Koblitzove eliptičke krivulje

Sabljić, Marija

Master's thesis / Diplomski rad

2018

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Science / Sveučilište u Zagrebu, Prirodoslovno-matematički fakultet**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:217:608255

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-10-09**

Repository / Repozitorij:

Repository of the Faculty of Science - University of Zagreb

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Marija Sabljić

KOBLITZOVE ELIPTIČKE KRIVULJE

Diplomski rad

Voditelj rada:
prof. dr. sc. Andrej Dujella

Zagreb, srpanj 2018.g.

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

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

Povjerenstvo je rad ocijenilo ocjenom _____.

Potpisi članova povjerenstva:

1. _____
2. _____
3. _____

Ovaj rad posvećujem svojim roditeljima i sestri.

Veliko hvala mom mentoru prof.dr.sc. Andreju Dujelli na pristupačnosti, uloženom trudu i korisnim savjetima.

Sadržaj

Uvod

Danas, kada su razne informacije lako dostupne, a većina transakcija i povjerljivih podataka putuje nesigurnim komunikacijskim kanalima, gdje postoji mogućnost prisluškivanja i krađe podataka, izazito je važno naći način kojim se podaci mogu zaštititi. Upravo se time bavi kriptografija, koja proučava metode kojima se poruka može poslati drugoj osobi, bez straha da će ju pročitati neka treća osoba. Kriptografija obuhvaća razne metode, no u ovom radu fokus je na primjeni eliptičkih krivulja, posebice, Koblitzovih eliptičkih krivulja. Općenito, eliptičke krivulje imaju povoljno svojstvo da je na njima lako šifrirati poruku, ali bez ključa, neprijatelj teško može dešifrirati sadržaj poruke. O tome će biti govora u sljedećem poglavlju, gdje će se pojasniti problem diskretnog logaritma na eliptičkim krivuljama, na kojem se i zasniva kriptografija eliptičkih krivulja. Koblitzove eliptičke krivulje su eliptičke krivulje posebnog oblika na kojima su izračuni posebno efikasni. Višekratnici točaka lako se mogu izračunati primjenom raznih algoritama, koji će se spomenuti u ovom radu, a koji omogućuju brže računanje i manje memorije. Za ostale eliptičke krivulje računanje višekratnika svodi se na dupliciranje točaka, koje zauzima više memorije i troši više vremena. Zato ne čudi da su Koblitzove eliptičke krivulje u širokoj primjeni gdje je potrebna zaštita podataka, primjerice u državnim agencijama, operacijskim sustavima, pa čak i u Bitcoinu.

U prvom poglavlju rada ukratko će se opisati pojam kriptografije. Navest će se i osnovni pojmovi iz algebarskih struktura koji su nužni za razumijevanje eliptičkih krivulja, kao i problem diskretnog logaritma na eliptičkim krivuljama te Diffie-Hellmanov protokol za razmjenu ključa. U ovom poglavlju korištena je literatura iz algebarskih struktura [10], kriptografije [5] i eliptičkih krivulja u kriptografiji [4]. Također, korišten je članak *"Koblitz curve cryptosystems"* [7] od Tanje Lange te [2]. U drugom poglavlju razrađuju se Koblitzove eliptičke krivulje, nabrajaju njihova svojstva te detaljnije opisuje Frobeniusov endomorfizam, koji zamjenjuje dupliciranje točaka, a zbog kojeg je računanje na tim krivuljama toliko efikasno. U ovom poglavlju korištene su sljedeće knjige: *"Handbook of Elliptic and Hyperelliptic Curve Cryptography"* [3], autora G. Cohena i H. Freya, *"Guide to Elliptic Curve Cryptography"* [6], autora D. Hankersona, A. Menezesa i S. Vanstonea te članak *"Efficient arithmetic on Koblitz curves"* [9] od J. Solinasa. U trećem poglavlju detaljnije se proučavaju različiti prikazi elemenata iz $\mathbb{Z}[\tau]$, kao i algoritmi koji su neophodni

za izračunavanje viškratnika točke, a koji koriste te iste prikaze elemenata. Obrađena je i vrlo važna *metoda prozora*, koja omogućuje brže izračunavanje višekratnika točke. U ovom poglavlju također su korištene već spomenute knjige [6], [3] i [9]. U posljednjem poglavlju ukratko se opisuje gdje se eliptičke krivulje danas koriste te se spominju Koblitzove eliptičke krivulje koje su odabrane kao standard. Za to poglavlje korišten je službeni dokument [1] koji je propisao *National Institute of Standards and Technology*.

Diplomski rad napravljen je u sklopu aktivnosti Projekta KK.01.1.1.01.0004 - Znanstveni centar izvrsnosti za kvantne i kompleksne sustave te reprezentacije Liejevih algebri.

Poglavlje 1

O eliptičkim krivuljama u kriptografiji

1.1 Uvodno o kriptografiji

Kriptografija je znanstvena disciplina koja se bavi proučavanjem metoda kojima se podaci mogu čuvati na sigurnom ili poslati komunikacijskim kanalom uz sigurnost da ih može pročitati samo onaj kome su oni namijenjeni. Želja za sigurnom razmjenom informacija javlja se još kod starih Grka, raste kroz stoljeća, da bi najveći zamah doživjela u 20. stoljeću, kada je u ratnom dobu odigrala značajnu ulogu. Osnovna zadaća kriptografije je osigurati komunikaciju dvjema osobama, koje se u službenoj kriptografskoj literaturi nazivaju Alice i Bob. Ta komunikacija odvija se preko nesigurnog komunikacijskog kanala na kojem postoji mogućnost prisluškivanja, krađe podataka ili sličnog nepovoljnog događaja kojeg može izvršiti protivnik, imena Oskar. Alice će svoju poruku, takozvani *otvoreni tekst*, transformirati koristeći unaprijed dogovoreni ključ. Taj postupak naziva se *šifriranje*, a izmijenjena poruka *šifrat*. Uloga kriptografije je u tome da se poruka, koju Alice želi poslati Bobu toliko transformira da Oskar, kada zaprimi šifrat, može otkriti sadržaj šifrata, ali ne i njegovo značenje prije šifriranja, to jest sadržaj otvorenog teksta. Međutim, Bob zna ključ kojim je poruka šifrirana, pa lako može dešifrirati šifrat i odrediti otvoreni tekst.

U [5] opisane su razne metode za šifriranje poruka kroz povijest, međutim, ovdje će se opisati samo šifriranje s javnim ključem, zbog svoje direktne veze s eliptičkim krivuljama. Za početak treba pojasniti da su *simetrični kriptosustavi* sustavi s tajnim ključem takvi da pošiljatelj i primatelj biraju ključ K koji generira funkciju šifriranja e_K i funkciju dešifriranja d_K. Naravno, taj ključ K se treba često mijenjati, jer šifriranje i dešifriranje velike količine poruka istim ključem znatno smanjuje sigurnost prijenosa poruka. Tu se javlja problem razmjene ključa između dvije osobe, jer i on treba putovati istim nesigurnim komunikacijskim kanalom kao i poruke. Tom problemu doskočili su Whitfield Diffie i Martin Hellman koji su 1976.godine razvili protokol za razmjenu ključeva zasnovan na činjenici da je u nekim grupama potenciranje puno jednostavnije od logaritmiranja. Taj

protokol detaljnije će biti objašnjen u 1.3.

1.2 Eliptičke krivulje nad konačnim poljima

Za početak slijede definicije polja, grupe i prstena, važnih za razumijevanje *problema diskretnog logaritma*, koji će se definirati u nastavku, a zbog kojeg eliptičke krivulje imaju primjenu u kriptografiji.

Definicija 1.2.1. *Neka je G neprazan skup definiran sa $(G, \cdot)$, gdje je $\cdot$ binarna operacija $\cdot : G \times G \to G$. G je grupa ako vrijede sljedeći aksiomi grupe:*

- $(x \cdot y) \cdot z = x \cdot (y \cdot z)$,
- $(\exists e \in G)\ e \cdot x = x \cdot e = x$,
- $(\forall x \in G)(\exists! x^{-1} \in G)\ x \cdot x^{-1} = x^{-1} \cdot x = e$.

Ako vrijedi i $x \cdot y = y \cdot x$, tada je G komutativna (Abelova) grupa.

Definicija 1.2.2. *Skup R definiran sa $(R, +, \cdot)$ zovemo prsten, ako je za operacije zbrajanja $+ : R \times R \to R$ i množenja $\cdot : R \times R \to R$ ispunjeno sljedeće:*

- *$(R, +)$ je komutativna grupa s neutralom 0,*
- *$(\forall x, y \in R)\ x \cdot y \in R$, te je množenje asocijativno,*
- *vrijedi distributivnost množenja prema zbrajanju:*
  $x \cdot (y + z) = x \cdot y + x \cdot z, \quad$ *za sve* $x, y, z \in R$,
  $(x + y) \cdot z = x \cdot z + y \cdot z, \quad$ *za sve* $x, y, z \in R$

Definicija 1.2.3. *Prsten R je tijelo ako je svaki ne-nul element u R invertibilan, to jest, vrijedi $R^* = R \backslash \{0\}$.*

Definicija 1.2.4. *Komutativno tijelo naziva se polje.*

U nastavku rada konačno polje s q elemenata označavat će se s $\mathbb{F}_q$, a koristit će se i oznaka $GF(q)$. $\mathbb{F}_q$ sadrži prosto polje $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, pa je konačno dimenzionalan vektorski prostor nad $\mathbb{F}_p$, te se svaki element iz $\mathbb{F}_q$ može izraziti kao linearna kombinacija elemenata iz $\mathbb{F}_p$. Stoga se svakom elementu može pridružiti k-torka iz $\mathbb{F}_p$, pa je $q = p^k$. Elementi polja $\mathbb{F}_q$ različiti od 0 tvore Abelovu grupu s obzirom na množenje koja se označava sa $\mathbb{F}_q^*$. Ta je grupa *ciklička*, jer je generirana samo jednim elementom $g \in \mathbb{F}_q$ te se svaki element iz $\mathbb{F}_q^*$ može dobiti kao neka potencija od g. Taj element naziva se *generator grupe*.

Definicija 1.2.5. *Grupa G je konačna, ako je G konačan skup. Red grupe je broj elemenata u skupu G, te se označava kao #G.*

Sada slijedi općenita definicija eliptičke krivulje nad konačnim poljem $\mathbb{F}_q$, za $q = p^k$.

Definicija 1.2.6. *Neka je E eliptička krivulja nad poljem $\mathbb{F}_q$, za $q = p^k$. Definiramo njen oblik na sljedeći način: ako je $p > 3$, tada je E oblika $y^2 = x^3 + ax + b$. Ako je $p = 3$, tada E ima oblik $y^2 = x^3 + ax^2 + bx + c$. Za $p = 2$, može imati jedan od ova dva oblika: $y^2 + cy = x^3 + ax + b$ ili $y^2 + xy = x^3 + ax^2 + b$.*

Eliptička krivulja E nad poljem $\mathbb{F}_{2^d}$ označava se sa $E(\mathbb{F}_{2^d})$.

Definicija 1.2.7. *Neka je E eliptička krivulja te P i Q točke na E definirane kao $P = (x_1, y_1)$ i $Q = (x_2, y_2)$. Operacije na eliptičkoj krivulji definiraju se na sljedeći način:*

- $-P_\infty = P_\infty$,
- $-P = (x_1, -y_1)$,
- $P_\infty + P = P$,
- *ako je $Q = -P$, onda je $P + Q = P_\infty$*
- *ako je $Q \neq -P$, onda je $P+Q = (x_3, y_3)$, gdje su $x_3 = \lambda^2 - x_1 - x_2$, $y_3 = -y_1 + \lambda(x_1 - x_3)$ te*

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

Potrebno je pojasniti pojam tzv. *točke u beskonačnosti*, koja se u gornjoj definiciji označava sa P_∞, a pojavljuje se kada se eliptička krivulja prikaže u projektivnoj ravnini $\mathbb{P}^2(\mathbb{K})$. Dakle, na skupu $\mathbb{K}^3 \backslash \{0, 0, 0\}$, gdje je $\mathbb{K}$ neko polje, uvodi se relacija ekvivalencije $(X, Y, Z) \sim (kX, kY, kZ)$ za $k \in \mathbb{K}$, $k \neq 0$. Tada se uz supstituciju $x = \frac{X}{Z}$ te $y = \frac{Y}{Z}$, dobiva projektivna jednadžba $Y^2Z = X^3 + aXZ^2 + bZ^3$, te su točke za koje je $Z = 0$ upravo točke klase ekvivalencije koja ima reprezentant $(0, 1, 0)$, što je točka P_∞.

1.3 Problem diskretnog logaritma

Problem diskretnog logaritma, skraćeno DLP, definira se na ovaj način:

Neka je $(G, *)$ konačna grupa, $g \in G$, $H = \{g^i : i > 0\}$ podgrupa od G generirana s g, te $h \in H$. Treba naći najmanji nenegativni cijeli broj x takav da je $h = g^x$, gdje je $g^x = g * g * ... * g$. Taj broj x naziva se diskretni logaritam i označava se s $\log_g h$.

Diffie i Hellman su se, pri razvoju rješenja za problem sigurne razmjene ključeva, oslonili upravo na činjenicu da je za neke grupe problem diskretnog logaritma vrlo težak. Za grupu G uzima se multiplikativna grupa $\mathbb{F}_q^*$ svih ne-nul ostataka modulo q, te se pogodnim grupama smatraju one kod kojih je za $\mathbb{F}_q^*$ broj q dovoljno velik i prost te kod kojih $q - 1$ ima barem jedan veliki prosti faktor.

Za eliptičke krivulje važnija je varijanta problema diskretnog logaritma koja se naziva problem diskretnog logaritma za eliptičke krivulje, skraćeno ECDLP.

Neka je E eliptička krivulja nad konačnim poljem K. Neka su točke $P, Q \in E(K)$ takve da je točka Q element podgrupe od $E(K)$ generirane točkom P. Treba odrediti k za kojeg vrijedi $Q = kP$, odnosno $\underbrace{Q = P + P + ... + P}_{k \text{ puta}}$.

Taj problem je razlog zbog kojeg su eliptičke krivulje toliko proučavane u kriptografiji i zbog čega se koriste i danas. Naime, zbog posebnog načina računanja višekratnika točke i svojstva da sve točke čine cikličku grupu, za dovoljno veliki k protivniku je gotovo nemoguće riješiti problem ECDLP u nekom razumnom vremenu. Treba napomenuti da je problem DLP u grupi $E(\mathbb{F}_{2^d})$ još teži od problema DLP u $\mathbb{F}_q^*$. U grupi $\mathbb{F}_q^*$ postoji subeksponencijalni algoritam za rješavanje problema DLP pod nazivom *index calculus metoda*, koja se detaljnije može pogledati u [4]. Ukratko, za danu cikličku grupu G reda n i generator g, računa se diskretni logaritam $log_g h$ proizvoljnog elementa h iz grupe G. Međutim, kod eliptičkih krivulja takva metoda se ne može primijeniti jer je teško naći eliptičku krivulju nad $\mathbb{Q}$ velikog ranga, teško je naći eliptičku krivulju generiranu točkama s malim brojnicima i nazivnicima te je te teško "podići" točke iz$E(\mathbb{F}_q)$ do točaka iz $E(\mathbb{Q})$. Trenutno ne postoji niti polinomijalni niti subeksponencijalni algoritam za rješavanje problema ECDLP.

Kao što je ranije spomenuto, u ovom odjeljku definirat će se Diffie-Hellmanov protokol za razmjenu ključeva, primjenjen na eliptičke krivulje.

Diffie-Hellmanov protokol za razmjenu ključeva

Alice i Bob žele komunicirati porukama preko nesigurnog komunikacijskog kanala. Zajedno se dogovaraju o eliptičkoj krivulji E koju će koristiti i o točki $P \in E(\mathbb{F}_{2^d})$. Protokol se odvija na sljedeći način:

1. Alice generira slučajan prirodan broj $k_A \in \{1, 2, ..., \#E - 1\}$. Zatim, računa element $P_A = k_A P$.
2. Bob generira slučajan prirodan broj $k_B \in \{1, 2, ..., \#E - 1\}$. Zatim, računa element

$P_B = k_B P$.
3. Alice i Bob razmjenjuju P_A i P_B.
4. Alice izračuna $P_{AB} = k_A P_B$.
5. Bob izračuna $P_{AB} = k_B P_A$.

Dakle, i Alice i Bob odabrali su svoje privatne ključeve k_A i k_B, koje nisu direktno izmijenili komunikacijskim kanalom, već u sklopu poruka P_A i P_B. Na taj način, njihovi privatni ključevi ostali su sigurni. Ukoliko prisluškuje, njihov protivnik Oskar može saznati jedino elemente E, P, P_A i P_B. Međutim, ono što Oskaru treba za napad je broj P_{AB}, to jest, treba mu ili k_A ili k_B. No, u svakom slučaju, on za to treba riješiti problem diskretnog logaritma kako bi se iz P_A domogao k_A ili P_B kako bi se domogao k_B.

Većina protokola za kriptografiju javnog ključa oslanja se upravo na upotrebu cikličkih grupa. Smatra se da je odabir grupe povoljan ako su operacije množenja i potenciranja u njoj lake za izračunati, ako se red grupe može efikasno izračunati te, najvažnije, da je diskretni logaritamski problem teško izračunati. Primjerice, tu se ubrajaju i eliptičke krivulje, jer trenutno ne postoji subeksponencijalni algoritam koji bi riješio DLP na krivuljama reda ≤ 3. Također, na eliptičkim krivuljama postoje eksplicitne formule za zbrajanje i udvostručavanje, zbog čega su izrazito praktične u primjeni, a ako se još k tome koriste i specijalne eliptičke krivulje, poput Koblitzovih eliptičkih krivulja, kriptosustavi temeljeni na krivuljama značajno se mogu ubrzati. Koblitzove eliptičke krivulje, kako će se pokazati u nastavku ovog rada, definirane su na malom konačnom polju te se promatraju na njegovom proširenom polju, koristi se Frobeniusov endomorfizam, te se izračuni znatno ubrzavaju.

Poglavlje 2

Koblitzove eliptičke krivulje

2.1 Otkriće Koblitzovih eliptičkih krivulja

Kako bi ubrzali izračune na eliptičkim krivuljama, 1990. godine Alfred J. Menezes i Scott A. Vanstone po prvi puta u tu svrhu rabe Frobeniusov endomorfizam.

Definicija 2.1.1. *Frobeniusov endomorfizam τ nad eliptičkom krivuljom E definiranom nad poljem $\mathbb{F}_{2^d}$, je preslikavanje $\tau : E(\mathbb{F}_{2^d}) \rightarrow E(\mathbb{F}_{2^d})$ koje (x_1, y_1) preslikava u $({x_1}^2, {y_1}^2)$, dok točku P_∞ preslikava u sebe samu.*

Za taj pokušaj koristili su eliptičku krivulju $y^2 + y = x^3$ nad poljem $\mathbb{F}_{2^d}$. Karakteristični polinom tog Frobeniusovog endomorfizma, nadalje označen s ϕ_2, glasi:

$$\chi_E(T) = \phi_2(T) = T^2 + 2.$$

Ovime je udvostručavanje točaka zamijenjeno dvostrukom primjenom Frobeniusova endomorfizma i uzimanjem negativne vrijednosti, jer za svaku točku $P \in E(\mathbb{F}_{2^d})$ vrijedi:

$${\phi_2}^2(P) = -2[P].$$

Iako je ova ideja dovela do brojnih efikasnih implementacija, eliptička krivulja E je supersingularna, a time i slaba, jer ne pruža dovoljnu sigurnost za kriptografske primjene. Upravo iz tog razloga Neil Koblitz 1992. godine predlaže korištenje dviju ne-supersingularnih eliptičkih krivulja definiranih nad poljem $\mathbb{F}_2$. Zbog svojstva ne-supersingularnosti, krivulja je "zaštićena" od Menezes-Okamoto-Vanstone (MOV) napada. Zbog svog svojstva efikasnog množenja skalarom, koje je Koblitz prvi uspio pokazati, krivulje dobivaju ime njemu u čast.

2.2 O Koblitzovim eliptičkim krivuljama

Definicija 2.2.1. *Koblitzove eliptičke krivulje su krivulje definirane nad GF*(2)*, odnosno nad* $\mathbb{F}_2$ *kao:*

$$E_{a_2} : y^2 + xy = x^3 + a_2x^2 + 1, \quad uz\ a_2 = 0\ ili\ 1 \tag{2.1}$$

Koblitzove eliptičke krivulje imaju poželjno svojstvo za primjenu u kriptografiji, što će se uskoro i pokazati. Naime, omogućuju lako izračunavanje višekratnika točke korištenjem zbrajanja i Frobeniusovog endomorfizma.

U kriptografskim primjenama, koriste se grupe $E_0(\mathbb{F}_{2^d})$ i $E_1(\mathbb{F}_{2^d})$ s točkama definiranim nad proširenim poljem $\mathbb{F}_{2^d}$. Zbog svojih pogodnih svojstava, na njima se izvode, primjerice, protokoli s javnim ključem. Međutim, vrlo je važno da se te grupe biraju tako da je "protivniku" teško izračunati diskretni logaritam elemenata, a time i onemogućiti pronalazak ključa za šifriranje.

Definicija 2.2.2. *Koblitzova krivulja* E_{a_2} *ima skoro prost red grupe nad poljem* $\mathbb{F}_{2^d}$ *ako* $\#E_{a_2}(\mathbb{F}_{2^d}) = cN$*, gdje je N prost broj, a c je definiran na sljedeći način:*

$$c = \begin{cases} 4, & ako\ a = 0 \\ 2, & ako\ a = 1. \end{cases}$$

c još nazivamo i kofaktor.

Napomena 2.2.3. *Za* $a_2 \in \{0, 1\}$ *i za djelitelj l od d, vrijedi da je* $E_{a_2}(\mathbb{F}_{2^l})$ *podgrupa grupe* $E_{a_2}(\mathbb{F}_{2^d})$*, pa zato* $\#E_{a_2}(\mathbb{F}_{2^l})$ *dijeli* $\#E_{a_2}(\mathbb{F}_{2^d})$*.*

Za kriptografske primjene, red $\#E_{a_2}(\mathbb{F}_{2^d})$ mora biti djeljiv s velikim prostim brojem, jer se na takvu eliptičku krivulju ne može primijeniti Pohlig-Hellmanova metoda redukcije. Idealno bi bilo kada bi sam red $\#E_{a_2}(\mathbb{F}_{2^d})$ bio prost broj ili produkt prostog broja i malog cijelog broja, međutim to se može dogoditi samo ako je d prost.
Takoder, treba naglasiti da $\#E_{a_2}(\mathbb{F}_{2^d})$ nikad nije prost za $d > 1$, ali je zato često skoro prost. U skladu s definicijom 2.2.2, poznato je da se $\#E_{a_2}(\mathbb{F}_{2^d})$ može prikazati kao umnožak kofaktora iz skupa $\{2, 4\}$, ovisno o obliku eliptičke krivulje i prostog broja N. U sljedećoj tablici navedene su sve vrijednosti $d < 512$ za koje će red $\#E_{a_2}(\mathbb{F}_{2^d})$ biti moguće prikazati kao "dva puta N", odnosno "četiri puta N".

Tablica 2.1: Stupnjevi d

a_2	Stupanj d
0	5, 7, 13, 19, 23, 41, 83, 97, 103, 107, 131, 233, 239, 277, 283, 349, 409, 571
1	3, 5, 7, 11, 17, 19, 23, 101, 107, 109, 113, 163, 283, 311, 331, 347, 359

Kasnije će se pokazati koji su stupnjevi d od navedenih u tablici najpovoljniji za kriptografske primjene.

2.3 Problem računanja višekratnika točke

Za eliptičke krivulje definirane nad $\mathbb{F}_{2^d}$, a tada i za Koblitzove eliptičke krivulje, koje su definirane nad $\mathbb{F}_2$, vrijedi i sljedeće svojstvo:
ako je $P = (x, y)$ točka na eliptičkoj krivulji $E_{a_2}(\mathbb{F}_{2^d})$, tada je na toj krivulji i točka (x^2, y^2). Štoviše, vrijedi da je:

$$(x^4, y^4) + 2(x, y) = \mu \cdot (x^2, y^2), \quad \textit{za svaki } (x, y) \textit{ na } E_{a_2}(\mathbb{F}_{2^d}), \tag{2.2}$$

gdje vrijedi da je $\mu = (-1)^{(1-a_2)}$. Međutim, jednadžba prikazana u (2.2) može se jednostavnije napisati koristeći već spomenuti Frobeniusov endomorfizam:

$$\tau(\tau P) + 2P = \mu\tau P, \quad \textit{za svaki } P \textit{ na } E_{a_2}(\mathbb{F}_{2^d})$$

Ili, urednije zapisano:

$$(\tau^2 + 2)P = \mu\tau P, \quad \textit{za svaki } P \textit{ na } E_{a_2}(\mathbb{F}_{2^d})$$

Karakteristični polinom Frobeniusovog endomorfizma za ove dvije krivulje tada glasi:

$$\chi_{a_2}(T) = T^2 - \mu T + 2, \tag{2.3}$$

gdje uzimamo da je $\mu = (-1)^{1-a_2}$. Iz karakterističnog polinoma dobivamo sljedeći izraz:

$$[2]P = [\mu]\phi_2(P) \ominus {\phi_2}^2(P), \tag{2.4}$$

koji pokazuje da se udvostručavanje točaka lako može zamijeniti primjenom operacija s Frobeniusovim endomorfizmom.

Na idućim primjerima prikazano je kako se višekratnici proizvoljne točke P jednostavnije mogu izraziti preko Frobeniusovog endomorfizma, nego množenjem točaka na eliptičkoj krivulji. Za višekratnik $[k]P$ točke P kao k uzete su potencije broja 2 (to jest 2, 4, 8 i 16), a kao koeficijent a_2 odabran je 1:

$$\begin{aligned}
[2]P &= \phi_2(P) \ominus {\phi_2}^2(P) \\
[4]P &= -{\phi_2}^2(P) \ominus {\phi_2}^3(P) \\
[8]P &= -{\phi_2}^3(P) \oplus {\phi_2}^5(P) \\
[16]P &= {\phi_2}^4(P) \ominus {\phi_2}^8(P)
\end{aligned}$$

U gornjim jednadžbama korištene su oznake $\oplus$ i $\ominus$. Za proizvoljne točke $P = (p_1, p_2)$ i $Q = (q_1, q_2) \in E_{a_2}(\mathbb{F}_{2^d})$, sa $P \oplus Q$ označava se izraz: $P \oplus Q = (p_1, p_2) \oplus (q_1, q_2) = (p_1 + q_1, p_2 + q_2)$. Analogno, sa $P \ominus Q$ označava se izraz: $P \ominus Q = (p_1, p_2) \ominus (q_1, q_2) = (p_1 - q_1, p_2 - q_2)$. Izraz iz (2.3) može se zapisati i preko kompleksnog broja τ koji zadovoljava jednadžbu:

$$\tau^2 + 2 = \mu\tau, \tag{2.5}$$

pa se uzima da je $\tau = (\mu + \sqrt{-7})/2$. Njegovo kompleksno konjugirano rješenje glasi: $\overline{\tau} = (\mu - \sqrt{-7})/2$.

Neka $\mathbb{Z}[\tau]$ označava prsten polinoma od τ s cjelobrojnim koeficijentima. Množenje točaka na eliptičkoj krivulji $E_{a_2}(\mathbb{F}_{2^d})$ s elementima prstena $\mathbb{Z}[\tau]$ definira se na ovaj način: ako su $u_{l-1}\tau^{l-1} + \ldots + u_1\tau + u_0 \in \mathbb{Z}[\tau]$ i $P \in E_{a_2}(\mathbb{F}_{2^d})$, tada vrijedi:

$$(u_{l-1}\tau^{l-1} + \cdots + u_1\tau + u_0)\, P = u_{l-1}\tau^{l-1}\,(P) + \cdots + u_0\,(P). \tag{2.6}$$

Na taj način, može se izračunati točka $[k]P$ za prirodni broj k na Koblitzovoj eliptičkoj krivulji $E_{a_2}(\mathbb{F}_{2^d})$. Međutim, efikasnost ovog algoritma uvelike ovisi o raspisu prirodnog broja k. Naime, smatra se da je izraz $k = \sum_{i=0}^{l-1} u_i\tau^i$ „dobar“ ako mu je l relativno malen, a znamenke u_i, koje su različite od nule, su male i raspršene unutar zapisa (primjerice znamenke ± 1) .

2.4 Svojstva prstena $\mathbb{Z}[\tau]$

Korištenjem formule $\tau^2 = \mu\tau - 2$ svaki se element $\eta \in \mathbb{Z}[\tau]$ može izraziti u kanonskoj formi $\eta = n_0 + n_1\tau$, gdje su $n_0, n_1 \in \mathbb{Z}[\tau]$. Također, svakom se elementu $\eta = n_0 + n_1\tau$ može pridružiti forma od η (prema propoziciji 2.77 iz [3]), iskazana sljedećom definicijom.

Definicija 2.4.1. *Norma od $\eta = n_0 + n_1\tau \in \mathbb{Z}[\tau]$ je produkt η i njegovog kompleksnog konjugata $\overline{\eta}$:*

$$N(n_0 + n_1\tau) = {n_0}^2 + \mu n_0 n_1 + 2{n_1}^2.$$

Norma ima sljedeća svojstva:

- $N(\alpha) \geq 0$ za svaki $\alpha \in \mathbb{Z}[\tau]$ te vrijedi $N(\alpha) = 0$ ako i samo ako $\alpha = 0$.
- 1 i -1 su jedini elementi prstena $\mathbb{Z}[\tau]$ s normom 1.
- $N(\tau) = 2$ i $N(\tau - 1) = c$, gdje je c kao u Definiciji 2.2.2.
- $N(\tau^d - 1) = \#E_{a_2}(\mathbb{F}_{2^d})$ i $N((\tau^d - 1)/(\tau - 1)) = N$, gdje je N kao u Definiciji 2.2.2.
- Norma ima multiplikativno svojstvo, to jest $N(\alpha_1\alpha_2) = N(\alpha_1)N(\alpha_2)$ za sve $\alpha_1,\ \alpha_2 \in \mathbb{Z}[\tau]$.

- Za normu vrijedi nejednakost trokuta, to jest $\sqrt{N(\alpha_1 + \alpha_2)} \leq \sqrt{N(\alpha_1)} + \sqrt{N(\alpha_2)}$, za sve $\alpha_1,\ \alpha_2 \in \mathbb{Z}[\tau]$.
- za sve $\alpha,\ \beta \in \mathbb{Z}[\tau]$ uz $\beta \neq 0$, postoje $\eta,\ \rho \in \mathbb{Z}[\tau]$ (ne nužno jedinstveni) takvi da vrijedi $\alpha = \eta\beta + \rho$ i $N(\rho) < N(\beta)$.

2.5 Lucasovi nizovi

U klasičnoj teoriji brojeva koriste se Lucasovi nizovi koji se pridružuju kvadratnim polinomima. U ovom slučaju se, primjenom formule (2.3) , dobiva sljedeća rekurzivna formula:

$$L_{k+1} = \mu L_k - 2L_{k-1}, \quad za\ k \geq 1. \tag{2.7}$$

Prva dva elementa niza $(U_k)_{k\geq 0}$ definiramo kao:

$$U_0 = 0,\ U_1 = 1, \tag{2.8}$$

a prva dva elementa niza $(V_k)_{k\geq 0}$ kao:

$$V_0 = 2,\ V_1 = \mu. \tag{2.9}$$

$(U_k)_{k\geq 0}$ i $(V_k)_{k\geq 0}$ zadovoljavaju rekuziju definiranu u (2.7), pa se ostali elementi računaju iz nje. Slijede još dva rekurzivna izraza, koja će biti korisna u nastavku:

$$\tau^k = -2U_{k-1} + U_k\tau \tag{2.10}$$

$$\tau^k + \overline{\tau}^{\,k} = -2V_{k-1} + V_k\tau \tag{2.11}$$

Pomoću drugog rekurzivnog izraza (2.11) dobije se rekurzivna formula iz koje se izračuna kardinalnost od $E_{a_2}(\mathbb{F}_{2^d})$:

$$\#E_{a_2}(\mathbb{F}_{2^d}) = (1 - \tau^d)(1 - \overline{\tau}^{\,d}) = 2^d + 1 - (\tau^d + \overline{\tau}^{\,d}) = 2^d + 1 - V_d. \tag{2.12}$$

Međutim, za izračunavanje reda grupe možemo koristiti i rastav iz definicije 2.2.2. Ovdje će vrijediti: $c = \#E_{a_2}(\mathbb{F}_{2^d}) = N(\tau - 1)$, a $N = N(\delta)$, gdje je $\delta = \dfrac{\tau^d - 1}{\tau - 1}$. U praksi, najvažnije je naći prošireno polje $\mathbb{F}_{2^d}$ s velikom podgrupom od $E_{a_2}(\mathbb{F}_{2^d})$ prostog reda. No to nije teško, jer je broj N iz definicije 2.2.2 prost za većinu proširenih polja sa stupnjem d. U sljedećoj tablici navedeni su povoljni stupnjevi za kriptografske primjene.

Tablica 2.2: Povoljni stupnjevi d

a_2	Stupanj d
0	233, 239, 277, 283, 349, 409, 571
1	163, 283, 311, 331, 347, 359

Poglavlje 3

Prikazi elemenata u $\mathbb{Z}[\tau]$

3.1 τ-prikaz

Definicija 3.1.1. *Analogno binarnom prikazu, definiramo τ-prikaz od $\eta \in \mathbb{Z}[\tau]$ kao*

$$\eta = \sum_{i=0}^{l-1} r_i \tau^i, \tag{3.1}$$

gdje su $r_i \in \{0, 1\}$, za svaki i. τ-prikaz se označava se s: $(r_{l-1} \ldots r_0)_\tau$.

Pojednostavljeno, τ-prikaz nekog elementa $\eta \in \mathbb{Z}[\tau]$ definiranog kao $\eta = n_0 + n_1\tau$ može se postići dijeljenjem n_0 s 2, krenuvši od najmanje značajne znamenke. Postupak je sličan binarnom rastavu, samo što se broj 2 zamjenjuje izrazom $\mu\tau - \tau^2$. Ostaci koji se dobiju predstavljaju koeficijente, pa slijedi da svaki $\eta \in \mathbb{Z}[\tau]$ ima jedinstveni τ-prikaz.

Primjer 3.1.2. *Sljedeće jednadžbe pokazuju nastanak τ-prikaza broja 5, uz pretpostavku da je μ =1.*

$$\begin{aligned} 5 &= 1 + 2 \cdot 2 = \\ &= 1 + (\tau - \tau^2) \cdot (\tau - \tau^2) = \\ &= 1 + (\tau - \tau^2) \cdot (\tau - \tau^2) = \\ &= 1 + \tau^2 - (\tau - \tau^2) \cdot \tau^3 + \tau^4 = \\ &= 1 + \tau^2 + \tau^5 \end{aligned}$$

Pomoću τ-prikaza, za neku točku P na eliptičkoj krivulji $E_{a_2}(\mathbb{F}_{2^d})$ možemo izračunati točku nastalu skalarnim množenjem točke P s k, tj $[k]P$. Pritom se τ-prikaz izražava u

obliku Frobeniusovog endomorfizma uz operacije među njima. Primjerice, za točku P na eliptičkoj krivulji $E_1(\mathbb{F}_{2^d})$, točku $[5]P$ možemo lako izračunati preko izraza:

$$[5]P = P \oplus \phi_2(P)^2 \oplus \phi_2{}^5(P).$$

Na složenost tog izračuna utječe broj koeficijenata različitih od 0 u τ-prikazu, jer se za te koeficijente izvode zbrajanja. Raspršeniji prikaz od ranije navedenog ima τ-prikaz s predznakom, takozvani τNAF prikaz, kojeg je predložio Neil Koblitz. τNAF prikaz vrlo je sličan NAF prikazu, koji se detaljnije može pogledati u [3].

3.2 τNAF prikaz

Definicija 3.2.1. *Element $\eta = n_0 + n_1\tau \in \mathbb{Z}[\tau]$ ima τ-nesusjedni prikaz, skraćeno, τNAF ili TNAF, ako vrijedi*

$$\eta = \sum_{i=0}^{l-1} r_i \tau^i, \tag{3.2}$$

uz dodatne uvjete da su $r_i \in \{0, \pm 1\}$ i $r_i r_{i+1} = 0$ za svaki i. τNAF se označava kao: $(r_{l-1} \ldots r_0)_{\tau NAF}$. Duljina τNAF prikaza tada iznosi l .

Važno je napomenuti da svaki $\eta \in \mathbb{Z}[\tau]$ ima jedinstveni τNAF prikaz. U sljedećem teoremu nabrojana su i dokazana svojstva τNAF prikaza.

Teorem 3.2.2. *Neka je $\eta \in \mathbb{Z}[\tau]$ te $\eta \neq 0$.*

(i) Vrijedi: $\log_2(N(\eta)) - 0.55 < l(\eta) < \log_2(N(\eta)) + 3.52$, za η čija je duljina $l(\eta) > 30$

(ii) Omjer znamenaka različitih od 0 i znamenaka 0 je u svakom τNAF prikazu duljine n otprilike jednak $1/3$.

Dokaz. (i) Neka je $l > 2d$ i η element iz $\mathbb{Z}[\tau]$ duljine l. Vrijedi (iz [9]):

$$\left(\sqrt{N_{min}(d)} - \frac{\sqrt{N_{max}(d)}}{2^{d/2} - 1} \right)^2 \cdot 2^{l-d} < N(\eta) < \frac{N_{max}(d)}{2^{d/2} - 1^2} \cdot 2^l.$$

Uzet ćemo mali d i ocijeniti $N_{min}(d)$ i $N_{max}(d)$ za svaki element iz $\mathbb{Z}[\tau]$ duljine d. Neka je d=15. Tada su:

$$N_{min}(15) = 2996, \ a \ N_{max}(15) = 47324.$$

Uvrštavanjem i računanjem, dolazi se do izraza:

$$1.399009614 \cdot 2^{l-4} < N(\eta) < 0.7301517653 \cdot 2^{l+1}$$

To jest, za $l > 30$ vrijedi.

$$\log_2(N(\eta)) - 0.5430352713 < l(\eta) < \log_2(N(\eta)) + 3.51559412,$$

što je upravo tvrdnja teorema.

(ii) Omjer znamenaka različitih od 0 i znamenaka 0 za obični NAF prikaz duljine n je $\frac{2^n(3n-4)-(-1)^n(6n-4)}{9(n-1)(2^n-(-1)^n)}$, što je približno 1/3. Isti omjer vrijedi i za τNAF prikaz duljine n, pa rezultat slijedi iz dokaza u [9].

□

Napomena 3.2.3. *Broj elemenata niza koji su različiti od 0 naziva se još i Hammingova težina.*

Algoritmom 1 bit će pokazano da se τNAF prikaz može efikasno izračunati, te da je sličan algoritmu za izračunavanje običnog NAF prikaza. Dijeljenjem η s τ dobivaju se ostaci 0, 1 ili -1, koji čine elemente τNAF prikaza. U slučaju da η nije djeljiv s τ, odabire se ostatak r iz skupa $\{-1, 1\}$ tako da je izraz $(\eta - r)/\tau$ djeljiv s τ, što osigurava da je sljedeća τNAF znamenka jednaka 0. Sljedeći teorem opisuje uvjete pod kojima se $\eta \in \mathbb{Z}[\tau]$ može podijeliti s τ i τ^2.

Teorem 3.2.4. *(dijeljenje s* τ *i* τ^2 *u* $\mathbb{Z}[\tau]$ *) Neka je* $\eta = n_0 + n_1\tau \in \mathbb{Z}[\tau]$.

(i) η *je djeljiv s* τ *ako i samo ako je* n_0 *paran. Tada još vrijedi:*

$$\eta/\tau = (n_1 + \mu n_0/2) - (n_0/2)\tau. \tag{3.3}$$

(ii) η *je djeljiv s* τ^2 *ako i samo ako vrijedi:* $n_0 \equiv 2n_1 \pmod 4$.

Dokaz. (i) $\Rightarrow$ Svaki višekratnik od τ ima sljedeći oblik:

$$(d_0 + d_1\tau)\tau = -2d_1 + (d_0 + \mu d_1)\tau.$$

Slijedi:

$$\begin{aligned} n_0 &= -2d_1, \\ n_1 &= d_0 + \mu d_1. \end{aligned}$$

Očito, n_0 je paran.
$\Leftarrow$ Pretpostavimo da je n_0 paran. Tada slijedi da je:

$$\frac{n_0 + n_1\tau}{\tau} = \frac{\mu n_0 + 2n_1}{2} - \frac{n_0}{2}\tau$$

element iz $\mathbb{Z}[\tau]$ i da je $n_0 + n_1\tau$ djeljiv s τ.

(ii) $\Rightarrow$ Svaki višekratnik od τ^2 ima sljedeći oblik:

$$(d_0 + d_1\tau)(\mu\tau - 2) = -2(d_0 + \mu d_1) + (\mu d_0 - d_1)\tau,$$

iz čega slijedi da su vrijednosti n_0 i n_1:

$$n_0 = -2(d_0 + \mu d_1),$$
$$n_1 = \mu d_0 - d_1.$$

Za n_0 očito vrijedi da zadovoljava tvrdnju iz (ii).
$\Leftarrow$ Pretpostavimo da vrijedi $n_0 \equiv 2n_1 (\text{mod } 4)$. Tada slijedi da je:

$$\frac{n_0 + n_1\tau}{\tau^2} = -\frac{(1 + 2\mu)n_0 + 2\mu n_1}{4} + \mu \cdot \frac{n_0 - 2n_1}{4}\tau$$

element iz $\mathbb{Z}[\tau]$ i da je $n_0 + n_1\tau$ djeljiv s τ^2.

□

Slijedi algoritam 1 za izračun τNAF prikaza.

Algoritam 1: Izračunavanje τNAF prikaza elementa iz $\mathbb{Z}[\tau]$

Ulaz: element $\eta = n_0 + n_1\tau \in \mathbb{Z}[\tau]$
Izlaz: τNAF prikaz $(r_{l-1} \dots r_0)_{\tau NAF}$ od η

```
1  i = 0;
2  while n_0 ≠ 0 ili n_1 ≠ 0 do
3      if n_0 ≡ 1(mod 2) then
4          r_i = 2 − ((n_0 − 2n_1) mod 4));
5          n_0 = n_0 − r_i;
6      else
7          r_i = 0;
8      t = n_0;
9      n_0 = n_1 + μn_0/2;
10     n_1 = −t/2;
11     i = i + 1;
12 return (r_{l−1} ... r_0)
```

Primjer 3.2.5. Neka je $\mu = 1$ te $\eta = 7 \in \mathbb{Z}[\tau]$. Pomoću Algoritma 1, lako se dobije τNAF prikaz od 7:

$$7 = (1, 0, 0, \overline{1})_{\tau NAF}$$

S druge strane, τ-prikaz od 7 je:

$$7 = (1, 0, 0, 0, 1, 1)_\tau$$

Dakle, u ovom slučaju je τNAF prikaz kraći od τ-prikaza, te je broj jedinica manji. Inače, može se dogoditi da su τNAF prikaz i τ-prikaz iste duljine, ali će zasiguno τNAF prikaz biti raspršeniji od τ-prikaza, odnosno, broj ne-nul elemenata bit će manji.

Za izračunavanje točke $[k]P$, potrebno je prvo naći τNAF prikaz i zatim iskoristiti izraz naveden u (2.5). Iz teorema 3.2.4 slijedi da je duljina τNAF-a otprilike $\log_2(N(k)) = 2\log_2 k$, što je dvostruko veće od duljine običnog NAF-a.

Zbog toga se sve prednosti dobivene eliminiranjem udvostručavanja točaka i uvođenjem Frobeniusovog endomorfizma pri računanju višekratnika točke umanjuju, jer se broj elemenata različitih od nule povećao, što znači da se povećao i broj operacija.

U idućem potpoglavlju objašnjeno je kako se ta duljina može reducirati, a da povoljna svojstva ostanu nepromijenjena. Štoviše, pokazat će se da će duljina τNAF prikaza reducirane vrijednosti od n biti dvaput manja od duljine τNAF prikaza za vrijednost n te iste duljine kao i binarni zapis od n.

3.3 Reduciranje duljine τNAF prikaza

Neka je P točka na eliptičkoj krivulji $E_{a_2}(\mathbb{F}_{2^d})$. Kako bi se izbjegao problem predugačkog τNAF prikaza, koristi se sljedeći zaključak:

$$ako\ je\ n \equiv\ \eta\ (\mathrm{mod}\ (\tau^d - 1)),\ onda\ je\ [n]P\ =\ [\eta]P.$$

To vrijedi jer je ${\phi_2}^d$ identiteta, pa:

$$(\tau^d - 1)(P) = \tau^d(P) - P = P - P = \infty.$$

Ranije je definirano da je $\#E_{a_2}(\mathbb{F}_{2^d}) = cN$, uz $c = 2$ ili 4. Ako postoji točka Q takva da je $P = [c]Q$, tada se, za računanje $[n]P$, vrijednost n može reducirati modulo $\delta = (\tau^d - 1)/(\tau - 1)$. To vrijedi zbog svojstava norme: $N(\tau - 1) = c$, $N(\tau^d - 1) = \#E_{a_2}(\mathbb{F}_{2^d})$ i $N((\tau^d - 1)/(\tau - 1)) = N$.

Stoga slijedi da za $\rho = n(\mathrm{mod}\ (\delta))$ možemo izračunati reducirani τNAF- prikaz te vrijedi: $R\tau NAF(n) = \tau NAF(\rho)$, gdje je $R\tau NAF$ oznaka za reducirani τNAF prikaz.

Sada je cilj pronaći takav $\rho \in \mathbb{Z}[\tau]$, s najmanjom mogućom normom, za koji također vrijedi sljedeće: ako je $n \equiv \rho(\mathrm{mod}\ (\delta))$ (to jest $n = \kappa\delta + \rho$), onda je:

$$\begin{aligned}[n]P &= [\kappa][\delta]P \oplus [\rho]P = \\ &= \left\{ zbog\ [\delta]P = P_\infty,\ pa\ je\ i\ [k]P_\infty = P_\infty \right\} \\ &= [\rho]P.\end{aligned}$$

U praksi, za izračun ρ, zbog $n \equiv \rho(\mathrm{mod}\ (\delta))$, prvo treba odrediti δ. Već je poznato da je $\delta = (\tau^d - 1)/(\tau - 1)$, pa za daljnji raspis koristimo Lucasove nizove $(U_k)_{k\geq 0}$

$$\begin{aligned}
\delta = (\tau^d - 1)/(\tau - 1) = &\quad \left\{ zbog\ \tau^d = -2U_{d-1} + U_d\tau \right\} = \\
= (-2U_{d-1} + U_d\tau - 1)/(\tau - 1) = &\quad \left\{ zbog\ c = (\tau - 1)(\overline{\tau} - 1) \right\} = \\
= (-2U_{d-1} + U_d\tau - 1)(\overline{\tau} - 1)/c = &\quad \left\{ zbog\ \mu = \tau + \overline{\tau} \right\} = \\
= ((2 - 2\mu)U_{d-1} + 2U_d - \mu + 1 + (2U_{d-1} - U_d + 1)\tau)/c = & \\
= \delta_0 + \delta_1\tau. &
\end{aligned} \tag{3.4}$$

Dakle, δ se može prikazati kao kombinacija $\delta_0 + \delta_1\tau$, gdje su:

$$\delta_0 = \frac{(2 - 2\mu)U_{d-1} + 2U_d - \mu + 1}{c},$$

$$\delta_1 = \frac{(2U_{d-1} - U_d + 1)\tau}{c}.$$

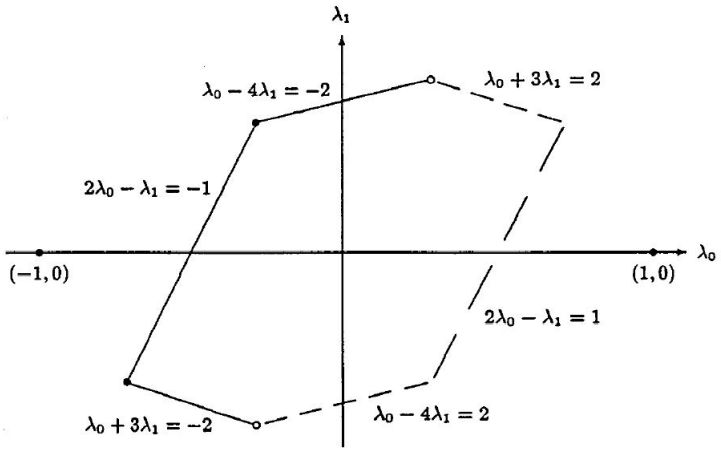
Kako bi dijeljenje s ostatkom za izraz $n = \kappa\delta + \rho$ uopće bilo moguće, potrebno je definirati operaciju zaokruživanja (*eng. rounding notion*), to jest za neki $\lambda \in \mathbb{Q}(\tau)$ pronaći najbližeg "susjeda" od λ u prstenu $\mathbb{Z}[\tau]$.

Operacija zaokruživanja u $\mathbb{Z}[\tau]$

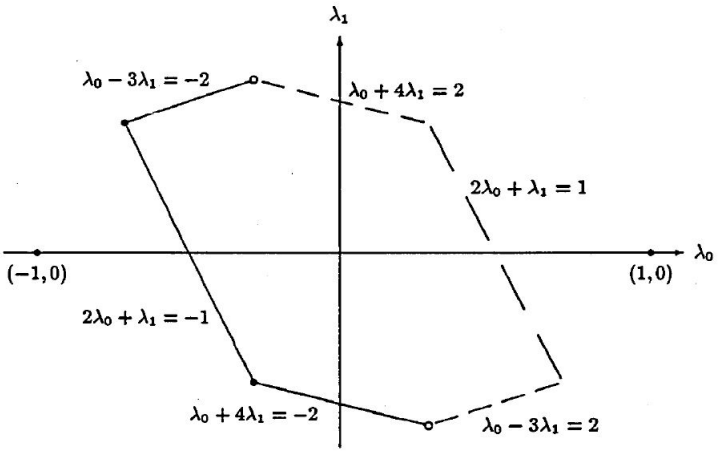
Neka je $\lambda = \lambda_0 + \lambda_1\tau$ neki element iz $\mathbb{Q}(\tau)$, gdje su λ_i realni brojevi. Kako bi se $\lambda \in \mathbb{Q}(\tau)$ mogao zaokružiti na element $\kappa \in \mathbb{Z}[\tau]$, potrebno je definirati područje $\mathcal{U}$ koje se nalazi unutar ravnine definirane s osima (λ_0, λ_1) i nejednakostima:

$$\begin{aligned}
-1 \leq 2\lambda_0 + \mu\lambda_1 < 1 \\
-2 \leq \lambda_0 + 4\mu\lambda_1 < 2 \\
-1 \leq \lambda_0 - 3\mu\lambda_1 < 2.
\end{aligned} \tag{3.5}$$

Na sljedećim slikama nalazi se prikaz područja $\mathcal{U}$ u ovisnosti o a. (Izvor: [9])



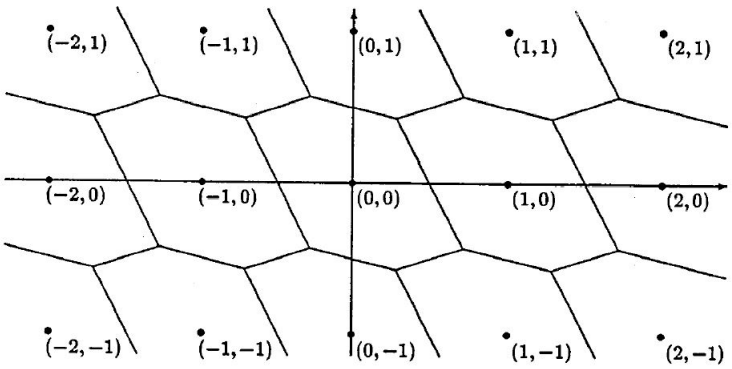
Slika 3.1: Područje $\mathcal{U}$ za $a = 0$



Slika 3.2: Područje $\mathcal{U}$ za $a = 1$

Ponavljanjem tog područja diljem ravnine, dobije se tzv. rešetka, koja ima za svojstvo da je svaki element koji se nalazi u središtu pojedinog područja element iz $\mathbb{Z}[\tau]$. Ideja je da se svaka točka koja se nalazi u unutrašnjosti nekog područja, a koja je element iz $\mathbb{Q}(\tau)$, može zaokružiti na element koji se nalazi u centru toga područja. Takva se operacija može naznačiti kao: $(q_0, q_1) = Round(\lambda_0, \lambda_1)$.

Na sljedećoj slici prikazan je primjer rešetke dobivene kopiranjem područja $\mathcal{U}$ za $a = 1$. (Izvor: [9])



Slika 3.3: Rešetka za $a = 1$

Slijedi nekoliko rezultata koji opisuju odnos norme nekog elementa i područja na kojem je taj element definiran.

Lema 3.3.1. *Pretpostavimo da se λ nalazi unutar područja $\mathcal{U}$. Tada vrijedi: $N(\lambda) < \frac{4}{7}$.*

Dokaz. Skup točaka u (λ_0, λ_1) - ravnini norme $\frac{4}{7}$ formira elipsu ${\lambda_0}^2 + \mu\lambda_0\lambda_1 + 2(\lambda_1)^2 = \frac{4}{7}$. Slijedi da svaki od šest vrhova te elipse ima normu $\frac{4}{7}$. Međutim, s obzirom na to da cijelo područje $\mathcal{U}$ leži na elipsi, pa sve točke unutar elipse imaju normu manju od $\frac{4}{7}$. □

Korolar 3.3.2. *Ako je $\kappa = Round(\lambda)$ i $\xi = \lambda - \kappa$, tada vrijedi:*

(i) $N(\xi) \leq N(\xi + \alpha)$, *za svaki* $\alpha \in \mathbb{Z}[\tau]$

(ii) $N(\xi) \leq \frac{4}{7}$.

Dokaz. (i) Pokazat će se da je element dobiven zaokruživanjem λ zapravo element najbliži λ u $\mathbb{Z}[\tau]$. Vrijedi da je:

$$N(\lambda) < N(\lambda \pm 1) \text{ ako i samo ako } |2\lambda_0 + \mu\lambda_1| < 1$$
$$N(\lambda) < N(\lambda \pm \tau) \text{ ako i samo ako } |\mu\lambda_0 + 4\lambda_1| < 2$$
$$N(\lambda) < N(\lambda \pm \overline{\tau}) \text{ ako i samo ako } |\mu\lambda_0 - 3\lambda_1| < 2.$$

S obzirom na to da λ leži u unutrašnjosti $\mathcal{U}$, prema (3.5) vrijedi da zadovoljava sve tri nejednakosti, pa je tvrdnja dokazana za $\alpha = \pm 1, \pm\tau, \pm\overline{\tau}$. Neka je α neki element iz $\mathbb{Z}[\tau]$ različit od $0, \pm 1, \pm\tau, \pm\overline{\tau}$. Tada je njegova norma $N(\alpha) \geq 4$, a vrijedi i $N(\lambda) < \frac{4}{7}$. Rezultat slijedi iz nejednakosti trokuta.

(ii) Tvrdnja je dokazana u [8].

□

Kako $\mathbb{Q}(\tau) \subset \mathbb{C}$ i $\mathbb{Z}[\tau]$ čine dvodimenzionalnu rešetku, koristi se apsolutna vrijednost kako bi se izračunala udaljenost u kompleksnoj ravnini. Stoga je element $q_0 + q_1\tau \in \mathbb{Z}[\tau]$ element rešetke koji je najbliži λ ako vrijedi sljedeće:

$$N(\lambda - q_0 - q_1\tau) \leq N(\lambda - \alpha), \quad za\ sve\ \alpha\ \in \mathbb{Z}[\tau],\ te\ q_0, q_1 \in \mathbb{Q}$$

Slijedi algoritam 2 koji izračunava taj element, u oznaci $\lfloor\lambda\rceil_\tau$.

Algoritam 2: Zaokruživanje elementa iz $\mathbb{Q}(\tau)$ na element iz $\mathbb{Z}[\tau]$

Ulaz: $\lambda_0, \lambda_1 \in \mathbb{Q}$ takvi da vrijedi $\lambda = \lambda_0 + \lambda_1\tau \in \mathbb{Q}(\tau)$
Izlaz: $q_0, q_1 \in \mathbb{Z}$ takvi da vrijedi $q_0 + q_1\tau = \lfloor\lambda\rceil_\tau$

for *i od* 0 *do* 1 **do**
  $f_i = \lfloor\lambda_i + \frac{1}{2}\rfloor; \eta_i = \lambda_i - f_i; h_i = 0;$
$\eta = 2\eta_0 + \mu\eta_1$;
if $\eta \geq 1$ **then**
  if $\eta_0 - 3\mu\eta_1 < -1$ **then**
    $h_1 = \mu$;
  else
    $h_0 = 1$;
else
  if $\eta_0 + 4\mu\eta_1 \geq 2$ **then**
    $h_1 = \mu$;
if $\eta < -1$ **then**
  if $\eta_0 - 3\mu\eta_1 \geq 1$ **then**
    $h_1 = -\mu$;
  else
    $h_0 = -1$;
else
  if $\eta_0 + 4\mu\eta_1 < -2$ **then**
    $h_1 = -\mu$;
$q_0 = f_0 + h_0$;
$q_1 = f_1 + h_1$;
return (q_0, q_1)

Primjer 3.3.3. *Neka je* $\lambda = 0.8 + 2.7\tau$. *Koristeći algoritam 2, dobije se da je* $\lfloor\lambda\rceil_\tau = 0 + 3\tau$, *a ne* $1 + 3\tau$ *kako bi se možda očekivalo.*

Dijeljenje s ostatkom u $\mathbb{Z}[\tau]$

Zaokruživanje elementa $\mathbb{Q}(\tau)$ na element iz $\mathbb{Z}[\tau]$ je neophodno kako bi se mogao provesti algoritam za dijeljenje s ostatkom u $\mathbb{Z}[\tau]$. Preciznije, za $\eta = n_0 + n_1\tau$ i $\delta = d_0 + d_1\tau \in \mathbb{Z}[\tau]$ potrebno je izračunati elemente $\kappa = q_0 + q_1\tau$ i $\rho = r_0 + r_1\tau \in \mathbb{Z}[\tau]$ takve da vrijedi: $\eta = \kappa\delta + \rho$ te da je ρ najmanje moguće norme.

U idućem algoritmu pokazat će se da je za dva elementa $\eta = n_0 + n_1\tau$ i $\delta = d_0 + d_1\tau \in \mathbb{Z}[\tau]$ prvo potrebno izračunati njihov kvocijent u $\mathbb{Q}(\tau)$. Formalno,

$$\begin{aligned} \eta/\delta = \eta\overline{\delta}/N(\delta) &= (n_0 + n_1\tau)(d_0 + d_1\overline{\tau}) = \\ &= n_0d_0 + n_1d_0\tau + n_0d_1(\mu - \tau) + n_1d_1\tau\overline{\tau} \ = \left\{ zbog\ \tau\cdot\overline{\tau} = 2 \right\} = \\ &= n_0d_0 + n_1d_0\tau + n_0d_1\mu - n_0d_1\tau + 2n_1d_1 = \\ &= (d_0 + \mu d_1)n_0 + 2n_1d_1 + (n_1d_0 - n_0d_1)\tau. \end{aligned} \tag{3.6}$$

Dobiveni raspis koristi se u sljedećem algoritmu.

Algoritam 3: Dijeljenje s ostatkom u $\mathbb{Z}[\tau]$

Ulaz: Elementi $\eta = n_0 + n_1\tau$ i $\delta = d_0 + d_1\tau \in \mathbb{Z}[\tau]$

Izlaz: Elementi $\kappa = q_0 + q_1\tau$ i $\rho = r_0 + r_1\tau \in \mathbb{Z}[\tau]$ takvi da vrijedi: $\eta = \kappa\delta + \rho, N(\rho) < \frac{4}{7}N(\delta)$

1 $g_0 = n_0d_0 + \mu n_0d_1 + 2n_1d_1$;
2 $g_1 = n_1d_0 - n_0d_1$;
3 $N = N(\delta) = (d_0)^2 + \mu d_0d_1 + 2(d_1)^2$;
4 $q_0 + q_1\tau = \left\lfloor \frac{g_0}{N} + \frac{g_1}{N}\tau \right\rceil_\tau$;
5 $r_0 = n_0 - d_0q_0 + 2d_1q_1$;
6 $r_1 = n_1 - d_1q_0 - d_0q_1 - \mu d_1q_1$;
7 $\kappa = q_0 + q_1\tau$;
8 $\rho = r_0 + r_1\tau$;
9 **return** κ i ρ

Gore navedeni algoritam može se koristiti kako bi se izračunala redukcija od n modulo δ, gdje je δ:

$$\delta = \delta_0 + \delta_1\tau = (\tau^d - 1)/(\tau - 1)$$

Algoritam 4: Redukcija modulo $\delta = (\tau^d - 1)/(\tau - 1)$

Ulaz: Element $n \in [1, N-1]$, gdje je $N = N(\delta)$, a elementi q_0 i q_1 kao u (3.4)
Izlaz: Element $\rho = r_0 + r_1\tau \equiv n \pmod{\delta}$

$d_0 = \delta_0 + \mu\delta_1$;
$\lambda_0 = d_0 n/N$;
$\lambda_1 = -\delta_1 n/N$;
$q_0 + q_1\tau = \left\lfloor \lambda_0 + \lambda_1\tau \right\rceil_\tau$;
$r_0 = n - \delta_0 q_0 + 2\delta_1 q_1$;
$r_1 = -\delta_1 q_0 - d_0 q_1$;
return $\rho = r_0 + r_1\tau$

Važno je primijetiti da se u četvrtom koraku algoritma 3 i u drugom i trećem koraku algoritma 4 zahtijeva precizno dijeljenje dva cijela broja, što u nekim slučajevima može predstavljati problem. Kako bi se jednostavnije mogla izračunati redukcija modulo δ, koristi se modifikacija početne ideje navedene u algoritmu 4 te se računa element $\rho' \equiv n \pmod{\delta}$ pomoću algoritma koji ne zahtijeva dijeljenje cijelih brojeva. Taj element označuje se i s $\rho' = n \text{(partmod } \delta)$ kako bi se naglasilo da je taj element dobiven algoritmom za parcijalnu redukciju modulo δ.

Algoritam 5: Parcijalna redukcija modulo $\delta = (\tau^d - 1)/(\tau - 1)$

Ulaz: Element $n \in [1, N-1]$, gdje je $N = N(\delta)$, $C \geq 2$, $s_0 = \delta_0 + \mu\delta_1$, $s_1 = -\delta_1$, gdje su elementi q_0 i q_1 kao u (3.4) te $K = (d+2)/2 + C$
Izlaz: Element $\rho' = r_0 + r_1\tau \equiv n \text{(partmod } \delta)$

$n' = \lfloor n/(2^{d-K-2+a_2}) \rfloor$;
$V_d = 2^d + 1 - \#E_{a_2}(\mathbb{F}_{2^d})$;
for *i od* 0 *do* 1 **do**
    $g'_i = s_i n'$;
    $h'_i = \lfloor g'_i/2^d \rfloor$;
    $j'_i = V_d h'_i$;
    $\lambda'_i = \lfloor (g'_i + j'_i)/2^{K-C} + 1/2 \rfloor / 2^C$;
Pomoću algoritma 2 izračunava se $Round(\lambda'_0, \lambda'_1)$ i dobiva (q'_0, q'_1) ;
$r'_0 = n - (s_0 + \mu s_1) q'_0 - 2 s_1 q'_1$;
$r'_1 = s_1 q'_0 - s_0 q'_1$;
return $\rho' = r'_0 + r'_1\tau$

Pokazano je u [9] kako je $l(\rho) \leq m + a_2$, a da za konstantu $C \geq 2$ vrijedi da je $l(\rho') \leq m + a_2 + 3$. Treba napomenuti da se, iako je $\rho' = r_0 + r_1\tau$ ekvivalentan n (partmod δ),

može dogoditi da je duljina od ρ' značajno veća od duljine od ρ koji je dobiven kao rezultat algoritma 4. Međutim, vjerojatnost da je $\rho \neq \rho'$ je manja od $1/2^{C-5}$. Stoga, sam odabir dovoljno velikog C osigurava da je $\rho = \rho'$.

Konačno, nakon što se izračuna reducirani element ρ pomoću jednog od gore navedenih algoritama 4 ili 5, može se naći i njegov τNAF prikaz, što je zapravo ranije spomenuti $R\tau NAF$ prikaz. Ukoliko se želi osigurati raspršeniji prikaz, to jest s više elemenata 0, koristi se tzv. *metoda prozora* definirana u jednom od sljedećih poglavlja.

3.4 Računanje višekratnika točke

Za računanje višekratnika nP neke točke P na Koblitzovoj eliptičkoj krivulji primjenjuje se algoritam 6 koji koristi gore objašnjeni reducirani τNAF prikaz. S obzirom na to da je duljina $\tau\text{NAF}(\rho')$ otprilike d, taj algoritam obavlja $d/3$ zbrajanja, ali ni u jednom koraku ne izvršava udvostručavanje točaka, zbog čega je barem 50% brži od svih prije navedenih verzija. U idućem algoritmu pokazana je τNAF metoda za izračunavanje višekratnika točke na Koblitzovoj eliptičkoj krivulji.

Algoritam 6: τNAF metoda za izračunavanje višekratnika točke

Ulaz: element $n \in [1, N-1]$, $P \in E(\mathbb{F}_{2^d})$ reda N
Izlaz: nP

Pomoću algoritma 5 izračunati $\rho' = n \pmod{\delta}$;
Pomoću algoritma 1 izračunati $\tau NAF(\rho') = \sum_{i=0}^{l-1} r_i \tau^i$;
$Q = \infty$;
for i *od* $l-1$ *do* 0 **do**
    $Q = \tau Q$;
    if $u_i = 1$ **then**
        $Q = Q + P$;
    if $u_i = -1$ **then**
        $Q = Q - P$;
return Q

3.5 Metoda prozora

Vrijeme izvođenja algoritma 6 može se smanjiti uvođenjem takozvane *metode prozora širine* τ, ili skraćeno τ*-metode prozora*. Ta metoda zahtijeva dodatnu slobodnu memoriju, jer istovremeno obrađuje τ znamenaka od ρ'.

Za početak spomenut će se NAF širine w te obična metoda prozora širine w, ili kraće *w-metoda prozora*.

Definicija 3.5.1. *Neka je w parametar veći od 1. Svaki prirodan broj* $r \in \mathbb{N}$ *ima jedinstveni raspis:*

$$r = \sum_{i=0}^{l-1} r_i 2^i, \tag{3.7}$$

gdje vrijedi:

- *svaki* r_i *je 0 ili neparan,*
- $|r_i| < 2^{w-1}$,
- *među svakih w susjednih koeficijenata, najviše jedan je različit od 0.*

Ovakav rastav naziva se NAF širine w, ili kraće NAF_w *i označava se s* $(r_{l-1}\ldots r_0)_\tau$

Ukratko će se pojasniti w-metoda prozora, koja je detaljnije objašnjena u [3] i [6]. U početku se izračunavaju i spremaju u memoriju sve točke uP, gdje je u dobiven kao reprezentant svake neparne kongruencije s klasom (mod 2^w). Za odabrani neparni broj c, ispituje se w znamenaka brojeći zdesna na lijevo te se utvrđuje kojoj klasi kongruencije (mod 2^w) taj broj c pripada. Uzima se da je reprezentant te klase koeficijent e. Oduzima se odgovarajuća točka eP te je sada novi koeficijent $c - e$ djeljiv s 2^w.

Sljedeći teorem opisuje svojstva Lucasovih nizova koji će biti korisni u nastavku za opis τ-metode prozora.

Teorem 3.5.2. *Neka je* $\{U_k\}$ *niz brojeva definiranih sa:* $U_0 = 0$, $U_1 = 1$, $U_{k+1} = \mu U_k - 2U_{k-1}$ *za* $k \geq 1$.

(i) $U_k^2 - \mu U_{k-1}U_k + 2U_{k-1}^2 = 2^{k-1}$ *za sve* $k \geq 1$.

(ii) Neka je $t_k = 2U_{k-1}U_k^{-1} (\text{mod } 2^k)$ *za* $k \geq 1$. *Tada* $t_k^2 + 2 \equiv \mu t_k (\text{mod } 2^k)$ *za sve* $k \geq 1$.

Dokaz. (i) U [9] je dana sljedeća formula koja se može dokazati indukcijom:

$$\tau^k = U_k\tau - 2U_{k-1}, \text{ za sve } k \geq 1.$$

Množenjem te jednakosti s kompleksnim konjugatom od τ^k, to jest sa $\overline{\tau}^k$, dobiva se tražena jednakost.

(ii) Neka je $t_k = 2U_{k-1}U_k^{-1} \pmod{2^k}$ za $k \geq 1$. S obzirom na to da su elementi Lucasovog niza neparni, slijedi da su elementi t_k parni i dobro definirani modulo 2^k, ali nisu djeljivi s 4. Dakle, $U_k^{-1} \pmod{2^k}$ doista postoji. Korištenjem zaključka iz dijela (i) ovog teorema slijedi,

$$t_k^2 - \mu t_k + 2 \equiv 0 \pmod{2^k}.$$

To jest, vrijedi:

$$t_k^2 + 2 \equiv \mu t_k \pmod{2^k},$$

što je trebalo i pokazati.

□

Iz (2.5) i teorema 3.5.2 slijedi da je preslikavanje $\phi_k : \mathbb{Z}[\tau] \to \mathbb{Z}_{2^k}$ (to jest $\tau \to t_k$) surjektivni homomorfizam prstena s jezgrom $\{\alpha \in \mathbb{Z}[\tau] : \tau^k \text{ dijeli } \alpha\}$.

Lema 3.5.3. *Neka je* $\alpha \in \mathbb{Z}[\tau]$. *Tada je* $\phi_k(\alpha) = 0$ *ako i samo ako je* α *djeljiv s* τ^k.

Dokaz. S obzirom na to da je $\phi_k(\tau) = t_k \equiv 2 \pmod 4$, slijedi da je $\phi_k(\tau^j) = t_k^j$ djeljivo s 2^j, ali ne i s 2^{j+1}. Stoga slijedi da je potencija broja 2 koja dijeli $\phi_k(\alpha)$ zapravo potencija od τ koja dijeli α. □

Skup svih reprezentanata klase ekvivalencije u $\mathbb{Z}[\tau]$ modulo τ^w je

$$\{0, \pm 1, \pm 2, \pm 3, ..., \pm(2^{w-1} - 1), -2^{w-1}\},$$

od čega treba izdvojiti skup $\{\pm 1, \pm 3, ..., \pm(2^{w-1} - 1)\}$ koji predstavlja neparne brojeve koji nisu kongruentni modulo τ^w. Iz toga direktno slijedi da ako je:

$$\alpha_u = u \pmod{\tau^w},$$

tada brojevi $\pm\alpha_1, \pm\alpha_3, ..., \pm\alpha_{2^{w-1}-1}$ također nisu kongruentni modulo τ^w. Sada se može definirati τNAF širine w, sličan NAF-u širine w, ali koji je primjenjen na τNAF prikaz.

Definicija 3.5.4. *Neka je* w *parametar veći od 1. Svaki element* $\eta \in \mathbb{Z}[\tau]$ *se može prikazati kao:*

$$\eta = \sum_{i=0}^{l-1} r_i \tau^i, \tag{3.8}$$

gdje vrijedi:

- *svaki* r_i *je 0 ili* $r_i = \pm\alpha_u$, *gdje je* $\alpha_u \equiv u \pmod{\tau^w}$, *za neki neparni* $u \in [1, 2^{w-1} - 1]$,
- $r_{l-1} \neq 0$,
- *među svakih w susjednih koeficijenata, najviše jedan je različit od 0.*

Takav raspis naziva se τ*-nesusjedni prikaz širine w ili skraćeno,* τNAF_w *te se označava s* $(r_{l-1}...r_0)_{\tau NAF_w}$*. Njegova duljina označava se s l.*

Potrebno je istaknuti kako su za $w = 2$, $\tau\text{NAF}_w(\eta)$ prikaz i $\tau\text{NAF}(\eta)$ prikaz u raspisu jednaki, to jest općenito vrijedi $\tau\text{NAF}_2 = \tau\text{NAF}$.

Prije samog izvršavanja algoritma, vrijednosti $\alpha_u \in \mathbb{Z}[\tau]$ se unaprijed izračunavaju. Ti elementi α_u su takvi da vrijedi $\alpha_u \equiv u(\text{mod } \tau^w)$, gdje je u neparan i element iz skupa $\{1, 3, 5, ..., 2^{w-1} - 1\}$. Koristeći algoritam 2, ostatak $\beta_u + \gamma_u\tau$ pri dijeljenju u sa τ^w postaje linearan, zbog čega se svaki izraz α_u kraće može zapisati kao kombinacija potencije od τ i nekog prethodno izračunatog izraza α_u. Na taj način, izračun točke $\alpha_u P$ može se ostvariti korištenjem najviše jedne operacije zbrajanja na eliptičkoj krivulji.

τNAF_w prikaz od η efikasno se može izračunati koristeći algoritam 7, gdje $k(\text{mods } 2^w)$ označava broj u koji zadovoljava $u \equiv k(\text{mod } 2^w)$ i za kojeg vrijedi $-2^{w-1} \leq u < 2^{w-1}$. Znamenke tog τNAF_w prikaza od η dobivaju se tako da se η dijeli s τ, a ostaci su iz skupa $\{0, \pm\alpha_1, \pm\alpha_3, ..., \pm\alpha_{2^{w-1}-1}\}$. U slučaju da η nije djeljiv s τ, a ostatak je α_u za $u = \phi_k(\eta) \text{ mods } 2^w$, tada se uzima da je $(\eta - \alpha_u)/\tau$ djeljiv s τ^{w-1}, čime se osigurava da je sljedećih $w - 1$ znamenaka jednako 0.

Slijedi algoritam za izračunavanje τNAF_w prikaza koji je prvi puta predložen u [9].

Algoritam 7: Računanje τNAF_w prikaza elementa iz $\mathbb{Z}[\tau]$

Ulaz: Element $\eta = n_0 + n_1\tau \in \mathbb{Z}[\tau]$, parametar $w > 1$ te parametri $h_w, \alpha_u, \beta_u, \gamma_u$ definirani kao $\alpha_u = \beta_u + \gamma_u\tau$ za $u \in [1, 3, 5, ..., 2^{w-1} - 1]$.

Izlaz: $\tau\text{NAF}_w(\eta)$ prikaz u obliku $(r_{l-1}\ldots r_0)_\tau$

```
1  l = 0;
2  while n_0 ≠ 0 ili n_1 ≠ 0 do
3      if n_0%2 == 1 then
4          u = (n_0 + n_1 h_w) mods 2^w;
5          if u > 0 then
6              s = 1;
7          else
8              s = −1;
9              u = −u;
10         n_0 = n_0 − sβ_u;
11         n_1 = n_1 − sγ_u;
12         r_l = sα_u;
13     else
14         r_l = 0;
15     t = n_0;
16     n_0 = n_1 + μn_0/2;
17     n_1 = −t/2;
18     l = l + 1;
19 return (r_{l−1}, r_{l−2}...r_0)_τ
```

Treba napomenuti da je broj u u 4. koraku jedinstveni broj iz $[-2^{w-1}, 2^{w-1}]$, a koji je kongruentan $(n_0 + n_1 h_w)$ mods 2^w.

Duljina, označena s l, ovog τNAF_w prikaza od $\eta = n_0 + n_1\tau$ je otprilike jednaka duljini binarnog rastava norme od tog η. Dakle, ako je $\eta = n \in \mathbb{Z}$, tada je $l \approx 2 \lg n$. Prosječna gustoća ne-nul elemenata u τNAF_w prikazu od η je jednaka $1/(w + 1)$ te se taj broj ne povećava. Stoga, ukoliko je n reduciran kao u ulazu algoritma 7, za izračunavanje točke $[n]P$ potrebno je prosječno $2^{w-2} - 1 + \frac{d}{w+1}$ zbrajanja na eliptičkoj krivulji. U to su uračunate i sve vrijednosti α_u definirane u ulazu algoritma koje je potrebno unaprijed izračunati, a kojih ima $2^{w-2} - 1$. Na sljedećem primjeru bit će prikazano kako izgledaju izračunati α_u te kako se iz njih mogu izračunati točke $P_u = \alpha_u P$.

Primjer 3.5.5. *Neka su* $u = 1, 3, ...15$*,* $w = 5$ *i* $a = 0$*. Slijedi raspis vrijednosti* α_u*:*

$$\begin{aligned}
\alpha_1 &= 1 \\
\alpha_3 &= \tau^2 - 1 \\
\alpha_5 &= \tau^2 + 1 \\
\alpha_7 &= \tau^3 - 1 \\
\alpha_9 &= \tau^5 + \tau^3 + 1 = \tau^3\alpha_5 + 1 \\
\alpha_{11} &= -\tau^4 - \tau^2 - 1 = -\tau^2\alpha_5 - 1 \\
\alpha_{13} &= -\tau^4 - \tau^2 + 1 = -\tau^2\alpha_5 + 1 \\
\alpha_{15} &= \tau^4 - 1 = \tau^2\alpha_5 - \alpha_5
\end{aligned}$$

Iz tih vrijednosti sada se lako mogu izračunati točke $P_u = \alpha_u P$*:*

$$\begin{aligned}
P_1 &= P \\
P_3 &= \tau^2 P - P \\
P_5 &= \tau^2 P + P \\
P_7 &= \tau^3 P - P \\
P_9 &= \tau^5 P + \tau^3 P + P = \tau^3 P_5 + P \\
P_{11} &= -\tau^4 P - \tau^2 P - P = -\tau^2 P_5 - P \\
P_{13} &= -\tau^4 P - \tau^2 P + P = -\tau^2 P_5 + P \\
P_{15} &= \tau^4 P - P = \tau^2 P_5 - P_5
\end{aligned}$$

Očito je da računanje svake točke P_u zahtijeva jedno zbrajanje na eliptičkoj krivulji. Na taj način dobivene su i vrijednosti u sljedeće dvije tablice, gdje se preglednije mogu vidjeti raspisi za α_u, gdje je $w \in [3, 5]$ te su $a = 0$ i $a = 1$. Dakle, izračunavaju se elementi $\alpha \in \mathbb{Z}[\tau]$ takvi da je $\alpha_u \equiv u (\mathrm{mod}\ \tau^w)$ za neparni $u \in [1, 2^{w-1} - 1]$. Taj ostatak u (mod τ^w) može se izraziti i u obliku $\beta_u + \gamma_u\tau$. Kada je to moguće, izraz α_u može se jednostavnije zapisati i preko τNAF prikaza ili koristeći α_u izračunate u prethodnim koracima.

Tablica 3.1: Izrazi $\alpha_u = u(\mathrm{mod}\ \tau^w)$ za $a = 0$ te $w \in [3, 5]$

w	u	$u(\mathrm{mod}\ \tau^w) = \beta_u + \gamma_u\tau$	τNAF($u(\mathrm{mod}\ \tau^w)$)	α_u
3	1	1	(1)	1
3	3	τ +1	(-1,0,-1)	$\tau + 1$
4	1	1	(1)	1
4	3	-τ - 3	(1,0,-1)	τ^2 - 1
4	5	-τ - 1	(1,0,1)	τ^2 + 1
4	7	-τ +1	(1,0,0,-1)	τ^3 - 1
5	1	1	(1)	1
5	3	-τ - 3	(1,0,-1)	τ^2 - 1
5	5	-τ -1	(1,0,1)	τ^2 + 1
5	7	-τ +1	(1,0,0,-1)	τ^3 - 1
5	9	-2τ -3	(1,0,1,0,0,1)	$\tau^3\alpha_5$ + 1
5	11	-2τ - 1	(-1,0,-1,0,-1)	-$\tau^2\alpha_5$ - 1
5	13	-2τ +1	(-1,0,-1,0,1)	-$\tau^2\alpha_5$ + 1
5	15	3τ +1	(1,0,0,0,-1)	$\tau^2\alpha_5 - \alpha_5$

Tablica 3.2: Izrazi $\alpha_u = u(\mathrm{mod}\ \tau^w)$ za $a = 1$ te $w \in [3, 5]$

w	u	$u(\mathrm{mod}\ \tau^w) = \beta_u + \gamma_u\tau$	τNAF($u(\mathrm{mod}\ \tau^w)$)	α_u
3	1	1	(1)	1
3	3	-τ +1	(-1,0,-1)	-τ + 1
4	1	1	(1)	1
4	3	τ - 3	(1,0,-1)	τ^2 - 1
4	5	τ - 1	(1,0,1)	τ^2 + 1
4	7	τ +1	(-1,0,0,-1)	-τ^3 - 1
5	1	1	(1)	1
5	3	τ - 3	(1,0,-1)	τ^2 - 1
5	5	τ -1	(1,0,1)	τ^2 + 1
5	7	τ +1	(-1,0,0,-1)	-τ^3 - 1
5	9	2τ -3	(-1,0,-1,0,0,1)	-$\tau^3\alpha_5$ + 1
5	11	2τ - 1	(-1,0,-1,0,-1)	-$\tau^2\alpha_5$ - 1
5	13	2τ +1	(-1,0,-1,0,1)	-$\tau^2\alpha_5$ + 1
5	15	-3τ +1	(1,0,0,0,-1)	$\tau^2\alpha_5 - \alpha_5$

Kao i ranije, postoji i reducirani τNAF_w prikaz elementa iz $\mathbb{Z}[\tau]$, nužan u tzv. *τNAF metodi prozora širine w*, koja će izračunavati višekratnik neke zadane točke. Reducirani τNAF_w prikaz označava se s $\text{R}\tau\text{NAF}_w$, te vrijedi $\text{R}\tau\text{NAF}_w(n) = \tau\text{NAF}_w(\rho)$, gdje je $\rho = n(\text{mod } \delta)$.

Slijedi algoritam za τNAF metodu prozora širine *w* koji koristi RτNAF. On se svodi na takozvanu *metodu kliznog prozora* ([3]) u kojoj je definiran "prozor" širine *k*, koji se može pomicati lijevo ili desno, preskačući uzastopne nule koje se pojavljuju iza ne-nul elementa koji je u danom trenutku u obradi algoritma. Takvo pomicanje označeno je u algoritmu kao *LeftShift* za pomak ulijevo, odnosno *RightShift* za pomak udesno.

Algoritam 8: τNAF metoda prozora širine w

Ulaz: Broj $n \in [1, N-1]$ i $P \in E(\mathbb{F}_{2^d})$ reda N
Izlaz: Točka nP na eliptičkoj krivulji

1 Izračunati točke $P_u = \alpha_u P$ za $u = 1, 3, ...(2^{w-1} - 1)$;
2 $i = 0$;
3 Pomoću algoritma 4 izračunati r_0 i r_1 ;
4 $Q = \infty$;
5 **while** $r_0 \neq 0$ *ili* $r_1 \neq 0$ **do**
6 **if** $r_0 \% 2 == 1$ **then**
7 $u = (r_0 + r_1 h_w) \text{ mods } 2^w$ **if** $u > 0$ **then**
8 $s = 1$;
9 **else**
10 $s = -1$;
11 $u = -u$;
12 $Q = Q + sP_u$;
13 $i = i + 1$;
14 $Q = \tau^{-1} Q$ `// LeftShift [Q]`
15 $r_0 = r_1 + \mu r_0/2$;
16 $r_1 = -r_0/2$;
17 $Q = \tau^i Q$ `// RightShift [Q] (i puta)`
18 **return** Q

U 15. koraku algoritma koristi se upravo *LeftShift*, koji se formalno definira kao invertiranje Frobeniusovog endomorfizma, to jest τ^{-1}, što se u slučaju Koblitzovih eliptičkih krivulja može efikasno izračunati. Treba napomenuti da je trošak izračuna τ i τ^{-1} približno jednak. Frobeniusov endomorfizam ranije je definiran u definiciji 2.1.1, te se slično definira i njegov inverz kao preslikavanje $\tau^{-1} : E_{a_2}(\mathbb{F}_{2^d}) \rightarrow E_{a_2}(\mathbb{F}_{2^d})$ koje (x_1, y_1) preslikava u

$(\sqrt{x_1}, \sqrt{y_1})$, dok točku P_∞ preslikava u sebe samu.

Međutim, postoji i algoritam koji izračunava višekratnik nP neke točke P na $E(\mathbb{F}_{2^d})$ bez korištenja pomaka ulijevo i pomaka udesno. Taj algoritam također koristi reducirani τNAF$_w$ prikaz od n, to jest τNAF$_w$ prikaz od ρ'.

Algoritam 9: τNAF metoda prozora širine w za Koblitzove eliptičke krivulje

Ulaz: Broj $n \in [1, N-1]$ i $P \in E(\mathbb{F}_{2^d})$ reda N
Izlaz: Točka nP na eliptičkoj krivulji

```
1  Pomoću algoritma 5 izračunati ρ' = n (partmod δ) ;
2  Pomoću algoritma 7 izračunati τNAF_w(ρ') = Σ_{i=0}^{l-1} r_i τ^i ;
3  Izračunati točke P_u = α_u P za u = 1, 3, ...(2^{w-1} − 1);
4  Q = ∞;
5  for i od l − 1 do 0 do
6      Q = τQ ;
7      if r_0 ≠ 0 then
8          Neka je u takav da je α_u = u_i ili α_{-u} = −u_i;
9          if u > 0 then
10             Q = Q + P_u;
11         else
12             Q = Q − P_{-u};
13 return Q
```

3.6 Zajednički raspršeni τ prikaz

Zajednički raspršeni prikaz (eng. *JSF*) za obični NAF prikaz dva velika broja a i b prvi put je spomenuo Solinas, a detaljnije se može pogledati u [3]. Tu ideju proširio je Ciet, primjenivši ju na τNAF prikaz brojeva a i b koristeći endomorfizam ϕ pri izračunu $aP+bQ$, gdje su P i Q dvije točke na eliptičkoj krivulji. Njihova prednost u primjeni na Koblitzove eliptičke krivulje odnosi se na bržu verifikaciju potpisa, ali i na brže skalarno množenje ako se radi velikoj količini elemenata koji se moraju unaprijed izračunati. Slijedi definicija za zajednički raspršeni τ prikaz.

Definicija 3.6.1. *Neka su*

$$\eta_0 = \sum_{j=0}^{l-1} n_{0,j}\, \tau^j \quad i \quad \eta_1 = \sum_{j=0}^{l-1} n_{1,j}\, \tau^j$$

dva elementa iz $\mathbb{Z}[\tau]$ *te neka je* $n_{i,j} \in \{0, \pm 1\}$. *Zajednički raspršeni* τ *prikaz od* η_0 *i* η_1, *skraćeno* τ*JSF, je prikaz oblika*

$$\begin{pmatrix} \eta_0 \\ \eta_1 \end{pmatrix} = \begin{pmatrix} r_{0,l+2} \ldots r_{0,0} \\ r_{1,l+2} \ldots r_{1,0} \end{pmatrix},$$

gdje su $r_{i,j} \in \{0, \pm 1\}$, *takvi da vrijede sljedeća svojstva:*

- *od bilo koja tri uzastopna elementa, barem jedan ima stupac koje čine nule, to jest, za svaki* i i $j > 0$ *jedan je stupac takav da vrijedi* $r_{i,j+k} = r_{1-i,j+k} = 0$ *za barem jedan* $k \in \{0, \pm 1\}$,
- *ni u jednom slučaju ne vrijedi* $r_{i,j} r_{i,j+1} = \mu$,
- *ako je* $r_{i,j+1} r_{i,j} \neq 0$, *tada vrijedi* $r_{1-i,j+1} = \pm 1$ *i* $r_{1-i,j} = 0$.

U nastavku će se opisati algoritam koji računa takvu formu. Iako je taj algoritam prikladan za sve vrste τ formi koje su detaljnije opisane u [3], ovdje će se pokazati primjena na τNAF prikaz, jer je prethodno obrađen. Treba napomenuti da se taj algoritam koristi i u verifikaciji potpisa uz dodatni korak koji se izvodi na samom početku. Naime, brojeve η_1 i η_2 potrebno je reducirati modulo δ. U tom slučaju, ne računa se τNAF prikaz, već se u ulazu algoritma uzima reducirani τNAF prikaz. Analogni korak vrijedi i za ostale općenite τ prikaze.

Algoritam 10 se može primijeniti i za izračunavanje višekratnika nP neke točke P na krivulji. U tom slučaju, broju n se računa τNAF prikaz, ili općenito τ prikaz, koji je duljine $d + a_2$ i razdvaja se na dva izraza:

$$\eta_0 = \sum_{i=0}^{\lfloor d/2 \rfloor - 1} r_i \, \tau^i \quad i \quad \eta_1 = \sum_{i=\lfloor d/2 \rfloor}^{d-1+a_2} r_i \, \tau^j,$$

tako da vrijedi $n = \eta_0 + \tau^{\lfloor d/2 \rfloor} \eta_1$.

Algoritam 10: Metoda za izračunavanje zajedničkog raspršenog τ prikaza

Ulaz: Dva τNAF prikaza $\eta_0 = \sum_{j=0}^{l-1} n_{0,j}\,\tau^j$ i $\eta_1 = \sum_{j=0}^{l-1} n_{1,j}\,\tau^j$, za koje vrijedi $n_{i,j} \in \{0, \pm 1\}$.

Izlaz: Zajednički raspršeni τ prikaz od η_0 i η_1

```
1  j = 0;
2  S_0 = ();
3  S_1 = ();
4  for i od 0 do 1 do
5      d_{i,0} = 0 ;
6      d_{i,1} = 0 ;
7      a_i = n_{i,0} ;
8      b_i = n_{i,1} ;
9      c_i = n_{i,2} ;
10 while l − j > 0 ili |d_{0,0}| + |d_{0,1}| + |d_{1,0}| + |d_{1,1}| > 0 do
11     for i od 0 do 1 do
12         if d_{i,0} ≡ a_i(mod 2) then
13             r_i = 0;
14         else
15             r_i = (d_{i,0} + a_i + 2μ(d_{i,1} + b_i)) mods 4;
16             t_{i,0} = d_{i,0} + a_i − 2μ(d_{i,1} + b_i) − 4c_i;
17             if t_{i,0} ≡ ±3(mod 8) then
18                 t_{i,1} = d_{1−i,0} + a_{1−i} + 2(d_{1−i,1} + b_{1−i}) ;
19                 if t_{i,1} ≡ 2(mod 4) then
20                     r_i = −r_i ;
21         S_i = r_i || S_i ;
22     for i od 0 do 1 do
23         d_{i,0} = μ(d_{i,0} + a_i + −r_i)/2 + d_{i,j};
24         d_{i,1} = μ(d_{i,1} − d_{i,0};
25         a_i = b_i;
26         b_i = c_i;
27         c_i = η_{i,j+3};
28     j = j + 1;
29 return S_0 i S_1
```

Zajednički raspršeni τ prikaz postoji za sve η_0 i η_1, te je taj prikaz jedinstven.

Poglavlje 4

Primjena Koblitzovih eliptičkih krivulja

Eliptičke krivulje važne su za osnaživanje kriptografije s obzirom na to da zahtjevi za sigurnošću iz dana u dan postaju sve veći. Stoga je američki *National Institute of Standards and Technology*, skraćeno NIST, standardizirao upotrebu eliptičkih krivulja u kriptografiji u svrhu odabira ključa u diskretnom logaritamskom problemu koji je pojašnjen ranije u radu, ali i za algoritme s digitalnim potpisima. Ukratko, digitalni potpis može se shvatiti kao elektronički analogon uobičajenom potpisu, uz dodatna dva svojstva: daje osiguranje da je osoba navedena kao autor doista autor dokumenta, ali i da dokument nije bio promijenjen nakon generiranja potpisa.

Kriptografski standard, pod imenom *FIPS 186*, propisao je NIST 1994. godine te je specificirao algoritam za generiranje i verifikaciju digitalnih potpisa *DSA*. U kasnijim nadopunama pojavljuju se još dva algoritma - *ECDSA* i *RSA algoritam digitalnog potpisa*. U tom dokumentu, NIST također preporučuje petnaest eliptičkih krivulja, svaku sa svojom razinom sigunosti, za upotrebu u kriptografske svrhe. Od njih petnaest, njih pet su Koblitzove eliptičke krivulje koje će biti navedene u nastavku. Kako se standard dugo nije mijenjao, za to vrijeme se znanje o eliptičkim krivuljama u kriptografiji povećalo pa su se pojavile i nove eliptičke krivulje i algoritmi čiji su autori tvrdili da imaju bolja svojstva od prethodnih. U tu svrhu, 2015. godine NIST objavljuje poboljšani standard pod imenom *FIPS 186-4*, koji vrijedi i danas.

4.1 NIST-ove krivulje

Prije navođenja pet Koblitzovih eliptičkih krivulja, koje je NIST odobrio, treba istaknuti nekoliko detalja. Naime, parametri koji će biti važni za definiranje krivulja su koeficijent a_2, red N, te x i y koordinate točke generatora G, to jest G_x i G_y. Stupnjevi m preporučnih Koblitzovih eliptičkih krivulja su 163, 233, 283, 409 i 571. Polje $\mathbb{F}_{2^d}$ je vektorski prostor nad $\mathbb{F}_2$ dimenzije d te se može reprezentirati kao skup svih ireducibilnih polinoma $f(x)$

nad $\mathbb{F}_2$ stupnja manjeg od d, s operacijama modulo $f(x)$. Takva repezentacija naziva se polinomna baza te je za navedena za svaku od ovih pet krivulja.

Krivulja K-163

$p(t) = t^{163} + t^7 + t^6 + t^3 + 1$
$a = 1$
$N = 5846006549323611672814741753598448348329118574063$
$G_x = 2\ fe13c053\ 7bbc11ac\ aa07d793\ de4e6d5e\ 5c94eee8$
$G_y = 2\ 89070fb0\ 5d38ff58\ 321f2e80\ 0536d538\ ccdaa3d9$

Krivulja K-233

$p(t) = t^{233} + t^{74} + 1$
$a = 0$
$N = 3450873173395281893717377931138512760570940988862252126328087024$
741343
$G_x = 172\ 32ba853a\ 7e731af1\ 29f22ff4\ 149563a4\ 19c26bf5\ 0a4c9d6e\ efad6126$
$G_y = 1db\ 537dece8\ 19b7f70f\ 555a67c4\ 27a8cd9b\ f18aeb9b\ 56e0c110\ 56fae6a3$

Krivulja K-283

$p(t) = t^{283} + t^{12} + t^7 + t^5 + 1$
$a = 0$
$N = 3885337784451458141838923813647037813284811733793061324295874997$
529815829704422603873
$G_x = 03213f\ 78ca4488\ 3f1a3b81\ 62f188e5\ 53cd265f\ 23c1567a\ 16876913\ b0c2ac24$
58492836
$G_y = ccda38\ 0f1c9e31\ 8d90f95d\ 07e5426f\ e87e45c0\ e8184698\ e4596236\ 4e341161$
$77dd2259$

Krivulja K-409

$p(t) = t^{409} + t^{87} + 1$
$a = 0$
$N = 330527984395124299475957654016385519914202341482140609642324395022$

88071128924919105067325845777745801409636659061773135867 1

G_x = 060*f*05*f* 658*f*49*c*1 *ad*3*ab*189 0*f*718421 0*efd*0987 *e*307*c*84*c* 27*accfb*8 *f*9*f*67*cc*2 *c*460189*e* *b*5*aaaa*62 *ee*222*eb*1 *b*35540*cf* *e*9023746

G_y = 1*e*36905 0*b*7*c*4*e*42 *acba*1*dac* *bf*04299*c* 3460782*f* 918*ea*427 *e*6325165 *e*9*ea*10*e*3 *da*5*f*6*c*42 *e*9*c*55215 *aa*9*ca*27*a* 5863*ec*48 *d*8*e*0286*b*

Krivulja K-571

$p(t) = t^{571} + t^{10} + t^5 + t^2 + 1$

$a = 0$

N = 193226876150862917234767594546599367214946366485321749932861762572 5759571144780212268133978522706711834706712800825351461273674974066617 3119296824216170925035555733685276673

G_x = 26*eb*7*a*8 59923*fbc* 82189631 *f*8103*fe*4 *ac*9*ca*297 0012*d*5*d*4 60248048 01841*ca*4 43709584 93*b*205*e*6 47*da*304*d* *b*4*ceb*08*c* 100*bbd*1*ba*39 494776*fb* 988*b*4717 4*dca*88*c*7 *e*2945283 *a*01*c*8972

G_y = 349*dc*80 7*f*4*fbf*37 4*f*4*aeade* 3*bca*9531 4*dd*58*cec* 9*f*307*a*54 *ffc*61*efc* 006*d*8*a*2*c* 9*d*4979*c*0 *ac*44*aea*7 4*fbebbb*9 *f*772*aedc* *b*620*b*01*a* 7*ba*7*af*1*b* 320430*c*8 591984*f*6 01*cd*4*c*14 3*ef*1*c*7*a*3

Usprkos svemu navedenom, dugoročna sigurnost Koblitzovih krivulja postaje upitna zbog pojave kvantne kriptografije. To je vrsta kriptografije koja se pri šifriranju i dešifriranju oslanja na saznanja iz kvantne fizike, čime omogućuje brže računanje i primjenu složenijih algoritama, pa uzrokuje ranjivost dosada sigurnih algoritama. U skladu s time, američka *National Security Agency*, skraćeno NSA, 2015. godine objavljuje kako se u budućnosti planira odmaknuti od kriptografije s eliptičkim krivuljama i početi koristiti algoritme koji će biti tzv. *kvantno otporni*.

Bibliografija

[1] *https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf*.

[2] *http://www.crypto-textbook.com/*.

[3] Cohen, G. Frey, H.: *Handbook of Elliptic and Hyperelliptic Curve Cryptography*. Chapman and Hall/CRC, 2005.

[4] Dujella, A.: *Eliptičke krivulje u kriptografiji*. PMF - MO, Sveučilište u Zagrebu, 2013.

[5] Dujella, A. Maretić, M.: *Kriptografija*. Element, 2007.

[6] Hankerson, D. Menezes, A. Vanstone S.: *Guide to Elliptic Curve Cryptography*. Springer-Verlag, 2004.

[7] Lange, T.: *Koblitz curve cryptosystems*. Finite Fields and Their Applications 11 (2005), 200-229.

[8] Meier, W. Staffelbach, O.: *Efficient multiplication on certain non-supersingular elliptic curves*. Proc. Crypto '92, Springer-Verlag (1993), 333-344.

[9] Solinas, J.: *Efficient arithmetic on Koblitz curves*. Des. Codes Cryptogr. 19 (2000), 195-249.

[10] Širola, B.: *Algebarske strukture*. PMF - MO, Sveučilište u Zagrebu.

Sažetak

Ovaj rad proučava Koblitzove eliptičke krivulje, to jest, krivulje oblika oblika $y^2 + xy = x^3 + a_2x^2 + 1$ za $a_2 = 0$ ili 1. Njihovi koeficijenti su iz polja $\mathbb{F}_2$, no u primjenama ih se promatra kao krivulje nad $\mathbb{F}_{2^d}$ za veliki d. Obrađeni su osnovni algoritmi za računanje s Koblitzovim krivuljama, a posebno računanje višekratnika točaka, kod kojeg se dupliciranje točaka može zamijeniti primjenom Frobeniusovog endomorfizma.

U prvom poglavlju dane su osnove kriptografije i korištenja eliptičkih krivulja u kriptografiji.

U drugom poglavlju detaljnije se opisuju Koblitzove eliptičke krivulje te se, pri razlaganju problema računanja višekratnika, objašnjava pojam Frobeniusovog endomorfizma.

U trećem poglavlju pojašnjavaju se različiti načini na koje se elementi iz $\mathbb{Z}[\tau]$ mogu prikazati. Takvi prikazi koriste se u algoritmima koji računaju višekratnike točaka, koji su puno brži od uobičajenih metoda za izračunavanje višekratnika. Obrađuje se i metoda prozora, koja osigurava još efikasnije računanje višekratnika na eliptičkoj krivulji.

U posljednjem poglavlju nabrajaju se Koblitzove eliptičke krivulje koje su odobrene za korištenje te se razmatra budućnost eliptičkih krivulja.

Summary

This thesis studies Koblitz elliptic curves, that are defined over binary field $\mathbb{F}_2$ as $y^2 + xy = x^3 + a_2x^2 + 1$, where $a = 0$ or 1. In cryptographic protocols, they can also be defined as curves over extension field $\mathbb{F}_{2^d}$ for large d. Some basic methods for efficient computation with those curves were introduced in this paper, but most importantly, it was shown that by using Frobenius endomorphism, scalar multiplication can be efficiently implemented without the need for point doubling.

First chapter contains general overview of cryptography and describes advantages of using elliptic curves in modern cryptography.

Second chapter introduces Koblitz elliptic curves and its properties as well as the Frobenius endomorphism in detail.

In third chapter it was analyzed how different types of expansion, used on elements in $\mathbb{Z}[\tau]$, effect on efficiency of scalar multiplications and speed of computation. It was shown that some expansions can significantly improve efficiency of computation on Koblitz elliptic curves. Also, windowing method can be used for faster scalar multiplication and is described in detail in this chapter.

Last chapter gives an update of current elliptic curve standards and considers the future of elliptic curves in modern cryptography.

Životopis

Rođena sam 13. srpnja 1992. godine u Zagrebu. Završila sam Osnovnu školu "Sesvete" u Sesvetama, gdje sam pohađala i istoimenu opću gimnaziju. 2011. godine upisala sam Prirodoslovno-matematički fakultet Sveučilišta u Zagrebu, smjer Matematika. 2015. godine završila sam preddiplomski studij matematike i stekla titulu sveučilišne prvostupnice matematike, univ.bacc.math. Te godine upisujem i diplomski studij Matematike i računarstva na istom fakultetu, koji trenutno završavam.