Eliptičke krivulje i kriptiranje

Musulin, Zdravko

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Zdravko Musulin

ELIPTIČKE KRIVULJE I KRIPTIRANJE

Diplomski rad

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

Zagreb, lipanj, 2016.

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. _____

Sadržaj

Uvod

Ljudi su oduvijek imali potrebu čuvanja informacija i tajni jedni od drugih. Primjerice kraljevi ili zapovjednici koji su u komunikaciji s vojnicima, koristeći osnovne kriptografske metode, nastojali spriječiti neprijatelja od saznavanja nekih strateški bitnih informacija. Tako je i jedan jednostavan šifrat, kojeg je koristio Cezar, nazvan po njemu. Od tada je, paralelno s napretkom društva, rasla i potreba za mnogo sofisticiranijim metodama, osobito danas u dobu koje nazivamo „informacijskim". Kako svijet postaje sve više povezan, zahtjevi za brzim razmjenama informacija i elektroničkim uslugama također se povećavaju, a samim time i ovisnost o elektroničkim sustavima. Tako je razmjena osjetljivih informacija, primjerice brojeva kreditnih kartica, postala naša stvarnost, pa je zaštita podataka i elektroničkih sustava koji ih pohranjuju krucijalna. Tehnike potrebne za zaštitu podataka spadaju u područje kriptografije. Ta se znansvena disciplina bavi istraživanjem, razvojem i implementacijom metoda zaštite podataka, dok joj je komplementarna tzv. kriptoanaliza, koja je usmjerena napadima i „razbijanjima" kriptosustava. Ove dvije discipline tvore i općenitiju, tzv kriptologiju, koja proučava komunikaciju nesigurnim kanalima i s tim povezane probleme.

Eliptičke krivulje intenzivno se pučavaju već preko 100 godina u algebarskoj geometriji te postoji značajna količina literature o njima. Tako je i poznati matematičar Serge Lang (1927.–2005.) u jednoj od svojih studija napisao: „O eliptičkim je krivuljama moguće beskonačno pisati. (Ovo nije prijetnja.)" Međutim, u posljednja dva-tri desetljeća zauzimaju posebno istaknuto mjesto u teoriji brojeva i srodnom području, kriptografiji. Naime, 1980-ih godina razvile su se tehnike koje koriste eliptičke krivulje u faktorizaciji i dokazivanju prostosti, a uočila se i težina problema diskretnog logaritma u grupi točaka eliptičkih krivulja, pa su pronalazile svoju primjenu u kriptosustavima zasnovanima na tom problemu. Možda je ipak najznačajniji poticaj za njihovu primjenu, daljnja istraživanja i implementacije dao dokaz Velikog Fermatovog teorema od A. Wilesa, 1995. godine, u kojem se one koriste.

U ovom radu, zbog mnogih ograničenja, ipak nije beskonačno pisano o eliptičkim krivuljama, ali je u prvom poglavlju dan njihov općeniti pregled. Isto tako, navedni su neki

temeljni matematičkim pojmovima potrebni za daljnji rad te svojstva eliptičkih krivulja nad poljem racionalnih brojeva i nad konačnim poljima. Ova posljednja su posebno naglašena, osobito računanje reda grupe točaka eliptiče krivulje nad njima, jer imaju važnu ulogu pri izboru parametara u algoritmima i kriptosustavima koji koriste eliptičke krivulje.

U drugom poglavlju opisana je kriptografija javnog ključa, od same ideje i potrebe za nastankom, pa do implementacije eliptičkih krivulja u kriptosustave. Također, posebno je objašnjen problem diskretnog algoritma, kako običnog, tako i onog za eliptičke krivulje. Dakle, izloženi su kriptosustavi koji koriste eliptičke krivulje (kraće ECC), a u osnovi imaju problem diskretnog logaritma. Zbog cjelovitije slike i boljeg razumijevanja, opisan je i klasik među kriptosustavima javnog ključa - RSA kriptosustav, koji je utemeljen na faktorizaciji velikih prirodnih brojeva. Na kraju, komentira se izbor parametara ECC kriptosustava te ih se uspoređuje s RSA sustavom, ali i sa simetričnim kriptosustavima.

Poglavlje 1

Eliptičke krivulje

1.1 Uvod i motivacija

Piramida topovskih kugli

Neka je skup topovskih kugli posložen u obliku pravilne četverostrane piramide s jednom kuglom na vrhu (u prvom sloju), četiri u drugom sloju, devet u trećem sloju, itd. Ako se takva gomila uruši, je li moguće presložiti sve kugle tako da dobijemo kvadrat?

Slika 1.1: Piramida topovskih kugli

Ako piramida ima tri sloja, onda to nije moguće napraviti budući da je $1 + 4 + 9 = 14$, a to nije potpuni kvadrat. Naravno ako je samo jedna kugla, tada je ona i piramida visine 1, ali i jedinični kvadrat, a u slučaju da nema kugli, poimanje „prazne" piramide i kvadrata nema smisla. Ima li još nekih slučajeva, pored ovih trivijalnih ? Pronaći ćemo još neke slučajeve koristeći metodu koja potječe od Diofanta (oko 250. godine pr.Kr.).

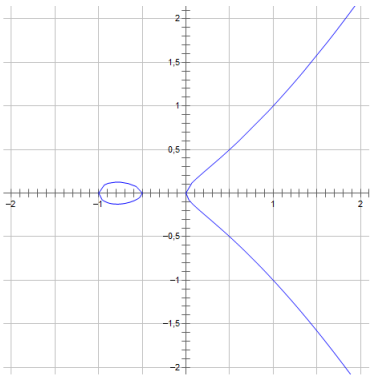
Neka je x visina piramide. Tada je ukupno

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

kugli. Želimo da ovo bude potpuni kvadrat pa tražimo rješenje jednadžbe

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

u pozitivnim cijelim brojevima x i y. Jednadžba ovog oblika predstavlja jednu **eliptičku krivulju**.



Slika 1.2: Eliptička krivulja

Za pronalaženje novih točaka, Diofantova metoda koristi one koje već znamo. Počnimo s točkama $(0, 0)$ i $(1, 1)$. Pravac kroz ove dvije točke je $y = x$. Presjek s krivuljom daje nam jednadžbu

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

Sređivanjem slijedi

$$x^3 - \frac{3}{2}x^2 + \frac{1}{2}x = 0.$$

Znamo da su rješenja ove jednadžbe 0 i 1 budući da su to $x-$koordinate sjecišta pravca i krivulje. Mogli bismo faktorizirati polinom kako bismo pronašli treće rješenje, međutim postoji i bolji način. Znamo da za bilo koje a, b, c vrijedi

$$(x-a)(x-b)(x-c) = x^3 - (a+b+c)x^2 + (ab+ac+bc)x - abc.$$

Kako je koeficijent uz x^3 jednak 1, negativna vrijednost koeficijenta uz x^2 suma je rješenja jednadžbe. U našem slučaju to znači

$$0 + 1 + x = \frac{3}{2}.$$

Slijedi da je $x = \frac{1}{2}$, a kako je pravac $y = x$, vrijedi i da je $y = \frac{1}{2}$. U smislu topovskih kugli ovo ne smatramo rješenjem, ali smo barem uspjeli pronaći još jednu netrivijalnu i racionalnu točku na krivulji. Zbog simetrije krivulje, pronašli smo još jednu točku, $(\frac{1}{2}, -\frac{1}{2})$. Kako tražimo sjecište u prvom kvadrantu, možemo ponoviti prethodnu proceduru s točkama $(\frac{1}{2}, -\frac{1}{2})$ i $(1, 1)$. Pravac koji prolazi ovim točkama je $y = 3x - 2$, a presjek s krivuljom daje nam jednadžbu

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

Sređivanjem slijedi

$$x^3 - \frac{51}{2}x^2 + ... = 0.$$

Znamo da su rješenja $\frac{1}{2}$ i 1, pa zaključivanjem kao u prethodnom slučaju slijedi

$$\frac{1}{2} + 1 + x = \frac{51}{2}.$$

Stoga je $x = 24$, a kako je pravac $y = 3x - 2$, vrijedi da je $y = 70$.. To znači da je

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

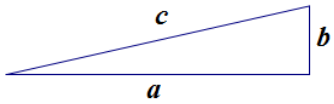
Dakle, 4900 topovskih kugli, možemo raspodijeliti u piramidu visine 24 ili u kvadrat dimenzija 70×70. Ako nastavimo s gore navedenom procedurom, koristeći, primjerice, upravo dobivene točke, dobit ćemo beskonačno mnogo racionalnih rješenja jednadžbe.

Pravokutni trokut

Postoji li, uz poznatu cijelu vrijednost d, pravokutni trokut s racionalnim stranicama kojem je površina upravo d ? Primjerice, neka je $d = 5$. Najmanja Pitagorina trojka je $(2, 4, 5)$ te je povšina tog trokuta 6. Stoga ne možemo razmatrati cijelobrojne, tj. prirodne vrijednosti stranica. Pitagorina trojka $(8, 15, 17)$ tvori trokut površine 60, a ukoliko svaku od stranica dvostruko skratimo dobijemo trokut sa stranicama 4, $\frac{15}{2}$ te $\frac{17}{2}$ kojem je površina 15. Stoga, na temelju ovog primjera uočavamo da postoji trokut s racionalnim stranicama čija je površina cijelobrojna.

Neka su stranice trokuta kojeg tražimo označene s a, b, c kao na slici 1.3. Kako je njegova površina $\frac{ab}{2}$=5, tražimo racionalne brojeve a, b, c takve da vrijedi

$$a^2 + b^2 = c^2, \quad ab = 10$$



Slika 1.3: Pravokutni trokut

Transformacijom slijedi

$$\left(\frac{a+b}{2}\right)^2 = \frac{a^2+2ab+b^2}{4} = \frac{c^2+20}{4} = \left(\frac{c}{2}\right)^2 + 5$$

$$\left(\frac{a-b}{2}\right)^2 = \frac{a^2-2ab+b^2}{4} = \frac{c^2-20}{4} = \left(\frac{c}{2}\right)^2 - 5$$

Neka je $x = \left(\frac{c}{2}\right)^2$. Tada je

$$x-5 = \left(\frac{a-b}{2}\right)^2, \qquad x+5 = \left(\frac{a+b}{2}\right)^2.$$

Dakle, tražimo racionalni broj x takav da su $x-5, x, x+5$ istovremeno kvadrati racionalnih brojeva. Pretpostavimo da postoji takav broj x. Tada umnožak $(x-5)x(x+5) = x^3 - 25x$ također mora biti kvadrat pa tražimo racionalno rješenje jednadžbe

$$y^2 = x^3 - 25x.$$

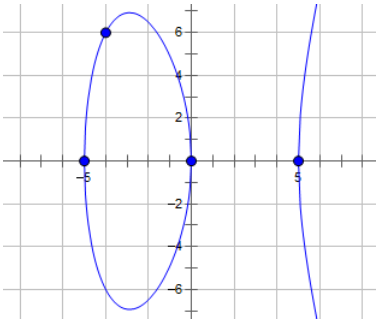
Jednadžba ovog oblika predstavlja jednu **eliptičku krivulju**.

Tri očite točke koje pripadaju krivulji su $(-5,0)$, $(0,0)$, $(5,0)$, međutim, to nam ne pomaže mnogo jer sve tri prolaze istim pravcem te ne tvore trokut. Gledajući krivulju prikazanu na slici 1.4 te uvrštavanjem, uočavamo da točka $(-4,6)$ pripada krivulji. Deriviranjem implicitno zadane funkcije možemo pronaći jednadžbu tangente na krivulju koja prolazi točkom $(-4,6)$. Dakle,

$$2yy' = 3x^2 - 25 \Leftrightarrow y' = \frac{3x^2-25}{2y}.$$

Uvrštavanjem vrijednosti slijedi da je jednadžbe tangente

$$y = \frac{23}{12}x + \frac{41}{3}.$$



Slika 1.4: Eliptička krivulja $y^2 = x^3 - 25x$

Za sjecište vrijedi

$$\left(\frac{23}{12}x + \frac{41}{3}\right)^2 = x^3 - 25x \Rightarrow x^3 - \left(\frac{23}{12}\right)^2 x^2 + \ldots = 0.$$

Kako je pravac tangenta na krivulju u $(-4, 6)$, $x = -4$ je dvostruko rješenje, pa je zbroj rješenja

$$-4 - 4 + x = \left(\frac{23}{12}\right)^2.$$

Iz toga zaključujemo da je $x = \dfrac{1681}{144} = \left(\dfrac{41}{12}\right)^2$, a $y = \dfrac{62279}{1728}$. Vraćanjem prethodne supstitucije $x = \left(\dfrac{c}{2}\right)^2$, slijedi da je $c = \dfrac{41}{6}$. Kako je

$$y = \sqrt{(x-5)x(x+5)} = \frac{(a-b)c(a+b)}{8} = \frac{(a^2-b^2)c}{8},$$

slijedi

$$\frac{62279}{1728} = y = \frac{(a^2-b^2)c}{8} = \frac{41(a^2-b^2)}{48} \Rightarrow a^2 - b^2 = \frac{1519}{36}.$$

Kako je trokut pravokutan, znamo da mora vrijediti i

$$a^2 + b^2 = c^2 = \left(\frac{41}{12}\right)^2,$$

pa rješavanjem danog sustava slijedi $a^2 = \dfrac{400}{9}$ i $b^2 = \dfrac{9}{4}$. Uzimajući u obzir samo pozitivne vrijednosti, konačna rješenja su

$$a = \frac{20}{3}, \quad b = \frac{3}{2}, \quad c = \frac{41}{6}.$$

To su dakle racionalne stranice trokuta kojem je površina 5, a može se primijetiti da je to Pitagorina trojka $(40, 9, 41)$ umanjena 6 puta. Ako nastavimo s gore navedenom procedurom, koristeći, primjerice, upravo dobivene točke, dobit ćemo beskonačno mnogo racionalnih rješenja jednadžbe.

1.2 Neki matematički pojmovi

Prije nego razjasnimo što su to eliptičke krivulje, treba nam koncept jednostavnijih algebarskih struktura - grupe, prstena i polja. Stoga ćemo navesti niz matematičkih pojmova i tvrdnji, prvenstveno iz područja algebre, a sve sa ciljem boljeg razumijevanja glavne teme.

Grupe

Definicija 1.2.1. *Neprazan skup $G = (G, \cdot)$ je **grupa** obzirom na binarnu operaciju*

$$\cdot : G \times G \to G$$

ako vrijede sljedeća svojstva (aksiomi grupe)*:*

1. $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ *za sve* $x, y, z \in G$ (asocijativnost)*,*
2. $(\exists\, e \in G) : \quad e \cdot x = x \cdot e = x \quad \forall x \in G$ (neutralni element)*,*
3. $(\forall x \in G)(\exists!\, x^{-1} \in G) : \quad x \cdot x^{-1} = x^{-1} \cdot x = e$ (inverzni element)*.*

Ako vrijedi i svojstvo $x \cdot y = y \cdot x$, $\forall x \in G$ (komutativnost), onda kažemo da je grupa **Abelova** ili **komutativna**. U suprotnom govorimo o **neabelovoj** ili **nekomutativnoj** grupi. Apstraktna grupa $(G, \cdot)$ zove se **multiplikativna** grupa, a binarna operacija zove se množenje. To je neprecizan naziv jer operacija u konkretnoj situaciji može biti zbrajanje, kompozicija funkcija itd.

Ako je u nekoj grupi binarna operacija zadana aditivno, odnosno zadana je grupa $(G, +)$, grupu zovemo **aditivnom** grupom.

Podskup H grupe G koji je i sam grupa s obzirom na istu operaciju kao i G naziva se **podgrupa** od G. Pišemo $H \leq G$.

Propozicija 1.2.2. *Podskup $H \subseteq G$ je podgrupa grupe G ako i samo ako vrijedi sljedeće:*

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

Budući se lako može pokazati da je presjek bilo koje množine podgrupa od G ponovo podgrupa od G, smisleno je promatrati sljedeći skup. Za proizvoljan podskup S neke grupe G definiramo

$$\langle S \rangle := \bigcap_{\substack{H<G \\ S \subseteq G}} H.$$

Kako je taj presjek podgrupa od G također podgrupa, opravdano ga je nazvati **grupa generirana** sa S. Sam skup S zove se **skup generatora**.

Grupa G je **konačnogenerirana** ako postoji konačan podskup $S = \{x_1, ..., x_n\}$ takav da je $G = \langle S \rangle$, a **ciklička** je ako se može generirati jednim elementom, tj. ako postoji neki $g \in G$ takav da je $G = \langle g \rangle$. Takav g zovemo **generatorom** grupe G. Primjerice, grupa $\mathbb{Q} = (\mathbb{Q}, +)$ nije ciklička, točnije, ni konačno generirana, dok je $\mathbb{Z} = (\mathbb{Z}, +)$ beskonačna ciklička grupa s -1 i 1 kao generatorima. Grupa ostataka modulo n, u oznaci $(\mathbb{Z}/n\mathbb{Z}, +)$ konačna je ciklička grupa, a broj njenih generatora dan je *Eulerovom funkcijom* $\varphi : \mathbb{N} \to \mathbb{N}$;

$$\varphi(n) := \text{ card}\{1 \leq k \leq n \,|\, (k, n) = 1\}.$$

Tako, npr. grupa $(\mathbb{Z}/10\mathbb{Z}, +)$ ima $\varphi(10) = 4$ generatora; to su $\overline{1}, \overline{3}, \overline{7}$ i $\overline{9}$.

Red grupe G je $|G| := card(G)$, odnosno red grupe kardinalni je broj skupa G. Grupa G je **konačna grupa** ako je $|G| < \infty$, a inače je G **beskonačna grupa**.
Za svaku konačnu grupu G, red (broj elemenata) podgrupe H od G dijeli red od G. Stoga red podgrupe ne može biti proizvoljan, pa ako je $|G| = p$ gdje je p prosti broj, tada je $|H| = 1$ ili $|H| = p$ što povlači da G ima samo trivijalne podgrupe $H = \{e\}$ i $H = G$.

Prsten i polje

Definicija 1.2.3. *Neprazan skup $R = (R, +, \cdot)$ je **prsten** obzirom na binarne operacije zbrajanja $+ : R \times R \to R$ i množenja $\cdot : R \times R \to R$ ako vrijedi sljedeće:*

1. *$(R, +)$ je komutativna grupa s neutralnim elementom $0 = 0_R$ (nula);*
2. *$(R, \cdot)$ je polugrupa, tj. množenje je asocijativno;*
3. *vrijedi distributivnost množenja prema zbrajanju, tj.*

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

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

Ako postoji **jedinični element** ili kraće **jedinica**, $1 = 1_R \in R$, takav da je

$$1 \cdot x = x \cdot 1 = x, \quad \forall x \in R,$$

onda kažemo da je R prsten s jedinicom. Nadalje, prsten R je **komutativan** ako je množenje komutativno, tj.

$$x \cdot y = y \cdot x, \quad \forall x, y \in R.$$

Inače, govorimo o **nekomutativnom** prstenu.

Element $a \neq 0 \in R$ (tj.,$b \neq 0 \in R$) takav da je $ax = 0$ (tj. $xb = 0$), za neki $0 \neq x \in R$ zove se **lijevi** (tj. **desni**) **djelitelj nule**. Prsten R je **integralna domena**, skraćeno **domena**, ako nema ni lijevih ni desnih djelitelja nule.

Element $a \in R$, gdje je R prsten s jedinicom, **invertibilan** je ako postoji $a' \in R$ takav da je $aa' = a'a = 1$. Skup svih invertibilnih elemenata u R označavamo sa $R^\times$. Može se lako ustanoviti da je $R^\times$ grupa, pa ju zovemo **grupa invertibilnih elemenata** (ponekad i **grupa jedinica**).

Definicija 1.2.4. *Neka je R prsten. Ako postoji prirodan broj m takav da je*

$$m \cdot x = 0, \quad \forall x \in R,$$

*tada najmanji prirodan broj sa takvim svojstvom zovemo **karakteristika prstena** R. Ako takav prirodan broj m ne postoji kažemo da je **prsten karakteristike nula**. Karakteristiku prstena R označavamo sa $k(R)$ ili* $\operatorname{char} K$.

Lema 1.2.5. *Neka je R prsten sa jedinicom* 1. *Vrijedi:*

1) *Karakteristika $k(R)$ prstena R je prirodan broj ako i samo ako je $k(R)$ najmanji prirodan broj m za koji vrijedi $m \cdot 1 = 0$.*

2) *Prsten R je karakteristike nula ako i samo ako $\forall x \in R$ vrijedi $n \cdot 1 \neq 0$.*

Kako bismo u jednoj algebarskoj strukturi mogli izvoditi operacije zbrajanja, oduzimanja, množenja i dijeljenja (osim dijeljenja s nulom) ona treba sadržavati i aditivnu i multiplikativnu grupu. Takva struktura je polje.

Definicija 1.2.6. *Prsten R je **tijelo**, tj. **prsten s dijeljenjem**, ako je svaki ne-nul element u R invertibilan, odnosno, ukoliko je*

$$R^\times = R \backslash \{0\}.$$

*Komutativno tijelo zovemo **polje**.*

Definicija 1.2.7. *Ako je broj elemenata polja K konačan, kažemo da je K **konačno polje**, a spomenuti broj elemenata zovemo **red konačnog polja** i označavamo ga s $|K|$.*

Definicija 1.2.8. ***Karatkeristika polja*** *K je najmanji prirodni broj n takav da je*

$$1 + 1 + ... + 1 = n \cdot 1 = 0,$$

gdje su 0 *i* 1 *neutralni elementi za zbranjanje i množenje. Označava se s* $\text{char}\, K$. *Ako takav n ne postoji, onda govorimo da je polje K* ***karakteristike nula*** *i pišemo* $\text{char}\, K = 0$.

Osnovni primjer polja je $\mathbb{Q}$, polje racionalnih brojeva, a ostali važni primjeri su polje realnih brojeva $\mathbb{R}$, te polje kompleksnih brojeva $\mathbb{C}$. Naravno, riječ je o beskonačnim poljima jer imaju beskonačno mnogo elemenata. Skup $\mathbb{Z}$ nije polje, jer samo 1 i -1 imaju inverz obzirom na operaciju množenja. Za bilo koji prost broj p, polje cijelih brojeva modulo p, u oznaci $\mathbb{Z}/p\mathbb{Z}$ primjer je konačnog polja.

Teorem 1.2.9. *Ako je $R \neq \{0\}$ prsten s jedinicom bez djelitelja nule, tada vrijedi jedna od slijedećih tvrdnji:*

1) Karakteristika p prstena R je prost broj, te vrijedi da je $m \cdot x = 0$ ako i samo ako $p \mid m$ ili $x = 0$.

2) Prsten R je karakteristike 0, te vrijedi da je $m \cdot x = 0$ ako i samo ako $x = 0$.

Teorem 1.2.10. *Karakteristika konačnog polja K je prost broj.*

Dokaz. Pokažemo li da je karakteristika konačnog polja K prirodan broj, tada iz prethodnog teorema slijedi da je taj broj prost. Promotrimo skup

$$\{n \cdot 1; n \in \mathbb{N}\} \subseteq K.$$

Svi elementi tog skupa ne mogu biti različiti, jer je polje K konačno. Prema tome postoje $k, l \in \mathbb{N}$, $k \neq l$, tako da je $k \cdot 1 = l \cdot 1$. Bez smanjenja općenitosti možemo pretpostaviti da je $l > k$, pa je $l - k \in \mathbb{N}$ i $(l - k) \cdot 1 = 0$. Iz Leme 1.2.5, slijedi da je karakteristika polja K prirodan broj. □

Eliptičke krivulje može se promatrati 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.

Polja $\mathbb{Q}, \mathbb{R}$ i $\mathbb{C}$ su karakteristike 0, dok je karakteristika od $\mathbb{F}_q$ jednaka p, gdje je p prost broj i $q = p^m$ za neki prirodan broj m. Naglasimo da, primjerice, postoje konačna polja s 13 elemenata, s 27 elemenata (jer je $3^3 = 27$), ili s 512 elemenata (jer je $2^9 = 512$), ali ne postoji konačno polje s 14 elemenata, jer 14 nije potencija niti jednog prostog broja.

Definicija 1.2.11. *Ako su L, K polja takva da je $L \subseteq K$, onda kažemo da je L* ***potpolje*** *od K, ili da je K proširenje od L. To označavamo*

$$L \mid K.$$

Ustvari, L nasljeđuje strukturu polja od K. Na primjer, $\mathbb{Q}$ i $\mathbb{R}$ su potpolja u $\mathbb{C}$. Najmanje potpolje od K je presjek svih njegovih potpolja. To je u biti polje generirano s neutralni elementom množenja 1. Svako polje K ima najmanje potpolje koje zovemo **prosto** potpolje i ono je izomorfno ili polju racionalnih brojeva $\mathbb{Q}$ ili polju $\mathbb{Z}_p$, u ovisnosti od karakeristike polja.

Polinomi

Definicija 1.2.12. ***Polinom*** *stupnja n nad poljem K je izraz* $f(x)$ *oblika*

$$a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0, \quad a_i \in K.$$

Za polinom $f(x)$ kažemo da je normiran ukoliko je $a_n = 1$. Prsten polinoma nad poljem K u varijabli x označavamo s $K[x]$.

Ako za neki $k \in K$ vrijedi $f(k) = 0$, kažemo da je k **korijen** ili **nul-točka** polinoma $f(x)$. Tada je polinom $f(x)$ djeljiv polinomom $x - k$, tj. postoji polinom $q(x)$ nad K takav da je $f(x) = (x-k)q(x)$. Ako je $f(x)$ djeljiv polinomom $(x-k)^m$, a nije djeljiv s $(x-k)^{m+1}$, za k kažemo da je $m-$struki korijen ili $m-$struka nultočka polinoma $f(x)$.

Ireducibilni polinom u $K[x]$ polinom je koji se ne može prikazati kao umnožak dva nekonstantna polinoma iz $K[x]$. Ako polinom $f(x)$ nije ireducibilan, kažemo da je reducibilan, rastavljiv na umnožak dva polinoma od kojih niti jedan nije konstantan. Ireducibilni polinomi u prstenu $K[x]$ imaju ulogu koju prosti brojevi imaju u prstenu cijelih brojeva $\mathbb{Z}$, a nijedan korijen ireducibilnog polinoma nije sadržan u polju K.

Za polje K kažemo da je **algebarski zatvoreno** ako svaki polinom nad K ima barem jednu nultočku. Primjer algebarski zatvorenog polja je $\mathbb{C}$, dok primjerice $\mathbb{R}$ nije algebarski zatvoreno.

Vektorski prostor

Definicija 1.2.13. *Neka je V neprazan skup i neka je K polje skalara. Uređena trojka* $V = (V, +, \cdot)$ *naziva se* ***vektorski prostor*** *nad poljem K ako za binarnu operaciju* $+ : V \times V \to V$ *i operaciju* $\cdot : K \times V \to V$ *te za sve* $\alpha, \beta \in K$ *i* $x, y \in V$ *vrijede sljedeća svojstva:*

1) $(V, +)$ *je Abelova grupa;*

2) $\alpha \cdot (x + y) = \alpha \cdot x + \alpha \cdot y$;

3) $(\alpha +_K \beta) \cdot x = \alpha \cdot x + \beta \cdot x$;

4) $\alpha \cdot (\beta \cdot x) = (\alpha \cdot_K \beta) \cdot x$;

5) $1_K \cdot x = x$.

Elemente vektorskog prostora V zovemo ***vektorima****, elemente polja K* ***skalarima****. Binarna operacija naziva se zbrajanje vektora,* $a \cdot : K \times V \to V$ *operacija množenjenja vektora skalarom.*

Govorimo o kompleksnom vektorskom prostoru za vektorski prostor nad poljem $\mathbb{C}$, odnosno o realnom vektorskom prostoru za vektorski prostor nad poljem $\mathbb{R}$. Vektorski prostor geometrijski interpretiramo kao „ravninu" kroz ishodište.

Definicija 1.2.14. *Neka je V vektorski prostor nad poljem K te* $n \in \mathbb{N}$. *Za* $v_1, \ldots, v_n \in V$ *i* $\alpha_1, \ldots, \alpha_n \in K$ *vektor*

$$v' = \alpha_1 \cdot v_1 + \cdots + \alpha_n \cdot v_n = \sum_{i=1}^{n} \alpha_i v_i$$

nazivamo ***linearnom kombinacijom*** *vektora* $v_1, \ldots, v_n$.

Definicija 1.2.15. *Ako je V vektorski prostor nad poljem K, za* $S \subseteq V$, $S \neq \emptyset$, ***linearnu ljuska*** *skupa S označava se simbolom* $[S]$ *i definira kao skup svih linearnih kombinacija vektora iz S, tj.*

$$[S] = \left\{ \sum_{i=1}^{k} \alpha_i v_i : \alpha_i \in K, v_i \in S, k \in \mathbb{N} \right\}.$$

Dodatno se definira $[\emptyset] = \{0\}$.

Definicija 1.2.16. *Neka je V vektorski prostor nad poljem K. Za vektore* $v_1, \ldots, v_n \in V$ *kažemo da su* ***linearno zavisni*** *ako postoje skalari* $\alpha_1, ..., \alpha_n \in K$ *takvi da je barem jedan različit od nule i pri tome vrijedi:*

$$\alpha_1 \cdot v_1 + \cdots + \alpha_n \cdot v_n = \sum_{i=1}^{n} \alpha_i v_i = 0.$$

U suprotnom za vektore $v_1, \ldots, v_n \in V$ *kažemo da su* ***linearno nezavisni****.*

U prostoru R^2 su vektori $v_1 = (1, 0)$ i $v_2 = (0, 1)$ linearno nezavisni. Također su takvi i vektori $w_1 = (3, 4)$ i $w_2 = (-1, 5)$. Doista, iz $\alpha_1 w_1 + \alpha_2 w_2 = 0$ slijedi $3\alpha_1 - \alpha_2 = 0$ i $4\alpha_1 + 5\alpha_2 = 0$, a taj sustav ima rjesenje $\alpha_1 = \alpha_2 = 0$.

Definicija 1.2.17. *Neka je V vektorski prostor i* $S \subseteq V$. *Kažemo da je skup S* ***sustav izvodnica*** *za V, tj. da S* ***generira*** *V ako vrijedi* $[S] = V$.

Definicija 1.2.18. *Neka je V vektorski prostor nad poljem K i $B \subseteq V$. Konačan skup vektora B je **baza** vektorskog prostora V ako je B linearno nezavisan sustav izvodnica za V.*

Vektorski prostor je **konačnogeneriran** ako postoji konačan skup izvodnica. Svaki konačnogeneriran skup ima i konačnu bazu. Prostor koji ima konačnu bazu naziva se **konačnodimenzionalan**. Svake dvije baze vektorskog prostora su jednakobrojne, pa ima smisla definirati **dimenziju** vektorskog prostora V kao broj elementata baze, u oznaci $\dim V$.

Primjer 1.2.19. *a) Skup $\{(1,0,0),(0,1,0),(0,0,1)\}$ je baza prostora $\mathbb{R}^3$, ali također i baza kompleksnog prostora $\mathbb{C}^3$.*

b) Općenito, u prostoru $\mathbb{R}^n$ promotrimo vektore $e_1 = (1,0,0,\ldots,0)$,$e_2 = (0,1,0,\ldots,0)$,... $e_n = (0,0,0,\ldots,1)$. Skup $\{e_1, e_2, \ldots, e_n\}$ je baza prostora $\mathbb{R}^n$, ali i prostora $\mathbb{C}^n$.

c) $\{1, t, t^2, \ldots, t^n\}$ je baza prostora P^n tj. prostora svih polinoma stupnja $\leq n$.

d) Skupovi $\{(1,1,1),(1,2,0),(1,0,0)\}$ i $\{(2,1,0),(1,1,7),(-1,-2,4)\}$ su također baze prostora $\mathbb{R}^3$.

Baze u primjerima (a), (b), (c), zovu se standardne ili kanonske baze navedenih prostora. Svaki se vektor tih prostora prirodno prikazuje kao jedistvena linearna kombinacija elemenata ovih baza, dok primjer (e) nije standardan. Želimo li prikazati vektor $x = (x_1, x_2, x_3) \in \mathbb{R}^3$ kao linearnu kombinaciju vektora jedne ili druge navedene baze, trebat ćemo riješiti sustav od tri linearne jednadžbe s tri nepoznanice.

1.3 Definicija eliptičke krivulje

Neka je K polje. Eliptička krivulja nad K općenito je nesingularna projektivna krivulja nad K s barem jednom točkom. Njena je jednadžba oblika

$$F(x,y) = ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0, \qquad (1.1)$$

pri čemu su koeficijenti $a, b, c, \ldots, j \in K$, a nesingularnost znači da u svakoj točki na krivulji, promatranoj u projektivnoj ravnini $\mathbb{P}^2(\overline{K})$ nad algebarskim zatvorenjem od K postoji barem jedna parcijalna derivacija funkcije F; $\dfrac{\partial F}{\partial x}, \dfrac{\partial F}{\partial y}$ koja je različita od nule. Geometrijski, nesingularnost znači da nema „šiljaka" i ne postoje točke u kojima se krivulja siječe sama sa sobom te nema izoliranih točaka.

Svaka jednadžba oblika (1.1)može se transformacijama svesti na oblik

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \qquad (1.2)$$

koji nazivamo **generalizirana Weierstrassova forma**. Oblik (1.2) koristi se u poljima koja su karakteristike 2 ili 3. Eliptičke krivulje u takvim poljima popularne su u kriptografiji jer se njihova aritmetika može učinkovitije implementirati na računala. Ako je karakteristika polja različita od 2, možemo dijeljenjem s 2 te nadopunom kvadrata:

$$\left(y + \frac{a_1 x}{2} + \frac{a_3}{2}\right)^2 = x^3 + \left(a_2 + \frac{a_1^2}{4}\right)x^2 + \left(a_4 + \frac{a_1 a_3}{2}\right)x + \left(\frac{a_3^2}{4} + a_6\right),$$

dovesti do

$$y_1^2 = x^3 + a_2' x^2 + a_4' x + a_6'$$

gdje je $y_1 = y + \frac{a_1 x}{2} + \frac{a_3}{2}$, a a_2', a_4' i a_6' neke konstante. Ukoliko je karakteristika polja različita i od 3, možemo označiti da je $x_1 = x + \frac{a_2'}{3}$ te pisati

$$y_1^2 = x_1^3 + Ax_1 + B, \tag{1.3}$$

za neke konstante A i B. Oblik (1.3)zovemo **kratka Weierstrassova forma**. Uvjet nesingularnosti sada je da kubni polinom $f(x) = x^3 + Ax + B$ nema višestrukih nultočaka (u $\overline{K}$).

Definicija 1.3.1. *Neka je $f(x)$ polinom u jednoj varijabli stupnja n s nultočkama $r_1, r_2, \ldots, r_n$.* ***Diskriminanta*** *od $f(x)$ je veličina*

$$D = \prod_{i \neq j} \left(r_i - r_j\right)^2.$$

Valja napomenuti da se nultočka kratnosti k uzima u obzir k puta, pa je stoga $D = 0$ ako i samo ako $f(x)$ ima višestrukih nultočaka. Ako je $f(x) = x^2 + bx + c$, tada kvadratna formula ukazuje da je

$$D = b^2 - 4c.$$

Formula vrijedi i za diskriminantu kubnog polinoma, a u slučaju kada je koeficijent uz x^2 jednak 0, vrlo je jednostavna.

Teorem 1.3.2. *Ako je $f(x) = x^3 + Ax + B$, tada je*

$$D = -4A^3 - 27B^2. \tag{1.4}$$

Dokaz. Kako je vodeći koeficijent od $f(x)$ jednak 1, slijedi

$$f(x) = (x - r_1)(x - r_2)(x - r_3).$$

Proširivanjem desne strane jednakosti te uspoređivanjem s formulom $f(x) = x^3 + Ax + B$ imamo

$$\begin{aligned} 0 &= -r_1 - r_2 - r_3 \\ A &= r_1r_2 + r_1r_3 + r_2r_3 \\ B &= -r_1r_2r_3. \end{aligned}$$

Iz prve jednakosti slijedi da je $r_3 = -(r_1 + r_2)$, pa je

$$D = (r_1 - r_2)^2(2r_1 + r_2)^2(r_1 + 2r_2)^2.$$

Formule za A i B također možemo drugačije zapisati kao

$$\begin{aligned} A &= -r_1^2 - r_1r_2 - r_2^2 \\ B &= r_1^2r_2 + r_1r_2^2. \end{aligned}$$

Lako se pokazuje da vrijedi identitet

$$(r_1 - r_2)^2(2r_1 + r_2)^2(r_1 + 2r_2)^2 = -4(-r_1^2 - r_1r_2 - r_2^2)^3 - 27(r_1^2r_2 + r_1r_2^2)^2,$$

pa smo dokazali tvrdnju. □

Korolar 1.3.3. *Krivulja $y^2 = x^3 + Ax + B$ je nesingularna ako i samo ako je*

$$-4A^3 - 27B^2 \neq 0.$$

Definicija 1.3.4. *Neka su $A, B \in K$ i $-4A^3 - 27B^2 \neq 0$. **Eliptička krivulja nad poljem** K, čija je karakteristika različita od 2 i 3, skup je točaka $(x, y) \in K \times K$ koje zadovoljavaju jednadžbu*

$$E: \quad y^2 = x^3 + Ax + B,$$

zajedno s „točkom u beskonačnosti" $\mathcal{O}$. Takav skup označavamo s $E(K)$.

Kako bismo razumjeli pojam „točke u beskonačnosti" eliptičku krivulju prikazujemo u projektivnoj ravnini. Najprije uvodimo sljedeću relaciju. Reći ćemo da su $(X_1, Y_1, Z_1) \in K^3$ i $(X_2, Y_2, Z_2) \in K^3$ ekvivalentni ako postoji $\lambda \in K$, $\lambda \neq 0$ takav da je

$$X_1 = \lambda X_2,\ Y_1 = \lambda Y_2,\ Z_1 = \lambda Z_2.$$

Pokazuje se da je ova relacija jedna relacija ekvivalencije na skupu $K^3 \backslash \{(0, 0, 0)\}$ i pišemo

$$(X_1, Y_1, Z_1) \sim (X_2, Y_2, Z_2)$$

.

Definicija 1.3.5. ***Projektivna ravnina*** $\mathbb{P}^2(K)$ *je kvocijentni skupa od* $K^3\backslash\{(0,0,0)\}$ *po relaciji* $\sim$*. Klasu ekvivalencije kojoj je* (X,Y,Z) *reprezentant, označavamo s* $(x:y:z)$*.*

Uvedemo li supsptituciju $x = \dfrac{X}{Z}$, $y = \dfrac{Y}{Z}$, od afine jednadžbe eliptičke krivulje dobivamo onu projektivnu

$$Y^2Z = X^3 + AXZ^2 + BZ^3.$$

Ako je $Z \neq 0$, onda klasa ekvivalencije od (X,Y,Z) ima reprezentant $(x:y:1)$, pa se može identificirati s (x,y). Također, postoji i jedna klasa ekvivalencije koja sadrži točke za koje je $Z = 0$ te ima reprezentant $(0:1:0)$. Upravo tu klasu identificiramo s „točkom u beskonačnosti" $\mathcal{O}$.

Općenito se definira da su eliptičke krivulje nad poljem K projektivne krivulje **genusa** 1 s izdvojenom točkom. Da bismo razumijeli tu karakterizaciju potrebno je određeno znanje algebarske geometrije. Budući da to u našem radu nije potrebno, dovoljno je ugrubo napomenuti da je klasifikacija ploha po genusu ustvari prema broju njihovih „rupa", pa primjerice sfera ima genus 0, a torus genus 1.

1.4 Grupovni zakon

Teorem 1.4.1. *Neka je* $f(x)$ *polinom trećeg stupnja u jednoj varijabli s racionalnim koeficijentima, te* $y = mx + b$ *pravac,* $m, b \in \mathbb{Q}$*. Kubna krivulja* $y^2 = f(x)$ *i pravac* $y = mx + b$ *sijeku se u točno tri točke iz* $\mathbb{C}^2$*, uzimajući u obzir njihove kratnosti. Ako su koordinate dviju točaka presjeka racionalne, takve su i koordinate treće točke.*

Dokaz. Ostaje za dokazati zadnju tvrdnju. Neka su x_1, x_2 i x_3 $x-$koordinate točaka presjeka. Tada je

$$f(x) - (mx + b)^2 = (x - x_1)(x - x_2)(x - x_3).$$

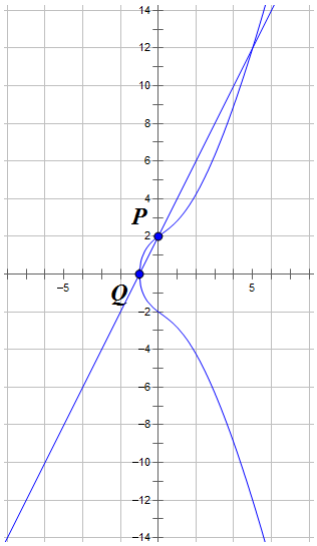
Koeficijent uz x^2 na lijevoj strani jednakosti racionalan je broj, pa takav mora biti i koeficijent uz x^2 na desnoj strani, $-(x_1 + x_2 + x_3)$. Ako pretpostavimo da su x_1 i x_2 racionalni, onda je i x_3. Druga koordinata treće točke presjeka je $mx_3 + b$, pa njena racionalnost slijedi iz racionalnosti od x_3. □

Primjer 1.4.2. *Promotrimo eliptičku krivulju* $y^2 = x^3 + 3x + 4$ *i pravac kroz dvije poznate točke, slika 1.5. Konkretno dane točke krivulje su* $Q = (-1, 0)$ *i* $P = (0, 2)$*, a da bismo odredili treću izračunat ćemo jednadžbu pravca kroz njih. Kako je* $\dfrac{2-0}{0-(-1)} = 2$ *te je*

odsječak na y−osi 2, jednadžba pravca kroz Q i P je $y = 2x + 2$*. Uvrštavanjem tog izraza u jednadžbu krivulje slijedi*

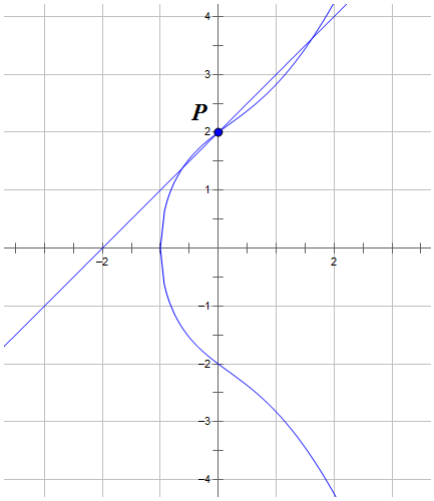
$$(2x + 2)^2 = x^3 + 3x + 4,$$

što se da pojednostavniti do $x(x + 1)(x - 5) = 0$ *iz čega slijedi da je tražena x−koordinata treće točke* $x = 5$*, a pripadna y-koordinata je* $y = 12$*. Dakle, treća točka je* $(5, 12)$*.*



Slika 1.5:

Eliptička krivulja $y^2 = x^3 + 3x + 4$ i pravac kroz dvije poznate točke



Slika 1.6:

Eliptička krivulja $y^2 = x^3 + 3x + 4$ i pravac kroz jednu poznatu točku

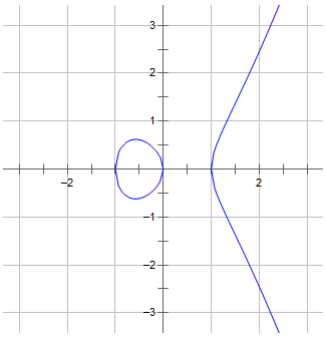
U prethodnom primjeru koristili smo se geometrijom kako bismo pronašli treću točku uz dvije koje smo već znali. Također, kako su obje bile racionalne, morala je biti i treća. Međutim, ako znamo da je jedna točka racionalna, tada preostale dvije na pravcu koji prolazi tom točkom, ne moraju biti racionalne. U to se možemo konkretno uvjeriti iz sljedećeg primjera.

Primjer 1.4.3. *Promotrimo istu eliptičku krivulju* $y^2 = x^3 + 3x + 4$*, pri čemu ćemo prepostaviti da imamo jednu poznatu točku* $P = (0, 2)$*, slika 1.6. Jednadžba pravca kroz P je* $y = x + 2$*. Uvrštavanjem tog izraza u jednadžbu krivulje slijedi*

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

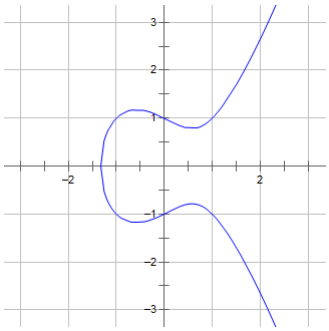
što se da pojednostavniti do $x(x^2 - x - 3) = 0$*. Kvadratna jednadžba* $x^2 - x - 3$ *ima rješenja* $x_{1,2} = \dfrac{1 \pm \sqrt{13}}{2}$ *koja nisu racionalna.*

Jedan od centralnih rezultata teorije eliptičkih krivulja jest da se na njima može, na prirodan način, uvesti operacija uz koju one postaju Abelove grupe. U slučaju da je $K = \mathbb{R}$ polje realnih brojeva, eliptička krivulja $E(\mathbb{R})$ (bez točke u beskonačnosti) može se prikazati kao krivulja u $\mathbb{R}^2$, tj. podskup ravnine. Ovisno o tome je li vrijednost diskriminante(1.4) pozitivna ili negativna, polinom $f(x)$ će imati jednu ili tri nultočke nad $\mathbb{R}$, a graf pripadne eliptičke krivulje jednu ili dvije komponente povezanosti. Primjer eliptičke krivulje s pozitivnom 1.7 i negativnom 1.8 diskriminantom. Na kvadrikama (kružnica, elipsa, hiperbola)



Slika 1.7:

Eliptička krivulja $y^2 = x^3 - x$



Slika 1.8:

Eliptička krivulja $y^2 = x^3 - x + 1$

nove racionalne točke dobiju se metodom sekante, dok je pristup na kubikama drugačiji, jer pravac (općenito) siječe kubiku u tri točke.

Ukoliko želimo da točke na eliptičkoj krivulji tvore grupu, tada ona treba imati dobro definiranu binarnu operaciju, primjerice zbrajanja. Binarna operacija, odnosno zbrajanje na skupu $E(\mathbb{R})$ uvodi se „geometrijski".

Neka su $P = (x_1, y_1)$, $Q = (x_2, y_2)$ točke na eliptičkoj krivulji E čija je jednadžba

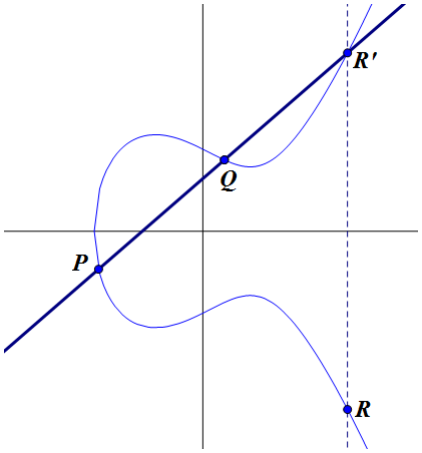
$$y^2 = x^3 + Ax + B.$$

Neka je točka R' presjek pravca L kroz P i Q te krivulje E. Definiramo točku R kao osnosimetričnu točku obzirom na $x-$os točki R' (ima suprotan predznak $y-$koordinate). Tada je

$$P + Q = R,$$

kao što je prikazano na slici 1.9.

Valja napomenuti da to nije isto kao zbrajanje po koordinatama. Pretpostavimo da je $P \neq Q$ te da nijedna točka nije O. Nagib pravca L kroz P i Q je $m = \dfrac{y_2 - y_1}{x_2 - x_1}$. Ako je



Slika 1.9: Zbrajanje točaka na eliptičkoj krivulji ($P + Q = R$)

$x_1 = x_2$, pravac L okomit je na $x-$os. Za sada pretpostavljamo da je $x_1 \neq x_2$ (poslije ćemo promatrati slučaj kada je L okomit na x-os). Jednadžba pravca L je $y = m(x - x_1) + y_1$. Kako bismo odredili presjek, supstituiramo y te slijedi

$$(m(x - x_1) + y_1)^2 = x^3 + Ax + B.$$

To se može zapisati i u obliku

$$0 = x^3 - m^2x^2 + ...$$

Budući da znamo dva rješenja ove jednadžbe, x_1 i x_2, nije teško odrediti i treće. Ako je kubni polinom $x^3 + ax^2 + bx + c$ s korijenima r, s i t, tada vrijedi

$$x^3 + ax^2 + bx + c = (x - r)(x - s)(x - t) = x^3 - (r + s + t)x^2 + ...$$

pa je $r + s + t = -a$. Ukoliko su nam r i s poznati, lako odredimo da je $t = -a - r - s$. U našem je slučaju

$$x = m^2 - x_1 - x_2 \quad \text{i} \quad y = m(x - x_1) + y_1.$$

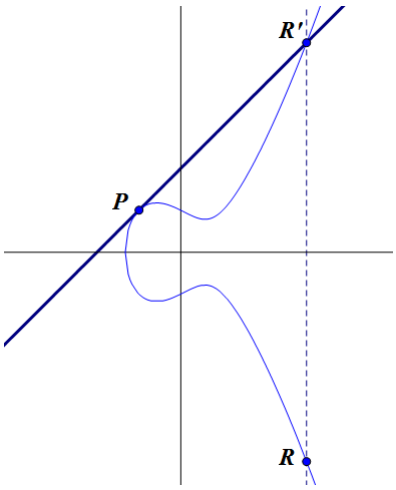
Konačno, „prevaljivanjem" preko $x-$osi dobijemo da je $R = (x_3, y_3)$, pri čemu je

$$x_3 = m^2 - x_1 - x_2, \quad y_3 = m(x_1 - x_3) - y_1.$$

U slučaju da je $x_1 = x_2$, a $y_1 \neq y_2$, pravac kroz P i Q okomit je na $x-$os te je stoga treća točka presjeka O, a njoj osnosimerična točka obzirom na $x-$os je ista ta točka O. Stoga je sada

$$P + Q = O.$$

Idući slučaj je $P = Q = (x_1, y_1)$. Kada su dvije točke na krivulji veoma blizu jedna drugoj, pravac kroz njih aproksimira tangentu. Stoga, kada se one poklope, pravac L je ustvari tangenta, kao što je prikazano na slici 1.10.



Slika 1.10: Zbrajanje (dupliranje) točaka na eliptičkoj krivulji ($P + P = R$)

Deriviranjem implicitno zadane funkcije možemo pronaći nagib tog pravca:

$$2yy' = 3x^2 + A \Rightarrow m = y' = \frac{3x_1^2 + A}{2y_1}.$$

Ako je $y_1 = 0$, pravac je okomit na $x-$os, pa je $P + Q = \mathcal{O}$, kao i prije. Pretpostavimo stoga da je $y_1 \neq 0$. Jednadžba pravca L je $y = m(x - x_1) + y_1$, kao i prije, a supstitucijom i sređivanjem dobijemo

$$0 = x^3 - m^2x^2 + ...$$

Poznato nam je samo jedno rješenje, međutim ono je dvostruko, budući da je L tangenta u točki P. Zaključivanjem kao i prije, slijedi da je

$$x_3 = m^2 - 2x_1, \quad y_3 = m(x_1 - x_3) - y_1.$$

Konačno, neka je $Q = \mathcal{O}$. Pravac kroz P i $\mathcal{O}$ je okomit te siječe krivulju E u točki P' koja je osnosimetrična točki P obzirom na $x-$os. Kada reflektiramo P' oko osi x kako bismo dobili $R = P + Q$, opet smo u točki P te je stoga

$$P + \mathcal{O} = P.$$

To vrijedi za sve točke na krivulji E, a podrazumijevamo i da je $\mathcal{O} + \mathcal{O} = \mathcal{O}$.

Iduća definicija formalizira prethodnu diskusiju, odnosno definira zbrajanje točaka analitički.

Definicija 1.4.4. *Neka je E eliptička krivulja čija je jednadžba*

$$y^2 = x^3 + Ax + B$$

te $P = (x_1, y_1)$ i $Q = (x_2, y_2)$ točke na toj eliptičkoj krivulji takve da je $P,\ Q \neq \mathcal{O}$. Definirajmo $P + Q = R = (x_3, y_3)$ na sljedeći način:

1) Ako je $x_1 \neq x_2$, tada je

$$x_3 = m^2 - x_1 - x_2, \quad y_3 = m(x_1 - x_3) - y_1, \quad \textit{gdje je } m = \frac{y_2 - y_1}{x_2 - x_1}.$$

2) Ako je $x_1 = x_2$, a $y_1 \neq y_2$, tada je $P + Q = \mathcal{O}$.

3) Ako je $P = Q$ te $y_1 \neq 0$, tada je

$$x_3 = m^2 - 2x_1, \quad y_3 = m(x_1 - x_3) - y_1, \quad \textit{gdje je } m = \frac{3x_1^2 + A}{2y_1}.$$

4) Ako je $P = Q$ te $y_1 = 0$, tada je $P + Q = \mathcal{O}$.

Dodatno definiramo i da je $P + \mathcal{O} = P$ za sve točke na krivulji E.

Možemo primijetiti da ako P i Q imaju koordinate u polju K koje sadrži A i B, tada $P + Q$ također ima koordinate u K. Stoga je $E(K)$ zatvorena na ovako definiranu operaciju zbrajanja, koja na prvu možda izgleda neprirodno.

Teorem 1.4.5. *Zbrajanje točaka na eliptičkoj krivulji E zadovoljava sljedeća svojstva:*

1) $P + Q = Q + P$ za sve točke P, Q na krivulji E (komutativnost)*;*

2) $P + \mathcal{O} = P$ za sve točke P na krivulji E (postojanje neutralnog elementa)*;*

3) Za svaku točku P na krivulji E postoji P', također na E, takva da je $P + P' = \mathcal{O}$ (postojanje inverznog elementa)*;*

4) $(P + Q) + R = P + (Q + R)$ za sve točke P, Q, R na krivulji E (asocijativnost).

Drugim riječima, $(E(K), +)$ je **Abelova grupa** čiji je neutralni element (nula) već spomenuta točka u beskonačnosti $\mathcal{O}$. Komutativnost je očita, bilo iz formula, bilo iz činjenice da je pravac kroz P i Q jednak onom kroz Q i P. Postojanje neutralnog elementa slijedi iz same definicije, kao i inverza, budući da je točka P' simetrična obzirom na $x-$os točki P, slijedi da je $P + P' = (x, y) + (x, -y) = \mathcal{O}$. Obično točku P' označavamo s $-P$.

Najteže je dokazati asocijativnost, a najpoznatiji kompletni dokazi zasnovani su na projektivnoj geometriji ili na kompleksnoj analizi s dvostruko periodičnim funkcijama. Mi se nećemo baviti tim dokazom, dovoljni su nam već navedeni analitički izraz za zbrajanje na eliptičkoj krivulji te geometrijski uvid u ovu operaciju. Valja napomenuti da su analitički izrazi za zbrajanje na eliptičkoj krivulji nad poljima karakteristike 2 ili 3 slični, uz male modifikacije.

Za primjene u kriptografiji najznačajnije su eliptičke krivulje nad konačnim poljima $\mathbb{F}_q$ s q elemenata. Stoga ćemo se njima više baviti, a kako u teoriji brojeva važnu ulogu imaju eliptičke krivulje nad poljem $\mathbb{Q}$ racionalnih brojeva, o njima ćemo spomenuti samo najvažnije činjenice.

1.5 Eliptičke krivulje nad $\mathbb{Q}$

Ako je $E(\mathbb{Q})$ eliptička krivulja nad $\mathbb{Q}$, a P točka na $E(\mathbb{Q})$ takva da je

$$nP = \underbrace{P + P + \ldots + P}_{n \text{ puta}} = O,$$

za neki $n \in \mathbb{N}$, tada P zovemo **torzijskom točkom** ili **točkom konačnog reda**. Najmanja takva vrijednost n naziva se **redom** točke P. Točku O nazivamo trivijalnom torzijskom točkom, a ako P nije torzijska točka, kažemo da je **točka beskonačnog reda**.

Teorem 1.5.1. (Mordell - Weil) *$E(\mathbb{Q})$ je konačno generirana Abelova grupa.*

Drugim riječima, postoji konačan skup racionalnih točaka $\{P_j\}_{j=1}^{k}$ na E iz kojih se sve ostale racionalne točke na E mogu dobiti metodom sekante i tangente. Svaka konačno generirana Abelova grupa izomorfna je produktu cikličkih grupa pa je

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

$E(\mathbb{Q})_{tors}$ se sastoji od svih točaka konačnog reda, podgrupa je od $E(\mathbb{Q})$ te se naziva **torzijska grupa** od E, a cijeli broj r, koji je nenegativan, naziva se **rang** od E te se označava s rank E. Dakle, postoji r racionalnih točaka $P_1, P_2, ..., P_r$ na krivulji E, takvih da se svaka racionalna točka P na E može prikazati kao

$$P = T + m_1P_1 + ... + m_rP_r,$$

gdje je T neka točka konačnog reda, a $m_1, m_2, ..., m_r$ cijeli brojevi.

Definicija 1.5.2. *Neka je P točka na eliptičkoj krivulji E. Za $m \in \mathbb{Z}$ definiramo preslikavanje $[m] : E \to E$ kao:*

$$[m]\,P = \begin{cases} P + P + ... + P \ (m \ puta), & ako \ je \ m > 0 \\ \mathcal{O}, & ako \ je \ m = 0 \\ (-P) + (-P) + ... + (-P) \ (-m \ puta), & ako \ je \ m < 0. \end{cases}$$

Ovo je ustvari množenje točke P skalarom m . Zato smo m_1P_1 mogli označiti kao $[m_1]\,P_1$, što je suma $P_1 + P_1 + ... + P_1$ od m_1 pribrojnika. Inače, ovo preslikavanje primjer je izogenije. Izogenije su racionalna preslikavanja među eliptičkim krivuljama E_1, E_2, za koja $\mathcal{O}_{E_1} \to \mathcal{O}_{E_2}$ te se može pokazati da su izogenije homomorfizmi grupa pripadnih krivulja. (Vidi Teorem III.4.8[10])

Ako su A i B u

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

veliki brojevi, moguće je da bude dosta torzijskih točaka, međutim, Mazur je 1978. godine dokazao da postoji samo 15 mogućih torzijskih grupa.

Teorem 1.5.3. (Mazur) *Ako je $E(\mathbb{Q})$ eliptička krivulja, tada je*

$$E(\mathbb{Q})_{tors} \cong \mathbb{Z}_n$$

za neki $n \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12\}$ ili

$$E(\mathbb{Q})_{tors} \cong \mathbb{Z}_2 \times \mathbb{Z}_n$$

za neki $n \in \{2, 4, 6, 8\}$.

Iz ovog teorema, zaključujemo da ne postoji racionalna torzijska točka reda većeg od 12 (sve takve su beskonačnog reda) kao ni torzijska grupa većeg reda od 16 za eliptičke krivulje nad $\mathbb{Q}$. Idući teorem omogućuje nam efikasno računanje torzijske grupe od E nad Q.

Teorem 1.5.4. (Lutz-Nagell) *Neka je eliptička krivulja E zadana jednadžbom*

$$y^2 = x^3 + Ax + B, \quad A, B \in \mathbb{Z}.$$

Ako je $P = (x, y) \in E(\mathbb{Q})_{tors}$, tada su $x, y \in \mathbb{Z}$ te vrijedi da je točka P reda 2 (tj. $y = 0$) ili $y^2 | D$, gdje je $D = -4A^3 - 27B^2$.

Primjer 1.5.5. *Odredimo torzijsku grupu eliptičke krivulje* $E : y^2 = x^3 + 4$.
Imamo $D = -432$. *Prema prethodnom teoremu znamo da je* $y = 0$ *ili* $y^2 | 432$. *Dakle,* $y \in \{0, \pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12\}$. *Provjeravanjem se utvđuje da je jedino za* $y = \pm 2$ *i* $x \in \mathbb{Z}$, *točnije* $x = 0$. *Stoga treba provjeriti točke* $(0, -2)$ *i* $(0, 2)$, *a kako je* $(0, -2) = -(0, 2)$, *dovoljno je samo provjeriti za* $P = (0, 2)$. *Pomoću algoritma zbrajanja točaka 1.4.4 može se utvrditi da je*

$$2P = P + P = (0, 2) + (0, 2) = (0, -2) = -P,$$

pa je $3P = 2P + P = -P + P = \mathcal{O}$. *Iz toga slijedi da su točke* P *i* $-P$ *reda* 3, *te je*

$$E(\mathbb{Q})_{tors} = \{\mathcal{O}, (0, 2), (0, -2)\}$$

što je izomorfno grupi $\mathbb{Z}_3$.

Lutz-Nagellov teorem daje konačnu listu kandidata za torzijske točke, točnije, daje nam kandidate za $y-$koordinate točaka. Primjerice, za krivulju $E : y^2 = x^3 + 4$ prema tvdrnji tog teorema, među potencijalnim točkama možemo provjeriti i $(1, \pm 3)$ te $(2, \pm 4)$, međutim kako

$$2(1, 3) = \left(\frac{-7}{4}, \frac{-13}{8}\right) \quad \text{te} \quad 2(2, 4) = \left(\frac{-7}{4}, \frac{13}{8}\right)$$

nemaju racionalne koordinate, ne mogu biti konačnog reda. Ako je P torzijska točka, onda za svaki prirodan broj n, točka nP mora biti ili $\mathcal{O}$ ili jedna od točaka na listi. Kako je lista konačna, dobije se da je $nP = mP$ za neki $m \neq n$, te je tada točka P torzijska, a $(n-m)P = \mathcal{O}$ ili će, kao u navedenom primjeru, neki višekratnik nP biti izvan liste, pa P nije torzijska. Može se koristiti i Mazurov teorem, po kojem je red svake torzijske točke $\leqslant 12$, pa ako je $nP \neq \mathcal{O}$ za $n \leqslant 12$, onda P nije torzijska. Međutim, kako je ponekad teško faktorizirati diskriminantu D ili ima previše faktora, koriste se neke druge tehnike, a kao pomoć nam može koristiti i redukcija modulo p, gdje je p prost broj. Pitanja vezana za rang inače su puno teža od pitanja vezanih uz torzijske grupe. Vjeruje se da rang može biti proizvoljno velik, tj. da za svaki $N \in \mathbb{N}$ postoji eliptička krivulja E nad $\mathbb{Q}$ takva da je rank $E \geqslant N$. Do danas se tek zna da postoji eliptička krivulja ranga $\geqslant 28$ koju je 2006. godine pronašao Noam Elkies. Vrlo je značajan rezultat o rangu Bhargave i Shankara, koji su pokazali da je prosječni rang svih eliptičkih krivulja E nad $\mathbb{Q}$ manji od 1, s tim da se vjeruje da je on točno $\frac{1}{2}$. (Vidi[8])

1.6 Eliptičke krivulje nad konačnim poljima

Prije nego što počnemo proučavati eliptičke krivulje nad konačnim poljima nužno je reći nešto o samim konačnim poljima.

Konačna polja

Konačno polje s q elemenata označavat ćemo s $\mathbb{F}_q$ (koristi se još i oznaka $GF(q)$ koja dolazi od „Galoisovog polja"). Ako je p karakteristika polja $\mathbb{F}_q$, tada $\mathbb{F}_q$ sadrži prosto polje $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ te je $\mathbb{F}_q$ vektorski prostor nad $\mathbb{F}_p$ čiju dimenziju možemo označiti s m. Tada $\mathbb{F}_q$ ima p^m elemenata, tj. $q = p^m$, a vrijedi i obrat; za svaku potenciju prostog broja $q = p^m$ postoji polje od q elemenata, i ono je jedinstveno do na izomorfizam.

Elementi polja $\mathbb{F}_q$ različiti od nule tvore Abelovu grupu s obzirom na množenje koju označavamo sa $\mathbb{F}_q^*$. Grupa $\mathbb{F}_q^*$ je ciklička, a kako vrijedi da red podgrupe dijeli red grupe, slijedi da red svakog elementa $a \in \mathbb{F}_q^*$ dijeli $q-1$. Stoga, ako je g generator od $\mathbb{F}_q^*$, onda je g^j također generator ako i samo ako je $nzd\,(j, q-1) = 1$, pa postoji točno $\varphi(q-1)$ generatora grupe $\mathbb{F}_q^*$.

Eliptičke krivulje koje se koriste u kriptografiji, definirane su s dva tipa konačnih polja:

- polje $\mathbb{F}_p$, gdje je $p > 3$ (veliki) prosti broj;
- polje $\mathbb{F}_{2^m}$, $m \in \mathbb{N}$.

O polju $\mathbb{F}_p$

Sastoji se od p elemenata koji su cijeli brojevi $\{0, 1, ..., p-1\}$ s operacijama zbrajanja i množenja definiranima tzv. „modularnom aritmetikom" na sljedeći način:

- Zbranjanje: Ako je $a, b \in \mathbb{F}_p$, tada je $a + b = r \in \mathbb{F}_p$, gdje je $r \in [0, p-1]$ ostatak pri dijeljenju cijelog broja $a + b$ i p. Kraće zapisano: $a + b = r \mod p$.
- Množenje: Ako je $a, b \in \mathbb{F}_p$, tada je $a \cdot b = s \in \mathbb{F}_p$, gdje je $s \in [0, p-1]$ ostatak pri dijeljenju cijelog broja $a \cdot b$ i p. Kraće zapisano: $a \cdot b = s \mod p$.

Neutralni element zbrajanja u $\mathbb{F}_p$ je 0, a neutralni element množenja je 1. Za aditivni inverz od $a \in \mathbb{F}_p$, tj. $-a$, vrijedi da je jedinstveno rješenje jednadžbe $a + x \equiv 0 \pmod p$. Za multiplikativni inverz od a vrijedi da jedinstveno rješenje jednadžbe $a \cdot x \equiv 1 \pmod p$, Označavamo ga s a^{-1}. Multiplikativni se inverz dobiva pomoću proširenog Euklidovog algoritma.

Možemo definirati i operacije oduzimanja i dijeljenja u smislu aditivnog i multiplikativnog inverza; $a - b = a + (-b) \pmod p$, te $a : b = a \cdot b^{-1} \pmod p$.

O polju $\mathbb{F}_{2^m}$

Karakteristika polja je 2, a polje se sastoji od 2^m elemenata. Iako postoji jedno konačno polje $\mathbb{F}_{2^m}$ karakteristike 2 za svaku potenciju 2^m gdje je $m \geqslant 1$, postoji mnogo načina reprezentacije elemenata od $\mathbb{F}_{2^m}$. Ovisno o mogućnostima možemo birati izmedu normalnih

i polinomijalnih baza, ili pak njihove kombinacije preko baza potpolja. U reprezentaciji pomoću polinomijalne baze, elementi od $\mathbb{F}_{2^m}$ su „binarni" polinomi, tj. polinomi čiji su koeficijenti 0 ili 1, dok im stupanj nije veći od $m-1$;

$$\left\{a_{m-1}x^{m-1} + a_{m-2}x^{m-2} + \cdots + a_1x + a_0 : a_i \in \{0,1\}\right\}.$$

Zbrajanje i množenje definirani su pomoću ireducibilnog polinomoma $P(x)$ stupnja m. Da bi operacije u polju bile što efikasnije, taj se polinom bira tako da ima što manju težinu W, tj. što manj broj koeficijenata različitih od 0. Možemo uočiti da su koeficijenti uz x^m i $x^0 = 1$ uvijek prisutni, te da polinom s parnim W ne može biti ireducibilan, pa se izbor za $P(x)$ svodi na trinome (W = 3) i pentanome (W = 5). Više o tome ima u [1].

Također, elementi polja mogu biti predstavljeni nizom od m-bitova, pri čemu svaki bit u nizu odgovara koeficijentu polinoma na istoj poziciji. Primjerice, polje $\mathbb{F}_{2^3}$ sadrži 8 elemenata koje reprezentiramo sljedećim polinomima

$$0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1.$$

Na primjer, polinom $x + 1 = 0 \cdot x^2 + 1 \cdot x + 1 \cdot 1$ odgovara nizu bitova 011.

Definicija 1.6.1. *Neka su $A(x)$ i $B(x)$ polinomi iz $\mathbb{F}_{2^m}$. Suma ta dva elementa računa se kao:*

$$S(x) = A(x) + B(x) = \sum_{i=0}^{m-1} s_i x^i, \;\; s_i \equiv a_i + b_i \pmod 2,$$

a razlika kao

$$D(x) = A(x) - B(x) = \sum_{i=0}^{m-1} d_i x^i, \;\; d_i \equiv a_i - b_i \equiv a_i + b_i \pmod 2.$$

Primjetimo da koeficijente zbrajamo (oduzimamo) modulo 2, što su zapravo iste operacije. Zbrajanje (oduzimanje) elemenata modulo 2 implementira se kao "ekskluzivni ili" (XOR, oznaka $\oplus$) po komponentama i ne ovisi o bazi, dok je s druge strane, izbor baze bitan za množenje u polju. Primjerice, u prethodno spomenutom polju $\mathbb{F}_{2^3}$ vrijedi: $(x^2 + x + 1) + (x + 1) = x^2 + 2x + 2$, a budući da je $2 \equiv 0 \pmod 2$ konačan je rezultat x^2. Isti rezultat dobije se i pomoću reprezentacije nizom bitova, $111 \oplus 011 = 100$.

Neka su $A(x)$ i $B(x)$ polinomi iz $\mathbb{F}_{2^m}$. Običnim množenjem ovih polinoma dobivamo

$$\begin{aligned} C(x) &= A(x) \cdot B(x) = (a_{m-1}x^{m-1} + ... + a_0) \cdot (b_{m-1}x^{m-1} + ... + b_0) \\ &= c_{2m-2}x^{2m-2} + ... + c_0; \end{aligned}$$

gdje su

$$\begin{aligned} c_0 &= a_0 b_0 \pmod 2, \\ c_1 &= a_0 b_1 + a_1 b_0 \pmod 2, \\ &\vdots \\ c_{2m-2} &= a_{m-1} b_{m-1} \pmod 2. \end{aligned}$$

Dakle, problem je što će umnožak $C(x)$ biti većeg stupnja od $m-1$ te ga trebamo reducirati. Osnovna je ideja slična množenju u prostim poljima: pomnožimo dva cijela broja, rezultat podijelimo prostim brojem i na kraju promatramo samo ostatak. U ovom slučaju umnožak polinoma dijelimo određenim ireducibilnim polinomom te rezultat množenja prikazujemo kao ostatak pri dijeljenju s tim ireducibilnim polinomom. Dakle, slijedi precizna definicija.

Definicija 1.6.2. *Umnožak polinoma $A(x), B(x)$ je polinom $U(x)$ koji predstavlja ostatak pri dijeljenju standardnog umnoška polinoma $C(x) = A(x) \cdot B(x)$ polinomom $P(x)$. Pišemo*

$$U(x) = A(x) \cdot B(x) \mod P(x).$$

Primjer 1.6.3. *Želimo pomnožiti dva polinoma $A(x) = x^2 + x + 1$ i $B(x) = x^2 + 1$ u polju $\mathbb{F}_{2^3}$. Običan umnožak polinoma je*

$$C(x) = A(x) \cdot B(x) = x^4 + x^3 + 2x^2 + x + 1 = x^4 + x^3 + x + 1.$$

Isto se dobije i računanjem pomoću nizova bitova:

$$111 \cdot 101 = 11100 \oplus 111 = 11011,$$

što odgovara polinomu $x^4 + x^3 + x + 1$. Uočimo da je stupanj polinoma $C(x)$ veći od $m-1$ pa ga je potrebno reducirati u modulu ireducibilnog polinoma. Ireducibilni polinom ovog konačnog polja je $P(x) = x^3 + x + 1$. Vrijedi da je

$$x^3 \equiv x^3 + x + 1 + x + 1 \equiv 1 \cdot P(x) + x + 1 \equiv x + 1 \pmod{P(x)}.$$

Stoga je

$$x^4 \equiv x^2 + x \pmod{P(x)}.$$

Konačno je

$$x^4 + x^3 + x + 1 \equiv x^4 + 1 \cdot P(x) \equiv x^4 \equiv x^2 + x \pmod{P(x)}.$$

Međutim, kako ovu operaciju izvesti ukoliko imamo prikaz pomoću nizova bitova? To se provodi pomoću tzv. pomaka i XOR-a. Razjasnimo to na primjeru.

Primjer 1.6.4. *Bitovna reprezentacija polinoma* $x^4 + x^3 + x + 1$ *je* 11011*, a* 1011 *polinoma* $x^3 + x + 1$*. Kako je stupanj polinoma reprezentiranog s* 11011 *četiri, a stupanj ireducibilnog polinoma tri, redukciju započinjemo pomakom* 1011 *jedan bit ulijevo, nakon čega slijedi* $11011 \oplus 10110 = 1101$*. Stupanj od* 1101 *je tri, što je još uvijek veće od* $m - 1 = 2$*, pa trebamo novu redukciju. Međutim, ovaj put ne trebamo pomak ireducibilnog polinoma jer je* $1101 \oplus 1011 = 0110$*, što je upravo reprezentacija polinoma* $x^2 + x$*.*

Normalna baza od $\mathbb{F}_{2^m}$ nad $\mathbb{F}_2$ baza je oblika $\left\{\beta, \beta^2, \beta^{2^2}, \ldots, \beta^{2^{2m-1}}\right\}$ za neki $\beta \in \mathbb{F}_{2^m}$. Takva baza uvijek postoji, a dok je u ovoj reprezentaciji kvadriranje u polju trivijalno, množenje je kompliciranije, pa su od interesa tzv. optimalne normalne baze (ONB). Optimalna normalna baza ne mora postojati, a ukoliko vrijedi da $8 \nmid m$ tada sigurno postoji. Također, jedan od nužnih uvjeta postojanja ONB je taj da je barem jedan od brojeva $m + 1$ i $2m + 1$ prost. Danas su popularni izbori $m = 163, 191, 239$ i 431.

Eliptičke krivulje nad $\mathbb{F}_p$

Definicija 1.6.5. *Neka je* $p \neq 2$ *prost i* $A, B \in \mathbb{F}_p$ *za koje* $4A^3 + 27B^2 \not\equiv 0 \pmod 2$*.* ***Eliptička krivulja nad poljem*** $\mathbb{F}_p$ *je skup točaka* $(x, y) \in \mathbb{F}_p \times \mathbb{F}_p$ *koje zadovoljavaju jednadžbu*

$$E: \quad y^2 \equiv x^3 + Ax + B \pmod p,$$

zajedno s „točkom u beskonačnosti" O. Takav skup označavamo s $E(\mathbb{F}_p)$*.*

Vrijede svi prethodno nabrojani analitički izrazi za zbrajanje na eliptičkoj krivulji 1.4.4, modulo p, uz iznimku kada je $p = 3$, a u tom je slučaju i sama jednadžba eliptičke krivulje oblika

$$E: \quad y^2 = x^3 + Ax^2 + Bx + C.$$

Primjer 1.6.6. *Promotrimo eliptičku krivulju* $E: \quad y^2 = x^3 + x + 1$ *nad poljem* $\mathbb{F}_5$*. Kako bismo odredili točke na E, napravimo listu mogućih vrijednosti x, zatim od* $x^3 + x + 1 \pmod 5$ *te y-korijena od* $x^3 + x + 1 \pmod 5$*. Računanjem i uvrštavanjem dobijemo sljedeću tablicu:*

x	$x^3 + x + 1$	y	*Točke*
0	*1*	± 1	*(0,1), (0,4)*
1	*3*	-	-
2	*1*	± 1	*(2,1), (2,4)*
3	*1*	± 1	*(3,1), (3,4)*
4	*4*	± 2	*(4,2), (4,3)*
∞	∞	∞	∞

Konačno dobivamo da je

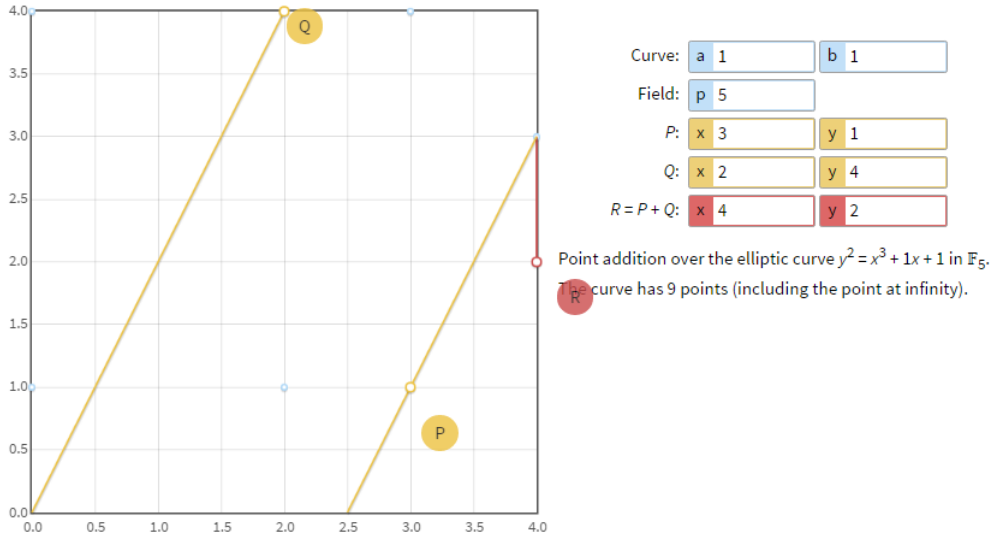
$$E(\mathbb{F}_5) = \{\mathcal{O}, (0,1), (0,4), (2,1), (2,4), (3,1), (3,4), (4,2), (4,3)\}.$$

Izračunajmo $(3,1) + (2,4)$ *na* E. *Prvo računamo:* $m = \dfrac{y_2 - y_1}{x_2 - x_1} = \dfrac{4-1}{2-3} \equiv 2 \pmod 5$. *Tada je*

$$x_3 = m^2 - x_1 - x_2 = 4 - 3 - 2 \equiv 4 \pmod 5,$$

$$y_3 = m(x_1 - x_3) - y_1 = 2(3-4) - 1 \equiv 2 \pmod 5.$$

Ovime smo dobili da je $(3,1) + (2,4) = (4,2) \in \mathbb{F}_5$. *Rezultat zbrajanje prikazan je i na slici 1.11.*



Slika 1.11:

Zbrajanje točaka u $\mathbb{F}_5$ (pomoću *software-a*: `https://cdn.rawgit.com/andreacorbellini/ecc/5c61d93/interactive/modk-add.html`;*public domain*).

Također, da se primijetiti i da za svaki x postoje najviše dvije točke te simetrija obzirom na $y = p/2$. *Odredimo sada strukturu grupe* $E(\mathbb{F}_5)$. *Uzmimo točku* $P = (0,1)$ *i izračunajmo njezine višekratnike. Slijedi:*

$$[2]P = (4,2),\ [3]P = (2,1),\ [4]P = (3,4),\ [5]P = (3,1),$$

$$[6]P = (2,4),\ [7]P = (4,3),\ [8]P = (0,4),\ [9]P = \mathcal{O}.$$

Dakle, $E(\mathbb{F}_5)$ je ciklička grupa reda 9, a točka P je njezin generator. Ako bismo dalje računali višekratnike, lako se uoči pravilnost u obliku cikličkog ponavljanja koja se može prikazati kao: $kP = (k \bmod 9)P$. Također, pokazuje se da je skup višekratnika točke P ciklička podgrupa grupe $E(\mathbb{F}_5)$. Prilikom računanja višekratnika

$$[m]P = \underbrace{P + P + \ldots + P}_{m \text{ pribrojnika}}$$

neke točke P, osobito ako je m izuzetno veliki broj, postoje puno efikasniji algoritmi od uzastopnog zbrajanja. Primjerice, umjesto računanja $[9]P$ pomoću 9 zbrajanja, metodom „udvostruči i zbroji" prvo se 9 prikaže u binarnoj bazi (1001_2), a zatim se to interpretira kao $[9]P = 2^3P + 2^0P$, iz čega slijedi da $[9]P$ dobijemo pomoću tri množenja i jednog zbrajanja:

$$P \xrightarrow{\text{udvostručenje}} [2]P \xrightarrow{\text{udvostručenje}} [4]P \xrightarrow{\text{udvostručenje}} [8]P + P = [9]P$$

Broj operacija za računanje $[m]P$ u ovom je slučaju $O(\log m)$ što je svakako bolje od inicijalnih $O(m)$. Međutim, budući da je u grupi točaka na eliptičkoj krivulji nad konačnim poljem, inverzna operacija (oduzimanje) jednako kompliciranа kao originalna grupovna operacije (zbrajanje), postoje i puno efikasniji algoritmi čija je glavna ideja zamjena binarnog zapisa onim u kojem su dopuštene znamenke $-1, 0, 1$. Broj operacija za računanje $[m]P$ za eliptičku krivulju nad poljem $\mathbb{F}_p$ pomoću takvih algoritama je $O(\ln m \ln^2 q)$, a više o tome ima u poglavlju 5.1.3. u [3].

Eliptičke krivulje nad $\mathbb{F}_{2^m}$

Svaka se eliptička krivulja nad poljem $\mathbb{F}_{2^m}$, koje je karakteristike 2, može transformirati u jedan od ova dva oblika:

$$y^2 + Cy = x^3 + Ax + B \quad \text{ili} \quad y^2 + xy = x^3 + Ax + B.$$

Krivulje prvog oblika su tzv. **supersingularne krivulje**, koje nisu prikladne za primjenu u kriptografiji, što ćemo pojasniti u idućem radu.

Definicija 1.6.7. *Neka je $m \in \mathbb{N}$ i $A, B \in \mathbb{F}_{2^m}$, $B \neq 0$ i $4A^3 + 27B^2 \neq 0$. **Eliptička krivulja nad poljem** $\mathbb{F}_{2^m}$ je skup točaka $(x, y) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ koje zadovoljavaju jednadžbu*

$$E: \quad y^2 + xy = x^3 + Ax + B, \tag{1.5}$$

zajedno s „točkom u beskonačnosti" $\mathcal{O}$. Takav skup označavamo s $E(\mathbb{F}_{2^m})$.

Možemo navesti i formule za zbrajanje točaka na eliptičkoj krivulji zadanih jednadžbom (1.5) nad poljem $\mathbb{F}_{2^m}$. Naime, ako je $P = (x_1, y_1)$ i $Q = (x_2, y_2)$, tada je $-P = (x_1, x_1 + y_1)$ te $P + Q = (x_3, y_3)$, $P + P = [2]P = (x_4, y_4)$, gdje su:

$$x_3 = \lambda^2 + \lambda + x_1 + x_2 + A \quad \text{i} \quad y_3 = \lambda(x_1 + x_3) + x_3 + y_1 \quad \text{za} \quad \lambda = \frac{y_1 + y_2}{x_1 + x_2};$$

$$x_4 = \delta^2 + \delta + A = x_1^2 + \frac{B}{x_1^2} \quad \text{i} \quad y_4 = x_1^2 + \delta x_3 + x_3 \quad \text{za} \quad \delta = \frac{x_1 + y_1}{x_1}.$$

Vizualno se suma dviju točaka predočava kao sjecište eliptičke krivulje $E(\mathbb{F}_{2^m})$ te pravca kojeg te točke određuju, dok je u slučaju udvostručenja točke riječ o sjecištu eliptičke krivulje $E(\mathbb{F}_{2^m})$ i tangente na krivulju u toj točki. $E(\mathbb{F}_{2^m}, +)$ je **Abelova grupa**.

Određivanje reda grupe $E(\mathbb{F}_q)$

Prikladnost primjene konkretne eliptičke krivulje u kriptografiji, prvenstveno ovisi o **redu grupe** $E(\mathbb{F}_q)$. Za red grupe, u oznaci $\#E(\mathbb{F}_q)$, lako je zaključiti da je $\#E(\mathbb{F}_q) \in [1, 2q + 1]$ budući da, osim točke O, na krivulji E, najviše 2 $y-$a odgovaraju svakom od q mogućih $x-$eva. Kako samo pola elemenata od $\mathbb{F}_q$ imaju kvadratni korijen, za očekivati je da je $\#E(\mathbb{F}_q) \approx q + 1$, a precizniju granicu reda grupe $E(\mathbb{F}_q)$ daje nam sljedeći, tzv. Hasseov teorem.

Teorem 1.6.8. *Neka je E eliptička krivulja definirana nad $\mathbb{F}_q$. Tada je*

$$q + 1 - 2\sqrt{q} \leq \#E(\mathbb{F}_q) \leq q + 1 + 2\sqrt{q}.$$

Drugim riječima, za proizvoljnu eliptičku krivulju E nad $\mathbb{F}_q$ je $\#E(\mathbb{F}_q) = q + 1 - t$, pri čemu je $|t| \leq 2\sqrt{q}$. Broj $t = q + 1 - \#E(\mathbb{F}_q)$ naziva se **Frobeniusov trag** eliptičke krivulje E, a $\left[q + 1 - 2\sqrt{q}, q + 1 + 2\sqrt{q}\right]$ je tzv. **Hasseov interval**. Vrijedi i svojevrstan obrat ovog teorema koji kaže da, za svaki broj m iz Hasseovog intervala, postoji eliptička krivulja nad $\mathbb{F}_q$ kojoj je red upravo m. Idući teorem govori o mogućim redovima grupe $E(\mathbb{F}_q)$ u općem slučaju $q = p^k$.

Teorem 1.6.9. *Neka je $q = p^k$. Tada postoji eliptička krivulja E definirana nad $\mathbb{F}_q$ takva da je $\#E(\mathbb{F}_q) = q + 1 - t$ ako i samo ako je $|t| \leq 2\sqrt{q}$ i t zadovoljava jedan od sljedećih uvjeta:*

1) $(t, p) = 1$*;*

2) k je paran i

   a) $t = \pm 2\sqrt{q}$ *ili*

   b) $t = \pm\sqrt{q}$ *i* $p \not\equiv 1 \pmod 3$ *ili*

c) $t = 0 \quad i \quad p \not\equiv 1 \pmod 4$;

3) k je neparan i

a) $t = 0 \quad ili$

b) $t = \pm\sqrt{2q} \quad i \quad p = 2 \quad ili$

c) $t = \pm\sqrt{3q} \quad i \quad p = 3.$

Posljedica teorema (1.6.9)je ta da za svaki prost broj p i veličinu t koja zadovoljava $|t| \leq 2\sqrt{q}$, postoji eliptička krivulja E definirana nad $\mathbb{F}_p$ takva da je $\#E(\mathbb{F}_p) = p + 1 - t$. O tome govori sljedeći primjer.

Primjer 1.6.10. *Neka je* $p = 37$. *U tablici su, za svaki broj m iz Hasseovog intervala* $\left[37 + 1 - 2\sqrt{37}, 37 + 1 + 2\sqrt{37}\right]$, *prikazani koeficijenti* (a, b) *eliptičke krivulje* $E : y^2 = x^3 + ax + b$ *definirane nad* $\mathbb{F}_{37}$, *takvi da je* $\#E(\mathbb{F}_{37}) = m$.

m	***(a,b)***	***m***	***(a,b)***	***n***	***(a,b)***	***m***	***(a,b)***	***m***	***(a,b)***
26	*(5,0)*	*31*	*(2,8)*	*36*	*(1,0)*	*41*	*(1,16)*	*46*	*(1,11)*
27	*(0,9)*	*32*	*(3,6)*	*37*	*(0,5)*	*42*	*(1,9)*	*47*	*(3,15)*
28	*(0,6)*	*33*	*(1,13)*	*38*	*(1,5)*	*43*	*(2,9)*	*48*	*(0,1)*
29	*(1,12)*	*34*	*(1,18)*	*39*	*(0,3)*	*44*	*(1,7)*	*49*	*(0,2)*
30	*(2,2)*	*35*	*(1,8)*	*40*	*(1,2)*	*45*	*(2,14)*	*50*	*(2,0)*

O samoj strukturi grupe $E(\mathbb{F}_q)$ govori nam idući teorem.

Teorem 1.6.11. *Neka je E eliptička krivulja definirana nad* $\mathbb{F}_q$. *Tada je*

$$E(\mathbb{F}_q) \cong \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2},$$

gdje su $m_1, m_2 \in \mathbb{N}$ *te vrijedi* $m_1 \mid m_2$ *i* $m_1 \mid q - 1$.

Ako je $m_1 = 1$, onda je grupa $E(\mathbb{F}_q)$ **cikličk**a, a iz uvjeta da $m_1 \mid (m_2, q - 1)$ može se zaključiti da će m_1 općenito biti mali prirodan broj.

Problem izračunavanja reda grupe E ekvivalentan je problemu izračunavanja Frobeniusovog traga eliptičke krivulje E, a na osnovu njega definiraju se i tzv. **anomalne** i **supersingularne krivulje**. Za eliptičku krivulju E nad konačnim poljem $\mathbb{F}_q$ kažemo da je **anomalna** ako je njen Frobeniusov trag $t = 1$, tj. ako je $\#E(\mathbb{F}_q) = q$. Za eliptičku krivulju E nad konačnim poljem $\mathbb{F}_q$, gdje je $q = p^k$, kažemo da je **supersingularna** ako karakteristika polja $p = char\,\mathbb{F}_q$ dijeli Frobeniusov trag t krivulje E, što za $p > 3$ znači da je $\#E(\mathbb{F}_p) = p + 1$.

Stoga se u kriptografiji najčešće izbjegavaju anomalne i supersingularne krivulje te je vrlo važno poznavati red grupe točaka eliptičke krivulje. Kako bi probem disketnog logaritma kojeg ćemo objasniti u sljedećem poglavlju bio dovoljno težak, $\#E(\mathbb{F}_q)$ bi trebao imati barem jedan prosti faktor veći od 2^{160}. Obično se bira takva krivulja E da je broj $\#E(\mathbb{F}_q)$ oblika $h \cdot r$, gdje je r prost broj, a $h \in \{1, 2, 4\}$. Kofaktor h je jedan od parametara domene kriptosustava koji koriste eliptičke krivulje te vrijedi da je $h = \#E(\mathbb{F}_q)/n$, gdje je n red bazične točke eliptičke krivulje E. Ukoliko se ne vodi računa od izboru parametara, mogu se kreirati vrlo efikasni napadi, primjerice MOV (Menezes-Okamoto-Vanstone), napad koji uspješno rješava problem diskretnog logaritma nad supersingularnom krivuljom. Sada ćemo samo ukratko objasniti neke metode za određivanje reda $\#E(\mathbb{F}_q)$.

Prethodno smo, prilikom pravljenja liste točaka eliptičke krivulje $E: \ y^2 = x^3 + Ax + B$, uvrštavali svaku vrijednost x-a te pronalazili y koji je kvadratni korijen od $x^3 + Ax + B$, ako je postojao. Taj je postupak osnova sljedećeg jednostavnog algoritma brojenja točaka. Prisjetimo se Legendreovog simbola $\left(\frac{x}{p}\right)$ koji je za neparan prost broj p ovako definiran:

$$\left(\frac{x}{p}\right) = \begin{cases} 1, & \text{ako } t^2 \equiv x \pmod{p} \text{ ima rješenje } t \not\equiv 0 \pmod{p}, \\ -1, & \text{ako } t^2 \equiv x \pmod{p} \text{ nema rješenje}, \\ 0, & \text{ako je } x \equiv 0 \pmod{p}. \end{cases}$$

Također vrijedi i generalizacija za konačno polje $\mathbb{F}_q$, gdje je q neparan prost, pa za $x \in \mathbb{F}_q$ imamo:

$$\left(\frac{x}{\mathbb{F}_q}\right) = \begin{cases} 1, & \text{ako je } t^2 = x, \text{ za neki } t \in \mathbb{F}_q^* \\ -1, & \text{ako } t^2 = x \text{ nema rješenje}, \\ 0, & \text{ako je } x = 0. \end{cases}$$

Teorem 1.6.12. *Neka je $E: \ y^2 = x^3 + Ax + B$ eliptička krivulja definirana nad $\mathbb{F}_q$. Tada je*

$$\#E(\mathbb{F}_q) = q + 1 + \sum_{x \in \mathbb{F}_q} \left(\frac{x^3 + Ax + B}{\mathbb{F}_q}\right).$$

Primjer 1.6.13. *Zadana je eliptička krivulja $E: \ y^2 = x^3 + x + 1$ nad poljem $\mathbb{F}_5$ kao u primjeru 1.6.6. Kvadratni ostaci* mod 5 *su* 1 *i* 4*, pa imamo:*

$$\begin{aligned} \#E(\mathbb{F}_5) &= 5 + 1 + \sum_{x=0}^{4} \left(\frac{x^3 + x + 1}{5}\right) \\ &= 6 + \left(\frac{1}{5}\right) + \left(\frac{3}{5}\right) + \left(\frac{1}{5}\right) + \left(\frac{1}{5}\right) + \left(\frac{4}{5}\right) \\ &= 6 + 1 - 1 + 1 + 1 + 1 = 9. \end{aligned}$$

Složenost ovog algoritma, poznatog i kao **Lang-Trotterova metoda**, jest $O(p \ln^2 p)$ te je on vrlo efikasan za male $q-$ove, dok je praktički neprimjenjiv za $q > 10000$.

Slijedi opis **Shanks-Mestreove metode** čija je složenost $O(p^{1/4+\epsilon})$ te se primjenjuje za $p < 10^{30}$. Algoritam se zasniva na Shanksovoj metodi **„malih i velikih koraka"**.
Neka je $P \in E(\mathbb{F}_q)$ kojoj želimo odrediti red. Prvo želimo pronaći broj k takav da je $kP = \mathcal{O}$. Neka je $\#E(\mathbb{F}_q) = N$. Po Lagrangeovom teoremu slijedi da je $NP = \mathcal{O}$. Za takav N vrijedi da je:

$$q + 1 - 2\sqrt{q} \leq N \leq q + 1 + 2\sqrt{q}.$$

Naivan bi način za pronalaženje broja N bilo ispitivanje svih mogućnosti u navedenom intervalu koje zadovoljavaju $NP = \mathcal{O}$, za što je potrebno $4\sqrt{q}$ koraka, ali se korištenjem sljedećeg algoritma postupak ubrza do otprilike $4q^{1/4}$ koraka:

1. Izračunamo $Q = (q + 1)\, P$.
2. Izaberemo broj m takav da je $m > q^{1/4}$ te izračunamo i pohranimo točke jP za $j = 0, 1, 2, \ldots, m$.
3. Izračunamo točke

   $$Q + k\,(2mP) \quad \text{za} \quad k = -m, -(m-1), \ldots, m$$

   sve dok se ne dogodi jednakost $Q + k\,(2mP) = \pm jP$.
4. Zaključimo da je $(q + 1 + 2mk \mp j)\, P = \mathcal{O}$. Označimo $M = q + 1 + 2mk \mp j$.
5. Faktoriziramo M te označimo različite proste faktore od M s $p_1, \ldots, p_r$.
6. Izračunamo $(M/p_i)\, P$ za $i = 1, \ldots, r$. Ako je $(M/p_i)\, P = \mathcal{O}$ za neki i, zamjenimo M s M/p_i te se vratimo na prethodan korak. Ako je $(M/p_i)\, P \neq \mathcal{O}$ za svaki i, tada je M red točke P.
7. Ukoliko tražimo $\#E(\mathbb{F}_q)$, tada ponavljamo prvih šest koraka s nasumično odabranim točkama iz $E(\mathbb{F}_q)$, sve dok najmanji zajednički višekratnik njihovih redova ne bude dijelio samo jedan N sa svojstvom $q + 1 - 2\sqrt{q} \leq N \leq q + 1 + 2\sqrt{q}$. Tada je $N = \#E(\mathbb{F}_q)$.

Djelovanje opisanog algoritma prikazat ćemo na idućem primjeru.

Primjer 1.6.14. *Zadana je eliptička krivulja* $E : y^2 = x^3 - 10x + 21$ *nad poljem* $\mathbb{F}_{557}$. *Neka je* $P = (2, 3)$. *Slijedimo proceduru:*

1. $Q = 558P = (418, 33)$.

2. *Neka je* $m = 5$*, što je veće od* $557^{1/4}$*. Lista* jP *je sljedeća:*

$$O, (2, 3), (58, 164), (44, 294), (56, 339), (132, 364).$$

3. *Za* $k = 1$ *je* $Q + k\,(2mP) = (2, 3)$ *što se podudara s točkom naše liste za* $j = 1$.

4. *Imamo* $(q + 1 + 2mk - j)\,P = 567P = O$.

5. *Faktoriziramo* $567 = 3^4 \cdot 7$ *te računamo* $(567/3)\,P = 189P = O$*. Stoga nam je sada* 189 *kandidat za red točke* P.

6. *Faktoriziramo* $189 = 3^3 \cdot 7$ *te računamo* $(189/3)\,P = (38, 535) \neq O$ *te* $(189/7)\,P = (136, 360) \neq O$*. Stoga je* 189 *red točke* P.

7. *Budući da je* 567 *jedini višekratnik od* 189 *sa svojstvom*

$$557 + 1 - 2\sqrt{557} \leq N \leq 557 + 1 + 2\sqrt{557},$$

zaključujemo da je $\#E(\mathbb{F}_{557}) = 567$.

Prvi polinomijalni algoritam za računanje $\#E(\mathbb{F}_q)$ dao je Rene Schoof 1995. godine u svom radu [9]. To je deterministički algoritam koji, za dano polje $\mathbb{F}_q$ i eliptičku krivulju E nad tim poljem, računa točnu vrijednost Frobeniusovog traga eliptčke krivulje E u $O(ln^8 q)$ bitovnih operacija. Kasnije su Atkin i Elkies dali poboljšanu verziju **Schoofovog algoritma** s kompleksnošću $O(ln^6 q)$, tako da je danas moguće izračunati $\#E(\mathbb{F}_q)$ za sve $q < 10^{500}$. U ovom radu nećemo ulaziti u detalje ovog algoritma, ali možemo spomenuti osnovne ideje. Kreće se od računanja ostataka t mod l za male proste brojeve l te se koristi Kineski teorem o ostacima. Frobeniusov se trag može izračunati iz poznavanja t mod l za $2 \leq l \leq l_{max}$, pri čemu je l_{max} najmanji prost broj takav da je

$$\prod_{\substack{l \text{ prost} \\ l \leq l_{max}}} l > 4\sqrt{q}.$$

Poglavlje 2

Kriptografija javnog ključa

2.1 Ideja javnog ključa

Kriptografija (tajnopis) je znanstvena disciplina koja se bavi pohranom informacija u onoj formi koja će biti čitljiva samo onima kojima je informacija namijenjena dok će za ostale biti neupotrebljiva. U širem je smislu to pojam koji obuhvaća probleme i tehnike koje koristimo za čuvanje ili prenošenje informacija.

Ideju **kriptosustava sa javnim ključem**, tj. **asimetričnog kriptosustava** predložili su 1976. godine Whitfield Diffie i Martin Hellman u svom djelu [2]. Naime, osnovni je nedostatak klasičnih simetričnih kriptosustava nužnost da prije šifriranja pošiljatelj i primatelj (u kriptografskoj literaturi za njih su rezervirana imena Alice i Bob, a za njihovog protivnika Eve) najprije razmijene tajni ključ preko nekog sigurnog komunikacijskog kanala ili se osobno sretnu.

Kriptografija javnog ključa počiva na činjenici da je u nekim matematičkim strukturama (grupama) potenciranje puno jednostavnije od logaritmiranja. Konstruira se kriptosustav u kojem je funkcija **šifriranja** e_K javna, ali je unatoč tome, u razumnom vremenu, praktički nemoguće izračunati funkciju **dešifriranja** d_K. Ključnu ulogu u realizaciji te ideje imaju tzv. **osobne jednosmjerne funkcije**. Jednosmjerna funkcija je ona funkcija koja se vrlo lako (brzo, efikasno) izračunava, no jako se teško (npr. u eksponencijalnom vremenu) invertira. Ako se pri tome lako invertira u slučaju da je poznat neki dodatni podatak (eng. trapdoor – skriveni ulaz) tada je f osobna jednosmjerna fukcija. Sada formalno možemo definirati kriptosustav sa javnim ključem.

Definicija 2.1.1. *Kriptosustav s javnim ključem sastoji se od dviju familija, funkcija šifriranja* $\{e_K\}$ *te funkcija dešifriranja* $\{d_K\}$*, pri čemu K prolazi skupom svih mogućih korisnika uz sljedeća svojstva:*

1. $d_K = e_K^{-1}$;

2. *e_K je javan, dok je d_K poznat samo osobi K ;*

3. *e_K je osobna jednosmjerna funkcija.*

Uz spomenuta svojstva, e_K se naziva **javnim ključem**, a d_K **osobnim** ili **tajnim ključem**. Ukoliko Alice želi poslati poruku Bobu, on joj najprije pošalje svoj javni ključ e_B pomoću kojeg Alice šifrira svoju poruku, tzv. **otvoreni tekst**. Dobiveni rezultat $y = e_B(x)$, tzv. **šifrat**, Alice zatim šalje preko nekog komunikacijskog kanala Bobu, koji ga lako može dešifrirati koristeći svoj tajni ključ d_B te dobiva

$$d_B(y) = d_B(e_B(x)) = x.$$

U modernoj, komercijalnoj kriptografiji (primjerice kupnja preko interneta) pojavljuju se različiti problemi, a sigurnost informacija zasniva se na ispunjavanju idućih zahtjeva:

1. **Povjerljivost** (eng. confidentiality) - Informacije smiju biti dostupne samo ovlaštenim korisnicima, tj. poruku koju osoba A šalje osobi B nitko drugi ne može pročitati.

2. **Vjerodostojnost** (eng. autenticity) - Osoba B treba biti uvjerena da je jedino osoba A mogla poslati poruku koju je ona primila.

3. **Netaknutost** (eng. integrity) - Informacije smiju mijenjati samo za to ovlašteni korisnici, tj. osoba B zna da poruka, poslana od osobe A, nije promijenjena prilikom slanja.

4. **Nepobitnost** (eng. non-repudiation) - Ovlašteni korisnik, osoba A, ne može opovrgavati poslanu poruku tvrdeći da ju je poslao uljez.

Po pitanju vjerodostojnosti, tj. autentičnosti, neki sustavi omogućuju **digitalni potpis** poruke. Naime, uz prepostavku da je $\mathcal{P} = C$, gdje je $\mathcal{P}$ konačan skup svih otvorenih tekstova, a C konačan skup svih šifrata, osoba A može potpisati poruku x osobi B slanjem šifrata $z = d_A(y) = d_A(e_B(x)) =$. Osoba B pri primitku poruke za koju pretpostavlja da mu je poslao A najprije primijenu javni ključ e_A te nakon njega vlastiti tajni ključ d_B:

$$d_B(e_A(z)) = d_B(e_A(d_A(e_B(x)))) = x.$$

Kako je samo osoba A mogla upotrijebiti funkciju d_A, osoba B sigurna je da ju je upravo ona poslala, a u slučaju da je upotrijebljena neka funkcija d_C, poruka koju bismo dobili ne bi bila smislena. Dokaz slijedi iz jednakosti $e_B(x) = e_A(z)$.

U konstrukciji kriptosustava s javnim ključem, tj. osobnih jednosmjernih funkcija, najčešće se koriste neki „teški" matematički problemi iz teorije brojeva:

1. Problem faktorizacije velikih prirodnih brojeva čija je težina presudna za sigurnost RSA kriptosustava.

2. Problem diskretnog logaritma koji se primjerice koristi u ElGamalovom kriptosustavu te njegovim preinakama, kao što je DSA.

3. Problem diskretnog logaritma za eliptičke krivulje koji je temelj sigurnosti svih kriptosustava koji koriste eliptičke krivulje, npr. Menezes-Vanstoneovog kriptosustava.

U daljnjim ćemo se poglavljima pobliže upoznati s navedim kriptosustvima. Iako kriptosustavi s javnim ključem imaju određene prednosti nad simetričnim sustavima, kao što su izuzeće potrebe za sigurnim komunikacijskim kanalom pri razmjeni ključeva, potreba za manjim brojem ključeva (u grupi od N ljudi, omjer je $2N$ naprema $\frac{N(N-1)}{2}$ kod simetričnih kriptosustava) i mogućnost potpisa poruke, valja napomenuti da su kriptosustavi s javnim ključem puno sporiji od modernih simetričnih kriptosustava te se danas kriptografija javnog ključa više koristi za šifriranje ključeva, a same poruke se šifriraju simetričnim kriptosustavima. Takav se oblik naziva **hibridni kriptosustav**.

2.2 Problem diskretnog logaritma

Neka je G konačna Abelova grupa, koju zapisujemo multiplikativno. Takve grupe, osobito one u kojima su operacije množenja i potenciranja jednostavne, dok je logaritmiranje vrlo teško, predstavljaju dobar izbor za jednosmjerne funkcije. Inverz potenciranja fiksnog elementa u konačnoj grupi zovemo **diskretni logaritam**.

Definicija 2.2.1. *Neka je $(G, *)$ konačna grupa, $g \in G$, $H = \{g^i : i \geqslant 0\}$ podgrupa od G generirana s g te $h \in H$. **Diskretni logaritam** je najmanji nenegativni cijeli broj x, još i u oznaci $\log_g h$, takav da je $h = g^x$, gdje je*

$$g^x = \underbrace{g * g * \ldots * g}_{x\,puta}.$$

Primjerice, G može biti multiplikativna grupa konačnog polja $\mathbb{F}_q^*$ ili $E(\mathbb{F}_q)$ gdje za dvije točke $P, Q \in E(\mathbb{F}_q)$ na eliptičkoj krivulji problem diskretnog logaritma (za eliptičke krivulje) predstavlja određivanje nenegativnog cijelog broja d iz intervala $[0, n-1]$, pri čemu je n red točke P, takvog da vrijedi $Q = dP$, uz pretpostavku da takav d postoji. Kada su E i P ispravno odabrani, rješavanje problema diskretnog logaritma za eliptičke krivulje smatra se nemogućim, a potrebno je naglasiti kako je jedan od uvjeta sigurnosti taj da je n, red točke P, dovoljno velik da je teško provjeriti sve mogućnosti od d. Algoritmi za rješavanje problema diskretnog algoritma općenito se mogu podijeliti u 3 grupe:

1. Algoritmi koji rade u proizvoljnim grupama, kao što su iscrpno pretraživanje, algoritam „malih i velikih koraka" (eng. baby step - giant step, skraćeno BSGS) te Pollardova ρ-metoda.

2. Algoritmi koji rade u proizvoljnim grupama, s posebnom efikasnošću ukoliko red tih grupa ima samo male proste faktore, primjerice Pohlig-Hellman algoritam.

3. Algoritmi koji rade u specijalnim grupama, s točno određenim svojstvima, primjerice Index Calculus metoda, za koju je presudna mogućnost izbora relativno malog podskupa $\mathcal{B}$ grupe G (faktorske baze), koji ima svojstvo da se velik broj elemenata iz G može efikasno prikazati kao produkt elemenata iz $\mathcal{B}$.

Nećemo ulaziti u detalje nevedenih algoritama, a više o tome ima u [6]. Možemo se osvrnuti na složenost algoritama, prikazanih u sljedećoj tablici.

Algoritam	Složenost
Iscrpno pretraživanje	$O(n)$
BSGS	$O(\sqrt{n})$
Pollardova ρ-metoda	$O(\sqrt{n})$
Pohlig-Hellman algoritam	$O(\sqrt{q'})$, gdje je q' najveći prosti faktor od $p-1$
Index Calculus metoda	$O(e^{(c+o(1))(\log_2 q)^{1/2}(\log_2 \log_2 q)^{1/2}})$, gdje je $q = p$, a $c > 0$ konstanta

Uočavamo da Index Calculus metoda jedina ima subeksponencijalnu složenost te stoga predstavlja najbolji napad na problem diksretnog logaritma, naravno, onda kada ju je moguće koristiti. Budući da je dosta teško pronaći eliptičku krivulju velikog ranga ili generiranu točkama s malim brojnicima i nazivnicima, vrlo je ograničavajuća primjena ove metode na grupe eliptičkih krivulja nad konačnim poljem, pa je to predstavljalo i svojevrsnu motivaciju za uvođenje eliptičkih krivulja u kriptografiju.

Problem diskretnog logaritma za eliptičke krivulje mnogo je teži nego u multiplikativnoj grupi konačnog polja, pa se tražena sigurnost dobiva sa ključem manje duljine nego kod standardnih shema, što je osobito važno kod medija kojima je prostor pohrane ograničen. Valja napomenuti i da su algoritmi za rješavanje problema diskretnog logaritma za eliptičke krivulje, kao što su primjerice MOV ili Frey-Rückeov napad, zasnovani na uparivanjima, konkretno Weilovom spustu i Teteovom uparivanju, koji reduciraju problem diskretnog logaritma za eliptičke krivulje na onaj u multiplikativnoj grupi konačnog polja. Danas se najuspješnijom metodom za rješavanje problema diskretnog logaritma za eliptičke krivulje smatra Pollardova ρ-metoda, kojoj je za to potrebno otprilike $\frac{\sqrt{\pi n}}{2}$ zbrajanja točaka na eliptičkoj krivulji. Za neke specijalne slučajeve postoje još i efikasniji napadi, što nam ukazuje koje eliptičke krivulje trebamo izbjegavati u kriptografskim primjenama. Detaljnije o metodama za rješavanje problema diskretnog logaritma za eliptičke krivulje te specijalnim slučajevima ima u [14] (V. poglavlje).

2.3 RSA

Algoritam za kriptiranje javnih ključeva idejno je predstavljen 1977. godine od strane Ron Rivesta, Adi Shamira i Len Adlemana s Tehnološkog Instituta Massachusetts (MIT) te je 1983. godine i patentiran. RSA je prvi poznati algoritam pogodan za operacije kriptiranja i digitalnog potpisa te predstavlja veliki pomak u kriptografiji javnih ključeva, a zbog svoje sigurnosti vrlo je raširen u protokolima elektroničkog poslovanja. Njegova je sigurnost zasnovana na teškoći faktorizacije velikih prirodnih brojeva te se danas smatra gotovo nemogućim rastaviti na faktore pažljivo odabran prirodan broj s više od 250 znamenaka. Šifriranje i dešifriranje poruka u ovom kriptosustavu koristi modularno potenciranje, a ključno dobivanje dodatnog podatka temelji se na faktorizaciji. Sada ćemo samo navesti Eulerov teorem koji je temelj RSA kriptosustava, a za dokaz vidi [12].

Teorem 2.3.1. *Ako su x i n relativno prosti, tj. ako je $nzd\,(x, n) = 1$, vrijedi*

$$x^{\varphi(n)} \equiv 1 \pmod{n}.$$

Sijedi formalna definicija RSA kriptosustava.

Definicija 2.3.2. *Neka je $n = pq$, gdje su p i q prosti brojevi. Također, neka je $\mathcal{P} = C = \mathbb{Z}_n$, te*

$$\mathcal{K} = \{(n, p, q, d, e) \,:\, n = pq,\ de \equiv 1 \pmod{\varphi(n)}\}.$$

Za $K \in \mathcal{K}$ definiramo

$$e_K(x) = x^e \mod n, \quad d_K(y) = y^d \mod n, \quad x, y \in \mathbb{Z}_n.$$

Javni ključ sastoji se od modula n i javnog eksponenta e, a privatni od p, q te privatnog eksponenta d.

Ukoliko Alice želi poslati Bobu poruku, potrebni su idući koraci koji predstavljaju shemu RSA kriptosustava:

1. Bob tajno odabire dva različita velika prosta broja p i q, svaki otprilike iste veličine, te računa $n = pq$ i $\varphi(n) = (p-1)(q-1)$.

2. Bob također na slučajan način bira cijeli broj e, $1 < e < \varphi(n)$ sa svojstvom $nzd\,(e, \varphi(n)) = 1$ te nakon toga, pomoću proširenog Euklidovog algoritma, računa d tako da vrijedi

$$de \equiv 1 \pmod{\varphi(n)} \equiv 1 \pmod{(p-1)(q-1)}.$$

3. Bob javno objavi e i n, dok d, p i q zadrži tajnima.

4. Alice otvorenom tekstu pridružuje cijeli broj $x \pmod n$, šifrira ga kao $y \equiv x^e \pmod n$ te šalje y Bobu.

5. Bob dešifrira poruku računanjem $x \equiv y^d \pmod n$.

Ovdje je $e_K(x) = x^e \pmod n$ jednosmjerna funkcija, a dodatni podatak je poznavanje faktorizacije $n = pq$. Preostaje nam još provjeriti jesu li funkcije e_K i d_K jedna drugoj inverzne.

Dokaz. Imamo: $d_K(e_K(x)) \equiv x^{ed} \pmod n$. Kako je $de \equiv 1 \pmod{\varphi(n)}$, slijedi da postoji prirodan broj m takav da je $de = m\varphi(n) + 1$, iz čega dobivamo:

$$x^{de} = x^{m\varphi(n)+1} = x^{m\varphi(n)} \cdot x = \left(x^{\varphi(n)}\right)^m \cdot x.$$

U ovisnosti o n i x razlikujemo 2 slučaja:

1) $nzd\,(x, n) = 1$
Kako je tada, prema Eulerovom teoremu, $x^{\varphi(n)} \equiv 1 \pmod n$, vrijedi

$$x^{de} \equiv 1^m \cdot x \equiv x \pmod n.$$

2) $nzd\,(x, n) \neq 1$
Ako je $nzd\,(x, n) = n$, tada je $x^{de} \equiv 0 \equiv x \pmod n$.
Neka je $nzd\,(x, n) = p$ ili $nzd\,(x, n) = q$. Bez smanjenja općenitosti, uzmimo da je $(x, n) = p$, pa je $x^{de} \equiv 0 \equiv x \pmod p$. Budući da je $(pq, x) = p$, gdje su p i q prosti, slijedi da je $nzd\,(q, x) = 1$, pa je prema Eulerovom teoremu

$$x^{\varphi(q)} = x^{q-1} \equiv 1 \pmod q.$$

Stoga je

$$x^{de} = (x^{q-1})^{(p-1)m} \cdot x \equiv x \pmod q, \quad \text{tj.} \quad x^{de} \equiv x \pmod n.$$

Dakle, zaista je u svakom slučaju $x^{de} \equiv x \pmod n$., što je istovjetno $d_K(e_K(x)) = x$.

□

Sada ćemo, primjerom sa relativno malim i nesigurnim parametrima, ilustrirati šifriranje i dešifriranje u RSA kriptosustavu.

Primjer 2.3.3. *Bob odabire proste brojeve* $p = 101$ *i* $q = 113$ *te računa* $n = 11413$ *i* $\varphi(n) = 100 \cdot 112 = 11200$. *Kako je* $11200 = 2^5 5^2 7$, *cijeli broj e, javni eksponent, ne smije biti djeljiv sa* $2, 5$ *ili* 7.

Bob primjerice odabire $e = 3533$*, pa pomoću proširenog Euklidovog algoritma računa* d*, koji je ustvari multiplikativni inverz od* e*, pa se može označavati i s* e^{-1}*, te dobiva* $d = 6597$.

Dakle, Bobov javni ključ je $(n = 11413, e = 3533)$*, kojeg šalje Alice ili ga jednostavno upisuje u neki javni direktorij, dok je tajni ključ* $(p = 101, q = 113, d = 6597)$.

Sada, pretpostavimo da Alice želi poslati neku poruku čiji je numerički ekvivalent $x = 9726$*, pa modularnim potenciranjem računa*

$$y \equiv x^e \equiv 9726^{3533} \equiv 5761 \pmod{11413}.$$

Zatim taj dobiveni šifrat y *šalje Bobu, koji prilikom dešifriranja računa*

$$x \equiv y^d \equiv 5761^{6597} \equiv 9726 \pmod{11413}.$$

Valja napomenuti da se postupak šifriranja i dešifriranja obavlja nad cijelim brojevima. Naime, kako se alfabet otvorenog teksta sastoji od slova engleske abecede, svakom slovu se pridružuje odgovarajući redni broj (razmak $= 00, \mathrm{A} = 01, \mathrm{B} = 02, \mathrm{C} = 03, ..., \mathrm{Y} = 25, \mathrm{Z} = 26$). Ukoliko je broj x, pridružen poruci, veći od n, poruka se rastavlja na blokove od kojih je svaki manji od n. Za efikasnost RSA kriptosustava bitno je da se računanje $y = x^e \mod n$ može vrlo efikasno provesti upotrebom algoritma „kvadriraj i množi”:

1: $y = 1$

2: **za** $(s - 1 \geq i \geq 0)$ **radi**

3: $y = y^2 \mod n$

4: **ako** $(e_i = 1)$ **onda** $y = y \cdot x \mod n$

gdje je $e = \sum_{i=0}^{s-1} e_i 2^i$ binarni zapis broja e. Vidljivo je da ja ukupan broj množenja manji ili jednak $2s$, što znači da je ovaj algoritam polinomijalan sa složenošću $O(\log e \cdot \log^2 n)$.

Do sada smo mogli uočiti da je implementacija RSA vrlo jednostavna, pa je, analogno tome, napad na RSA jednostavno provediv ako je poznat eksponent d. Očit napad na RSA je faktorizacija od n, jer se iz poznavanja p i q lako odrede $\varphi(n)$, a onda i d. Međutim, trenutno najbrži algoritmi za faktorizaciju nisu polinomijalni te su brojevi od preko 250 znamenaka sigurni od ovog napada. Ipak, postoje neka pravila pri izboru parametara u RSA kriptosustavu, o kojima treba voditi računa kako bi ovaj sustav i dalje bio siguran. Navest ćemo neke od njih, a detaljnije o ovoj tematici ima u [11] (V. poglavlje) te [13] (VI. poglavlje).

Pri tajnom odabiru dvaju velikih prostih brojeva p i q, obično se prvo generira slučajan prirodan broj k s traženim brojem znamenaka, pa se pomoću nekog od testova prostosti (npr. Rabin-Miller testom) traži prvi prosti broj veći ili jednak k. Danas se pod velikim i

dovoljno sigurnim podrazumijevaju brojevi čija je bitovna prezentacija 1024 ili čak 2048 bitova, što znači da onda modulus n ima 2048 ili 4096 bitova. Također, potrebno je paziti da $n = pq$ bude otporan na efikasne metode faktorizacije, a to se postiže tako da $p \pm 1$ te $q \pm 1$ ne budu „glatki", tj. da imaju barem jedan veliki prosti faktor. Isto tako, p i q moraju biti dovoljno različiti, jer bi se u protivnom mogla iskoristiti činjenica da su približno jednaki $\sqrt{n}$.

Prilikom odabira javnog eksponenta e, u cilju smanjenja vremena potrebnog za šifriranje, mogli bismo izabrati neki mali broj. Stoga je $e = 3$ dugo bio popularan izbor, no izbor takvog eksponenta predstavlja opasnost za sigurnost, osobito ako više korisnika šalje identičnu poruku x, a svi upotrebljavaju isti javni eksponent. Da bi takav napad spriječio, generira se nasumično neki dodatak odgovarajuće duljine bitova koji se treba dodati prije šifriranja otvorenom tekstu poruke, nezavisno za svako šifriranje. Međutim, ni to ne osigurava potpunu sigurnost, pa se danas izbjegava korištenje $e < 10^5$ te je najčešći $e = 2^{16} + 1 = 65537$, osobito pogodan jer sadrži samo dvije jedinice u binarnom prikazu.

Isto tako, niti d ne smije biti mali broj. Naime, ako je duljina bitovnog zapisa dekripcijskog eksponenta d približno jednaka ili manja jednoj četvrtini bitovne duljine modula n, tada postoji efikasan polinomijalni algoritam koji računa d iz javne informacije (n, e).

Nekada se razmišljalo o tome da bi neka glavna, povjerljiva osoba trebala generirati jedinstveni modul n i onda distribuirati različite enkripcijske/dekripcijske eksponentske parove (e_i, d_i) korisnicima u mreži. No, poznavanje bilo kojeg para (e_i, d_i) omogućuje faktorizaciju od n te bi onda svaka osoba mogla posljedično odrediti dekripcijske eksponente svih drugih korisnika u mreži.

Možemo zaključiti da još uvijek nije pronađena metoda koja bi, uz pravilnu iplementaciju i odabir parametara, mogla razbiti RSA kriptosustav, pa se isti može smatrati vrlo sigurnim. Što se tiče kriptosustava koji koriste eliptičke krivulje, a utemeljeni su na problemu faktorizacije, oni postoje, međutim, nisu osobito popularni i korišteni, jer ne osiguravaju nikakvu praktičnu prednost nad RSA. Jedan takav sustav (Koyama - Maurer - Okamoto - Vanstone) opisan je u [14] (Poglavlje 6.8.).

2.4 Diffie-Hellman protokol

Diffie-Hellmanov protokol za razmjenu ključeva prvi je takav protokol koji je javno objavljen. On omogućuje razmjenu tajnih ključeva nekim nesigurnim komunikacijskim kanalom, a bez prethodne komunikacije sudionika. Ti se ključevi poslije obično koriste u bržim simetričnim kriptosustavima, primjerice DES-u. Sam postupak zasniva se na bitnoj razlici u složenosti modularnog potenciranja i izračunavanja diskretnog logaritma, a u njegovoj originalnoj definiciji uzima se ciklička multiplikativna grupa $\mathbb{Z}_p^*$ svih ne-nul ostataka modulo p, gdje je p dovoljno veliki prost broj. Generator ove grupe, $g \in \{1, 2, \ldots, p-1\}$, **primitivni** je **korijen** modulo p ako je g^{p-1} najmanja potencija broja g, koja pri dijeljenju

s p, daje ostatak 1. Jedina informacija o kojoj se sudionici, na bilo koji način (npr. objava na internetu), unaprijed dogovore jest grupa G i njezin generator g. Ako sa $|G|$ označimo broj elemenata u grupi G, koraci Diffie-Hellman protokola su sljedeći:

1. Alice generira slučajan prirodan broj $a \in \{1, 2, \ldots |G| - 1\}$ te pošalje Bobu element g^a.
2. Bob generira slučajan prirodan broj $b \in \{1, 2, \ldots |G| - 1\}$ te pošalje Alice element g^b.
3. Alice izračuna $\left(g^b\right)^a = g^{ab}$.
4. Bob izračuna $(g^a)^b = g^{ab}$.

Kako su ključevi koje su izračunali jednaki, oni su upravo razmjenili simetrični ključ kriptiranja $K = g^{ab}$.

Navedeni protokol ilustrirat ćemo i primjerom.

Primjer 2.4.1. *Alice i Bob dogovore se oko brojeva $p = 941$ te primitivnog korijena $g = 627$. Alice zatim odabire svoj privatni broj $a = 347$ te izračuna $A = 390 \equiv 627^{347} \pmod{941}$, što je moguće vrlo efikasno izvesti koristeći već opisani algoritam „kvadriraj i množi". Slično, Bob odabire $b = 781$ te izračuna $B = 691 \equiv 627^{781} \pmod{941}$. Brojeve A i B zatim međusobno razmjene preko nekog nesigurnog kanala, pa se oni smatraju javnima, dok a i b trebaju ostati tajnima. Sada su oboje u mogućnosti izračunati*

$$470 \equiv 627^{347 \cdot 781} \equiv A^b \equiv B^a \pmod{941},$$

pa je njihov tajni ključ 470. Pod pretpostavkom da Eve i vidi cijelu njihovu razmjenu, jedini način da sazna njihov tajni ključ je rješavanje bilo koje od ovih kongruencija:

$$627^a \equiv 390 \pmod{941} \qquad \textit{ili} \qquad 627^b \equiv 691 \pmod{941},$$

budući da bi onda otkrila neki od njihovih tajnih eksponenata.

Naravno, brojevi u ovom primjeru su premali kako bi osigurali sigurnost, pa se danas preporuča izbor prostog broja p od oko 1000 bitova ($\approx 2^{1000}$) te generatora g čiji je red također prost broj, približne veličine $p/2$. Općenito, Eva može saznati iduće podatke: G, g, g^a, g^b, te iz njih želi izračunati g^{ab}, tj. treba riješiti **Diffie-Hellmanov problem**. U većini grupa do danas nije poznat jednostavan način računanja g^{ab} isključivo iz poznavanja g^a i g^b bez prethodnog računanja diskretnih logaritama od a i b, pa se vjeruje da su Diffie-Hellmanov problem i problem diskretnog logaritma u tim grupama ekvivalentni. Međutim, primjerice, u grupi eliptičkih krivulja $E(\mathbb{F}_p)$ postoje slučajevi koji pokazuju da je

Diffie-Hellmanov problem lakši od problema diskretnog logaritma, jer se ovaj prvi može riješiti upotrebom samo Weilovog spusta. Diffie-Hellmanov problem lako se implementira i za eliptičke krivulje, gdje je za dane $\mathbb{F}_q, P, aP, bP \in E(\mathbb{F}_q)$ potrebno odrediti abP. Alice i Bob mogu se npr. unaprije dogovoriti da, nakon izračuna abP, za tajni ključ koriste posljednih 256 bitova $x-$kordinate od abP.

Diffie-Hellmanov protokol koristi se kod autentikacije u mrežama računala te u postupku stvaranja digitalnih potpisa i digitalnih certifikata, a što se tiče napada, osjetljiv je na one kada uljez presreće poruke koje šalju korisnici i nadomješta ih svojim porukama. To je tzv. napad s čovjekom u sredini (eng. man in the middle). Općenito protokoli koji koriste Diffie-Hellmanov protokol stoga obično imaju neku dodatnu zaštitu za sprječavanje ovog napada, primjerice zahtjev za autentikaciju pošiljatelja i primatelja prije same razmjene. Diffie-Hellmanov protokol također se može postaviti tako da se poboljša otpornost na napade grubom silom (eng. brute force), pravilnim odabirom parametara te kombiniranjem upotrebe statičnog i privremenog ključa tokom razmjene tajnog ključa. Unatoč stalnim istraživanja u području razmjene ključeva, Diffie-Hellmanov protokol još uvijek ostaje u upotrebi kao najpopularnije rješenje za razmjenu tajnih ključeva u kriptografskim sustavima.

2.5 ElGamalov kriptosustav

Iako je već spomenuti RSA kriptosustav povijesno prvi, najprirodniji nastavak razvoja kriptosustava s javnim ključem nakon objave [2] onaj je opisan od Taher ElGamala 1985. godine. Elgamalov kriptosustav zasnovan je na teškoći računanja diskretnog logaritma u grupi $(\mathbb{Z}_p^*, \cdot_p)$ koji je približno iste težine kao problem faktorizacije složenog broja n, pod uvjetom da su p i n istog reda veličine. Sada ćemo formalno definirati Elgamalov kriptosustav.

Definicija 2.5.1. *Neka je p prost broj i $g \in \mathbb{Z}_p^*$ primitivni korijen modulo p. Nadalje, neka je $\mathcal{P} = \mathbb{Z}_p^*$, $C = \mathbb{Z}_p^* \times \mathbb{Z}_p^*$ te*

$$\mathcal{K} = \{(p, g, m, h) \ : \ h = g^m \mod p\}.$$

Javni ključ je (p, g, h), dok je tajni ključ $m \in \{2, 3, \ldots, p-2\}$.
Za $K \in \mathcal{K}$ i tajni slučajno generirani broj $k \in \{0, 1, \ldots, p-1\}$ definiramo

$$e_K(x, k) = (g^k \mod p, xh^k \mod p).$$

Za $y_1, y_2 \in \mathcal{P} = \mathbb{Z}_p^*$ definiramo

$$d_K(y_1, y_2) = y_2(y_1^m)^{-1} \mod p.$$

Shema ElGamalovog kriptosustava izgleda ovako:

1. Bob odabire veliki prosti broj p, zatim g koji je primitivni korijen modulo p, te nasumični $m \in \{2, 3, \ldots, p-2\}$ koji će biti tajni ključ.
2. Bob nakon toga računa $h = g^m \mod p$, te objavljuje svoj javni ključ (p, g, h).
3. Alice preuzima Bobov javni ključ te otvorenom tekstu pridružuje $x \in \{1, 2, \ldots, p-1\}$.
4. Alice odabire tajni slučajni broj $k \in \{0, 1, \ldots, p-1\}$, računa $y_1 = g^k \mod p$ i $y_2 = xh^k \mod p$ te šalje Bobu šifriranu poruku (y_1, y_2).
5. Bob dešifrira poruku računanjem $x = y_2(y_1^m)^{-1} \mod p$.

Možemo se uvjeriti da $y_2(y_1^m)^{-1} \mod p$ doista je otvoreni tekst x. Naime,

$$y_2(y_1^m)^{-1} = xh^k g^{-k} = xg^{mk} g^{-mk} = xg^{mk-mk} = x \mod p.$$

Glavni cilj Eve je, naravno, određivanje otvorenog teksta x koji se u enkripciji „maskira" množenjem sa h^k. Ustvari joj je cilj otkrivanje tajnog eksponenta m jer iz g^k može izračunati h^k, invertirati ga i „ukloniti masku". Pri izboru broja p, danas se preporuča veličina od 1024 bita, s tim da bi također broj $p-1$ trebao imati barem jedan veliki prosti faktor. Ukoliko je x neka duža poruka, rastavlja se na blokove koji se zasebno kriptiraju, a pri tome se i za svaki blok koristi novi slučajni k. U protivnom bi Eve mogla, ukoliko presretne npr. dvije poruke s istim k, lako izračunati i drugu poruku, a da samo jednu od njih dešifrira gore navedenim postupkom. Naime, ako je $(y_{11}, y_{21}) = (g^k \mod p, x_1 h^k \mod p)$ te $(y_{12}, y_{22}) = (g^k \mod p, x_2 h^k \mod p)$, tada je $y_{22}{y_{21}}^{-1} \equiv x_2 {x_1}^{-1} \pmod p$, iz čega slijedi da je $x_2 \equiv y_{22}{y_{21}}^{-1} x_1 \pmod p$. Ilustrirajmo sada ElGamalov kriptosustav numeričkim primjerom.

Primjer 2.5.2. *Bob odabire* $p = 467, g = 2$ *te tajni ključ* $m = 153$. *Zatim računa* $h = g^m \mod p = 2^{153} \mod 467 = 224$*, te objavljuje svoj javni ključ* $(153, 2, 224)$.
Pretpostavimo sada da Alice želi Bobu poslati poruku $x = 331$. *Neka je njen tajno odabrani jednokratni ključ* $k = 197$. *Tada Alice računa*

$$y_1 = g^k \mod p = 2^{197} \mod 467 = 87,$$

$$y_2 = xh^k \mod p = 331 \cdot 224^{197} \mod 467 = 57,$$

te pošalje Bobu šifrat $(87, 57)$. *Bob, nakon što primi šifrat* $(87, 57)$*, računa*

$$x = y_2(y_1^m)^{-1} \mod p = 57 \cdot (87^{153})^{-1} \mod 467$$

$$= 57 \cdot 367^{-1} \mod 467 = 57 \cdot 14 \mod 467 = 331,$$

što predstavlja originalni otvoreni tekst.

Efikasnost se znatno može poboljšati koristeći algoritam „kvadriraj i množi" prilikom modularnog potenciranja te proširenog Euklidovog algoritma za inverz modulo p.

ElGamalov je kriptosustav, slično kao i Diffie-Hellmanov protokol, osjetljiv na napad s čovjekom u sredini, pa se često koriste neki dodatni zahtjevi za autentifikaciju koji povećavaju sigurnost. Dok je tranzicija iz enkripcije ka digitalnom potpisu, vrlo jednostavna i izravna kod RSA, u Elgamalovom kriptosustavu to nije slučaj. Prva Elgamalova shema digitalnog potpisa objavljena je 1985. godine, a modificirana verzija nazvana DSA, 1991. godine. Glavna prednost ovog potpisa u usporedbi sa Elgamalovom shemom digitalnog potpisa je dužina od samo 320 bitova, a i neki napadi koji mogu ugroziti Elgamalovu shemu ne mogu se primijeniti na DSA. Također, postoji i unapređenje DSA koje pruža manju veličinu ključa s približno jednakim razinama sigurnosti i vremenom obrade te identičnom duljinom generiranog sažetka, tzv. ECDSA koji u svom radu koristi eliptičke krivulje. Američki nacionalnoi institut za standardizaciju je 1998. godine prihvatio ECDSA kao standard. Budući da korištenje originalne poruke u generiranju digitalnog potpisa često rezultira vrlo dugačkim potpisom, umjesto originalne poruke često se koristi „sažetak poruke" koji se dobije pomoću neke **hash fukcije**. To su jednosmjerne funkcije koje za ulazni podatak proizvoljne duljine daju izlazni podatak fiksne duljine, uz svojstva:

1. Za zadanu M, lako se izračuna $h(M)$;
2. Za zadanu $h(M)$, praktički je nemoguće naći M;
3. Za zadanu M nemoguće je izračunati M' tako da je $h(M) = h(M')$, tj. otporna je na koliziju;
4. Izmjena ulaznih podataka čak i za samo jedan bit daje različit rezultat prilikom heširanja.

Detaljnije o spomenutim shemama digitalnog popisa ima u [5] (Poglavlje 7.3.) te [3] (Poglavlje 4.3.).

2.6 ElGamalov kriptosustav nad eliptičkim krivuljama

Ideju o tome da bi eliptičke krivulje mogle biti korisne u konstrukciji kriptosustava s javnim ključem prvi su javno iznijeli N. Koblitz i V. Miller 1985. godine. Svi sustavi koji

u originalnoj definiciji koriste grupu $\mathbb{Z}_p^*$, mogu se lako modificirati tako da koriste grupu $E(\mathbb{Z}_p)$. Definicija problema diskretnog logaritma vrijedi i u ovim grupama, čak štoviše, razlika u težini problema potenciranja i logaritmiranja još je veća. Naravno, ovdje treba napomenuti da je eliptička krivulja aditivna, a ne multiplikativna Abelova grupa, pa zapravo „potenciranje" točke na eliptičkoj krivulji predstavlja njeno uzastopno zbrajanje sa samom sobom, tj. množenje skalarom (prirodnim brojem). Točka $kP \in E(\mathbb{Z}_p)$, za danu točku p i prirodan broj k, jednostavno se pronalazi algoritmom „udvostruči i zbroji" koji smo opisali u nekom od prethodnih poglavlja. To je ustvari analogon algoritmu „kvadriraj i množi" za pronalaženje k-te potencije nekog elementa. Međutim, doslovno prevođenje ElGamalovog kriptosustava u eliptičke krivulje ima neke nedostatke.

Naime, elemente otvorenog teksta prije šifriranja potrebno je prebaciti u točke na eliptičnoj krivulji, a za to ne postoji deterministički, već samo vjerojatnosni algoritam, koji počiva na činjenici da polovinu svih elemenata u konačnoj grupi predstavljaju kvadrati. To znači da s vjerojatnošću od približno $1 - 1/2^k$ možemo očekivati da ćemo iz k pokušaja pronaći takav x, da je x^3+ax+b kvadrat u $\mathbb{Z}_p$. Primjerice, za $k = 30$, ta je vjerojatnost zadovoljavajuća. Pretpostavimo da su osnovne jedinice otvorenog teksta cijeli brojevi između 0 i M te da je $p > Mk$. Otvorenom tekstu m pridružujemo točku na eliptičkoj krivulji $E(\mathbb{Z}_p)$ tako da za brojeve x koji su oblika $mk + j, \quad j = 1, 2, \ldots, k$ provjerimo je li $x^3 + ax + b$ kvadrat u $\mathbb{Z}_p$, a ukoliko je, $y \in \mathbb{Z}_p$ izračunamo tako da zadovoljava $y^2 \equiv x^3 + ax + b \pmod{p}$. Sada broju m možemo pridružiti točku $(x, y) \in E(\mathbb{Z}_p)$, dok se obrnuti proces, računanje otvorenog teksta iz poznavanja točke, računa po formuli $m = \lfloor \frac{x-1}{k} \rfloor$. Ovaj proces možemo pokazati i na jednostavnom primjeru.

Primjer 2.6.1. *Neka je E eliptička krivulja nad $\mathbb{Z}_p$ zadana sa $y^2 = x^3 + 3x$, te neka je $p = 4177$, $m = 2174$. Za k izabiremo 30, a u praksi je on inače $30 \leq k \leq 50$. Isto tako u praksi bismo inače uzeli $p > 30m$, međutim ovo je samo ilustrativni primjer. Nakon toga računamo*

$$x = 30m + j, \quad j = 1, 2, \ldots, k$$

sve dok $x^3 + 3x$ nije kvadrat modulo 4177. Taj uvjet je zadovoljen za $j = 15$, jer je

$$x = 30 \cdot 2174 + 15 = 65235,$$

$$x^3 + 3x = 65235^3 + 3 \cdot 65235 = 277614407048580 \equiv 1444 \equiv 38^2 \pmod{4177}.$$

Dakle, odredili smo točku $(65235, 38) \in E(\mathbb{Z}_p)$ koja se može pridružiti otvorenom tekstu $m = 2174$.
Računanje otvorenog teksta m iz točke $(65235, 38) \in E(\mathbb{Z}_p)$ puno je jednostavnije. Naime,

$$m = \left\lfloor \frac{65235 - 1}{30} \right\rfloor = \left\lfloor \frac{65234}{30} \right\rfloor = \lfloor 2174.47 \rfloor = 2174.$$

Također, drugi nedostatak je i duljina poruke nakon šifriranja, jer se šifrat jednog elementa sastoji od uređenog para točaka na eliptičkoj krivulji te je stoga 4 puta dulji od originalne poruke. Slijedi shema Elgamalovog kriptosustava nad eliptičkim krivuljama:

- Generiranje ključeva
  Bob definira eliptičku krivulju E nad konačnim poljem $\mathbb{Z}_p$ te odabire bazičnu točku $G_B \in E(\mathbb{Z}_p)$, koja je obično takva da joj je red neki veliki prosti broj. Također odabire cijeli broj d_B za svoj tajni ključ. Nakon toga računa $P_B = d_B G_B$ i objavljuje svoj javni ključ $\{E(\mathbb{Z}_p), G_B, P_B\}$.

- Šifriranje
  Alice preuzima Bobov javni ključ te otvorenom tekstu pridružuje točku $m \in E(\mathbb{Z}_p)$ na način koji smo prije objasnili. Zatim odabire tajni slučajni broj $k \in \{0, 1, \ldots, p-1\}$ te „maskira" poruku dodavajući joj kP_B.

  $$c = m + kP_B$$

  Alice dodaje i sljedeći „hint" $r = kG_B$ šifratu c te ih šalje Bobu.

- Dešifriranje
  Bob množi „hint" r svojim privatnim ključem d_B te dobiveni rezultat oduzima od šifrata c kako bi dobio otvoreni tekst m.

  $$c - d_B r = m + kP_B - d_B k G_B = m + k d_B G_B - d_B k G_B = m.$$

Eve može saznati otvoreni tekst m iz šifrata c, samo ukoliko odredi k iz r, međutim, taj je problem vrlo težak. Ipak, radi dodatne sigurnosti, Alice svaki put treba generirati drugačiji k, jer bi u protivnom Eve mogla, ukoliko presretne više poruke s istim k, lako izračunati i ostale poruku, a da samo jednu od njih dešifrira.

ElGamalov kriptosustav nad eliptičkim krivuljama dodatno ćemo objasniti malim numeričkim primjerom.

Primjer 2.6.2. *Koristit ćemo notaciju $E_p(a, b)$ za skup točaka na eliptičnoj krivulji definiranoj nad $\mathbb{Z}_p$.*
Bob odabire bazičnu točku $G_B = (2, 7)$ u $E_{11}(1, 6)$ i tajni ključ $d_B = 5$. Red točke G_B je $n = 13$, jer je $13G_B = \mathcal{O}$. Zatim računa $P_B = d_B G_B = 5(2, 7) = (3, 6)$ i objavljuje svoj javni ključ $\{E_{11}(1, 6), G_B = (2, 7), P_B = (3, 6)\}$.
Pretpostavimo sada da Alice želi Bobu poslati poruku prezentiranu kao točka $m = (3, 5)$ na eliptičkoj krivulji. Neka je njen tajno odabrani jednokratni ključ $k = 6$. Tada Alice računa

$$r = kG_B = 6(2, 7) = (7, 9)$$

$$c = m + kP_B = (3,5) + 6(3,6) = (3,5) + (10,2) = (2,4)$$

te ih pošalje Bobu. Bob, nakon što primi „hint" $r = (7,9)$ i šifrat $c = (2,4)$ računa

$$m = c - d_B r = (2,4) - 5(7,9) = (2,4) - (10,2) = (2,4) + (10,9) = (3,5)$$

što predstavlja originalni otvoreni tekst.

(Napomena: $-(10,2) \equiv (10,9)$ jer je $4G_B = (10,2)$, $9G_B = (10,9)$, a $4G_B + 9G_B = O$.)

2.7 Menezes-Vanstoneov kriptosustav eliptičkih krivulja

Budući da se doslovnim prevođenjem ElGamalovog kriptosustava na eliptičke krivulje duljina poruke učetverostruči, predložene su i druge varijante ovog kriptosustava koje također koriste eliptičke krivulje. Jedna od njih je tzv. Menezes-Vanstoneov kriptosustav koji je prvi put predstavljen 1993. godine, a kod kojeg je šifrirana poruka „samo" 2 puta dulja od originalne. U ovom kriptosustavu, umjesto prevođenja jedinice otvorenog teksta u točku eliptičke krivulje, alati koje pružaju eliptičke krivulje koriste se samo za „maskiranje" jedinica otvorenog teksta, a otvoreni tekstovi i šifrati proizvoljno su uređeni parovi elemenata iz polja. Dakle, nema nikakve potrebe za kompliciranim postupkom prevođenja otvorenog teksta na jezik točaka eliptičke krivulje. Shema Menezes-Vanstoneovog kriptosustava izgleda ovako:

- Neka je E eliptička krivulja nad $\mathbb{Z}_p$ ($p > 3$ prost), te H ciklička podgrupa od E generirana točkom $P \in E(Z_p)$. Pretpostavimo da Alice želi Bobu poslati poruku $m = (m_1, m_2) \in Z_p^* \times Z_p^*$.

- Generiranje ključeva
  Bob odabire cijeli broj a za svoj tajni ključ. Nakon toga računa $\beta = aP$ i objavljuje svoj javni ključ $\{ E(\mathbb{Z}_p), P, \beta \}$.

- Šifriranje
  Alice preuzima Bobov javni ključ , a zatim odabire tajni slučajni broj $k \in \{0, 1, \ldots, |H|-1\}$ te računa $(y_1, y_2) = k\beta$, $c_0 = kP$ i $c_j = y_j m_j \mod p$ za $j = 1, 2$. Nakon toga šalje šifrat $e_K(m,k) = (c_0, c_1, c_2) = c$ Bobu.

- Dešifriranje
  Bob prvo računa $ac_0 = (y_1, y_2)$, a zatim konačno i

$$d_K(c) = (c_1(y_1)^{-1} \mod p \ , \ c_2(y_2)^{-1} \mod p) = m.$$

Možemo se uvjeriti da $(c_1(y_1)^{-1}, c_2(y_2)^{-1}) \mod p$ doista je otvoreni tekst m. Naime, Bob iz primljenog šifrata $c = (c_0, c_1, c_2)$ lako izračuna (y_1, y_2), jer vrijedi $(y_1, y_2) = k\beta = kaP = akP = ac_0$, što pokazuje da ne mora poznavati k. Onda, budući da je $(c_1, c_2) = (y_1 m_1, y_2 m_2) \mod p$, slijedi da je

$$(c_1(y_1)^{-1}, c_2(y_2)^{-1}) \mod p = (y_1(y_1)^{-1}m_1, y_2(y_2)^{-1}m_2) \mod p = (m_1, m_2) = m.$$

Glavni cilj Eve je, naravno, određivanje otvorenog teksta m, međutim, iz poznavanja šifrata c, a bez tajnog ključa a, to se svodi na problem diskrenog logaritma.
Sada ćemo ovaj kriptosustav dodatno objasniti malim numeričkim primjerom.

Primjer 2.7.1. *Neka je E eliptička krivulja nad $\mathbb{Z}_{13}$ zadana sa*

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

Bob odabire $P = (1, 3)$ koja je generator od $E(\mathbb{Z}_{13})$, a kako je $15P = \mathcal{O}$, slijedi da je $\#E(\mathbb{Z}_{13}) = 15$. Također, odabire i svoj tajni ključ $a = 2$ te računa $\beta = aP = 2(1, 3) = (12, 8)$ i objavljuje svoj javni ključ $\{E_{13}(4, 4), P = (1, 3), \beta = (12, 8)\}$.

Pretpostavimo sada da Alice želi Bobu poslati poruku $m = (12, 7)$. Neka je njen tajno odabrani jednokratni ključ $k = 5$. Tada Alice računa

$$(y_1, y_2) = k\beta = 5(12, 8) = (10, 11),$$

$$c_0 = kP = 5(1, 3) = (10, 2),$$

$$c_1 \equiv y_1 m_1 = 10 \cdot 12 \equiv 3 \pmod{13}, \; c_2 \equiv y_2 m_2 = 11 \cdot 7 \equiv 12 \pmod{13},$$

te šalje Bobu šifrat $c = (c_0, c_1, c_2) = \{(10, 2), 3, 12\}$.

Bob, po primitku c, prvo računa $ac_0 = 2(10, 2) = (10, 11) = (y_1, y_2)$, a onda i konačno

$$m = (3 \cdot 10^{-1} \mod p \;,\; 12 \cdot 11^{-1} \mod p) = (12, 7),$$

što predstavlja originalni otvoreni tekst.

2.8 Massey-Omura kriptosustav

Massey-Omura kriptografska shema, predstavljena 1982. godine, primjer je protokola s tri „predaje" (eng. three-pass protocol) koja ne zahtjeva razmjenu distribucijskih ključeva,

međutim zahtjeva da pošiljatelj i primatelj imaju svoje privatne ključeve za šifriranje i dešifriranje. Nematematičkim riječnikom, algoritam funkcionira tako da Alice zaključa lokotom svoju poruku P te ju predaje Bobu. On stavlja drugi lokot na poruku i predaje ju natrag Alice, koja nakon toga skida svoj lokot ostavljajući poruku samo sa Bobovim lokotom, te ju predaje ponovno natrag njemu. Konačno, nakon treće predaje, on skida lokot te dobiva originalnu poruku koju mu je Alice poslala. Valja napomenuti da se sve ovo odvija preko nekog javnog komunikacijskog kanala te da se može implementirati u bilo kojoj konačnoj grupi. Ovim se načinom, uz slanje kratkih poruka, mogu slati i tajni ključevi koji će se koristiti u drugim kriptosustavima. Zbog toga, kao i zbog toga što ne postoji javni ključ, neki ovaj algoritam više smatraju protokolom za razmjenu ključeva te se ne koristi previše u praksi. Međutim, zbog ilustracije drugačijeg pristupa u kriptografiji, svakako je vrijedan spomena, pa i daljnje analize.
Slijedi matematički opis Massey-Omura kriptosustava:

1) Alice i Bob javno se dogovore oko izbora eliptičke krivulje E nad poljem $\mathbb{F}_q$ gdje je $q = p^n$ takav da je problem diskretnog logaritma praktički nerješiv u $E(\mathbb{F}_q)$. Prepostavimo također da je q prost broj, te da je $\#E(\mathbb{F}_q) = N$ javno poznat.

2) Alice odabire tajni par brojeva (e_A, d_A) takav da je $e_A d_A \equiv 1 \pmod{N}$. Istovjetno, Bob odabire svoj tajni par brojeva (e_B, d_B) takav da je $e_B d_B \equiv 1 \pmod{N}$.

3) Pretpostavimo da Alice želi poslati poruku Bobu. Alice otvorenom tekstu pridružuje točku $P \in E(\mathbb{F}_q)$ na način koji smo objasnili u prethodnom poglavlju. Zatim slijedi procedura:

   a) Alice šalje $P_1 = e_A P$ Bobu.

   b) Bob šalje $P_2 = e_B P_1$ Alice.

   c) Alice šalje $P_3 = d_A P_2 = d_A e_B P_1 = d_A e_B e_A P = e_B P$ Bobu.

   c) Bob konačno računa $d_B P_3 = d_B e_B P = P$, te tako dobiva otvoreni tekst P.

Možemo se uvjeriti da je se $e_B d_B \equiv 1 \pmod{N}$, dovoljan uvjet da se e_B i d_B međusobno poništavaju, tj. da je $d_B P_3 = d_B e_B P = P$. Naime, iz $e_B d_B \equiv 1 \pmod{N}$ slijedi da je $e_B d_B = 1 + kN$, za neki cijeli broj k. Red grupe $E(\mathbb{F}_q)$ je N, pa po Lagrangeovom teoremu slijedi da je $NR = \mathcal{O}$, za svaki $R \in E(\mathbb{F}_q)$, pa i za P. Stoga je

$$d_B e_B P = e_B d_B P = (1 + kN)P = P + k \cdot \mathcal{O} = P.$$

Ista diskusija vrijedi i za e_A i d_A. Možemo primijetiti da Eve poznaje P_1, P_2 i P_3. Kada bi uspjela riješiti problem diskretnog logaritma na eliptičkoj krivulji, mogla bi pomoću prve dvije točke izračunati e_B , zatim $d_B = e_B^{-1} \mod N$, a konačno i $d_B P_3 = P$.

I kod ovog je kriptosustava izuzetno efikasan napad s čovjekom u sredini. Naime, Eve odabire neki cijeli broj e_E te odgovara na prvu poslanu poruku od Alice sa $e_E P_1$, na koju ona može, ukoliko ne prepozna da je riječ o lažnom predstavljanju, odgovoriti sa $P'_3 = e_E P$. Tada Eve lako doznaje originalnu poruku P računajući $d_E = e_E^{-1} \mod N$, tj. $d_E P'_3 = P$. Zbog toga se često koriste neki dodatni zahtjevi za autentifikaciju koji povećavaju sigurnost. Prikazat ćemo i pojednostavljeni primjer koji koristi ovaj algoritam.

Primjer 2.8.1. *Neka je E eliptička krivulja nad $\mathbb{Z}_{13}$ zadana sa*

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

kao u primjeru 2.7.1, pa znamo da je $\#E(\mathbb{Z}_{13}) = N = 15$.
Alice odabire tajni par brojeva $(e_A, d_A) = (7, 13)$. Primijetimo da je

$$e_A d_A = 7 \cdot 13 = 91 \equiv 1 \pmod{15}.$$

Bob odabire svoj tajni par brojeva $(e_B, d_B) = (2, 8)$. Također je

$$e_B d_B = 2 \cdot 8 = 16 \equiv 1 \pmod{15}.$$

Pretpostavimo da Alice želi Bobu poslati poruku $P = (12, 8)$. Slijedi procedura slanja međusobnih poruka:

- *Alice šalje $P_1 = e_A P = 7(12, 8) \equiv (1, 10) \pmod{13}$ Bobu.*
- *Bob šalje $P_2 = e_B P_1 = 2(1, 10) \equiv (12, 5) \pmod{13}$ Alice.*
- *Alice šalje $P_3 = d_A P_2 = 13(12, 5) \equiv (6, 6) \pmod{13}$ Bobu.*
- *Bob konačno računa $d_B P_3 = 8(6, 6) \equiv (12, 8) \pmod{13}$, te tako dobiva otvoreni tekst $P = (12, 8)$.*

Zaključak

Kao što smo već objasnili, kriptosustavi zasnovani na eliptičkim krivuljama, svoju su primjenu prvenstveno pronašli zbog nepostojanja subeksponencijalnih algoritama za rješavanje problema diskretnog logaritma za eliptičke krivulje, za razliku od postojanja istog u multiplikativnog grupi konačnog polja. Zbog toga se zadovoljavajuća sigurnost postiže s (puno) kraćim ključem nego kod kriptosustava zasnovanih na faktorizaciji ili običnom problemu diskrenog logaritma.

U usporedbi najboljih algoritama za probleme eliptičkog (u $E(\mathbb{F}_q)$) i običnog diskrenog logaritma (u $\mathbb{F}_p^*$), pri čemu je M broj bitova od p, a N broj bitova od q, pokazuje se da je duljina ključa N ugrubo treći korijen duljine ključa M. Kako je implementacija kompleksnija u slučaju eliptičkih krivulja, komparacija nije sasvim egzaktna, međutim, svakako pokazuje određenu prednost ECC kriptosustava.

Više od asimtotskog odnosa M i N svakako je važniji onaj kod standarnih vrijednosti, pa je tako za postizanje iste razine sigurnosti kao kod RSA s duljinom ključa od 1024 bita, kod eliptičkih krivulja dovoljno uzeti ključ duljine 160 bitova. Zbog toga se kod eliptičkih krivulja ključ puno brže generira, otprilike 40 puta. Kako šifriranje duljih ključeva zahjeva i više računanja, a samim time i tranzistora koji ih vrše, kao posljedicu imamo i potrebu za većom snagom i memorijom procesora. Zato eliptičke krivulje imaju sve veću važnost u aplikacijama koje uključuju mobilne uređaje, pametne kartice, bankarske aplikacije, aplikacije za elektroničko poslovanje, itd.

No, u usporedbi sa simetričnim kriptosustavima, kojima ja najveća zamjerka nužnost tajnosti ključa s obje strana komunikacije i stalna potreba za njegovim mijenjanjem, ECC kriptosustavi imaju dulje ključeve te su računski zahtjevniji, pa su samim time i sporiji. U 2001. godini, Lenstra i Verheul dali su preporuke i iznijeli predviđanja o duljini ključeva potrebnih za zadovoljavajuću sigurnost. Pri tome su u obzir uzeli više varijabilnih parametara, poput onoga da javno objavljeni rezultati u razbijanju pojedinih kriptosustava nisu nužno i najbolji, tj. da je moguće da postoje i bolji neobjavljeni rezultati. Preporučene duljine ključa u bitovima za simetrične kriptosustave (DES, AES), kriptosustave zasnovane na faktorizaciji ili diskretnom logaritmu u konačnom polju (RSA, ElGamal), te one zasnovane na eliptičkim krivuljama, prikazane su u sljedećoj tablici. Također je dana i procjena kompjuterskog vremena potrebnog za razbijanje šifrata u MIPS-godinama. Ta

se mjerna jedinica definira kao količina računanja na računalu koje je sposobno provesti milijun instrukcija u sekundi, u periodu od godinu dana.

Godina	DES duljina ključa	RSA duljina ključa	ECC duljina ključa	MIPS godina
1990	63	622	117	$3.51 \cdot 10^7$
2000	70	952	132	$7.13 \cdot 10^9$
2010	78	1369	146	$1.45 \cdot 10^{12}$
2020	86	1881	161	$2.94 \cdot 10^{14}$
2030	93	2493	176	$5.98 \cdot 10^{16}$
2040	101	3214	191	$1.22 \cdot 10^{19}$

Može se zaključiti kako kriptosustavi zasnovani na eliptičkim krivuljama trenutno imaju oko 7 puta manju duljinu ključeva, a da pritom pružaju istu sigurnost kao RSA kriptosustav. Isto tako, predviđa se još povoljniji omjer za ECC u budućnosti, kao i smanjenje razmjera u duljini ključeva sa simetričnim kriptosustavima. Ova predviđanja, doduše, nisu uzela u obzir moguću konstrukciju kvantnih računala, čiji najpoznatiji algoritmi, npr. onaj Shorov, brzim računanjem perioda periodičnih funkcija, daju polinomijalne kvantne algoritme za probleme faktorizacije i diskretnog algoritma. Dakle, efektivnom konstrukcijom dovoljno snažnih kvantnih računala, kriptosustavi javnog ključa zasnovani na faktorizaciji (RSA, Rabin) i problemu diskretnog logaritma (ElGamal, ECC), postali bi neupotrebljivi. Takva pitanja tzv. post-kvantne kriptografije, predmet su intenzivnih istraživanja.

Usprkos brojnim nabrojanim prednostima eliptičnih krivulja, one još uvijek nisu dovoljno implementirane u praksi zbog velikog broja prijavljenih patenata nad njima, kao i nedovoljnog istraživanja njihovih mogućnosti i primjena. No, svakako se ECC kriptosustavi smatraju za budućnost kriptografije, a s povećanjem interesa, raste i njihova uloga u rješavanju važnih matematičkih problema, dokazivanja prostosti, faktorizacije ili pak Velikog Fermatovog teorema.

Bibliografija

[1] I. F. Blake, G. Seroussi, N. P. Smart, *Elliptic Curves in Cryptography*, Cambridge University Press, 1999.

[2] W. Diffie, M. E. Hellman, *New directions in cryptography*, IEEE Trans. Information Theory, IT-22(6):644–654, 1976.

[3] A. Dujella, M. Maretić, *Kriptografija*, Element, Zagreb, 2008.

[4] M. Erickson, A. Vazzana, *Introduction to Number Theory*, Chapman & Hall/CRC,Boca Raton, 2008.

[5] J. Hoffstein, J. Pipher, J. H. Silverman, *An Introduction to Mathematical Cryptography*, Springer Publishing Company, New York, 2008.

[6] A. J. Menezes, P. C. van Oorschot, S. A. Vanstone, *Handbook of applied cryptography*, CRC Press, Boca Raton, FL, 1997.

[7] R. A. Mollin, *Advanced Number Theory with Applications*, Chapman & Hall/CRC, Boca Raton, 2010.

[8] B. Ponnen, *Average rank of elliptic curves*, dostupno na: `http://www-math.mit.edu/~poonen/papers/Exp1049.pdf` (svibanj, 2015.)

[9] R. Schoof, *Counting points on elliptic curves over finite fields*, J. Theorie des Nombres, Bordeaux, 7:219–254, 1995.

[10] J. H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, New York, 1986.

[11] D. R. Stinson, *Cryptography: Theory and Practice, Third Edition*, Chapman & Hall/CRC, Boca Raton, 2006.

[12] A, Tafro, *Kongruencije*, 2003. dostupno na: `hrcak.srce.hr/file/3247` (lipanj, 2016.)

[13] W. Trappe, L. C. Washington, *Introduction to Cryptography with Coding Theory, Second Edition*, Prentice Hall, Upper Saddle River, NJ, 2006.

[14] L. C. Washington, *Elliptic Curves: Number Theory and Cryptography*, Chapman & Hall/CRC, Boca Raton, 2008.

Sažetak

Eliptičke krivulje već se dugi niz godina intenzivno proučavaju s teorijskog stajališta, u sklopu algebarske geometrije. Međutim, osobito su razvojem računala doživjele svoj procvat te danas zauzimaju posebno istaknuto mjesto u teoriji brojeva i srodnom području, kriptografiji. Naime, tada su se razvile tehnike koje koriste eliptičke krivulje u faktorizaciji i dokazivanju prostosti, a uočila se i težina problema diskretnog logaritma u grupi točaka eliptičkih krivulja, pa su pronašle svoju primjenu u kriptosustavima zasnovanima na tom problemu.

Kriptografija fascinira zbog bliskih veza koje stvara između teorije i praksa. Zbog toga su današnje praktične primjene kriptografije sveprisutne i krucijalne komponente društva usmjerenog informacijama. Teorijski rad oplemenjuje i poboljšava praksu, a praktični izazovi inspiriraju studiju teorije. Kada se neki sustav „razbije", naše znanje o njemu se proširuje, pa sljedeći, unaprijeđeni sustav, popravlja prethodne pogreške. O važnosti eliptičkih krivilja govori i činjenica da ih je A. Wiles 1995. godine koristio u dokazu legendarnog Velikog Fermatovog teorema.

U radu je dan općeniti pregled eliptičkih krivulje te njihova svojstva nad poljem racionalnih brojeva, a zatim i nad konačnim poljima. Također je opisana kriptografija javnog ključa, s naglaskom na problem diskretnog logaritma, običnog i onog za eliptičke krivulje.

Ono što kriptosustave eliptičkih krivulja čini zanimljivima je to, da se danas, problem diskretnog logaritma za eliptičke krivulje čini „težim" u usporedbi s drugim sličnim problemima koji se koriste u kriptografiji. To znači da trebamo ključeve s manje bitova kako bi se postigla ista razinu sigurnosti kao kod drugih kriptosustava. Objašnjen je i Diffie-Hellmanov protokol za razmjenu ključeva te precizno opisani neki kriptosustavi javnog ključa, osobito oni koji koriste eliptičke krivulje.

Summary

Elliptic curves have been intensively studied in theory of algebraic geometry for many years. However, by development of computers they had a big breakthrough and have been playing an increasingly important role both in number theory and in related fields such as cryptography. At that time, elliptic curve techniques for factorization and primality testing were developed and also hardness of the elliptic curve discrete logarithm problem was discovered, which led to its application in algorithms based on that problem.

Cryptography is fascinating because of the close ties it forges between theory and practice. Because of that, today's practical applications of cryptography are pervasive and crucial components of our information-based society. The theoretical work refines and improves the practice, while the practice challenges and inspires the theoretical study. When some system is „broken", our knowledge expands and next, upgraded system repairs the previous defect. The importance of elliptic curves is best shown in 1995, when they figured prominently in the proof of Fermat's Last Theorem by A. Wiles.

This thesis provides a general overview of elliptic curves and their properties over the field of rational numbers and also over finite fields. Public key cryptography is also described, focusing on both the discrete logarithm problem and the elliptic curve discrete logarithm problem.

What makes ECC interesting is that, as of today, the discrete logarithm problem for elliptic curves seems to be „harder" if compared to other similar problems used in cryptography. This implies that we need keys with fewer bits in order to achieve the same level of security as with other cryptosystems. Furthermore, we explaine Diffie-Hellman key exchange protocol and finally study some public key cryptosystems, especially ones using elliptic curves.

Životopis

Rođen sam 07. ožujka 1991. godine u Mostaru. Osnovnu školu pohađao sam u Staševici, malom mjestu pokraj Ploča. U Pločama sam 2009. godine završio Opću gimnaziju, kao učenik generacije. Tijekom svog osnovnoškolskog i srednjoškolskog obrazovanja bio sam na raznim natjecanjima na općinskoj i županijskoj razini iz geografije, fizike i matematike te sam trenirao stolni tenis. Godine 2009. upisao sam nastavnički smjer Matematika i fizika na Prirodoslovno - matematičkom fakultetu u Zagrebu, da bih se 2009. godine prebacio na nastavnički smjer Matematika. Godine 2012. završavam preddiplomski studij i stječem akademski naziv sveučilišnog prvostupnika edukacije matematike. Te godine upisujem i diplomski studij Matematika; smjer nastavnički.