\mathbb{F}_q$ jednaka p, ako je p prost broj i $q = p^m$ za neki prirodan broj m.*

Neka je l pravac kroz točke P i Q ili tangenta na eliptičku krivulju E ako je $P = Q$. Presjek pravca l i eliptičke krivulje E je u točkama P, Q i R uzimajući u obzir da $\mathcal{O}$ leži na svim okomitim pravcima. Za $R = (a, b)$ suma od P i Q je definirana kao osnosimetrična točka $R' = (a, -b)$ točke R u odnosu na os x. Ovu sumu označavamo s $P \oplus Q$ ili jednostavnije s $P + Q$.

Ako je $P = (a, b)$ njenu osnosimetričnu točku označavamo s $\ominus P = (a, -b)$ ili jednostavnije s $-P$ i definiramo $P \ominus Q = P \oplus (\ominus Q)$. Nadalje, uzastopno zbrajanje točke je množenje točke s cijelim brojem, tj.

$$nP = \underbrace{P + P + P + \cdots + P}_{n\text{-puta}}.$$

Definicija 3.2. *Neka je E eliptička krivulja nad poljem realnih brojeva $\mathbb{R}$ te P i Q dvije točke na E. Unarna prefiksna operacija $-$ na E je funkcija $- : E \to E$, koja ima sljedeća dva svojstva*

a) Ako je $P = Q$, onda je $-P = \mathcal{O}$

b) Ako je $P \neq \mathcal{O}$, tj. $P = (x, y)$, pri čemu su $x, y \in \mathbb{R}$, onda je $-P = -(x, y) = (x, -y)$.

Iz definicije eliptičke krivulje, tj. iz jednadžbe je očigledno da ako je $(x, y) \in E$, tada je i $(x, -y) \in E$.

Teorem 3.1. *Neka je E eliptička krivulja. Tada operacija zbrajanja na E ima sljedeća svojstva:*

1. $P + \mathcal{O} = \mathcal{O} + P = P$ *za sve* $P \in E$. *[neutralni element]*
2. $P + (-P) = \mathcal{O}$ *za sve* $P \in E$. *[inverzni element]*
3. $(P + Q) + R = P + (Q + R)$ *za sve* $P, Q, R \in E$. *[asocijativnost zbrajanja]*
4. $P + Q = Q + P$ *za sve* $P, Q \in E$. *[komutativnost zbrajanja]*

Neka je K polje. Slijedi da je $(E(K), +)$ Abelova grupa.

Dokaz:

1. Kao što smo prethodno pokazali $P + \mathcal{O} = \mathcal{O} + P = P$ za sve $P \in E$ vrijedi jer $\mathcal{O}$ leži na okomici kroz točku P.

2. Kao što smo prethodno pokazali $P + (-P) = \mathcal{O}$ za sve $P \in E$ jer $\mathcal{O}$ leži na okomici kroz točku P.

3. Navest ćemo algebarski dokaz ove tvrdnje.
   Neka su $P = (x_1, x_2)$, $Q = (x_2, y_2)$ i $R = (x_r, y_r)$.
   Po Teoremu 3.2., čiji iskaz i dokaz ćemo napraviti neposredno poslije ovog teorema, vrijedi
   $$(x_1, y_1) + (x_2, y_2) = (x_r, y_r),$$
   gdje je
   $$x_r = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - (x_1 + x_2),$$
   $$y_r = -\left(\frac{y_2 - y_1}{x_2 - x_1}\right)^3 + \left(\frac{y_2 - y_1}{x_2 - x_1}(2x_1 + x_2) - y_1\right) \tag{4}$$
   Jednadžba pravca koji prolazi točkama P i Q je
   $$y = \frac{y_2 - y_1}{x_2 - x_1}(x - x_1) + y_1.$$
   Jednadžba eliptičke krivulje je
   $$y^2 = x^3 + ax + b$$
   $$y^2 = (x - x_1 + x_1)^3 + a(x - x_1 + x_1) + b$$

$$y^2 = (x-x_1)^3 + 3(x-x_1)^2x_1 + 3(x-x_1)x_1^2 + a(x-x_1) + x_1^3 + ax_1 + b$$
$$y^2 = (x-x_1)^3 + 3(x-x_1)^2x_1 + 3(x-x_1)x_1^2 + a(x-x_1) + y_1^2.$$

Kvadrirajući jednadžbu pravca dobijemo

$$y^2 = \Big(\frac{y_2-y_1}{x_2-x_1}\Big)^2(x-x_1)^2 + 2\frac{y_2-y_1}{x_2-x_1}(x-x_1)y_1 + y_1^2.$$

Sada je

$$\Big(\frac{y_2-y_1}{x_2-x_1}\Big)^2(x-x_1)^2 + 2\frac{y_2-y_1}{x_2-x_1}(x-x_1)y_1 + y_1^2 =$$
$$(x-x_1)^3 + 3(x-x_1)^2x_1 + 3(x-x_1)x_1^2 + a(x-x_1) + y_1^2.$$

Slijedi

$$\Big(\frac{y_2-y_1}{x_2-x_1}\Big)^2(x-x_1) + 2\frac{y_2-y_1}{x_2-x_1}y_1 = (x-x_1)^2 + 3x_1(x-x_1) + 3x_1^2 + a$$

$$(x-x_1)^2 - \Big(\Big(\frac{y_2-y_1}{x_2-x_1}\Big)^2 - 3x_1\Big)(x-x_1) + 3x_1^2 - 2\frac{y_2-y_1}{x_2-x_1}y_1 + a = 0.$$

Nultočke kvadratne jednadžbe su

$$x-x_1 = \frac{1}{2}\left(\Big(\frac{y_2-y_1}{x_2-x_1}\Big)^2 - 3x_1 \pm \sqrt{\left(\Big(\frac{y_2-y_1}{x_2-x_1}\Big)^2 - 3x_1\right)^2 - 4\left(3x_1^2 - 2\frac{y_2-y_1}{x_2-x_1}y_1 + a\right)}\right).$$

Označimo

$$* = \left(\Big(\frac{y_2-y_1}{x_2-x_1}\Big)^2 - 3x_1\right)^2 - 4\left(3x_1^2 - 2\frac{y_2-y_1}{x_2-x_1}y_1 + a\right).$$

Proširivanjem i uređivanjem dobije se

$$* = \Big(\frac{y_2-y_1}{x_2-x_1}\Big)^4 - 6x_1\Big(\frac{y_2-y_1}{x_2-x_1}\Big)^2 + 8\frac{y_2-y_1}{x_2-x_1}y_1 - 3x_1^2 - 4a.$$

Zatim

$$* = \Big(\frac{y_2-y_1}{x_2-x_1}\Big)^4 - 6x_1\Big(\frac{y_2-y_1}{x_2-x_1}\Big)^2 - 4\frac{(y_2-y_1)^2}{x_2-x_1} + 4\frac{(y_2-y_1)^2}{x_2-x_1} + 8\frac{y_2-y_1}{x_2-x_1}y_1 - 3x_1^2 - 4a.$$

$$* = \Big(\frac{y_2-y_1}{x_2-x_1}\Big)^4 - \Big(6x_1+4(x_2-x_1)\Big)\Big(\frac{y_2-y_1}{x_2-x_1}\Big)^2 + 4\frac{(y_2-y_1)\Big((y_2-y_1)+2y_1\Big)}{x_2-x_1} - 3x_1^2 - 4a$$
$$* = \Big(\frac{y_2-y_1}{x_2-x_1}\Big)^4 - 2(2x_2+x_1)\Big(\frac{y_2-y_1}{x_2-x_1}\Big)^2 + 4\frac{y_2^2-y_1^2}{x_2-x_1} - 3x_1^2 - 4a.$$

Koristeći jednakost

$$y_2^2 - y_1^2 = (x_2^3 + ax_2 + b) - (x_1^3 + ax_1 + b) = (x_2-x_1)(x_2^2 + x_2x_1 + x_1^2 + a)$$

dobivamo

$$* = \Big(\frac{y_2-y_1}{x_2-x_1}\Big)^4 - 2(2x_2+x_1)\Big(\frac{y_2-y_1}{x_2-x_1}\Big)^2 + 4(x_2^2 + x_2x_1 + x_1^2 + a) - 3x_1^2 - 4a$$

$$* = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^4 - 2(2x_2 + x_1)\left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 + 4x_2^2 + 4x_2x_1 + x_1^2$$

$$* = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^4 - 2(2x_2 + x_1)\left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 + (2x_2 + x_1)^2$$

$$* = \left(\left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - 2x_2 - x_1\right)^2.$$

Sada je

$$x - x_1 = \frac{1}{2}\left(\left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - 3x_1 + \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - 2x_2 - x_1\right)$$

$$x - x_1 = \frac{1}{2}\left(2\left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - 4x_1 - 2x_2\right)$$

$$x - x_1 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - (2x_1 + x_2).$$

Konačno dobivamo

$$x_r = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - (x_1 + x_2).$$

Drugo rješenje je $x = x_2$.
To daje

$$y_r = \frac{y_2 - y_1}{x_2 - x_1}(x_r - x_1) + y_1$$

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

$$y_r = \frac{y_2 - y_1}{x_2 - x_1}^3 - \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2(2x_1 + x_2) + y_1.$$

Tada je

$$(x_3, y_3) = (x_r, -y_r),$$

što daje formulu (4). □

4. Ovo svojstvo je lako provjeriti. Pošto pravac prolazi točkama P i Q to je isti pravac koji prolazi točkama Q i P, stoga druge točke nisu bitne.

□

Navedimo eksplicitne formule za koordinate zbroja točaka na eliptičkoj krivulji pomoću kojih ćemo lako zbrajati i oduzimati točke na eliptičkoj krivulji.

Teorem 3.2. *(Algoritam zbrajanja točaka na eliptičkoj krivulji) Neka je*

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

eliptička krivulja i neka su P i Q točke na toj krivulji.

1. *Ako je $P = \mathcal{O}$, tada je $P + Q = Q$.*
2. *Inače, ako je $Q = \mathcal{O}$, tada je $P + Q = P$.*
3. *Inače, zapisati $P_1 = (x_1, y_1)$ i $P_2 = (x_2, y_2)$*
4. *Ako $x_1 = x_2$ i $y_1 = -y_2$, tada $P + Q = \mathcal{O}$.*

5. *Inače definirati* λ

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

i neka je

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

Tada je $P + Q = (x_3, y_3)$.

Dokaz:

1. Slijedi iz tvrdnje 1. iz Teorema 3.1.

2. Slijedi iz tvrdnje 1. iz Teorema 3.1.

3. Očito.

4. Slučaj kada je pravac kroz točke P i Q okomica, stoga je $P + Q = \mathcal{O}$. Primjetimo ako je $y_1 = y_2 = 0$ tada je tangenta okomica i vrijedi izraz.

5. Ako je $P \neq Q$, tada je λ koeficijent smjera pravca kroz točke P i Q. Ako je $P = Q$ tada je λ koeeficijent smjera tangente kroz točku $P = Q$. U svakom slučaju pravac l je dobiven iz jednadžbe $y = \lambda x + \nu$ gdje je $\nu = y_1 - \lambda x_1$. Uvrštavanjem l u jednadžbu eliptičke krivulje E dobivamo

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

Slijedi

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

Znamo da ova kubna jednadžba ima rješenja x_1 i x_2. Ako je treće rješenje x_3 tada je faktorizacija

$$x^3 - \lambda^2 x^2 + (a - 2\lambda\nu)x + (b - \nu^2) = (x - x_1)(x - x_2)(x - x_3).$$

Nakon što pomnožimo desnu stranu jednakosti pogledajmo koeficijente uz x^2. Koeficijent uz x^2 na desnoj strani je $-x_1 - x_2 - x_3$ što mora biti jednako koeficijentu uz x^2 s lijeve strane, tj. jednako $-\lambda^2$. Tada je $x_3 = \lambda^2 - x_1 - x_2$. Slijedi da je y koordinata sjecišta pravca l i eliptičke krivulje E jednaka $\lambda x_3 + \nu$. Napokon, da bismo dobili $P + Q$ moramo pronaći osnosimetričnu točku oko osi x što znači zamijeniti y koordinatu s $-y$. □

4 Eliptičke krivulje nad konačnim poljem

U prethodnom smo poglavlju obradili geometrijsku teoriju eliptičkih krivulja. Na primjer, zbroj dviju različitih točaka P i Q na eliptičkoj krivulji E definirali smo crtanjem pravca l koji povezuje točku P i Q i zatim pronalaskom treće točke u kojoj se sijeku pravac l i eliptička krivulja E. Međutim, da bismo primijenili eliptičke krivulje u kriptografiji trebamo promatrati eliptičke krivulje čije točke imaju koordinate u konačnom polju $\mathbb{F}_p$, gdje je p prost broj.

Definirajmo eliptičku krivulju nad $\mathbb{F}_p$ kao jednadžbu oblika

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

gdje $a, b \in \mathbb{F}_p$ zadovoljavaju $4a^3 + 27b^2 \neq 0$, i tada eliptičku krivulju E s točkama u $\mathbb{F}_p$ označavamo

$$E(\mathbb{F}_p) = \{(x, y) : x, y \in \mathbb{F}_p \textit{ zadovoljavaju } y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}.$$

Napomena 4.1. *Zahtijevamo da je $p \geq 3$.*

Primjer 4.1. *Zadana je eliptička krivulja*

$$E : y^2 = x^3 + 7x + 5$$

nad poljem $\mathbb{F}_7$. Da bismo pronašli točke iz $E(\mathbb{F}_7)$ uvrstimo sve moguće vrijednosti za $x = 0, 1, 2, \ldots, 6$.

- *Ako stavimo $x = 0$ dobije se 5, a y^2 nikada nije kongruentno 5 modulo 7.*
- *Ako stavimo $x = 1$ dobije se $1 + 7 + 5 = 13$, a y^2 nikada nije kongruentno 13 modulo 7.*
- *Ako stavimo $x = 2$ dobije se $8 + 14 + 5 = 27$, a y^2 nikada nije kongruentno 27 modulo 7.*
- *Ako stavimo $x = 3$ dobije se $27 + 21 + 5 = 53$, a y^2 je kongruentno 53 modulo 7, tj.*

  $$2^2 \equiv 53 \pmod 7$$

  $$5^2 \equiv 53 \pmod 7,$$

  a to daje dvije točke $(3, 2)$ i $(3, 5)$ u $E(\mathbb{F}_7)$.
- *Ako stavimo $x = 4$, dobije se $64+28+5 = 97$, a y^2 nikada nije kongruentno 97 modulo 7.*
- *Ako stavimo $x = 5$, dobije se $125 + 35 + 5 = 165$, a y^2 je kongruentno 165 modulo 7, tj.*

  $$2^2 \equiv 165 \pmod 7$$

  $$5^2 \equiv 165 \pmod 7,$$

  a to daje dvije točke $(5, 2)$ i $(5, 5)$ u $E(\mathbb{F}_7)$.

- *Ako stavimo* $x = 6$, *dobije se* $216 + 42 + 5 = 263$, *a* y^2 *je kongruentno* 263 *modulo 7, tj.*

$$2^2 \equiv 263 \pmod 7$$
$$5^2 \equiv 263 \pmod 7,$$

a to daje dvije točke $(6, 2)$ *i* $(6, 5)$ *u* $E(\mathbb{F}_7)$.

Sada je

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

$E(\mathbb{F}_7)$ *sadrži 7 točaka.*

Pretpostavimo sada da su P i Q dvije točke u $E(\mathbb{F}_p)$ i da želimo "zbrojiti" točke P i Q. Jedna mogućnost je razvijati teoriju geometrijski koristeći polje $E(\mathbb{F}_p)$ umjesto polja $\mathbb{R}$. Tada bismo oponašali naše ranije konstrukcije za definiranje $P + Q$. Međutim, da bismo zbrojili točke u $E(\mathbb{F}_p)$ i koristit ćemo eksplicitne formule dane u Teoremu 3.2..

Neka su $P = (x_1, y_1)$ i $Q = (x_2, y_2)$ točke u $E(\mathbb{F}_p)$. Pretpostavimo da je zbroj $P+Q$ točka (x_3, y_3) dobivena primjenom algoritma zbrajanja točaka na eliptičkoj krivulji (Teorem 3.2). Primijetimo da se u ovom algoritmu koriste zbrajanje, oduzimanje, množenje i dijeljenje koeficijenata eliptičke krivulje E te koordinate točaka P i Q. Budući da su ti koeficijenti i koordinate u polju $\mathbb{F}_p$, znamo da su i koordinate točke (x_3, y_3) u $\mathbb{F}_p$. Međutim, nije potpuno jasno da je točka (x_3, y_3) u $E(\mathbb{F}_p)$.

Teorem 4.1. *Neka je* E *eliptička krivulja nad poljem* $\mathbb{F}_p$ *i neka su* P *i* Q *točke u* $E(\mathbb{F}_p)$.

a) Algoritam zbrajanja točaka na eliptičkoj krivulji (Teorem 3.2.) primijenjen na točke P *i* Q *daje točku u* $E(\mathbb{F}_p)$. *Ovu točku označavamo s* $P + Q$.

b) Ovakvo zbrajanje u $E(\mathbb{F}_p)$ *zadovoljava sva svojstva iz Teorema 3.1. Drugim riječima,* $\mathbb{F}_p$ *uz ovu operaciju zbrajanja je konačna grupa.*

Dokaz:

a) Formule u Teoremu 3.2. pod 5. izvedene su uvrštavanjem jednadžbe pravca u jednadžbu za eliptičke krivulje E te rješavanjem po x, tako da je točka koja se dobije kao rezultat automatski točka na eliptičkoj krivulji E, tj. ona je rješenje jednadžbe koja definira eliptičku krivulju E. To pokazuje zašto je ova tvrdnja istinita. U slučaju kada je $P = Q$, potreban je dodatni argument koji ukazuje zašto rezultirajući kubni polinom ima dvostruki korijen.

b) Postojanje neutralnog elementa slijedi iz koraka 1. i 2. Teorema 3.1., postojanje inverznog elementa slijedi iz koraka 4. Teorema 3.1., a komutativnost se pokaže direktno iz definicije. Primjenjujući algoritam zbrajanja točaka na eliptičkoj krivulji vidimo da zamjenivši dvije točke dobivamo isti rezultat. Asocijativnost je moguće provjeriti izravno pomoću formula algoritma zbrajanja točaka na eliptičkoj krivulji, iako postoji mnogo posebnih slučajeva koje treba uzeti u obzir. Alternativa je razviti općenitiju teoriju eliptičkih krivulja, kao što je učinjeno u dokazu Teorema 3.1.

□

Primjer 4.2. *Nastavit ćemo s eliptičkom krivuljom iz primjera 4.1. Dakle, zadana je eliptička krivulja*

$$E : y^2 = x^3 + 7x + 5$$

nad poljem $\mathbb{F}_7$. *Odredimo elemente od* $\mathbb{F}_7$, *tj,*

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

Koristimo algoritam zbrajanja točaka na eliptičkoj krivulji iz Teorema 3.2. kako bismo zbrojili točke $P = (3,5)$ *i* $Q = (6,2)$ *u* $E(\mathbb{F}_7)$.
Korak 5. algoritma kaže da izračunamo

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} = \frac{2-5}{6-3} = \frac{-3}{3} = \frac{4}{3}$$

Uočimo da zbog $E(\mathbb{F}_7)$ *vrijedi* $-3 = 4$ *i* $\frac{4}{3}$ *je zapravo* $3x \equiv 4 \pmod 7$ *iz čega dobijemo da je* $x = 6$. *Slijedi,* $\lambda = 6$.
Izračunajmo

$$\nu = y_1 - \lambda x_1 = 5 - 6 \cdot 3 = 5 - 18 = -13 = 1.$$

Sada je

$$x_3 = \lambda^2 - x_1 - x_2 = 36 - 3 - 6 = 27 = 6$$

$$y_3 = -(\lambda x_3 + \nu) = -(6 \cdot 6 + 1) = -37 = 5.$$

Slijedi da je $P + Q = (3,5) + (6,2) = (6,5) \in E(\mathbb{F}_7)$. *Slično, algoritam možemo primjeniti da bismo zbrojili točku* $P = (3,5)$ *samu sa sobom.*
Dobijemo

$$\lambda = \frac{3x_1^2 + a}{2y_1} = \frac{9+7}{10} = \frac{16}{10} = 3$$

$$\nu = y_1 - \lambda x_1 = 5 - 3 \cdot 3 = 5 - 9 = -4 = 3.$$

Sada je

$$x_3 = \lambda^2 - x_1 - x_2 = 9 - 3 - 3 = 3$$

$$y_3 = -(\lambda x_3 + \nu) = -(3 \cdot 3 + 3) = -12 = 2.$$

Slijedi da je $P + P = (3,5) + (3,5) = (3,2) \in E(\mathbb{F}_7)$. *Na isti način možemo izračunati sumu svih parova točaka iz* $E(\mathbb{F}_7)$.

Jasno je da je $E(\mathbb{F}_p)$ konačan skup. Svakom od p mogućih x odgovaraju najviše dva y. Dodavši točku $\mathcal{O}$ zaključujemo da $E(\mathbb{F}_7)$ ima $2p + 1$ točaka. Međutim, ova je procjena znatno veća od stvarne. Samo pola elemenata od $\mathbb{F}_p$ imaju kvadratni korijen pa možemo očekivati $p + 1$ elemenata. Preciznu informaciju o redu grupe $\mathbb{F}_p$ dat će sljedeći teorem.

Teorem 4.2. *(Hasse) Neka je* E *eliptička krivulja nad poljem* $\mathbb{F}_p$. *Tada je*

$$p + 1 - 2\sqrt{p} \leq |E(\mathbb{F}_p)| \leq p + 1 + 2\sqrt{p}.$$

Definicija 4.1. *Veličina* $t = p + 1 - |E(\mathbb{F}_p)|$ *naziva se Frobeniusov trag.*

Napomena 4.2. *Prema Hasseovom teoremu je* $|t| = 2\sqrt{p}$.

Napomena 4.3. *Vrijedi i svojevrstan obrat Hasseovog teorema - Deuringov teorem koji kaže da za svaki prirodan broj*

$$m \in -\langle p+1-2\sqrt{p}, p+1+2\sqrt{p}\rangle$$

postoji eliptička krivulja nad $\mathbb{F}_p$ *takva da je* $|E(\mathbb{F}_p)| = m$.

Primjer 4.3. *Neka je* E *dan jednadžbom*

$$E : y^2 = x^3 + 3x + 7.$$

E promatramo kao eliptičku krivulju nad poljem $\mathbb{F}_p$ *za različita konačna polja* $\mathbb{F}_p$ *i računamo broj elemenata od* $E(\mathbb{F}_p)$. *Tablica prikazuje rezultate za prvih nekoliko prostih brojeva, zajedno s vrijednostima Frobeniusovog traga i, u svrhu uspoređivanja, vrijednosti od* $2\sqrt{p}$.

p	$\lvert E(\mathbb{F}_p)\rvert$	t	$2\sqrt{p}$
3	4	0	3.46
5	5	1	4.47
7	6	2	5.29
9	7	3	6.63
11	10	2	6.63

Tablica 1: Broj elemenata $E(\mathbb{F}_p)$ i vrijednosti Frobeniusovog traga

Primjedba 4.1. *Hasseov teorem daje granicu za* $E(\mathbb{F}_p)$, *ali ne daje metodu za izračun. U principu,* $|E(\mathbb{F}_p)|$ *se može izračunati kao u prethodnim primjerima uvrštavajući sve vrijednosti za* x, *ali za ovo je potrebno vrijeme* $O(p)$, *pa je ova metoda vrlo neučinkovita. Međutim, postoji algoritam za izračunavanje* $|E(\mathbb{F}_p)|$ *složenosti* $O((\log p)^6)$ *poznat kao SEA algoritam*[2].

[2]Schoof-Elkies-Atkin algoritam ; efikasno izračunava $|E(\mathbb{F}_p)|$ za brojeve p s do 500 znamenaka

5 Problem diskretnog logaritma za eliptičke krivulje (ECDLP)

Problem diskretnog logaritma: Neka je $(G, *)$ konačna grupa, $g \in G$, $H = \{g^i : i \geq 0\}$ podgrupa od G generirana s g, te $h \in H$. Treba naći najmanji nenegativan cijeli broj x takav da je $h = g^x$, gdje je $g^x = \underbrace{g * g * g * \cdots * g}_{x\text{-puta}}$. Taj broj zove se diskretni logaritam i označava se s $\log_g h$. Specijalno, za $x = 0$ je $g^0 = e$, gdje je $e \in G$ neutralni element.

Teorem 5.1. *Neka je p prost broj. Tada postoji element $g \in \mathbb{F}_p^*$ takav da je*

$$\mathbb{F}_p^* = \{1, g, g^2, g^3, \ldots g^{p-2}\}.$$

Elementi s ovakvim svojstvom nazivaju se primitivni korijeni od $\mathbb{F}_p$ ili generatori od $\mathbb{F}_p^*$.

Kako bismo napravili kriptosustav temeljen na problemu diskretnog logaritma na $\mathbb{F}_p^*$ promotrimo sljedeće. Alice objavljuje dva broja g i h, a njezina je tajna eksponent x koji je rješenje kongruencije

$$h \equiv g^x \pmod{p}.$$

Razmotrimo kako Alice može učiniti nešto slično s eliptičkom krivuljom E nad poljem $\mathbb{F}_p$. Ako Alice promatra g i h kao elemente grupe $\mathbb{F}_p^*$, tada problem diskretnog logaritma zahtijeva Aliceinu protivnicu Eve da pronađe x takav da

$$h \equiv \underbrace{g \cdot g \cdot g \cdots g}_{x\text{-puta}} \pmod{p}.$$

Drugim riječima, Eve mora odrediti koliko puta se g množi sam sa sobom kako bi odredila h. Jasno je da Alice može učiniti istu stvar s grupom točaka $E(\mathbb{F}_p)$ eliptičke krivulje E nad konačnim poljem $\mathbb{F}_p$. Ona odabire i objavljuje dvije točke P i Q u $E(\mathbb{F}_p)$, a njezina je tajna cijeli broj n takav da

$$Q = \underbrace{P + P + P + \cdots + P}_{n\text{-puta}} = nP.$$

Eve mora otkriti koliko puta P mora biti dodan sebi kako bi dobila Q. Treba imati na umu da iako je "zbrajanje" na eliptičkim krivuljama uobičajeno napisano znakom plus, ono je zapravo vrlo kompliciranа operacija.

Definicija 5.1. *Neka je E eliptička krivulja nad konačnim poljem $\mathbb{F}_p$ i neka su P i Q točke u $E(\mathbb{F}_p)$. Problem diskretnog logaritma eliptičke krivulje (ECDLP) je problem pronalaska cijelog broja n takvog da je $Q = nP$. Cijeli broj n označavamo s*

$$n = \log_p(Q),$$

a n nazivamo eliptički diskretni logaritam Q u odnosu na P.

U svrhu razumjevanja sljedećeg teksta iskažimo bez dokaza propoziciju i teorem poznat pod nazivom Lagrangeov teorem.

Propozicija 5.2. *Neka je G konačna grupa. Svaki element od G ima konačni red. Ako je $a \in G$ reda d i ako je $a^k = e$, pri čemu je e neutralni element, onda vrijedi $d \mid k$.*

Teorem 5.3. *(Lagrangeov teorem) Neka je G konačna grupa i $a \in G$. Tada je red od G djeljiv redom od a. Točnije, neka je $n = |G|$ red od G i neka je d red od a, tj. a^d je najmanja pozitivna potencija od a koje je jednaka e. Tada je $d \mid n$ i*

$$a^n = e.$$

Prethodna definicija $\log_p(Q)$ nije sasvim precizna. Prva poteškoća je da mogu postojati točke $P, Q \in E(\mathbb{F}_p)$ takve da Q nije višekratnik od P. U ovom slučaju, $\log_p(Q)$ nije definiran. Međutim, u svrhu kriptografije, Alice započinje s javnom točkom P i privatnim cijelim brojem n te izračunava i objavljuje vrijednost $Q = nP$. Dakle, u praktičnoj primjeni postoji $\log_p(Q)$, a njegova vrijednost je Aliceina tajna.
Druga poteškoća je da ako postoji jedna vrijednost n koja zadovoljava $Q = nP$, onda takvih vrijednosti ima mnogo. Da bismo to vidjeli, prvo napominjemo da postoji pozitivni cijeli broj s takav da je $sP = \mathcal{O}$. Budući da je $E(\mathbb{F}_p)$ konačan, točke $P, 2P, 3P, 4P, ...$ ne mogu sve biti različite. Stoga, postoje cijeli brojevi $k > j$ takvi da je $kP = jP$ i možemo uzeti $s = k - j$. Najmanji takav $s \geq 1$ naziva se red od P. (Teorem 5.3. kaže da red od P dijeli red od $E(\mathbb{F}_p)$). Dakle, ako je s red od P i ako je n_0 bilo koji cijeli broj takav da je $Q = n_0P$, onda su rješenja od $Q = nP$ cijeli brojevi $n = n_0 + is \in \mathbb{Z}$, gdje je $i \in \mathbb{Z}$. To znači da je vrijednost $\log_p(Q)$ element iz $\mathbb{Z}/s\mathbb{Z}$, tj. $\log_p(Q)$ je cijeli broj modulo s, gdje je s red od P. Možemo staviti $\log_p(Q)$ jednako n_0. Međutim, prednost definiranja da su vrijednosti iz $\mathbb{Z}/s\mathbb{Z}$ je da eliptički diskretni logaritam tada zadovoljava

$$\log_p(Q_1 + Q_2) = \log_p(Q_1) + \log_p(Q_2) \text{ za sve } Q_1, Q_2 \in E(\mathbb{F}_p). \tag{5}$$

Primijetimo analogiju s običnim logaritmom $\log(\alpha\beta) = \log(\alpha) + \log(\beta)$ i diskretnim logaritmom za $\mathbb{F}_p^*$. Činjenica da diskretni logaritam za $E(\mathbb{F}_p)$ zadovoljava (5) znači da poštuje pravilo zbrajanja kada se grupa $E(\mathbb{F}_p)$ preslika u grupu $\mathbb{Z}/s\mathbb{Z}$. Kažemo da je log_P definira homomorfizam grupa

$$\log_p : E(\mathbb{F}_p) \to \mathbb{Z}/s\mathbb{Z}.$$

Primjer 5.1. *Neka je dana eliptička krivulja*

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

nad $\mathbb{F}_{17}$.
Točke $P = (5, 1)$ i $Q = (13, 10)$ su na krivulji $E(\mathbb{F}_{17})$.
Za $P + P = 2P$ računamo

$$\lambda = \frac{3x_1^2 + a}{2y_1} = \frac{75 + 2}{2} = \frac{77}{2} = 13$$

$$\nu = y_1 - \lambda x_1 = 1 - 13 \cdot 5 = 1 - 65 = -64 = 4.$$

Sada je

$$x_3 = \lambda^2 - x_1 - x_2 = 169 - 5 - 5 = 159 = 6$$

$$y_3 = -(\lambda x_3 + \nu) = -(13 \cdot 6 + 4) = -82 = 3.$$

Slijedi da je $P + P = 2P = (6, 3)$.
Postupak nastavljamo i dobivamo

$$3P = (10, 6)$$
$$4P = (3, 1)$$
$$5P = (9, 16)$$
$$6P = (16, 13)$$
$$7P = (0, 6)$$
$$8P = (13, 7)$$
$$9P = (7, 6)$$
$$10P = (7, 11)$$
$$11P = (13, 10)$$

Sada vidimo da je $Q = 11P$ *pa je* $\log_p(Q) = 11$.
Nastavimo li postupak dobijemo $19P = \mathcal{O}$,*a* $|E(\mathbb{F}_{17})| = 19$. *To znači da su sve točke iz* $\mathbb{F}_{17}$ *višekratnici točke* P.

5.1 "Dupliciraj i zbrajaj" algoritam

Primjetimo da je poprilično teško odrediti vrijednost n iz dviju točaka P i $Q = nP$ u $\mathbb{F}_p$, tj. teško je riješiti ECDLP. Da bismo koristili funkciju

$$\mathbb{Z} \to E(\mathbb{F}_p),\ n \to nP$$

moramo izračunati nP iz poznatih vrijednosti n i P. Ako je n velik, nema smisla računati nP izračunavanjem $P, 2P, 3P, 4P, \ldots$
U tu svrhu koristit ćemo algoritam "dupliciraj i zbrajaj" koji se još naziva i binarne ljestve jer koristi binarni zapis broja n. Binaran zapis broja n dan je s

$$n = n_0 + n_1 \cdot 2 + n_2 \cdot 4 + n_3 \cdot 8 + \cdots + n_r \cdot 2^r \quad za \quad n_0, n_1, \ldots, n^r \in \{0, 1\}.$$

Pretpostavljamo da je $n_r = 1$. Sada je

$$Q_0 = P,\ Q_1 = 2Q_0,\ Q_2 = 2Q_1,\ \ldots\ , Q_r = 2Q_{r-1}.$$

Primjetimo da je Q_i dvostruki Q_{i-1} stoga je

$$Q_i = 2^i P.$$

Računanje tih točaka zahtjeva r dupliciranja. Dakle, nP izračunavamo koristeći najviše r dodatnih podataka,

$$nP = n_0 Q_0 + n_1 Q_1 + n_2 Q_2 + \cdots + n_r Q_r.$$

Ukupno vrijeme izračuna nP je najviše $2r$ operacija u $E(\mathbb{F}_p)$. Primjetimo da je $n \geq 2r$ pa je za izračun nP potrebno najviše $2\log_2(n)$ operacija. To nam omogućava računanje nP za velike vrijednosti n. U nastavku je dan algoritam "dupliciraj i zbrajaj".

Algoritam "dulpiciraj i zbrajaj":
Neka je točka $P \in E(\mathbb{F}_p)$ i cijeli broj $n \geq 0$.
1. Postavi $Q = P$ i $R = \mathcal{O}$.
2. Sve dok je $n > 0$.
   3. Ako je $n \equiv 1 \pmod 2$, stavi $R = R + Q$.
   4. Postavi $Q = 2Q$ i $n = \lfloor \frac{n}{2} \rfloor$.
   5. Ako je $n > 0$, nastavi s petljom u koraku 2.
6. Vrati točku R koja je jednaka nP.

Primjer 5.2. *Pomoću algoritma "dupliciraj i zbrajaj" želimo izračunati* $71P$.
Binarni zapis broja 71 *je* $(1000111)_2$. *On se može prikazati kao zbroj potencija broja* 2 *na sljedeći način:*

$$71 = 1 \cdot 2^6 + 0 \cdot 2^5 + 0 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 = 2^6 + 2^2 + 2^1 + 2^0.$$

Tada je

$$71P = 2^6P + 2^2P + 2^1P + 2^0P.$$

Primjetimo da je jedna od posebnosti grupe točka na eliptičkoj krivulji da u njoj inverzna operacija oduzimanja nije kompliciranija od originalne grupovne operacije zbrajanja, tj. $-(x, y) = (x, -y)$. Ovo pomaže većoj efikasnosti multipliciranja. Pogledajmo sljedeći primjer.

Primjer 5.3. *Koristeći algoritam "dupliciraj i zbrajaj" izračunali smo* $509P$. *Naime, binaran zapis broja* 509 *je* $(111111101)_2$. *Dakle,*

$$509P = 2^8P + 2^7P + 2^6P + 2^5P + 2^4P + 2^3P + 2^2P + P.$$

Da bismo izračunali $509P$ *trebalo je 15 operacija (8 množenja i 7 zbrajanja). Isto tako,* $509P$ *možemo zapisati*

$$509P = 2^9P - 2P - P.$$

U ovom slučaju koristili smo 9 + 2 = 11 operacija.

Promatrajući Primjer 5.3. zanima nas koliko smo "uštedjeli". To će nam reći sljedeća propozicija.

Propozicija 5.4. *Neka je* n *pozitivan cijeli broj i* $k = \lfloor \log n \rfloor + 1$, *tj.* $2^k > n$. *Tada je*

$$n = t_0 + t_1 \cdot 2 + t_2 \cdot 4 + t_3 \cdot 8 + \cdots + t_k \cdot 2^k, \tag{6}$$

gdje su $t_0, t_1, t_2, \ldots, t_k \in \{-1, 0, 1\}$ *i najviše* $\frac{1}{2}k$ *takvih* t_i *je jednako 0.*

Dokaz:

Dokaz je zapravo zapis od n u zadovoljavajućoj formi. Binarni zapis od n je

$$n = n_0 + n_1 \cdot 2 + n_2 \cdot 4 + \cdots + n_{k-1} \cdot 2^{k-1}$$

gdje su $n_0, n_1 \ldots, n_{k-1} \in \{0, 1\}$.
Slijeva udesno, tražimo prvu pojavu dvaju ili više uzastopnih koeficijenata n_i koji nisu nula. Npr., pretpostavimo da je

$$n_s = n_{s+1} = \cdots = n_{s+u-1} = 1 \quad i \quad n_{s+u} = 0.$$

za $u \geq 1$. Drugim riječima,

$$2^s + 2^{s+1} + 2^{s+2} + \cdots + 2^{s+u-1} + 0 \cdot 2^{s+u} \tag{7}$$

se pojavljuje u binarnom zapisu od n. Primjetimo,

$$2^s + 2^{s+1} + 2^{s+2} + \cdots + 2^{s+u-1} + 0 \cdot 2^{s+u} = 2^s(1 + 2 + 4 + \cdots + 2^{u-1} = 2^s(2^u - 1),$$

stoga (7) možemo zamijeniti s

$$-2^s + 2^{s+u}.$$

Ponavljajući postupak završit ćemo s n u formi (6), gdje dva uzastopna koeficijenta t_i nisu 0. □

5.2 Koliko je zahtjevan ECDLP

Generalno, koliko je problem zahtjevan procijenjujemo brojem operacija koje su neophodne da se riješi problem najefikasnijom poznatom metodom. Glavni razlog zašto se koriste eliptičke krivulje u kriptografiji javnog ključa je činjenica da ne postoje poznati algoritmi izračuna za ECDLP, tj. ne postoje općeniti algoritmi koji rješavaju ECDLP u manje od $O(\sqrt{p})$. Problem diskretnog logaritma u $E(\mathbb{F}_p)$, je još teži od problema diskretnog logaritma u grupi $\mathbb{F}_p^*$.

Primjedba 5.1. *Najbrži poznati algoritam za rješavanje ECDLP u $E(\mathbb{F}_p)$ ima približno $\sqrt{p}$ koraka.*

6 Kriptosustavi koji koriste eliptičke krivulje

U ovom poglavlju analizirat ćemo kriptosustave koji koriste eliptičke krivulje. Za rješavanje problema razmjene ključeva koristit će se Diffie – Hellman protokol, koji je kompliciraniji od same zamjene problema diskretnog logaritma za konačno polje $\mathbb{F}_p$ s problemom diskretnog logaritma za eliptičku krivulju $E(\mathbb{F}_p)$. Zatim ćemo opisati ElGamalov kriptosustav koji je zasnovan na problemu računanja diskretnog logaritma u grupi $(\mathbb{F}_p, \cdot_p)$ te Menezes-Vanstoneov kriptosustav eliptičkih krivulja.

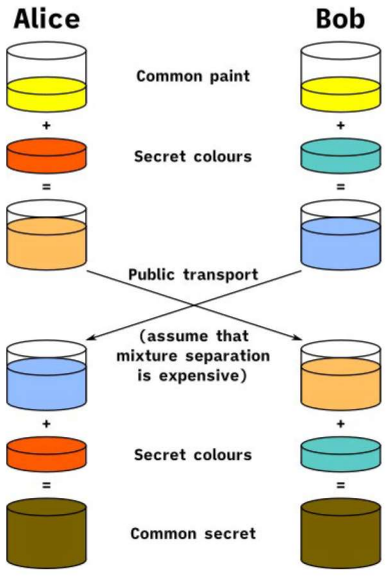
6.1 Eliptički Diffie - Hellman protokol za razmjenu ključeva (ECDH)

Da bismo razumjeli ECDH, prvo moramo pogledati standardni Diffie-Hellmanov protokol za razmjenu ključeva. Bio je to jedan od prvih protokola s javnim ključem koji je osmišljen 1976. godine i koji se i danas široko koristi. Ime je dobio po Whitfieldu Diffieu i Martinu Hellmanu, kriptografima koji su začetnici kriptografije javnog ključa.

Tradicionalno, mora se razmijeniti tajna putem sigurnog kanala između dviju strana. Mana je ta da treća strana može presresti tajnu ako je povjerena komunikacijskom kanalu. Ta se tajna tada može koristiti za dešifriranje šifriranih podataka između dviju strana, čineći ih beskorisnim.

Diffie-Hellman dopušta dvjema stranama da razmijene svoju tajnu bez potrebe za sigurnim kanalom za prijenos tajne. Zapravo se ovo može koristiti na bilo kojem nesigurnom kanalu.

Ilustrirat ćemo koncept razmjene javnih ključeva korištenjem boja umjesto vrlo velikih brojeva koji se zapravo koriste tijekom postupka.



Slika 9: Razmjena ključeva

Pretpostavimo da treća strana istražuje razmjenu u nesigurnoj komunikaciji. Vidjela bi samo zajedničku boju, u ovom slučaju žutu, i prvi set miješanih boja, tj. svijetlonarančastu i svijetloplavu. Bilo bi izuzetno teško izračunati konačnu boju. Umjesto boja, u praksi se koriste izuzetno veliki brojevi i ovo određivanje je računski "skupo". Nemoguće je pokušati izračunati konačnu boju, čak i za moderna superračunala. Drugim riječima, ideja javnog ključa da se konstruira kriptosustav iz kojeg bi bilo praktično nemoguće izračunati funkciju dešifriranja d_K pomoću funkcije šifriranja e_K. Dakle, Alice svoju poruku šifrira pomoću Bobovog javnog ključa i pošalje ju Bobu. On posjeduje dodatnu informaciju za svoj javni ključ i pomoću nje dešifrira šifrat koristeći svoj tajni ključ.

Diffie-Hellmanov protokol za razmjenu ključeva:

1. Neka je $\mathbb{F}_p^*$ multiplikativna ciklička grupa svih ne-nul ostataka modulo p, gdje je p dovoljno velik prost broj. Generator je primitivni korijen modulo p ako je g^{p-1} najmanja potencija broja g koja daje ostatak 1 pri djeljenju s p.

2. Alice generira slučajan cijeli broj a.

   Ona računa $A \equiv g^a \pmod{p}$.

3. Bob generira slučajan cijeli broj b.

   On računa $B \equiv g^b \pmod{p}$.

4. Alice šalje A Bobu $\longrightarrow A$.

   $B \longleftarrow$ Bob šalje B Alice.

5. Alice računa $B^a \pmod{p}$.

   Bob računa $A^b \pmod{p}$.

6. Njihov tajni ključ je $B^a \equiv (g^b)^a \equiv g^{ab} \equiv (g^a)^b \equiv A^b \pmod{p}$.

Dakle, sada kad znamo kako funkcionira standardna Diffie-Hellmanova razmjena ključeva, možemo promatrati Diffie-Hellman protokol na eliptičkoj krivulji. Koncept je više-manje isti. Postupak se odvija na isti način, ali koristi algebarske krivulje za generiranje ključeva koje će dvije strane koristiti. Također, obje strane moraju se prethodno dogovoriti oko eliptičke krivulje. Korištenje eliptičkih krivulja je puno brže od korištenja velikih brojeva potrebnih u standardnom Diffie-Hellmanovom protokolu.

Promotrimo sad eliptički Diffie-Hellmanov protokol za razmjenu ključeva. Alice i Bob su se dogovorili koristiti određenu eliptičku krivulju $E(\mathbb{F}_p)$ i određenu točku $P \in E(\mathbb{F}_p)$. Alice odabire tajni cijeli broj n_A, a Bob odabire tajni cijeli broj n_B. Tada izračunavaju pridružene višekratnike

$$\underbrace{Q_A = n_A P}_{\text{Izračunava Alice}}$$
$$\underbrace{Q_B = n_B P}_{\text{Izračunava Bob}}$$

i razmjenjuju vrijednosti od Q_A i Q_B. Alice tada koristi svoj tajni množitelj za izračunavanje $n_A Q_B$, a Bob slično izračunava $n_B Q_A$. Sad imaju zajedničku tajnu vrijednost

$$n_A Q_B = (n_a n_B)P = n_B Q_A,$$

koju mogu koristiti kao ključ za privatnu komunikaciju.

Eliptički Diffie-Hellmanov protokol za razmjenu ključeva:

1. Neka je p (veliki) prost broj, eliptička krivulja E nad poljem $\mathbb{F}_p$ i točka $P \in E(\mathbb{F}_p)$.
2. Alice generira slučajan cijeli broj n_A.
   Ona računa $Q_A = n_A P$.
3. Bob generira slučajan cijeli broj n_B.
   On računa $Q_B = n_B P$.
4. Alice šalje Q_A Bobu $\longrightarrow Q_A$.
   $Q_B \longleftarrow$ Bob šalje Q_B Alice.
5. Alice računa točku $n_A Q_B$.
   Bob računa točku $n_B Q_A$.
6. Njihov tajni ključ je $n_A Q_B = n_A(n_B P) = n_B(n_A P) = n_B Q_A$.

Primjer 6.1. *Zadana je eliptička krivulja* $E : y^2 = x^3 + 171x + 853$, $p = 2671$ *i* $P = (1980, 431) \in E(\mathbb{F}_{2671})$.
Alice odabire $n_A = 44$, *a Bob odabire* $n_B = 75$. *Tada Alice i Bob računaju*

$$Q_A = 44P = (1860, 2395) \in E(\mathbb{F}_{2671}),$$

$$Q_B = 75P = (2141, 1995) \in E(\mathbb{F}_{2671}).$$

Alice šalje Q_A *Bobu i Bob šalje* Q_B *Alice. Tada Alice i Bob računaju*

$$n_A Q_B = 44(2141, 1995) = (1411, 593) \in E(\mathbb{F}_{2671}),$$

$$n_B Q_A = 75(1860, 2395) = (1411, 593) \in E(\mathbb{F}_{2671})$$

Bob i Alice razmijenili su tajnu $(1411, 593)$. *Trebali bismo odbaciti y-koordinatu i gledati samo vrijednost* $x = 1411$ *kao tajni ključ.*

Jedan od načina da Eve otkrije tajnu Alice i Boba je rješavanje ECDLP-a

$$nP = Q_A$$

jer ako Eve može riješiti ovaj problem, onda ona zna n_A i može ga iskoristiti za izračunavanje $n_A Q_B$. Naravno, može postojati neki drugi način da Eve otkrije tajnu, a da zapravo ne riješi ECDLP.

Definicija 6.1. *Neka je* $E(\mathbb{F}_p)$ *eliptička krivulja nad konačnim poljem i neka je* $P \in E(\mathbb{F}_p)$. *Eliptički Diffie-Hellman problem je problem računanja vrijednosti* $n_1 n_2 P$ *ako znamo vrijednosti* $n_1 P$ *i* $n_2 P$.

Napomena 6.1. *Eliptički Diffie-Hellman protokol za razmjenu ključeva zahtjeva da Alice i Bob razmjene točke na eliptičkoj krivulji. Točka* Q *u* $E(\mathbb{F}_p)$ *ima dvije koordinate* $Q = (x_Q, y_Q)$, *gdje su* x_Q *i* y_Q *elementi konačnog polja* $\mathbb{F}_p$, *pa se čini da Alice mora poslati Bobu dva broja u* $\mathbb{F}_p$. *Međutim, ta dva broja modulo p ne sadrže toliko podataka koliko dva proizvoljna broja jer su povezani formulom*

$$y_Q^2 = x_Q^3 + a x_Q + b \text{ u } \mathbb{F}_p.$$

Treba imati na umu da Eve poznaje vrijednosti a i b pa ako može pogoditi točnu vrijednost x_Q, *tada su samo dvije moguće vrijednosti za* y_Q, *a u praksi nije previše teško izračunati te dvije vrijednosti* y_Q.

Dakle, nema razloga da Alice Bobu pošalje obje koordinate Q_A, budući da y koordinata sadrži tako malo dodatnih podataka. Umjesto toga, Alice šalje Bobu samo x koordinatu od Q_A. Bob tada izračuna i koristi jednu od dvije moguće y koordinate. Ako Bob odabere "ispravan" y onda koristi Q_A, a ako odabere "neispravan" y (što je negativno od "ispravan" y), tada koristi$-Q_A$. U svakom slučaju, Bob završava s računanjem jedne od

$$\pm n_B Q_A = \pm(n_A n_B)P.$$

Analogno, Alice izračunava jedan od $\pm(n_a n_B)P$. Zatim Alice i Bob koristite x koordinatu kao njihovu zajedničku tajnu vrijednost, jer je ta x koordinata ista bez obzira koju y koordinatu koriste.

Primjer 6.2. *Zadana je eliptička krivulja* $E : y^2 = x^3 + 171x + 853$, $p = 2671$ *i* $P = (1980, 431) \in E(\mathbb{F}_{2671})$.
Alice odabire $n_A = 33$, *a Bob odabire* $n_B = 60$. *Tada Alice i Bob računaju*

$$Q_A = 33P = (757, 232) \in E(\mathbb{F}_{2671}),$$

$$Q_B = 60P = (1183, 1887) \in E(\mathbb{F}_{2671}).$$

Za razliku od Primjera 5.2. Alice će Bobu poslati samo kordinatu $x_A = 2013$ *i Bob će Alice poslati samo koordinatu* $x_B = 1183$. *Kako bi pronašla* y, *imajući na umu da su operacije u* $\mathbb{F}_{2671}$, *Alice uvrštava* $x_B = 1183$ *u* E *i računa*

$$y_B^2 = 1183^3 + 171 \cdot 1183 + 853 = 326.$$

Alice sada mora izračunati $y^2 = 326 \pmod{2671}$. *Dobiva rješenja* $y_1 = 784$ *i* $y_2 = 1887$. *Odabire* $y = 784$, *tj.* $Q'_B = (x_B, y_B) = (1183, 784)$ *što nije točka koju je Bob izabrao. Sada Alice računa* $n_A Q'_B = 33(1183, 784) = (1744, 1694)$. *Istim postupkom, Bob uvrštava* $x_A = 757$ *u* E *i računa*

$$y_A^2 = 757^3 + 171 \cdot 757 + 853 = 404.$$

Bob sada mora izračunati $y^2 = 404 \pmod{2671}$. *Dobiva rješenja* $y_3 = 232$ *i* $y_4 = 2439$. *Odabire* $y = 2439$, *tj.* $Q'_A = (757, 2439)$ *što nije točka koju je izabrala Alice. Bob računa* $n_B Q'_A = 60(757, 2439) = (1744, 1694)$. *Vidimo da je da je dobiven isti tajni ključ.*
Primjetimo, u slučaju da je jedna strana izabrala upravo točnu y koordinatu, dok druga nije, tajni ključ bi imao istu x koordinatu, a različite y koordinate. Međutim, te dvije točke bile bi međusobno negativne u $\mathbb{F}_{2671}$ *što je u redu s obzirom da su x koordinate jednake.*

6.2 Eliptički ElGamalov kriptosustav javnog ključa

Pogledajmo najprije ElGamalov kriptosustav[3] koji se temelji na problemu računanja diskretnog logaritma u grupi $(\mathbb{F}_p, \cdot_p)$.

ElGamalov kriptosustav:

1. Neka je p veliki prost broj i $g \in \mathbb{F}_p^*$ primitivan korijen modulo p.
2. Alice izabire privatan ključ $1 \leq a \leq p-1$.

   Računa $A = g^a \pmod{p}$.

   Objavljuje javni ključ A.
3. Bob odabire otvoreni tekst m i proizvoljan kratkotrajan ključ k.

   Koristeći Alicein javni ključ A izračunava $c_1 = g^k \pmod{p}$ i $c_2 = mA^k \pmod{p}$.

   Šalje šifrat (c_1, c_2) Alice.
4. Alice izračunava $(c_1^a)^{-1} \cdot c_2 \pmod{p}$. To je jednako m.

Vidimo da se m pomnoži s A^k kako bi bio prikriven pa onaj koji zna tajni eksponent g može iz g^k izračunati A^k i otkriti ga. Kako bi g bio tajan, prost broj p mora biti dovoljno velik pa problem diskretnog algoritma u $\mathbb{Z}_p^*$ postaje gotovo nerješiv.

Sada promotrimo eliptički ElGamalov kriptosustav. Alice i Bob koriste određeni prost broj p, eliptičku krivulju E i točku $P \in E(\mathbb{F}_p)$. Alice odabire tajni multiplikator n_A i objavljuje točku $Q_A = n_A P$ kao svoj javni ključ. Bobov otvoreni tekst je točka $M \in E(\mathbb{F}_p)$. Odabire cijeli broj k koji će mu biti kratkotrajan ključ i izračunava

$$C_1 = kP \quad i \quad C_2 = M + kQ_A.$$

Bob šalje dvije točke (C_1, C_2) Alice, koja, da bi otkrila otvoreni tekst, izračunava

$$C_2 - n_a C_1 = (M + kQ_A) - n_A(kP) = M + k(n_A P) - n_A(kP) = M.$$

Eliptički ElGamalov kriptosustav javnog ključa:

1. Neka je p velik prost broj, E eliptička krivulja nad $\mathbb{F}_p$ i točka $P \in E(\mathbb{F}_p)$.
2. Alice izabire tajni ključ n_A.

   Računa $Q_A = n_A P$ u $\mathbb{F}_p$.

   Objavljuje javni ključ Q_A.
3. Bob odabire otvoreni tekst $M \in \mathbb{F}_p$ i kratkotrajni ključ k.

   Koristi Alicein javni ključ Q_A za izračunavanje $C_1 = kP \in E(\mathbb{F}_p)$ i $C_2 = M + kQ_A \in E(\mathbb{F}_p)$.

   Šalje šifrat (C_1, C_2) Alice.
4. Alice računa $C_2 - n_A C_1 \in E(\mathbb{F}_p)$. Ovo je jednako M.

[3] 1985. godine ga je predložio Taher ElGamal.

Postoji nekoliko nedostataka ElGamalovog kriptosustava. Prvi nedostatak je da elemente otvorenog teksta moramo prebaciti u točke na eliptičkoj krivulji. Za to ne postoji deterministički, nego vjerojatnosni algoritam koji koristi činjenicu da kvadrati u konačnom polju predstavljaju 50% svih elemenata. Drugi problem je da se šifrat jednog elementa otvorenog teksta sastoji od uređenog para točaka na eliptičkoj krivulji. To znači da prilikom šifriranja poruka postaje otprilike četiri puta dulja. To je posljedica činjenice da je otvoreni tekst M jedna točka u $E(\mathbb{F}_p)$. Tada po Hesseovom teoremu postoji približno p različitih točaka u $E(\mathbb{F}_p)$, dakle samo približno p otvorenih tekstova. Međutim, šifrirani tekst (C_1, C_2) se sastoji od četiri broja modulo p, jer svaka točka u $E(\mathbb{F}_p)$ ima dvije koordinate.

Primjer 6.3. *Neka je* $E : y^2 = x^3 + 19x + 17$ *eliptička krivulja nad* $\mathbb{F}_{1201}$ *i* $P = (1082, 336) \in E(\mathbb{F}_{1201})$.
Alicein tajni ključ je $n_A = 59$.
Sada izračunava

$$Q_A = n_A P = 59(278, 916) = (565, 569).$$

Bob odabire otvoren tekst $(1082, 336) \in \mathbb{F}_{1201}$ *i kratkotrajan ključ* $k = 5$. *Izračunava*

$$C_1 = 5(278, 916) = (439, 1196)$$

$$C_2 = (1082, 336) + 5(565, 569) = (1082, 865) + (557, 238) = (1074, 23).$$

Alice računa

$$(1074, 23) - 59(439, 1196) = (1074, 23) - (557, 238) = (1074, 23) + (557, 963) = (1082, 336).$$

Vidimo da smo dobili upravo otvoreni tekst koji je odabrao Bob.

6.3 Menezes-Vanstoneov kriptosustav

U ovom potpoglavlju navest ćemo varijantu ElGamalovog kriptosustava pod nazivom Menezes-Vanstoneov kriptosustav[4]. U njemu se eliptičke krivulje koriste za prikrivanje, a otvoreni tekstovi i šifrati su proizvoljni uređeni parovi elemenata iz polja koji ne odgovaraju nužno točkama na eliptičkoj krivulji. Kod ovakvog kriptosustava, šifrirana poruka je dva puta dulja. Kod ovog kriptosustava, umjesto prevođenja elemenata otvorenog teksta u točku eliptičke krivulje imamo samo "maskiranje" elemenata otvorenog teksta alatima koje pružaju eliptičke krivulje.
Menezes-Vanstoneov kriptosustav:

1. Neka je E eliptička krivulja nad $\mathbb{F}_p$ i $p > 3$ prost broj, te H ciklička podgrupa od E generirana s α. Neka je $\mathcal{P} = \mathbb{F}_p^* \times \mathbb{F}_p^*$ i $\mathcal{K} = \{(E, \alpha, a, \beta) : \beta = a\alpha\}$, gdje $a\alpha$ označava $\underbrace{\alpha + \alpha + \alpha + \cdots + \alpha}_{a\text{-puta}}$, pri čemu je $+$ je zbrajanje točaka na eliptičkoj krivulji.

   Vrijednost E, α, β su javne, a vrijednost a je tajna vrijednost.

2. Za $K \in \mathcal{K}$ i tajni slučajni broj $k \in \{0, 1, 2, \ldots, |H| - 1\}$, te za $x = (x_1, x_2) \in \mathbb{F}_p^* \times \mathbb{F}_p^*$ definiramo

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

   gdje je $y_0 = k\alpha$, $(c_1, c_2) = k\beta$, $y_1 = c_1 x_1 \pmod p$, $y_2 = c_2 x_2 \pmod p$.

[4] 1995. godine su ga predložili Alfred Menezes, Minghua Qu i Scott Vanstone.

3. Za šifrat $y = (y_0, y_1, y_2)$ definiramo

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

gdje je $ay_0 = (c_1, c_2)$.

Primjer 6.4. *Neka je* $E : y^2 = x^3 + 11x + 4$ *eliptička krivulja nad* $\mathbb{F}_{11}$.
Grupa $\mathbb{F}_{11}$ *je ciklička grupa s generatorom* $\alpha = (1, 4)$. *Pretpostavimo da Alice želi poslati poruku* $(x_1, x_2) = (10, 6)$ *Bobu, koji je odabrao tajni ključ* $a = 3$, *a javni ključ je* $\beta = a\alpha = 3(1, 4) = (3, 8)$. *Pretpostavimo da je Alice izabrala tajni broj* $k = 7$. *Tada ona računa*

$$(c_1, c_2) = 7\beta = 7(3, 8) = (3, 3),$$

$$y_0 = k\alpha = 7(1, 4) = (2, 10),$$

$$y_1 = c_1 x_1 = 3 \cdot 10 = 30 = 8 \pmod{11}$$

$$y_2 = c_2 x_2 = 3 \cdot 6 = 18 = 7 \pmod{11}.$$

Sada Alice šalje šifrat $(y_0, y_1, y_2) = ((2, 10), 8, 7)$ *Bobu. Nakon što je Bob primio šifrat, računa*

$$ay_0 = 3(2, 10) = (3, 3) = (c_1, c_2),$$

$$(8 \cdot 3^{-1} \bmod 11, 7 \cdot 3^{-1} \bmod 11) = (10, 6) = (x_1, x_2).$$

Literatura

[1] A. DUJELLA, *Eliptičke krivulje u kriptografiji* , PMF – Matematički odjel, Sveučilište u Zagrebu, 2013.

[2] A. DUJELLA, M. MARETIĆ, *Kriptografija*, Element, Zagreb, 2007.

[3] J. HOFFSTEIN, J. PIPHER, J. H. SILVERMAN, *An introduction to mathematical cryptography*, Springer, New York; London, 2008.

[4] A. KOKANOVIĆ, *RSA Kriptosustav*, Odjel za matematiku, Sveučilište u Osijeku, 2017.

[5] P. P. DU PREEZ, *Understanding EC Diffie-Hellman*, `https://medium.com/swlh/understanding-ec-diffie-hellman-9c07be338d4a`

[6] D. SEJDINOVIĆ, *Eliptičke krivulje u kriptografiji*, Osječki matematički list, 6 (2006), 85-97.

[7] N. SULLIVAN, A (Relatively Easy To Understand) Primer on Elliptic Curve Cryptography, `https://blog.cloudflare.com/a-relatively-easy-to-understand-primer-on-elliptic-curve-cryptography/`

[8] *ElGamal and Elliptic Curve*, `https://ece.uwaterloo.ca/~j25ni/CP460/CP460_Chap7_Elgamal.pdf`

* samostalno izrađeni grafovi pomoću alata Desmos

Sažetak

U ovom radu smo definirali eliptičke krivulje te smo dali geometrijsku i algebarsku interpretaciju operacije uz koju skup točaka na eliptičkoj krivulji $E(\mathbb{K})$ postaje Abelova grupa. Odredili smo problem diskretnog logaritma za eliptičke krivulje (ECDLP) i komentirali vremensku složenost problema. Naveli smo algoritam "dupliciraj i zbrajaj", poznat pod nazivom binarne ljestve, za računanje vrijednosti višekratnika neke točke na eliptičkoj krivulji. Opisali smo upotrebu eliptičkih krivulja u kriptografiji kroz eliptički Diffie-Hellman protokol (ECDH) te eliptički ElGamalov kriptosustav zasnovan na problemu računanja diskretnog logaritma u konačnim grupama gdje prilikom šifriranja poruka postaje otprilike četiri puta dulja. Na kraju smo naveli varijantu ElGamalovog kriptosustava pod nazivom Menezes-Vanstoneov kriptosustav kod kojeg je šifrirana poruka dva puta dulja.

Ključne riječi: eliptičke krivulje, problem diskretnog logaritma za eliptičke krivulje (ECDLP), algoritam "dupliciraj i zbrajaj", binarne ljestve, eliptički Diffie-Hellman protokol, eliptički ElGamalov kriptosustav, Menezes-Vanstoneov kriptosustav.

Title and summary

In this work, we defined the elliptic curves and gave the geometric and algebraic interpretation of the operation in which a set of points on an elliptic curve $E(\mathcal{K})$ becomes the Abel group. In addition, we determined the elliptic curve discrete logarithm problem (ECDLP) and commented time complexity of algorithm. We have listed a "double-and-add" algorithm, known as a binary ladder, to compute the multiple value of a point on an elliptic curve. Also, we have described the use of elliptic curves in cryptography through the elliptical Diffie-Hellman protocol (ECDH) and the elliptical ElGamal cryptosystem based on the problem of computing a discrete logarithm in finite groups where during encrypting messages become approximately four times longer. Finally, we have listed a variant of ElGamal's cryptosystem called the Menezes-Vanstone cryptosystem in which the encrypted message is twice as long.

Keywords: elliptic curves, the elliptic curve discrete logarithm problem (ECDLP), "double-and-add" algorithm, binary ladders, elliptical Diffie-Hellman key exchange, elliptical ElGamal public key cryptosystem, Menezes-Vanstone cryptosystem.

Životopis

Rođena sam 26. lipnja 1992. godine. u Županji. Od 1999. godine do 2007. godine pohađala sam Osnovnu školu Ivana Kozarca u Županji. Godine 2007. upisala sam Gimnaziju u Županji, smjer prirodoslovna matematička gimnazija. Nakon završene srednje škole upisala sam Preddiplomski studij na Odjelu za matematiku Sveučilišta Josipa Jurja Strossmayera u Osijeku, gdje 2018. godine stječem akademski naziv prvostupnice matematike uz mentorstvo izv.prof.dr.sc Ivana Matića na završnom radu "RSA kriptosustav". Iste godine upisujem Diplomski studij financijske matematike i statistike na Odjelu za matematiku u Osijeku. Na Filozofskom fakultetu u Osijeku 2018. godine upisujem i završavam program pedagoško-psihološko-didaktičko-metodičke izobrazbe.