

Sveučilište u Zagrebu
PMF - Matematički odjel

Marcel Maretić

ELIPTIČKE KRIVULJE U KRIPTOGRAFIJI

Diplomski rad

Zagreb, svibanj 2002.

Sveučilište u Zagrebu
PMF - Matematički odjel

Marcel Maretić

ELIPTIČKE KRIVULJE U KRIPTOGRAFIJI

Diplomski rad

Voditelj rada:
prof. dr. sc. Andrej Dujella

Zagreb, svibanj 2002.

Sadržaj

Predgovor	1
1 Uvod	3
1.1 Kriptografija javnog ključa	3
1.2 Eliptičke krivulje u kriptografiji	4
2 Eliptičke krivulje nad konačnim poljima	7
2.1 Aritmetika u konačnim poljima	7
2.2 Weierstrassova jednačba	10
2.3 Grupovni zakon	12
2.4 Klase krivulja nad konačnim poljima karakteristike 2	14
2.5 Izogenije	16
2.6 Polinomi dijeljenja	18
2.7 Hasseov teorem	19
3 Brojanje točaka na eliptičkoj krivulji	21
3.1 Schoofov algoritam	21
3.2 Primjer	25
3.3 Složenost Schoofovog algoritma	29
Dodatak	31
Literatura	33
Indeks	35

Predgovor

Predmet proučavanja ovog diplomskog rada su eliptičke krivulje nad konačnim poljima i njihova primjena u kriptografiji. Od interesa su eliptičke krivulje nad velikim prostim poljima i krivulje nad konačnim binarnim poljima. Prednost u ovom radu zbog jednostavne implementacije u računalu dobila su binarna polja.

Kriptografija je motiv koji međusobno povezuje cjeline rada. Pristup je konstruktivan i zaokružuje znanje potrebno za dizajn kriptosustava baziranog na eliptičkoj krivulji. Rezultati koji nisu vezani za kriptografiju, kao i dokazi nekih korištenih tvrdnji koji preduboko ulaze u okvire algebarske geometrije ili teorije brojeva su izostavljeni. Za izostavljene dokaze su uglavnom dane reference na literaturu.

Prvo poglavlje sažeto iznosi principe kriptografije javnog ključa, konkretnije kriptosustava s javnim ključem koji se baziraju na teškim matematičkim problemima i koji se mogu realizirati na eliptičkim krivuljama. Objašnjene su prednosti i mane takvih sustava.

U drugom poglavlju najprije se iznosi nekoliko jednostavnih operativnih rezultata iz teorije konačnih polja potrebnih za razumijevanje njihove aritmetike. Opisani su različiti načini implementacija konačnih polja u računalu. Zatim su prikazane eliptičke krivulje nad konačnim poljima, te su pokazani neki rezultati o klasama. Poglavlje završava Hasseovim teoremom koji govori o aproksimaciji broja točaka na krivulji. Umjesto dokaza, Hasseov rezultat ilustriran je heuristikom i zajedno s polinomima dijeljenja i Frobeniusovim endomorfizmom čini osnovu za treće poglavlje.

U trećem poglavlju govori se o algoritmima brojenja točaka na krivulji. Broj točaka je kritična stvar u odabiru krivulje, jer otkriva strukturu grupe, što je garancija sigurnosti kriptosustava. Traže se krivulje čije grupe racionalnih točaka sadrže velike cikličke grupe. Detaljno je obrađen Schoofov algoritam, pokazana njegova složenost i prezentiran konkretan primjer sa svim koracima algoritma. Na kraju, u dodatku, je objašnjen primjer eliptičke krivulje iz FIPS186-2 standarda.

Zahvaljujem profesoru Marku Tadiću na izboru teme, te profesoru Andreju Dujelli na pomoći pri izradi ovog rada, strpljenju i savjetima.

Uvod

1.1 Kriptografija javnog ključa

Kriptografija je pojam, koji u širem smislu, obuhvaća probleme i tehnike koje koristimo za čuvanje ili prenošenje informacija.

Kriptografija javnog ključa počiva na ideji jednosmjerne funkcije. Neformalno, jednosmjerna funkcija je funkcija koja se vrlo lako (brzo, efikasno) izračunava, no jako se teško (npr. u eksponencijalnom vremenu) invertira. Nama je neformalni opis dovoljan.

Konačne grupe mogu biti izvor jednosmjernih funkcija. Neka je G konačna Abelova grupa, koju zapisujemo multiplikativno. Zanimaju nas grupe G u kojima se potenciranje fiksnog elementa ponaša kao jednosmjerna funkcija. Inverz potenciranja fiksnog elementa u konačnoj grupi zovemo diskretni logaritam. Konkretno, neka je $g \in G$ generator velike podgrupe od G . **Problem diskretnog logaritma** (skr. DLP) je za zadane $g, h \in G$ odrediti najmanji prirodni broj x tako da vrijedi

$$h = g^x.$$

Trenutno ne postoji efikasan algoritam za računanje diskretnog logaritma, osim u specijalnim slučajevima. Nekoliko kriptosustava s javnim ključem bazira se na tome. Važno je da G sadrži veliku podgrupu prostog reda.

Primjer 1 (ElGamalov kriptosustav). Alice želi poslati Bobu poruku. Pretpostavimo da je poruka m kodirana kao element grupe G . Bob ima javni ključ (g, h) , gdje je $h = g^x$. $x \in \mathbb{N}$ je Bobov privatni ključ. Shema se odvija u tri koraka:

1. Alice generira slučajni prirodni broj $k \in \{1, \dots, \#G - 1\}$ i izračuna $a = g^k$, $b = h^k m$.
2. Alice šalje (a, b) (šifrirani m) Bobu.

$$\text{Alice} \xrightarrow{(a,b)} \text{Bob}$$

3. Bob može izračunati m

$$ba^{-x} = h^k m g^{-kx} = g^{xk - xk} m = m.$$

Kad bi treća osoba znala riješiti DLP, mogla bi iz g i h izračunati x i saznati sadržaj poruke.

Primjer 2. *Digital Signature Algorithm* ili kratko DSA je verzija ElGamalove sheme potpisa. Potpis u kriptografiji je shema kojom se potvrđuje identitet pošiljatelja poruke. Npr., Alice uz poruku koju pošalje Bobu može poslati i digitalni potpis, kojim će Bob moći provjeriti je li mu poruku zaista poslala Alice. Npr., u prethodnom primjeru treća osoba može poslati Bobu poruku i predstaviti se kao Alice.

Pretpostavimo sad da Bob želi Alice potpisati poruku $m \in \mathbb{Z}/(\#G)\mathbb{Z}$. Javni ključ od Boba je (g, h) kao i u prethodnom primjeru, a privatni je x . Alice i Bob koriste istu bijekciju $f : G \rightarrow \mathbb{Z}/(\#G)\mathbb{Z}$.

1. Bob generira slučajni $k \in \{1, \dots, \#G - 1\}$ i izračuna

$$a = g^k.$$

2. Bob računa rješenje b kongruencije

$$m \equiv -xf(a) + kb \pmod{\#G}.$$

3. Bob šalje Alice potpis (a, b) i poruku m .

$$\text{Alice} \xleftarrow{(a,b),m} \text{Bob}$$

4. Alice računa

$$u = mb^{-1} \pmod{\#G}, \quad v = f(a)b^{-1} \pmod{\#G}.$$

5. Alice računa

$$w = g^u h^v$$

i provjerava da je

$$\begin{aligned} w &= w = g^u h^v = g^{mb^{-1}} g^{vx} = g^{mb^{-1} + xf(a)b^{-1}} \\ &= g^{(m+xf(a))b^{-1}} = g^{kbb^{-1}} = g^k \\ &= a. \end{aligned}$$

Vjeruje se (nije dokazano) da je razbiti bilo koju od navedenih shema ekvivalentno rješavanju DLP-a. Rješavanje DLP-a je u svakom slučaju dovoljno za razbijanje navedenih shema.

DSA je posebno zanimljiv jer se verzija algoritma prilagođena eliptičkim krivuljima, tzv. ECDSA, već nalazi u raznim standardima.

1.2 Eliptičke krivulje u kriptografiji

Točke na eliptičkoj krivulji nad konačnim poljem \mathbb{F}_q čine Abelovu grupu. Zbrajanje u toj grupi svodi se na nekoliko aritmetičkih operacija u polju \mathbb{F}_q , te se lako implementira. DLP u eliptičkoj krivulji (pišemo ECDLP) je vrlo težak, čini se bitno teži nego DLP u polju F_q . Svjesni ovoga, Neal Koblitz i Victor Miller su nezavisno 1985. godine predložili upotrebu eliptičkih krivulja u kriptosustavima s javnim ključem.

Dosad navedene sheme čija se sigurnost bazira na DLP-u mogu se prilagoditi tako da koriste grupu točaka na eliptičkoj krivulji. Pošto je ECDLP teži od DLP-a, traženu sigurnost dobivamo sa ključem manje duljine nego kod standardnih shema. Najbolji općeniti algoritmi za rješavanje ECDLP-a u krivuljama nad konačnim poljima sa q elemenata su složenosti $O(2^{n/2})$, gdje je $n = \lceil \ln q \rceil$. Običan DLP u \mathbb{F}_p^* je složenosti $L_p(1/3, c_0)$, gdje je sa L_p označena funkcija

$$L_p(v, c) = \exp(c(\ln p)^v (\ln \ln p)^{1-v}),$$

a $c_0 \approx 1.92$. $L_p(c, v)$ je polinomijalna u $(\ln p)$ kad je $v = 0$, odnosno eksponencijalna kad je $v = 1$. Kad je $0 < v < 1$ kažemo da je L_p **subekspencijalna**. Dakle, DLP je subekspencijalne složenosti. Označimo sa $N = \lceil \ln p \rceil$. Izjednačavanjem složenosti uz zanemarivanje konstantnih faktora dobiva se aproksimacija

$$n \approx 4.91 \cdot N^{1/3} (\ln(N \ln 2))^{2/3}.$$

Za približno istu sigurnost, duljina ključa u sustavima nad eliptičkim krivuljama raste malo brže od trećeg korijena duljine ključa tradicionalnog DLP sustava.

Najbolji algoritmi za faktorizaciju imaju sličnu složenost kao algoritmi za rješavanje DLP-a. Npr. vjeruje se da je RSA (najpopularniji kriptosustav s javnim ključem, bazira se na problemu faktorizacije) s 1024-bitnim ključem jednako siguran kao kriptosustav sa 128-bitnim ključem baziran na ECDLP-u. Tako eliptičke krivulje postaju interesantna opcija za primjenu gdje je memorija važan kriterij u dizajnu sustava (npr. kod smart kartica).

Postoje sustavi koji se zasnivaju na eliptičkim krivuljama nad $\mathbb{Z}/n\mathbb{Z}$, gdje je n produkt dva prosta broja, za koje je pokazano da njihovo razbijanje povlači faktorizaciju od n . Postoje slični sustavi koji su svojevrsni analogoni RSA algoritma, no oni zbog inferiornih performansi nemaju praktičnu primjenu, već ih se proučava isključivo radi teorije.

Eliptičke krivulje nad konačnim poljima

Najprije bih dao kratak uvod u aritmetiku nad konačnim poljima, uz posebnu pažnju na polja \mathbb{F}_{2^m} karakteristike 2. Konačna polja karakteristike p označavati ćemo sa \mathbb{F}_q , gdje je $q = p^n$ potencija prostog broja p . Algebarsko zatvorenje od \mathbb{F}_q ćemo označavati sa $\overline{\mathbb{F}_q}$.

2.1 Aritmetika u konačnim poljima

Za implementaciju najprivlačnija su konačna polja \mathbb{F}_{2^n} karakteristike 2 zbog jednostavne aritmetike bez prijenosa (*carry-free*) i zbog izbora različitih načina reprezentacije elemenata u polju. Ovisno o mogućnostima (*hardware* ili *software*) možemo birati između normalnih i polinomijalnih baza, ili pak njihove kombinacije preko baza potpolja.

Polje \mathbb{F}_{2^n} je vektorski prostor dimenzije n nad \mathbb{F}_2 . Elemente polja \mathbb{F}_{2^n} prikazujemo kao binarne vektore duljine n prikazane u nekoj bazi $(\alpha_0, \dots, \alpha_{n-1})$. Zbrajanje elemenata implementira se kao “ekskluzivni *ili*” (XOR) po komponentama i ne ovisi o bazi. S druge strane, izbor baze je bitan za množenje u polju.

Polinomijalna (ili **standardna**) **baza** je oblika $(1, \alpha, \dots, \alpha^{n-1})$, gdje je α korijen ireducibilnog polinoma f stupnja n nad \mathbb{F}_2 . Polje \mathbb{F}_{2^n} realizira se kao $\mathbb{F}_2[x]/(f(x))$ s aritmetikom polinoma stupnja manjeg od n , modulo $f(x)$. Element (a_0, \dots, a_{n-1}) gledamo kao polinom $\sum_{i=0}^{n-1} a_i x^i$. Množenje elemenata u polju svodi se na množenje polinoma modulo ireducibilni $f(x)$. Izaberemo li ireducibilan $f(x)$ *male težine*, tj. polinom s malim brojem (označit ćemo sa W) ne-nul koeficijenata, modularna redukcija postaje vrlo efikasna ($O(Wn)$ operacija). Uočimo da su koeficijenti uz x^n i $x^0 = 1$ uvijek prisutni, te da polinom s parnim W ne može biti ireducibilan. Izbor za $f(x)$ se stoga svodi na trinome ($W = 3$) i pentanome ($W = 5$). Za polja dimenzije proširenja $n < 10000$ postoji ireducibilni pentanom, što je za potrebe kriptografije više nego dovoljno. Otvoreno je pitanje vrijedi li to za svaki $n \in \mathbb{N}$. Više o tome može se naći u [BSS99]. Trinomi i pentanomi za polja \mathbb{F}_{2^n} ($n < 1000$) mogu se naći u tablicama u literaturi.

Množenje polinoma nad \mathbb{F}_2 svodi se na množenje bez prijenosa. Koriste se modificirani algoritmi za cjelobrojno množenje. Zanimljivo je da u praksi (kriptografiji), za množenje polinoma, asimptotski superiorni algoritmi daju lošije rezultate, pošto brojevi od interesa nisu dovoljno veliki (do 500 bitova). Naime, kritična točka u kojoj brzi algoritam množenja prestiže naivni $O(n^2)$ algoritam nalazi se mnogo dalje od toga. Kada uzmemo u obzir da računalo barata s riječima od 32 bita, vidimo da brojevi od interesa zauzimaju desetak riječi. Zato je u većini slučajeva Karatsubin rekurzivni “podijeli pa vladaj” algoritam dobar izbor. Složenost je $O(n^{\log_2 3})$, gdje je n broj riječi, a množenje riječi smatramo osnovnom operacijom. Na današnjim računalima (npr. Intel x86 arhitektura) je u procesoru implementirana instrukcija koja vraća umnožak dvije riječi. Postojanje slične instrukcije koja bi vraćala polinomski umnožak dvije riječi moglo bi nekoliko puta ubrzati kriptosustav.

Kvadriranje polinoma nad \mathbb{F}_2 vrlo je jednostavno - između susjednih bitova umetnemo nule, pa zatim reduciramo. To je posljedica činjenice da za $a, b \in \mathbb{F}_2$ vrijedi $(a + b)^2 = a^2 + b^2$, pa kvadrat polinoma ne sadrži monome neparnih potencija, tj. na neparnim mjestima odgovarajućeg binarnog vektora stoje nule. Složenost kvadriranja (zajedno s modularnom redukcijom) je $O(n)$.

Za računanje inverza u polju koristimo binarni prošireni Euklidov algoritam za polinome. Postoje asimptotski bolje metode, no one daju dobre rezultate tek za velike n -ove. Invertiranje je složenije od množenja, ali budući da direktno ovisi o množenju, množenje je operacija o kojoj će ovisiti efikasnost aritmetike. Prosječno množenje točke na krivulji, a to je u kriptografiji glavna operacija, u pravilu troši preko 90% vremena na množenje polinoma nad konačnim poljem, te je brzina izvođenja najviše određena kvalitetom implementacije množenja polinoma.

Normalna baza polja \mathbb{F}_{2^n} nad \mathbb{F}_2 ima oblik $(\alpha, \alpha^2, \dots, \alpha^{2^{n-1}})$ za neki $\alpha \in \mathbb{F}_{2^n}$. Baza ovog oblika postoji za svaki $n \in \mathbb{N}$. Koristi se u hardware-skim implementacijama. Operacija kvadriranja svodi se na cikličku rotaciju koeficijenata. Efikasno množenje dizajnira se preko bit-serijskih množitelja. Hardware-ska složenost mjeri se brojem jedinica C_α u kvadratnoj $n \times n$ binarnoj matrici $T = (T_{ij})$ definiranoj tako da je

$$\alpha^{1+2^i} = \sum_{j=0}^{n-1} T_{ij} \alpha^{2^j}, \quad 0 \leq i \leq n-1,$$

tj. takvoj da je i -ti redak matrice prikaz od α^{1+2^i} u bazi. Iz ove matrice možemo jednostavno dobiti međusobne umnoške svih elemenata baze. Budući da kvadrirati znamo, pretpostavimo da su α^{2^i} i α^{2^j} različiti elementi baze, $0 \leq i < j \leq n-1$, te $j = i + k$, $k > 0$. Tada je

$$\alpha^{2^i} \cdot \alpha^{2^{i+k}} = \alpha^{2^i} \cdot \alpha^{2^i \cdot 2^k} = \alpha^{2^i} \cdot (\alpha^{2^i})^{2^k} = (\alpha^{2^i})^{1+2^k} = (\alpha^{1+2^k})^{2^i}.$$

Tj., umnožak α^{2^i} i α^{2^j} , uz $i < j$, je $(j - i)$ -i redak rotiran i puta. C_α je odozgo trivijalno ograničen sa n^2 . Odozdo je ograničen sa $2n - 1$. Kad je $C_\alpha = 2n - 1$ kažemo da α generira **optimalnu normalnu bazu**, kratko ONB. Za F_{q^n} postoji ONB (i jedinstvena je) ako i samo ako vrijedi jedan od uvjeta

- (i) $n + 1$ je prost i 2 je primitivan u \mathbb{F}_{n+1} (generira multiplikativnu grupu)
- (ii) $2n + 1$ je prost i vrijedi ili da je 2 primitivan u \mathbb{F}_{2n+1} ili da je $2n + 1 \equiv 3 \pmod{4}$ i multiplikativni red od 2 u \mathbb{F}_{2n+1} je n .

U pravilu se bit-serijski množitelji ne mogu iskoristiti za implementacije u software-u.

Baze sa potpoljima mogu se koristiti kod polja dimenzije $n = n_1 n_2$, gdje je n_2 dovoljno malen da se operacije u polju $\mathbb{F}_{2^{n_2}}$ mogu efikasno izvesti preko *look-up* tabela. Članak [Sma01] iz 2001. govori da su eliptičke krivulje nad poljima sa složenim bazama manje sigurne, pa o njima nećemo više govoriti.

Rješavanje kvadratne jednadžbe u \mathbb{F}_{2^n}

Neka je $F = \mathbb{F}_{q^m}$ konačno proširenje polja $K = \mathbb{F}_q$, koje možemo promatrati kao m -dimenzionalni vektorski prostor nad F , tj. ako je $(\alpha_1, \dots, \alpha_m)$ baza, svaki $\alpha \in F$ možemo jedinstveno prikazati kao

$$\alpha = c_1 \alpha_1 + \dots + c_m \alpha_m, \quad c_i \in K, \quad 1 \leq i \leq m.$$

Definicija 2.1. Neka je $\alpha \in F = \mathbb{F}_{q^m}$ i $K = \mathbb{F}_q$. **Linearni trag** $\text{Tr}_{F/K}(\alpha)$ od α definiramo sa

$$\text{Tr}_{F/K}(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{m-1}}.$$

Ako je K prosto potpolje od F , tada $\text{Tr}_{F/K}(\alpha)$ zovemo **apsolutni trag** od α i jednostavno označavamo sa $\text{Tr}_F(\alpha)$.

Neka je $\alpha \in \mathbb{F}_{q^m}$. Elemente $\alpha, \alpha^q, \dots, \alpha^{q^{m-1}}$ zovemo **konjugati** od α obzirom na polje \mathbb{F}_q . Drugim riječima, linearni trag od $\alpha \in F$ je zbroj njegovih konjugata obzirom na polje K . Trag možemo definirati na sasvim drugi način. Neka je $f \in K[x]$ minimalni polinom od $\alpha \in F$ stupnja d koji dijeli m . Definiramo **karakteristični polinom** $g(x) = f(x)^{m/d}$ od α nad K . Svi korijeni od f su $\alpha, \alpha^q, \dots, \alpha^{q^{d-1}}$. Svi korijeni od g su upravo konjugati od α obzirom na K . Slijedi da je

$$\begin{aligned} g(x) &= x^m + a_{m-1}x^{m-1} + \cdots + a_0, \\ &= (x - \alpha)(x - \alpha^q) + \cdots + (x - \alpha^{q^{m-1}}). \end{aligned}$$

Izjednačimo koeficijente i dobijemo da je $\text{Tr}_{F/K}(\alpha) = -a_{m-1}$. Odavde slijedi da je $\text{Tr}_{F/K}(\alpha) \in K$, za svaki $\alpha \in F$. Prisjetimo se da ako je $p = \text{char } F$, za $\alpha, \beta \in F$ vrijedi

$$(\alpha + \beta)^{p^i} = \alpha^{p^i} + \beta^{p^i}, \quad \forall i \in \mathbb{N},$$

te da još za $c \in K$ vrijedi da je $c^q = c$. Odavde slijedi da je linearni trag $\text{Tr}_{F/K}$ linearan operator sa F u K . Vrijedi još:

Propozicija 2.2. Neka su $K = \mathbb{F}_q$, $F = \mathbb{F}_{q^m}$. Linearni trag $\text{Tr}_{F/K}$ zadovoljava:

- (i) $\text{Tr}_{F/K}$ je surjektivan;
- (ii) $\text{Tr}_{F/K}(a) = ma$, za sve $a \in K$;
- (iii) $\text{Tr}_{F/K}(\alpha^q) = \text{Tr}_{F/K}(\alpha)$ za sve $\alpha \in F$.

Dokaz. (ii) i (iii) slijede iz prethodnih razmatranja. Da bismo dokazali surjektivnost, zbog linearnosti je dovoljno pokazati da postoji $\alpha \in F$ takav da $\text{Tr}_{F/K}(\alpha) \neq 0$. $\text{Tr}_{F/K}(\alpha) = 0$ ako i samo ako je α korijen polinoma $x^{q^{m-1}} + \cdots + x$. Pošto elementa u polju ima q^m , a nultočaka najviše q^{m-1} , tvrdnja slijedi. \square

Kad se radi sa proširenjem \mathbb{F}_q nad \mathbb{F}_2 , katkad se piše $\text{Tr}_{q|2}$ umjesto $\text{Tr}_{\mathbb{F}_q/\mathbb{F}_2}$. Primijetimo da je $\text{Tr}_{q|2}(1) = 1$ ako je stupanj proširenja $n = [\mathbb{F}_q : \mathbb{F}_2]$ neparan. Budući da je $\text{Tr}_{F/K}$ linearan operator, dovoljno je izračunati vrijednosti na bazi, iz kojih se efikasno može izračunati trag proizvoljnog elementa.

Jednadžbu $x^2 + \beta = 0$ se rješava trivijalno, $x_0 = \beta^{2^{n-1}}$. Ostale jednadžbe svodimo na tzv. **kanonski oblik**:

$$x^2 + x + \beta = 0, \quad \beta \in \mathbb{F}_q. \quad (2.1)$$

Propozicija 2.3. Kvadratna jednadžba (2.1) ima rješenja u \mathbb{F}_q ako i samo ako je $\text{Tr}_{q|2}(\beta) = 0$.

Dokaz. Uočimo najprije da ako je x_0 jedno rješenje, drugo je dano sa $x_0 + 1$. Nužnost slijedi iz prethodne propozicije:

$$\begin{aligned} 0 &= \text{Tr}_{q|2}(0) = \text{Tr}_{q|2}(x_0^2 + x_0 + \beta) = \text{Tr}_{q|2}(x_0^2 + x_0) + \text{Tr}_{q|2}(\beta) = \\ &= \text{Tr}_{q|2}(x_0) + \text{Tr}_{q|2}(x_0) + \text{Tr}_{q|2}(\beta) = \text{Tr}_{q|2}(\beta) \end{aligned}$$

Dovoljnost ćemo pokazati konstrukcijom rješenja. Postupak se razlikuje ovisno o parnosti od n . Ako je n neparan i $\text{Tr}_{q|2}(\beta) = 0$, rješenje je dano sa

$$x_0 = \sum_{j=0}^{(n-1)/2} \beta^{2^{2j}}.$$

Zaista,

$$x_0^2 + x_0 = \sum_{j=0}^{(n-1)/2} (\beta^{2^{2j+1}} + \beta^{2^{2j}}) = \beta + \dots + \beta^{2^n} = \text{Tr}_{q|2}(\beta) + \beta^{2^n} = 0 + \beta = \beta.$$

Postupak za n paran je nešto složeniji. Najprije odaberemo $\delta \in \mathbb{F}_q$ takav da je $\text{Tr}_{q|2}(\delta) = 1$. Zbog prethodne propozicije takav postoji. (Uoči da barem jedan vektor baze ima trag 1.) Rješenje je dano sa

$$x_0 = \sum_{i=0}^{n-2} \left(\sum_{j=i+1}^{n-1} \delta^{2^j} \right) \beta^{2^i}.$$

Uvrstimo:

$$\begin{aligned} x_0^2 + x_0 &= \sum_{i=1}^{n-1} \left(\sum_{j=i+1}^n \delta^{2^j} \right) \beta^{2^i} + \sum_{i=0}^{n-2} \left(\sum_{j=i+1}^{n-1} \delta^{2^j} \right) \beta^{2^i} \\ &= \delta(\beta^{2^{n-1}} + \beta^{2^{n-2}} + \dots + \beta^2) + (\delta^{2^{n-1}} + \delta^{2^{n-2}} + \dots + \delta^2)\beta \\ &= \delta(\text{Tr}_{q|2}(\beta) + \beta) + \underbrace{(\text{Tr}_{q|2}(\delta) + \delta)}_{=1}\beta \\ &= \delta \text{Tr}_{q|2}(\beta) + \delta\beta + \beta + \delta\beta \\ &= \delta \text{Tr}_{q|2}(\beta) + \beta. \end{aligned}$$

Slijedi da je $x_0^2 + x_0 = \beta$ ako i samo ako je $\text{Tr}_{q|2}(\beta) = 0$. □

2.2 Weierstrassova jednadžba

Neka je K savršeno polje. Projekтивni prostor $\mathbb{P}^2(K)$ je kvocijent skupa $\{(x, y, z) : (x, y, z) \neq (0, 0, 0)\}$ i relacije ekvivalencije \sim :

$$(x_1, y_1, z_1) \sim (x_2, y_2, z_2) \iff \exists \lambda \in K^* \text{ tako da } x_1 = \lambda x_2, y_1 = \lambda y_2, z_1 = \lambda z_2.$$

Klasu ekvivalencije točke (x, y, z) označavamo sa $[x, y, z]$. Točke $[x, y, z] \in \mathbb{P}^2(K)$ za koje je $Z = 0$ zovemo **točke u beskonačnosti**.

Općenito se definira da su eliptičke krivulje projekтивne krivulje (nad K) genusa 1 s izdvojenom točkom. Razumijevanje ove definicije traži određeno znanje algebarske geometrije, što se u ovom radu ne zahtijeva. Nama je bitan rezultat da se svaka eliptička krivulja može zapisati (realizirati) kao rješenje kubne jednadžbe u $\mathbb{P}^2(K)$

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3, \quad (2.2)$$

s točno jednom (baznom) točkom u beskonačnosti (točke na pravcu $Z = 0$) (v. [Sil86]). Uvrštavanjem $Z = 0$ dobivamo jedinstveno rješenje $[0, 1, 0]$. Označimo $\mathcal{O} = [0, 1, 0]$.

Jednadžba (2.2) zove se **Weierstrassova jednadžba** ili **normalna forma** eliptičke krivulje. Weierstrassovu jednadžbu kraće zapisujemo u nehomogenom obliku u afinoj ravnini K^2

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

uz uvjet da pamtimo točku $\mathcal{O} = [0, 1, 0]$. Ako su koeficijenti $a_1, \dots, a_6 \in K$, kažemo da je E definirana nad K , i pišemo E/K . Ako je $\text{char } K \neq 2$, supstitucijom $y \leftarrow \frac{1}{2}(y - a_1x - a_3)$ još pojednostavljujemo Weierstrassovu jednadžbu

$$E : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6,$$

gdje su

$$\begin{aligned} b_2 &= a_1^2 + 4a_2 \\ b_4 &= 2a_4 + a_1a_3 \\ b_6 &= a_3^2 + 4a_6. \end{aligned} \tag{2.3}$$

Također definiramo

$$\begin{aligned} b_8 &= a_1^2 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \\ c_4 &= b_2^2 - 24b_4 \\ c_6 &= -b_2^3 + 36b_2b_4 - 216b_6 \\ \Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \\ j &= c_4^3/\Delta. \end{aligned} \tag{2.4}$$

Ako je $\text{char } K \neq 2, 3$, supstitucijom $(x, y) \leftarrow (\frac{x-3b_2}{36}, \frac{y}{108})$ elimineramo x^2 član:

$$E : y^2 = x^3 - 27c_4x - 54c_6.$$

Δ zovemo **diskriminanta** Weierstrassove jednadžbe, j zovemo **j -invarijanta**.

Postavlja se pitanje do koje je mjere Weierstrassova jednadžba eliptičke krivulje E jedinstvena. Uz pretpostavku da pravac u beskonačnosti ($Z = 0$) u \mathbb{P}^2 siječe E samo u \mathcal{O} , jedina zamjena varijabli koja čuva Weierstrassov oblik jednadžbe i fiksira \mathcal{O} (vidi [Sil86], III.3.1) je

$$\begin{aligned} x &= u^2x' + r, \\ y &= u^3y' + u^2sx' + t, \end{aligned}$$

$u, r, s, t \in \overline{K}$, $u \neq 0$. Zamjena varijabli ovog oblika zove se **dopustiva zamjena varijabli**. Ova se transformacija lako invertira:

$$\begin{aligned} x' &= u^{-2}x - r, \\ y' &= u^{-3}y - u^{-3}sx' - (u^{-1}rs + u^{-3}t). \end{aligned}$$

Inverzna transformacija je također dopustiva zamjena varijabli ($u' = u^{-1}$, $r' = -r$, $s' = -u^{-1}s$, $t' = -(u^{-1}rs + u^{-3}t)$).

Kažemo da su eliptičke krivulje E i E' **izomorfne** ako i samo ako postoji dopustiva zamjena varijabli koja jednadžbu krivulje E prevodi u jednadžbu krivulje E' . Pogledajmo eliptičke krivulje nad K :

$$E_1 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{2.5}$$

$$E_2 : y^2 + a'_1xy + a'_3y = x^3 + a'_2x^2 + a'_4x + a'_6. \tag{2.6}$$

Pretpostavimo da je krivulja E_1 izomorfna E_2 , tj. da postoji dopustiva zamjena varijabli sa u, r, s, t koja prevodi (2.5) u (2.6). Uvrštavanjem dobivamo sustav:

$$\begin{aligned} ua'_1 &= a_1 + 2s \\ u^2a'_2 &= a_2 - sa_1 + 3r - s^2 \\ u^3a'_3 &= a_3 + ra_1 + 2t \\ u^4a'_4 &= a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st \\ u^6a'_6 &= a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1 \end{aligned} \quad (2.7)$$

Vrijedi sljedeći teorem:

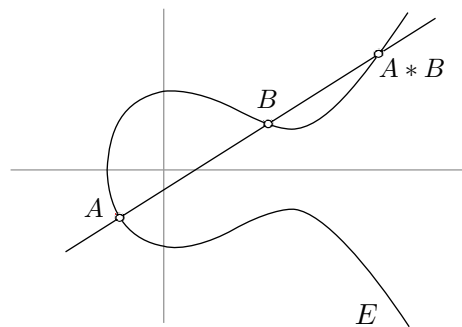
Teorem 2.4. *Eliptičke krivulje E_1/K i E_2/K zadane jednadžbama (2.5) i (2.6) su izomorfne ako i samo ako postoje $u \neq 0, r, s, t \in K$ koji zadovoljavaju sustav (2.7).*

Dopustiva zamjena varijabli ne mijenja j -invarijantu (odatle naziv). Za krivulje nad algebarski zatvorenim poljima vrijedi i obrat ([Sil86], III.1.4):

Propozicija 2.5. *Eliptičke krivulje E_1 i E_2 su izomorfne (nad \bar{K}) ako i samo ako imaju jednake j -invarijante.*

2.3 Grupovni zakon

Eliptičke krivulje pojavile su se u problemu traženja racionalnih rješenja ireducibilnih kubnih jednadžbi u dvije varijable nad \mathbb{Q} . Na kvadrikama (kružnica, elipsa, hiperbola) nove racionalne točke dobivamo metodom sekante. Pristup na kubikama je drugačiji, pošto pravac (općenito) siječe kubiku u tri točke. Metodom tetive (v. sl. 2.1) iz dvije racionalne točke A i B jednostavno dobivamo treću također racionalnu točku na krivulji koju označimo sa $A * B$. Ako je $A = B$, $A * A$ dobivamo tako da povučemo tangentu u točki A i gledamo sjecište sa krivuljom. Eliptičke krivulje su kubike za koje je operacija $*$ dobro definirana, tj. kubike koje pravac siječe u tri točke (brojano sa multiplicitetom).



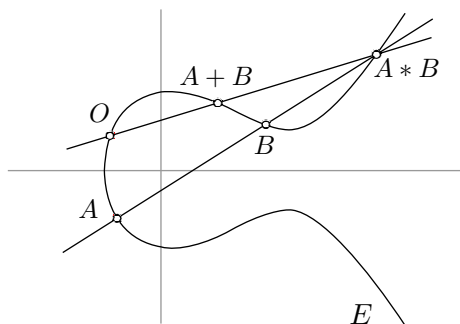
Slika 2.1.

Mordell¹ je 1922. dokazao da za svaku kubiku postoji konačan skup točaka iz kojeg se primjenom metodom tetive i tangente (konačno puta) mogu dobiti sve racionalne točke, ili drugim riječima, da je skup racionalnih točaka na E konačno generiran. Mordell nije uočio da ako fiksiramo točku na krivulji, nazovimo je O , te definiramo binarnu operaciju:

$$A + B = O * (A * B),$$

¹Louis Joel Mordell, 1888–1972, američki matematičar

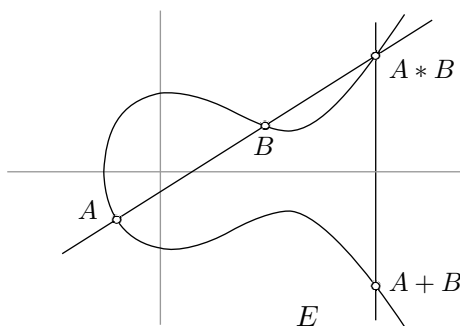
dobivamo asocijativnost. Skup točaka na krivulji E uz spretno odabir točke O postaje abelova grupa.



Slika 2.2.

Preciznije, dobar izbor točke O su točke infleksije na krivulji, tj. točke za koje vrijedi da svaki pravac kroz njih siječe krivulju u barem tri točke (broje se i multipliciteti). Tangentu u točki infleksije proglasimo pravcem u beskonačnosti, točka postaje točka u beskonačnosti i jednačba krivulje uz skaliranje varijabli prelazi u Weierstrassov oblik. Skup racionalnih točaka (označimo sa $E(\mathbb{Q})$) čini podgrupu grupe točaka na krivulji i u ovom kontekstu Mordellov teorem govori da je $E(\mathbb{Q})$ konačno generirana abelova grupa.

Eliptička krivulja zapisana Weierstrassovom jednačbom je abelova grupa čiji neutralni element (nula) je već spomenuta točka u beskonačnosti \mathcal{O} . U afinjoj ravnini pravac kroz \mathcal{O} je pravac paralelan s osi y (v. sl. 2.3). Koristeći algebarsku prirodu ove geometrijske



Slika 2.3.

definicije, grupovni zakon možemo proširiti na polja proizvoljne karakteristike.

Lema 2.6 (grupovni zakon). *Neka je E eliptička krivulja zadana Weierstrassovom jednačbom*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad (2.8)$$

i neka su $P_1 = (x_1, y_1)$ i $P_2 = (x_2, y_2)$ točke na E . Tada je

$$-P_1 = (x_1, -y_1 - a_1x - a_3).$$

Označimo $P_1 + P_2$ sa $P_3 = (x_3, y_3)$. Ako je $P_1 = -P_2$, stavimo da je $P_3 = \mathcal{O}$ (i gotovi smo).

Inače ($P_1 \neq -P_2$) računamo

$$\lambda, \mu = \begin{cases} \lambda = \frac{y_2 - y_1}{x_2 - x_1}, & \mu = \frac{y_1x_2 - y_2x_1}{x_2 - x_1}, & x_1 \neq x_2 \\ \lambda = \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y}{2y_1 + a_1x + a_3}, & \mu = \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}, & x_1 = x_2 \end{cases}$$

P_3 računamo iz formula:

$$\begin{aligned} x_3 &= \lambda^2 + a_1\lambda - a_2 - x_1 - x_2 \\ y_3 &= -(\lambda + a_1)x_3 - \mu - a_3. \end{aligned}$$

2.4 Klase krivulja nad konačnim poljima karakteristike 2

Neka je E/K eliptička krivulja definirana nad konačnim poljem K . Sa $E(K)$ ćemo označavati skup točaka iz $K \times K$ koje se nalaze na krivulji E . Očigledno je $E(K) \subseteq E(\overline{K})$. Ako je K konačno polje, $E(K)$ je konačan skup. Broj elemenata od $E(K)$ označavat ćemo sa $\#E(K)$. Uočite da je važno na koje se polje ovaj broj odnosi. Nas će u pravilu zanimati $\#E(\mathbb{F}_q)$ za krivulju definiranu kao E/\mathbb{F}_q .

Vezano uz $\#E(\mathbb{F}_q)$ definiramo **Frobeniusov trag** t kao cijeli broj za koji vrijedi

$$\#E(\mathbb{F}_q) = q + 1 - t.$$

U kriptografiji se izbjegavaju **anomalne** i **supersingularne** krivulje. Za krivulju $E(\mathbb{F}_q)$ kažemo da je anomalna ako je Frobeniusov trag $t = 1$, tj. $\#E(\mathbb{F}_q) = q$, odnosno da je supersingularna ako karakteristika $p|t$. Za supersingularne krivulje Menezes-Okamoto-Vanstone MOV napad (v. [BSS99]) na ECDLP je posebno efikasan. Može se pokazati da je krivulja nad poljem karakteristike p supersingularna ako i samo ako je $j(E) = 0$ (u karakteristikama 2, 3), odnosno $t = 0$ u (u karakteristikama $p \geq 5$).

Neka je $q = 2^n$. j -invarijanta krivulje u polju karakteristike 2 reducira se na $j(E) = a_1^{12}/\Delta$. Dakle, $j(E) = 0$ (supersingularna) ako i samo ako je $a_1 = 0$. Stoga pretpostavljamo da je $a_1 \neq 0$. Weierstrassovu jednadžbu možemo pojednostaviti (eliminirati x i y članove):

Propozicija 2.7. *Neka je E/\mathbb{F}_q eliptička krivulja zadana Weierstrassovom jednadžbom takva da $j(E) \neq 0$. Tada postoji dopustiva zamjena varijabli tako da je*

$$E: y^2 + xy = x^3 + a_2x^2 + a_6, \quad \Delta = a_6, j = 1/a_6. \quad (2.9)$$

Dokaz. Vrijedi $a_1 \neq 0$, pa supstitucijom $x = a_1^2x' + a_3/a_1$, $u = a_1^3 + (a_1^2a_4 + a_3^2)/a_1^3$ iz normalne forme dobivamo traženi oblik jednadžbe. \square

Jednadžbu oblika (2.9) zovemo **kratka Weierstrassova jednadžba**. Iz propozicije slijedi da sve non-supersingularne krivulje nad \mathbb{F}_q možemo zadati sa a_2 i $a_6 \in \mathbb{F}_q$. No, vrijedi i više:

Teorem 2.8. *Postoji $2(q-1)$ klasa izomorfizama nesupersingularnih eliptičkih krivulja nad \mathbb{F}_q , gdje je $q = 2^m$. Neka je $\gamma \in \mathbb{F}_q$ takav da je $\text{Tr}(\gamma) = 1$. Skup reprezentanata svih nesupersingularnih klasa je*

$$\{E: y^2 + xy = x^3 + a_2x^2 + a_6 \mid a_6 \in \mathbb{F}_q^*, a_2 \in \{0, \gamma\}\}.$$

Dokaz. Neka su E_1 i E_2 nesupersingularne krivulje nad \mathbb{F}_q :

$$\begin{aligned} E_1 : y^2 + xy &= x^3 + a_2x^2 + a_6 \\ E_2 : y^2 + xy &= x^3 + a'_2x^2 + a'_6. \end{aligned}$$

Pretpostavimo da su E_1 i E_2 izomorfne, tj. da postoji dopustiva zamjena varijabli u, r, s, t koja E_1 prevodi u E_2 . Uočimo da je

$$a'_1 = a_1 = 1, \quad a_3 = a'_3 = 0, \quad a_4 = a'_4 = 0 \quad (2.10)$$

Odavde i iz teorema 2.4 slijedi da je $u = 1, r = t = 0$, te

$$a_6 = a'_6, \quad a'_2 = a_2 + s + s^2.$$

Pošto je teorem 2.4 teorem ekvivalencije, vrijedi i obrat, tj. da su E_1 i E_2 izomorfne ako i samo ako $a_6 = a'_6$ te postoji $s \in \mathbb{F}_q$ takav da je $a'_2 = a_2 + s + s^2$. Drugi je uvjet ekvivalentan uvjetu da je $\text{Tr}_{q|2}(a'_2) = \text{Tr}_{q|2}(a_2)$ (vidi propoziciju 2.3).

Budući da $a_6 \in \mathbb{F}_q$ biramo na $(q-1)$, a a_2 na 2 načina, slijedi da je broj klasa $2(q-1)$. \square

Napomena 2.9. Za (čvrsti) $\gamma \in \mathbb{F}_q^*$ takav da je $\text{Tr}_{q|2}(\gamma) = 1$, sve klase krivulja koje nisu supersingularne $j(E) \neq 0$ reprezentirane su jednadžbom oblika

$$E_{a_2, a_6} : y^2 + xy = x^3 + a_2x^2 + a_6, \quad (2.11)$$

gdje je $a_2 \in \{0, \gamma\}$, a $a_6 \in \mathbb{F}_q^*$. U slučaju da je dimenzija polja $n = [\mathbb{F}_q : \mathbb{F}_2]$ neparan broj, vrijedi $\text{Tr}_{q|2}(1) = 1$, pa a_2 možemo birati iz skupa $\{0, 1\}$.

Lema 2.10. *Neka je E eliptička krivulja nad \mathbb{F}_q , $q = 2^n$, zadana jednadžbom (2.11). Vrijedi:*

$$\#E_{a_2, a_6}(\mathbb{F}_q) \equiv \begin{cases} 0 \pmod{4}, & \text{Tr}_{q|2}(a_2) = 0 \\ 2 \pmod{4}, & \text{Tr}_{q|2}(a_2) = 1. \end{cases}$$

Dokaz. Svaki element $a \in \mathbb{F}_q$ ima jedinstveni drugi korijen $\sqrt{a} = a^{q/2}$. Točka $(0, \sqrt{a_6})$ je jedinstvena točka reda 2 na krivulji. Pogledajmo točke (x, y) za koje je $x \neq 0$. Podijelimo (2.11) sa x^2 , stavimo $u \leftarrow y/x$ i dobijemo

$$u^2 + u = x + a_2 + \frac{a_6}{x^2}.$$

Ova je kvadratna jednadžba rješiva (v. prop. 2.1, rješenja su u_0 i $u_0 + 1$) ako i samo ako je

$$\text{Tr}_{q|2}\left(x + a_2 + \frac{a_6}{x^2}\right) = 0,$$

odnosno ako je

$$\begin{aligned} \text{Tr}_{q|2}(a_2) &= \text{Tr}_{q|2}(x) + \text{Tr}_{q|2}\left(\frac{a_6}{x^2}\right) = \text{Tr}_{q|2}(x^2) + \text{Tr}_{q|2}\left(\frac{a_6}{x^2}\right) = \\ \text{Tr}_{q|2}(a_2) &= \text{Tr}_{q|2}\left(x^2 + \frac{a_6}{x^2}\right). \end{aligned} \quad (*)$$

Ako x zadovoljava (*), onda to vrijedi i za $\sqrt{a_6}/x$. $x \neq \sqrt{a_6}/x$ ako je $x \neq \sqrt[4]{a_6}$, pa svaki $x \in \mathbb{F}_q^* \setminus \{\sqrt[4]{a_6}\}$ daje 4 točke. Za $x = \sqrt[4]{a_6}$ je $\text{Tr}_{q|2}\left(x^2 + \frac{a_6}{x^2}\right) = 0 = \text{Tr}_{q|2}(a_2)$, pa x daje dva rješenja ako i samo ako je $\text{Tr}_{q|2}(a_2) = 0$. Ubrojimo još točke $(0, \sqrt{a_6})$ i \mathcal{O} i lema je dokazana. \square

Za zadani a_6 krivulje E_{0,a_6} i E_{γ,a_6} su twistevi jedna drugoj, tj. izomorfne su nad algebarskim zatvorenjem od \mathbb{F}_q . Vrijedi

$$\#E_{0,a_6}(\mathbb{F}_q) + \#E_{\gamma,a_6}(\mathbb{F}_q) = 2q + 2. \quad (2.12)$$

Iz dokaza leme vidi se da svaki $x \in \mathbb{F}_q^*$ daje po dvije točke točno jednoj od krivulja E_{0,a_6} , E_{γ,a_6} , što daje $2q - 2$ točaka. Točke \mathcal{O} i $(0, \sqrt{a_6})$ nalaze se na obje krivulje (pa se broje dvaput), što ukupno daje $2q + 2$ točaka. Ova relacija ustvari govori da je dovoljno znati broj točaka jedne od ovih krivulja, pa tako za "cijenu jedne" dobivamo broj točaka dvije krivulje.

Napomena 2.11. E_{0,a_6} i E_{γ,a_6} nisu izomorfne nad \mathbb{F}_q , ali jesu nad \mathbb{F}_{q^2} . Iz propozicije 2.2 slijedi da je $\text{Tr}_{q^2}(a_2) = 2 \cdot a_2 = 0$ za $\forall a_2 \in \mathbb{F}_q$. Nadalje, iz teorema 2.8 zbog $\text{Tr}_{q^2}(a_2) = \text{Tr}_{q^2}(0)$ slijedi da su krivulje E_{0,a_6} i E_{γ,a_6} izomorfne nad \mathbb{F}_{q^2} .

Formule grupovnog zakona za krivulje nad poljem karakteristike 2, zadane kratkom Weierstrassovom jednadžbom, pojednostavljujemo (vidi lemu 2.6) te za $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2) \in E(\mathbb{F}_{2^n})$ računamo:

$$-P_1 = (x_1, x_1 + y_1),$$

$$\lambda, \mu = \begin{cases} \lambda = \frac{y_2 + y_1}{x_2 + x_1}, & \mu = \frac{y_1x_2 + y_2x_1}{x_2 + x_1}, & x_1 \neq x_2 \\ \lambda = \frac{x_1^2 + y_1}{x_1}, & \mu = x_1^2, & x_1 = x_2 \neq 0 \end{cases}$$

te za $P_3 = (x_3, y_3) = P_1 + P_2$, u slučaju da $P_1 \neq -P_2$

$$\begin{aligned} x_3 &= \lambda^2 + \lambda + a_2 + x_1 + x_2 \\ y_3 &= (\lambda + 1)x_3 + \mu \\ &= (x_1 + x_3)\lambda + x_3 + y_1. \end{aligned} \quad (2.13)$$

Uočimo da (nepokriveni) slučaj $x_1 = x_2 = 0$ ustvari znači da je $P_1 = P_2 = (0, \sqrt{a_6})$ (vidi dokaz leme 2.10), pa je $P_1 + P_2 = [2](P_1) = \mathcal{O}$.

2.5 Izogenije

Racionalna preslikavanja među eliptičkim krivuljama E_1, E_2 za koja $\mathcal{O}_{E_1} \mapsto \mathcal{O}_{E_2}$ zovemo **izogenije**. Pokazuje se da su izogenije homomorfizmi grupa pripadnih krivulja. Množenje točke sa $m \in \mathbb{N}$ je npr. izogenija na krivulji E u nju samu, koju označavamo sa $[m]$:

$$[m](P) = mP.$$

Prirodno proširimo na \mathbb{Z} :

$$[-m](P) = -mP, \quad [0](P) = \mathcal{O}, \quad m \in \mathbb{Z}.$$

Izogenije $E \rightarrow E$ sa zbrajanjem (po točkama) i kompozicijom (preslikavanja) čine prsten koji označavamo sa $\text{End}(E)$. Očigledno je \mathbb{Z} potprsten od $\text{End}(E)$. Kad je E krivulja nad poljem K karakteristike $\text{char } K = 0$, često su izogenije množenja sve izogenije, tj. $\text{End}(E) \cong \mathbb{Z}$. Ako $\text{End}(E) \not\cong \mathbb{Z}$ (tj. postoje izogenije koje nisu dobivene na ovaj način), kažemo da eliptička krivulja ima **kompleksno množenje**. Eliptičke krivulje nad konačnim poljima uvijek imaju kompleksno množenje.

Definicija 2.12. q -ti **Frobeniusov endomorfizam** φ , na eliptičkoj krivulji E/\mathbb{F}_q definiran je sa $\varphi : E(\overline{\mathbb{F}_q}) \rightarrow E(\overline{\mathbb{F}_q})$,

$$\begin{aligned} (x, y) &\mapsto (x^q, y^q) \\ \mathcal{O} &\mapsto \mathcal{O}. \end{aligned}$$

Frobeniusov endomorfizam φ je najjednostavniji primjer izogenije na $E(\mathbb{F}_q)$ koja nije dobivena množenjem cijelim brojem. Uočimo da je φ identiteta na $E(\mathbb{F}_q) \subseteq E(\overline{\mathbb{F}_q})$, baš kao i $[1]$ i $[N+1]$, gdje smo sa N označili broj točaka u $E(\mathbb{F}_q)$. Ipak, ove su izogenije različite na $E(\overline{\mathbb{F}_q})$. Na eliptičkoj krivulji E/\mathbb{F}_q , za $P \in E$ vrijedi da je $P \in E(\mathbb{F}_q)$ ako i samo ako je $\varphi(P) = P$.

Propozicija 2.13. Za svaku ne-konstantnu izogeniju $\phi : E_1 \rightarrow E_2$ postoji jedinstvena dualna izogenija

$$\widehat{\phi} : E_2 \rightarrow E_1,$$

tako da je $\widehat{\phi} \circ \phi = \phi \circ \widehat{\phi} = [n]$, $n \in \mathbb{Z}$, gdje je n stupanj izogenije ϕ .

Dokaz. Vidi [Sil86]. □

Stupanj izogenije je pojam koji ovdje neću definirati. Nama je dovoljno znati da je q -ti Frobeniusov endomorfizam φ izogenija stupnja q , tj. da prema prethodnoj propoziciji vrijedi

$$\varphi \circ \widehat{\varphi} = [q]. \quad (2.14)$$

Propozicija 2.14. Neka je φ q -ti Frobeniusov endomorfizam na eliptičkoj krivulji E/\mathbb{F}_q . Označimo sa $t = \#E(\mathbb{F}_q) - q - 1$ Frobeniusov trag, i sa $\widehat{\varphi}$ dualni Frobeniusov endomorfizam. Vrijedi:

$$\varphi + \widehat{\varphi} = [t]. \quad (2.15)$$

Dokaz. Vidi [Sil86]. □

Na (2.15) djelujemo sa $\widehat{\varphi}$ i dobijemo

$$\varphi^2 + \widehat{\varphi}\varphi - [t]\varphi = [0],$$

uvrstimo $\widehat{\varphi}\varphi = [q]$

$$\varphi^2 - [t]\varphi + [q] = [0] \quad (2.16)$$

tj. za $\forall P = (x, y) \in E(\overline{\mathbb{F}_q})$

$$(x^{q^2}, y^{q^2}) - [t](x^q, y^q) + [q](x, y) = \mathcal{O}.$$

Jednadžba (2.16) zove se **karakteristična jednadžba** (uoči Vietéove formule) Frobeniusovog endomorfizma φ u (2.14) i (2.15). Vrlo je bitna za Schoofov algoritam brojenja točaka budući da povezuje Frobeniusov trag t sa Frobeniusovim endomorfizmom φ , a problem određivanja traga je ekvivalentan određivanju broja točaka $\#E(\mathbb{F}_q)$ na krivulji E .

Napomena 2.15. Važno je da jednadžbu (2.16) zadovoljavaju sve točke krivulje, a ne samo \mathbb{F}_q -racionalne. Tako da bismo odredili Frobeniusov trag t možemo “izaći” iz $E(\mathbb{F}_q)$ i koristiti prikladno odabrane točke iz $E(\overline{\mathbb{F}_q})$. Upravo tako radi Schoofov algoritam, vidi pogl. 3.

2.6 Polinomi dijeljenja

Iz algebarske prirode grupovnog zakona slijedi da se koordinate u množenju točke sa m mogu prikazati kao racionalne funkcije u x i y

$$(x, y) \mapsto [m](x, y).$$

Lema 2.16. *Neka je E eliptička krivulja definirana nad poljem K i neka je $m \in \mathbb{N}$. Tada postoje polinomi $\psi_m, \theta_m, \omega_m \in K[x, y]$ tako da za točku $P = (x, y) \in E(\overline{K})$ za koju $[m](P) \neq \mathcal{O}$ vrijedi*

$$[m](P) = \left(\frac{\theta_m(x, y)}{\psi_m(x, y)^2}, \frac{\omega_m(x, y)}{\psi_m(x, y)^3} \right). \quad (2.17)$$

Polinom $\psi_m(x, y)$ zovemo m -ti **polinom dijeljenja** krivulje E . Nizove polinoma (θ_m) i (ω_m) možemo izraziti preko niza (ψ_m) . Za eliptičku krivulju zadanu Weierstrassovom jednadžbom (2.8) rekursivno definiramo niz (ψ_m) :

$$\begin{aligned} \psi_0 &= 0, \\ \psi_1 &= 1, \\ \psi_2 &= 2y + a_1x + a_3, \\ \psi_3 &= 3x^4 + b_2x^3 + 3b_6x + b_8, \\ \psi_4 &= (2x^6 + b_2x^5 + 5b_4x^4 + 10b_6x^3 + 10b_8x^3 + \\ &\quad + (b_2b_8 - b_4b_6)x + b_4b_8 - b_6^2) \psi_2, \\ &\vdots \\ \psi_{2m+1} &= \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3, \quad m \geq 2, \\ \psi_{2m} &= \frac{(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2) \psi_m}{\psi_2}, \quad m > 2, \end{aligned} \quad (2.18)$$

gdje su b_i konstante definirane iz Weierstrassove jednadžbe kao u (2.3) i (2.4). Brojnik u izrazu za ψ_{2m} je djeljiv sa ψ_m^2 , pa je ψ_{2m} polinom djeljiv sa ψ_m . Vrijednosti polinoma dijeljenja računamo samo u točkama na krivulji E , pa zato ψ_m možemo računati modulo E , tj. reducirati potencije od y veće od 1 sa

$$y^2 = x^3 + a_2x^2 + a_4x + a_6 - (a_1xy + a_3y),$$

što ćemo kasnije koristiti u Schoofovom algoritmu.

Za K konačno polje, $E(\overline{K})$ je torziona grupa, tj. svi elementi su konačnog reda. Za $m \in \mathbb{N}$ definiramo m -**torzionu podgrupu** od E sa

$$E[m] = \{P \in E(\overline{K}) : [m](P) = \mathcal{O}\}.$$

Sljedeći teorem karakterizira m -torzionu podgrupu $E[m]$ preko polinoma dijeljenja ψ_m .

Teorem 2.17. *Neka je P točka u $E(\overline{K}) \setminus \mathcal{O}$, i neka je $m \in \mathbb{N}$. Tada je $P \in E[m]$ ako i samo ako je $\psi_m(P) = 0$.*

Nad poljima karakteristike 2 promatramo nesupersingularne krivulje zadane jednadžbom oblika

$$y^2 + xy = x^3 + a_2x^2 + a_6.$$

Dakle, imamo $a_1 = 1$, $a_3 = a_4 = 0$ i $b_2 = 1$, $b_4 = b_6 = 0$, $b_8 = a_6$. Rekurzija (2.18) za niz (ψ_m) pojednostavljuje se na

$$\begin{aligned}
\psi_0 &= 0 \\
\psi_1 &= 1 \\
\psi_2 &= x \\
\psi_3 &= x^4 + x^3 + a_6 \\
\psi_4 &= x^6 + a_6 x^2 \\
&\vdots \\
\psi_{2m+1} &= \psi_{m+2}\psi_m^3 + \psi_{m-1}\psi_{m+1}^3, \quad m \geq 2 \\
\psi_{2m} &= (\psi_{m+2}\psi_{m-1}^2 + \psi_{m-2}\psi_{m+1}^2) \psi_m/x, \quad m > 2.
\end{aligned} \tag{2.19}$$

Polinomi ψ_m ovise samo o x . Zato definiramo polinome f_m u jednoj varijabli $f_m(x) = \psi_m(x, y)$ koje ćemo također zvati polinomi dijeljenja.

Preslikavanje $[m]$ je oblika

$$\begin{aligned}
[m](P)_X &= x + \frac{f_{m-1}f_{m+1}}{f_m^2}, \\
[m](P)_Y &= x + y + \frac{(x^2 + x + y)f_{m-1}f_m f_{m+1} + f_{m-2}f_{m+1}^2}{x f_m^3}.
\end{aligned} \tag{2.20}$$

Karakterizaciju iz teorema možemo prilagoditi karakteristici 2 i dobivamo

Korolar 2.18. *Neka je $P \in E(\overline{K}) \setminus E[2]$, i neka je $m > 2$. Tada je $P \in E[m]$ ako i samo ako je $f_m(x) = 0$.*

Treba primijetiti da svaka nultočka x_0 od f_l pripada nekoj točki krivulje E . Naime, postoji konačno polje \mathbb{F}_{q_1} koje sadrži x_0 . x_0 pripada ili $E(\mathbb{F}_{q_1})$ ili njenom twistu $E_1(\mathbb{F}_{q_1})$. Budući da su E , E_1 izomorfne nad $\mathbb{F}_{q_1^2}$, postoji $P \in E(\mathbb{F}_{q_1^2})$ kojoj x_0 pripada. Ovime je pokazana egzistencija l -torzionih točaka.

Napomena 2.19. Korolar 2.18 kao karakterizaciju l -torzione grupe koristit ćemo kasnije u Schoofovom algoritmu, kad ćemo tražiti točke l -torzione podgrupe sa posebnim svojstvima, odnosno točke koje zadovoljavaju polinomijalnu jednadžbu oblika

$$h(x) = 0.$$

Tada će zbog korolara 2.18 x koordinata zadovoljavati i $(\text{NZM}(h, f_l))(x) = 0$. Zbog ekvivalencije u korolaru za odrediti egzistenciju takve točke dovoljno je testirati je li $\text{NZM}(h, f_l) \neq 1$.

2.7 Hasseov teorem

Označimo sa \mathbb{F}_q konačno polje (ne nužno karakteristike 2). Neka je E eliptička krivulja nad \mathbb{F}_q

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{2.21}$$

Broj racionalnih točaka na krivulji je konačan. Označimo sa $\#E(\mathbb{F}_q)$ broj rješenja jednadžbe (2.21) u \mathbb{F}_q^2 , odnosno broj točaka na krivulji $E(\mathbb{F}_q)$. Sjetimo se, Frobeniusov trag $t \in \mathbb{Z}$ definirali smo kao cijeli broj za koji vrijedi $\#E(\mathbb{F}_q) = q + 1 - t$.

Frobeniusov trag t trivijalno je ograničen sa q^2 . No,

može i bolje: ako fiksiramo x dobivamo kvadratnu jednadžbu u y . Svaka kvadratna jednadžba daje dva rješenja (odavde slijedi trivijalna ograda). Budući da je “slučajno odabrana” kvadratna jednadžba rješiva sa vjerojatnošću $1/2$, možemo očekivati da je $\#E(\mathbb{F}_q) \approx q$, tj. da je t vrlo ograničen. E. Artin² je pretpostavio, a Hasse³ dokazao sljedeći teorem, koji opravdava prethodnu heuristiku.

Hasseov teorem (1933). *Neka je $E(\mathbb{F}_q)$ eliptička krivulja nad konačnim poljem \mathbb{F}_q . Za Frobeniusov trag t krivulje $E(\mathbb{F}_q)$ vrijedi:*

$$|t| \leq 2\sqrt{q}.$$

Dokaz. Vidi [Sil86]. □

Nad prostim poljem \mathbb{F}_p , za svaki m u Hasseovom intervalu $\langle p+1-2\sqrt{p}, p+1+2\sqrt{p} \rangle$ postoji krivulja sa $\#E(\mathbb{F}_p) = m$. U podintervalu $\langle p+1-\sqrt{p}, p+1+\sqrt{p} \rangle$ se svaki red pojavljuje s gotovo uniformnom distribucijom. Ova činjenica čini bazu Lenstrinog ECM (eng. *elliptic curve method*) algoritma za faktorizaciju. Nad binarnim poljima ova činjenica ne vrijedi.

Iz priče maloprije vidi se kako se mogu birati slučajne točke na krivulji. Odaberemo slučajan $x \in \mathbb{F}_q$, i pokušamo riješiti kvadratnu jednadžbu u y . Ako je jednadžba rješiva, “bacimo novčić” i odaberemo jedno od dva rješenja. Ako nije, pokušamo sa sljedećim x -om.

Slično tako možemo probabilistički kodirati abecedu \mathcal{A} od npr. a simbola u točke na krivulji. Podijelimo najprije \mathbb{F}_q u a (otprilike jednakih) komada. \mathbb{F}_q uredimo tako da elemente $a, b \in \mathbb{F}_q$ gledamo kao reducirane polinome, te kažemo da je $a \leq b$ ako i samo ako je $a(p) \leq b(p)$ u \mathbb{N} , za $p = \text{char } \mathbb{F}_q$. Na isti se način elementi polja kodiraju u prirodne brojeve i zapisuju u računalu. Sad možemo zamisliti da smo \mathbb{F}_q podijelili na a podjednakih uzastopnih cjelobrojnih segmenata - pretinaca. Odaberemo bijekciju sa \mathcal{A} u skup pretinaca, te za svaki simbol iz \mathcal{A} tražimo točku s koordinatom x iz pridruženog pretinca. To možemo raditi redom od “najmanjeg” x -a, sve dok ne uspijemo riješiti kvadratnu jednadžbu u y . Ako je veličina najmanjeg pretinca k , naivna vjerojatnost (kao i u heuristici) da ne postoji točka u pretincu je, tj. da kodiranje neće uspjeti je $\frac{1}{2^k}$. No, npr. ako kodiramo 128-bitnu abecedu u krivulju nad 191-bitnim binarnim poljem, veličina pretinca je $2^{191-128} = 2^{63}$, što daje zanemarivu vjerojatnost $(\frac{1}{2})^{2^{63}}$ za neuspjeh s određenim pretincom. Postoje rezultati koji govore o uniformnoj distribuciji točaka na $\mathbb{F}_q \times \mathbb{F}_q$, što dodatno umanjuje vjerojatnost za neuspjeh kodiranja.

²Emil Artin (1898–1962), austrijski matematičar

³Helmut Hasse (1898–1979), njemački matematičar

Brojanje točaka na eliptičkoj krivulji

Kao što je već spomenuto, u kriptografiji se zbog slabijeg ECDLP-a izbjegavaju supersingularne krivulje. Teorem 2.8 i jednačba (2.12) govore da je za određivanje broja točaka na nesupersingularnim krivuljama dovoljno promatrati krivulje zadane jednačbom

$$E_{0,a_6} : y^2 + xy = x^3 + a_6, \quad a_6 \in \mathbb{F}_q^*,$$

pošto je $\#E_{\gamma,a_6}(\mathbb{F}_q) = 2q + 2 - \#E_{0,a_6}(\mathbb{F}_q)$.

3.1 Schoofov algoritam

Prvi efikasan algoritam za brojenje točaka na eliptičkoj krivulji opisao je 1995. Rene Schoof u svome radu [Sch95]. Schoof je smanjio složenost problema brojenja točaka sa složenosti $O(q^{1/4+\varepsilon})$ dotadašnjih algoritama na $O(\ln^8 q)$.

Već smo spomenuli da je odrediti Frobeniusov trag t ekvivalentno određivanju broja točaka na krivulji. Hassev teorem kaže da se $t = q + 1 - \#E(\mathbb{F}_q)$ nalazi u intervalu

$$\langle -2\sqrt{q}, 2\sqrt{q} \rangle,$$

širine $4\sqrt{q}$. Jezgru algoritma čini određivanje ostataka $t_l = t \bmod l$, gdje su l prosti brojevi manji od l_{\max} , gdje je l_{\max} najmanji prosti broj za koji vrijedi

$$\prod_{\substack{2 \leq l \leq l_{\max} \\ l \text{ prost}}} l > 4\sqrt{q}.$$

Iz kineskog teorema o ostacima slijedi da iz t_l -ova možemo (jedinstveno) odrediti t .

Napomena 3.1. Za nesupersingularne krivulje je po definiciji $t \equiv 1 \pmod{2}$ (v. lemu 2.10), pa algoritam počinje sa $l = 3$.

Sjetimo se karakteristične jednačbe Frobeniusovog endomorfizma

$$\varphi^2(P) + [q](P) = [t](\varphi(P)). \quad (3.1)$$

Označimo $E[l] \setminus \mathcal{O}$ sa $E[l]^*$. Neka je $P = (x, y) \in E[l]^*$. Označimo sa q_l i t_l nenegativne ostatke pri dijeljenju q i t sa l . Primijetimo da je $\varphi(P)$ također u $E[l]^*$. To zajedno daje:

$$\varphi^2(P) + [q_l](P) = [t_l](\varphi(P)), \quad (3.2)$$

$\varphi, [q_l]$ su poznati, trebamo odrediti t_l .

Kako odrediti t_l ?

Jezgru algoritma čini određivanje t_l -ova. Tražimo ih tako da prolazeći kroz sustav ostataka testiramo lijevu i desnu stranu jednačbe (*). Pošto za $P \in E$ vrijedi

$$P_x = (-P)_x,$$

najbolje je prvo testirati x koordinate lijeve i desne strane izraza, i pustiti τ da ide skupom $\{0, \dots, \frac{l-1}{2}\}$, čime istovremeno testirajući po dva ostatka pokrивamo reducirani sustav $\{-\frac{l-1}{2}, \dots, \frac{l-1}{2}\}$ ostataka modulo l . Kad dobijemo jednakost u x koordinati, ponovimo račun za y koordinatu i ponovnom usporedbom odredimo predznak od τ .

Osnovni Schoofov algoritam glasi:

Algoritam 1 Osnovni Schoofov algoritam (skica)

ULAZ: Eliptička krivulja $E_{0,a_6}/\mathbb{F}_q$

IZLAZ: $\#E(\mathbb{F}_q)$

1: $M \leftarrow 2, l \leftarrow 3, S \leftarrow \{(t_2, 2) = (1, 2)\}$

2: **while** ($m < 4\sqrt{q}$) **do**

3: **for** $\tau = 0$ to $(l-1)/2$ **do**

4: Provjeri da li za $P \in E[l]$ vrijedi:

$$\varphi^2(P) + [q_l](P) = \pm[\tau]\varphi(P) \quad \{\text{Točno jedan } \tau \text{ prolazi ovaj test}\}$$

5: $S \leftarrow S \cup \{(\tau, l)\}$, odnosno $S \leftarrow S \cup \{(-\tau, l)\}$ $\{\text{odgovarajući } \tau\}$

6: $M \leftarrow M \cdot l$

7: $l \leftarrow \text{vrati_sljedeći_prosti_broj}(l)$

8: Izračunaj t iz S (pomoću kineskog teorema o ostacima)

9: **return** $q + 1 - t$

Sad možemo preciznije opisati detalje algoritma. l -torzione točke nemamo tek tako na raspolaganju, jer bismo za to trebali tražiti korijene polinoma stupnja l^2 koji mogu biti iz polja znatno većeg od \mathbb{F}_q . Tako ustvari ne uspoređujemo izraze u τ i P već se bavimo pitanjem egzistencije takvih točaka, za što će nam koristiti polinomi dijeljenja. Najprije nam treba propozicija koja kaže da je dovoljno naći jedan par τ i $P \in E[l]^*$ koji daju jednakost.

Propozicija 3.2. *Neka je $\tau \in \{0, \dots, l-1\}$. Ako postoji $P \in E[l]^*$ tako da vrijedi jednadžba*

$$\varphi^2(P) + [q_l](P) = [\tau](\varphi(P)), \quad (*)$$

tada je nužno $\tau = t_l$.

Dokaz. Pretpostavimo suprotno, tj. da je $t_l \neq \tau$, te da postoji $P \in E[l]^*$ koji zadovoljava jednadžbe (3.1) i (*). Oduzimanjem tih dviju jednadžbi dobijemo da je

$$[\tau - t_l]\varphi(P) = \mathcal{O},$$

što povlači da $\tau - t_l$ dijeli prosti broj l . To povlači da je $|\tau - t_l| = 1$, što je kontradikcija sa $P \neq \mathcal{O}$. \square

Posljedica ove propozicije je to da ne moramo početi sa točkom $P \in E[l]^*$ i tražiti τ za koji vrijedi (*), već možemo obratno - nakon što odaberemo τ tražimo postoji li l -torziona točka tako da vrijedi (*). Egzistenciju tražene točke ćemo provjeravati tražeći najveću zajedničku mjeru l -tog polinoma dijeljenja f_l i polinoma h dobivenog iz jednadžbe (*).

Prilikom računanja polinoma h razlikujemo dva slučaja koji proizlaze iz formula za zbrajanje točaka na eliptičkoj krivulji. Lijeva strana jednadžbe (*) dobiva se zbrajanjem dviju točaka krivulje, što znači da moramo razlikovati slučajeve koji proizlaze iz grupovnog zakona. Ideja je da se napravi particija od $E[l]^*$ na dva podskupa:

$$E_A[l] = \{P \in E[l]^* : \varphi^2(P) \neq \pm[q_l](P)\}$$

$$E_B[l] = E[l]^* \setminus E_A,$$

te da čim odaberemo l odlučimo u kojem ćemo od ovih skupova tražiti egzistenciju odgovarajuće l -torzione točke (uoči da particija ne ovisi o τ).

Pretpostavimo da je $E_B[l]$ neprazan, tj. da postoji $P \in E(\mathbb{F}_q)$ tako da $\varphi^2(P) = \pm[q_l](P)$. Za x koordinate to znači:

$$\varphi^2(P)_x = [q_l](P)_x$$

Ovo je upravo drugi slučaj u općim formulama zbrajanja (2.13) gdje računamo parametar λ kad je $x_1 = x_2 \neq 0$. Raspisimo prethodnu jednakost

$$x^{q^2} = x + \frac{f_{q_l-1}f_{q_l+1}}{f_{q_l}^2},$$

prebacimo sve na lijevu stranu i dobijemo:

$$\begin{aligned} x^{q^2} + x + \frac{f_{q_l-1}f_{q_l+1}}{f_{q_l}^2} &= 0, & / \cdot f_{q_l}^2 \\ (x^{q^2} + x)f_{q_l}^2 + f_{q_l-1}f_{q_l+1} &= 0. \end{aligned}$$

Dakle imamo točku $P = (x, y) \in E_B[l]$ čija x koordinata poništava gornji polinom. Ovo zajedno sa karakterizacijom l -torzione podgrupe (vidi (2.18) i napomenu 2.19) daje test – $E_B[l]$ je neprazan ako i samo ako je

$$\text{NZM}\left((x^{q^2} + x)f_{q_l}^2 + f_{q_l-1}f_{q_l+1}, f_l\right) \neq 1. \quad (\Delta)$$

Pošto je $q = 2^m$, a $l \geq 3$ prost, slijedi da je $q_l \neq 0$, tj. da $\text{NZM}(f_{q_l}, f_l) = 1$, pa racionalizacijom sa f_{q_l} nismo uveli nove nultočke.

Pokažimo sad kako se računa u svakom od slučajeva.

Slučaj A. $E_B[l]$ je prazan, tj. ne postoji točka $P \in E[l]^*$ za koju je $\varphi^2(P) = \pm[q_l](P)$. τ tražimo pomoću točaka skupa $E_A[l]$.

$$\varphi^2(P) + [q_l](P) = \pm[\tau]\varphi(P), \quad 1 \leq \tau \leq (l-1)/2, \quad q = 2^n.$$

Uočimo da ako (Δ) test ne prođe, znamo da je $t_l \neq 0$, pa τ (korak 3) ustvari “šeta” od 1, a ne od 0. x koordinate lijeve i desne strane prethodne jednadžbe možemo izračunati koristeći formule (2.13) i (2.20):

$$(\varphi^2(P) + [q_l](P))_x = x^{q^2} + x + \frac{f_{q_l-1}f_{q_l+1}}{f_{q_l}^2} + \lambda^2 + \lambda, \quad (3.3)$$

$$(\pm[\tau]\varphi(P))_x = x^q + \frac{f_{\tau-1}^q f_{\tau+1}^q}{f_{\tau}^{2q}}, \quad (3.4)$$

gdje λ označava

$$\lambda = \frac{(y^{q^2} + y + x)x f_{q_l}^3 + f_{q_l-2}f_{q_l+1}^2 + (x^2 + x + y)(f_{q_l-1}f_{q_l}f_{q_l+1})}{x f_{q_l}^3 (x + x^{q^2}) + x f_{q_l-1}f_{q_l}f_{q_l+1}},$$

pri čemu je f_i skraćena oznaka za $f_i(x)$ (f_i su polinomi dijeljenja). U računanju je korištena činjenica da su polinomi $f_i \in K[x]$, tj. da vrijedi $f_m(x^q) = f_m(x)^q$. U slučaju

da je $q_l = 1$, zanemarimo formulu (3.3) koja nema smisla za f_{q_l-2} , te jednostavno zbrojimo točke $\varphi^2(P)$ i P na uobičajeni način prema formuli (2.13).

Potencije od y koje u jednadžbu (3.3) ulaze kroz λ reduciraju se modulo jednadžba krivulje

$$E : y^2 + xy + x^3 + a_6 = 0,$$

što daje polinome najviše prvog stupnja u y . Kad izjednačimo desne strane (3.3) i (3.4), racionaliziramo s najmanjim zajedničkim višekratnikom polinoma u nazivnicima (obiju strana), prebacimo na lijevu stranu, dobijemo relaciju oblika

$$a(x) + yb(x) = 0.$$

Budući da je $P = (x, y) \in E[l]^*$, korolar 2.18 kaže da je $f_l(x) = 0$, pa je polinome $a(x)$ i $b(x)$ dovoljno računati modulo $f_l(x)$. Prilikom računanja, redukcije modulo E i modulo f_l izvode se (donekle) naizmjenice kako bi se izbjeglo da polinomi u izrazu nekontrolirano rastu. Ako su i $a(x)$ i $b(x)$ različiti od nule, relaciju $y = a(x)/b(x)$ uvrstimo u E , pomnožimo sa $b(x)^2$ i dobijemo

$$h_X(x) = a^2(x) + xa(x)b(x) + b^2(x)x^3 + b^2(x)a_6 = 0.$$

Ako je $b(x) = 0$, stavimo $h_X(x) = a(x)$, odnosno $h(x) = b(x)$ u slučaju da je $a(x) = 0$. Da bismo odredili postoji li točka $P \in E[l]^*$ čija x -koordinata poništava h_X , računamo najveći zajednički djelitelj polinoma h_X i f_l . Ako je $\text{NZM}(h_X, f_l) \neq 1$, prema korolaru 2.18 i napomeni 2.19 takva točka postoji, što znači da smo odabrali dobar τ . Sad još usporedimo y koordinate na isti način da odredimo točan predznak i stavimo $t_l = \tau$ odnosno $t_l = -\tau$.

Slučaj B. $E_B[l]$ je neprazan. Tražimo τ za točke u $E_B[l]$.

Očigledno je $t_l = 0$ ako i samo ako je $\varphi^2(P) = -[q_l](P)$. Točan predznak dobijemo uspoređivanjem $\varphi^2(P)_y$ i $[q_l](P)_y$. Ako je $\varphi^2(P)_y \neq [q_l](P)_y$ slijedi da je $t_l = 0$ i gotovi smo. U protivnom još uvijek ne znamo t_l . No, vrijedi

$$\varphi^2(P) = [q_l](P),$$

što uvrštavanjem u karakterističnu jednadžbu daje

$$\begin{aligned} [2q_l](P) - [\tau]\varphi(P) &= \mathcal{O}, \\ [2q_l](P) &= [\tau]\varphi(P) \end{aligned}$$

Sad ćemo notaciju $[\tau](P)$ množenja $P \in E[l]^*$ proširiti sa $\tau \in \mathbb{Z}$ na $\tau \in \mathbb{F}_l$. Naime, svi ostaci modulo l prost broj prirodno su elementi konačnog polja \mathbb{F}_l . Stoga ima smisla napisati

$$\varphi(P) = \left[\frac{2q_l}{\tau} \right] (P),$$

gdje je $\frac{2q_l}{\tau}$ element polja \mathbb{F}_l , a $\left[\frac{2q_l}{\tau} \right]$ predstavlja množenje prirodnim brojem (ostatkom modulo l) prirodno pridruženom elementu polja $\frac{2q_l}{\tau} \in \mathbb{F}_l$. Na prethodnu jednadžbu djelujemo sa φ

$$\begin{aligned} \varphi^2(P) &= \left[\frac{2q_l}{\tau} \right] \varphi(P) \\ [q_l](P) &= \left[\frac{4q_l^2}{\tau^2} \right] (P) \end{aligned}$$

odakle slijedi (jer je l prost) da je

$$\begin{aligned} \frac{4q_l^2}{\tau^2} &\equiv q \pmod{l}, & / \cdot \tau^2 \\ 4q_l^2 &\equiv \tau^2 q \pmod{l}. \end{aligned}$$

Pošto je $q_l \neq 0$, $\text{NZM}(q_l, l) = 1$, prethodnu kongruenciju možemo podijeliti sa q_l , pa dobijemo

$$\tau^2 \equiv 4q \pmod{l},$$

što znači da q ima (drugi) korijen modulo l . Označimo ga sa $w \in \mathbb{F}_l$. Vratimo na početak i dobijemo

$$\varphi(P) = [w_0](P), \quad w_0 \in \{-w, w\}.$$

Stavimo $t_l \equiv 2w_0 \pmod{l}$, predznak odredimo kao i ranije, provjeravajući y koordinate.

U ovom slučaju iz očiglednih razloga kažemo da Frobeniusovo preslikavanje ima **svojevlastvenu vrijednost** $w_0 \in \mathbb{F}_l$. Postojanje ovakvih svojstvenih vrijednosti u općenitijem slučaju čini osnovu Elkiesovog poboljšanja Schoofovog algoritma.

Elkies i Atkin kasnije su smanjili složenost Schoofovog algoritma. Novi algoritam nazvan je Schoof-Elkies-Atkin SEA algoritam. Po načinu rada sličan je Schoofovom algoritmu, no kad se odabere prosti l , najprije se gleda da li korijeni karakteristične jednadžbe Frobeniusovog endomorfizma reducirane modulo l

$$u^2 - t_l u + q_l = 0,$$

leže u \mathbb{F}_l ili ne, tj. da li je diskriminanta $\Delta_t = t^2 - 4q$ kvadrat ili ne. Ako jest, kažemo da je l Elkiesov prosti broj, ako ne kažemo da je Atkinov. Budući da ne znamo t_l , moramo se poslužiti drugim tehnikama da bismo odredili o kojem tipu pripada l . Tu pomažu modularni polinomi. Pomoću njih može se odrediti o kojem tipu prostog broja se radi. Računanje modularnih polinoma je zahtjevna operacija, no ovdje se isplati. Kad se odredi tip prostog broja, bira se odgovarajući algoritam. U Elkiesovom slučaju dobivamo faktor polinoma dijeljenja f_l stupnja $(l-1)/2$, što jako ubrzava redukcije modulo f_l . Atkinov slučaj ograničava skup mogućih τ -ova. Dobivene informacije pomoću kombinacije kineskog teorema o ostacima i provjeravanja kandidata za red grupe daju daju točan broj točaka krivulje.

3.2 Primjer

Gledamo krivulju

$$E: y^2 + xy = x^3 + 1$$

nad poljem \mathbb{F}_q sa $q = 2^5 = 32$ elemenata. Želimo izračunati $\#E(\mathbb{F}_{32})$. Pošto je

$$2 \cdot 3 \cdot 5 = 30 > 4\sqrt{q} = 16\sqrt{2},$$

dovoljno je odrediti Frobeniusov trag t modulo 2, 3, 5. Hassev teorem kaže da se broj točaka nalazi u skupu $\{22, \dots, 44\}$. Premda bi na krivulji ove veličine bilo jednostavnije redom testirati brojeve od 22 do 44 za nekoliko točaka, ovdje ćemo pokazati sve korake Schoofovog algoritma.

$l = 2$ Krivulja nije supersingularna pa je po definiciji $t_2 = 1$. Preostaje izračunati t_3 i t_5 .

$l = 3$ $q_3 = 2$, računamo polinome dijeljenja:

$$\begin{aligned} f_0(x) &= 0 \\ f_1(x) &= 1 \\ f_2(x) &= x \\ f_3(x) &= x^4 + x^3 + a_6 = x^4 + x^3 + 1 \end{aligned}$$

Računamo

$$\begin{aligned} x^{q^2} &= x^3 + 1 \\ x^q &= x^2 \\ y^{q^2} &= x^3y + 1 \\ y^q &= xy + (1 + x^2 + x^3) \end{aligned}$$

Najprije treba testirati ima li Frobeniusov endomorfizam svojstvenih vrijednosti (vidi test (Δ)).

Dobijemo

$$\text{NZM}(x^3 + x^2 + x + 1, x^4 + x^3 + 1) = 1,$$

pa slijedi da φ nema svojstvenih vrijednosti (slučaj A), te još da je $t_3 \neq 0$. Prema tome je $t_3 = -1$ ili $t_3 = 1$, jer je $\{-1, 0, 1\}$ potpun sustav ostataka modulo 3. Prisjetimo se, obično najprije provjeravamo za x koordinatu da odredimo t_l do na predznak, zatim provjerom y koordinate određujemo točan predznak. Ovdje znamo da je $|t_l| = 1$, pa možemo odmah provjeriti y koordinatu, no svejedno ćemo pokazati račun za $\tau = 1$. Označimo brojnik od λ sa λ_b , te nazivnik sa λ_n .

$$\begin{aligned} \lambda_b &= (y^{q^2} + y + x)xf_{q_1}^3 + f_{q_1-2}f_{q_1+1}^2 + (x^2 + x + y)(f_{q_1-1}f_{q_1}f_{q_1+1}) \\ &= (x^3y + 1 + y + x)x^4 + (x^2 + x + y)x(x^4 + x^3 + 1) \\ &= (x^7 + x^5 + x)y + (x^8 + x^7 + x^6 + x^5 + x^4 + x^2 + x) \end{aligned}$$

što nakon redukcije sa f_3 daje

$$\begin{aligned} \lambda_b &\equiv (x^3 + x^2 + x)y + x \pmod{f_3}, \\ \lambda_n &= xf_{q_1}^3(x + x^{q^2}) + xf_{q_1-1}f_{q_1}f_{q_1+1} \\ &= x^4(x + x^3 + 1) + x^2(x^4 + x^3 + 1) = x^7 + x^6 + x^4 + x^2 \\ &\equiv x^2 + 1 \pmod{f_3}. \end{aligned}$$

Racionalni dio iz $(\pm[1]\varphi(P))_x$ iščezava jer je $f_0 = 0$, pa je za racionalizaciju dovoljno uzeti

$$N(x) = \text{NZV}(x^2, (x^2 + 1)^2) = x^6 + x^2.$$

Desna strana postaje

$$D_X = x^q \cdot N(x) = (x^2)(x^6 + x^2) = x^8 + x^4 \equiv x^2 + x + 1 \pmod{f_3}.$$

Lijeva strana je

$$L_X = \underbrace{N(x)(x^{q^2} + x)}_{S_1} + \underbrace{\left(\frac{N(x)}{f_{q_i}^2}\right)(f_{q_i-1}f_{q_i+1})}_{S_2} + \underbrace{\left(\frac{N(x)}{\lambda_n^2}\right)\lambda_b(\lambda_b + \lambda_n)}_{S_3}.$$

Nakon redukcija sa f_3 dobivamo

$$\begin{aligned} S_1 &= x^3 + x \\ S_2 &= 0 \\ S_3 &= x^3 + x^2 + 1, \end{aligned}$$

odakle je $L = x^2 + x + 1$. Primijetimo da smo iz S_3 nakon redukcija izgubili y , što znači da je $b(x) = 0$, pa stavimo $h_X = a(x)$, gdje je $a(x) = L_X + D_X$. No, zbog ranijih redukcija sa f_3 dobili smo da je $a(x) = 0$, što upravo znači da je $\text{NZM}(h_X, f_3) \neq 1$, tj. da smo odabrali dobar τ .

Sad treba odrediti predznak od t_3 . Pogledajmo najprije lijevu stranu

$$(\varphi^2(P) + [q_l](P))_y = (x^{q^2} + x_3) \cdot \lambda + x_3 + y^{q^2} = \lambda \cdot x^{q^2} + \lambda \cdot x_3 + x_3 + y^{q^2},$$

gdje smo sa x_3 označili $(\varphi^2(P) + [q_l](P))_x$. Pomnožimo sa $N(x)$ i dobijemo

$$\begin{aligned} L'_Y &= (N\lambda)x^{q^2} + (N\lambda)x_3 + Nx_3 + Ny^{q^2} = (N\lambda)x^{q^2} + L_X\lambda + L_X + Ny^{q^2} \\ &= L_X(\lambda + 1) + N\lambda x^{q^2} + Ny^{q^2} \\ &= L_X \left(\frac{\lambda_b + \lambda_n}{\lambda_n} \right) + N\lambda x^{q^2} + Ny^{q^2}. \end{aligned}$$

Prvi sumand u L'_Y je jedini racionalni izraz. Iz izraza se vidi da je većina potrebnih sumanada gotovo izračunata prilikom računanja h_X . Pogledajmo sad desnu stranu:

$$D'_Y = N \cdot ([\tau]\varphi(P))_y = x^q + y^q + \frac{(x^{2q} + x^q + y^q)f_{\tau-1}^q f_{\tau}^q f_{\tau+1}^q + f_{\tau-2}^q f_{\tau+1}^{2q}}{x^q f_{\tau}^{3q}}$$

Dakle sad treba L'_Y i D'_Y racionalizirati sa $\text{NZV}(\lambda_n, x^q f_{\tau}^{3q})$. U našem je slučaju $D'_Y = N \cdot y^q$ (jer je $\tau = 1$), pa je dovoljno racionalizirati sa λ_n . Nakon redukcije imamo

$$\begin{aligned} L_Y &= y + (x^3 + x) \\ D_Y &= y + (x^3 + x), \end{aligned}$$

što ustvari zbog ranijih redukcija znači da je $\text{NZM}(h_Y, f_3) \neq 1$, tj. da je predznak od τ dobar pa stavimo $t_3 = 1$.

$l = 5$ $q_5 = 2$. Računamo

$$\begin{aligned} f_4 &= x^6 + x^2 \\ f_5 &= x^{12} + x^{11} + x^{10} + x^8 + x^6 + x^5 + x^4 + x^3 + x + 1, \end{aligned}$$

te ponovo

$$\begin{aligned}x^{q^2} &= x^8 \\x^q &= x^{11} + x^5 + x^4 + x^3 + x \\y^{q^2} &= x^7y + (x^{11} + x^9 + x^8 + x^5 + x^3 + x) \\y^q &= (x^{10} + x^4 + x^3 + x^2 + 1)y + (x^9 + x^7 + x^5 + x^4 + x^3 + x)\end{aligned}$$

Test (Δ) ponovo daje 1, pa slijedi da je $t_5 \neq 0$. Računamo dalje

$$\begin{aligned}\lambda_b &= (x^{11} + x^5 + x)y + (x^9 + x^8 + x^7 + x^5 + x^3 + x + 1) \\ \lambda_n &= x^{12} + x^6 + x^2.\end{aligned}$$

Stavimo $\tau = 1$. Racionaliziramo sa $N(x) = x^{24} + x^{12} + x^4$ i računamo S_1, S_2 i S_3 kao i ranije za $l = 3$. Kad zbrojimo dobijemo

$$\begin{aligned}L_X &= x^{10} + x^9 + x^6 + x^5 + 1 \\ D_X &= x^{11} + x^{10} + x^8 + x^5 + x^4 + x^3 + x^2 + x,\end{aligned}$$

odakle slijedi da je $a(x) = x^{11} + x^9 + x^8 + x^6 + x^4 + x^3 + x^2 + x$, $b(x) = 0$. Stavimo $h_X(x) = a(x)$, i računamo

$$\text{NZM}(h_X, f_l) = x^5 + x^4 + x + 1 \neq 1,$$

što znači da je $\tau = 1$ dobar. Sad ponavljamo račun za y da odredimo predznak.

$$\begin{aligned}L_Y &= (x^{11} + x^{10} + x^7 + x^3 + x^2)y + (x^{11} + x^8 + x^7 + x^6 + x^4 + x^2 + x) \\ D_Y &= (x^9 + x^8 + x^7 + x^5 + x^4)y + (x^{10} + x^8 + x^6 + x)\end{aligned}$$

odakle dobijemo

$$\begin{aligned}a(x) &= x^{11} + x^{10} + x^7 + x^4 + x^2 \\ b(x) &= x^{11} + x^{10} + x^9 + x^8 + x^5 + x^4 + x^3 + x^2\end{aligned}$$

što uvrstimo u $h_Y = a^2(x) + xa(x)b(x) + b^2(x)x^3 + b^2(x)a_6$ i nakon redukcija sa f_5 dobijemo

$$h_Y(x) = x^{10} + x^6 + x^5 + x + 1.$$

Pošto je $\text{NZM}(h_Y, f_5) = 1$, slijedi da je $t_5 \neq 1$, odnosno da je $t_5 = -1$.

Sad imamo sve potrebne t_l -ove:

$$t \equiv 1 \pmod{2}, \quad t \equiv 1 \pmod{3}, \quad t \equiv -1 \pmod{5}$$

Iz kineskog teorema o ostacima slijedi da je $t \equiv -11 \pmod{30}$. Nadalje, iz Hasseovog teorema slijedi da je t upravo -11 , što znači da je $\#E_{0,1}(\mathbb{F}_{32}) = 44$. Twist $E_{1,1}(\mathbb{F}_{32})$ je reda $66 - 44 = 22$.

Mi smo u primjeru uzeli $a_6 = 1$ zbog jednostavnijeg računa, jer tako svi polinomi u algoritmu ostaju u $\mathbb{F}_2[x]$, odnosno $\mathbb{F}_2[x, y]$, a u praksi se bira a_6 koji nije sadržan u pravom potpolju od \mathbb{F}_q . Tako smo točke ove krivulje mogli jednostavnije prebrojati pomoću sljedeće propozicije.

Propozicija 3.3. *Neka je E/\mathbb{F}_q eliptička krivulja, i neka je c_1 njen Frobeniusov trag. Označimo sa c_n broj za koji je $\#E(\mathbb{F}_q) = q^n + 1 - c_n$, za $n \geq 1$. Tada vrijedi*

$$c_n = c_1 c_{n-1} - q c_{n-2},$$

uz $c_0 = 2$ po definiciji.

Dokaz. Vidi [BSS99], str. 105. □

Krivulja E iz primjera definirana je nad \mathbb{F}_2 . Na prste možemo provjeriti da imamo četiri točke na krivulji \mathcal{O} , $(0, 1)$, $(1, 0)$ i $(1, 1)$. To znači da je $c_1 = -1$. Računamo

$$c_2 = -3, \quad c_3 = 5, \quad c_4 = 1, \quad c_5 = -11.$$

c_5 je upravo trag od $E(\mathbb{F}_{2^5})$, što znači da je račun u redu.

3.3 Složenost Schoofovog algoritma

Najzahtjevnija operacija u algoritmu je reduciranje polinoma x^{q^2} , x^q , y^{q^2} , y^q , modulo polinom f_l koji je stupnja $O(l^2)$ i modulo jednadžba krivulje E . Ove operacije izvodimo po jedan puta za svaki l , tj. ne moramo računati ponovno unutar τ petlje (korak 3–4). U slučaju x^q i x^{q^2} , a y slučaj je sličan, ovo potenciranje je ustvari operacija u prstenu $R = \mathbb{F}_q[x]/\langle f_l(x) \rangle$, što uzastopnim kvadriranjem i množenjem daje $O(\ln q)$ množenja u prstenu R . Ako pretpostavimo da je korišteno obično množenje (kvadratne složenosti), svako množenje u prstenu R traži $O(\ln^4 q)$ množenja elemenata iz \mathbb{F}_q . Svako množenje i svaka redukcija u \mathbb{F}_q zahtijevaju $O(\ln^2 q)$ bitovnih operacija. Sve skupa, broj bitovnih operacija potrebnih za odrediti t_l za čvrsti l je $O(\ln^7 q)$.

Da bismo odredili broj l -ova koje koristimo u algoritmu, koristimo aproksimaciju za produkt svih prostih brojeva do l_{\max}

$$\ln(2 \cdot 3 \cdot 5 \cdot 7 \cdots l_{\max}) \approx l_{\max}.$$

Slijedi da je l_{\max} najmanji prosti broj takav da je

$$l_{\max} \geq \ln(4\sqrt{q}).$$

Iskoristimo Čebiševljev teorem koji kaže da u svakom segmentu $[n, 2n]$ ima barem jedan prosti broj i dobijemo da je

$$l_{\max} \leq 2 \ln(4\sqrt{q}) = 4 \ln 2 + \ln q,$$

tj. da je $l_{\max} = O(\ln q)$. Kad još uzmemo u obzir da $\pi(x)$ (broj prostih brojeva manjih od x) možemo aproksimirati sa $x/\ln x$ slijedi da je $\pi(l_{\max}) = O(\ln q/\ln \ln q)$, što možemo grublje ocijeniti sa $O(\ln q)$. Sve zajedno daje ukupnu složenost od $O(\ln^8 q)$ bitovnih operacija.

U našem slučaju, kad je q potencija od 2, umjesto množenja $\log_2 q$ puta kvadriramo u R . Kvadriranje u polju \mathbb{F}_q je složenosti $O(\ln q)$, redukcija modulo f_l je $O(\ln^2 q)$, što daje ukupnu složenost kvadriranja u prstenu $O(\ln^3 q)$. Slijedi da je ukupna složenost Schoofovog algoritma nad binarnim poljima $O(\ln^7 q)$.

Nešto je teže odrediti složenost SEA algoritma. Ukupna složenost Elkiesovog dijela algoritma je $O(\log^6 q)$. Atkinov dio je eksponencijalne složenosti. To navodi da bismo za bolju složenost mogli koristiti Elkiesovih prostih brojeva koliko nam treba da upotrijebimo kineski teorem o ostacima, no u praksi se (za polja interesantna za kriptografiju) ipak pokazuje da najbolje rezultate (bolje od običnog Schoofovog algoritma) daje kombinacija s pažljivo odabranim podskupovima Atkinovih prostih brojeva.

Dodatak

Krivulja B-163

Posljednjih nekoliko godina vodeće svjetske organizacije za standardizaciju (ANSI, IEEE, ISO, NIST) uključile su eliptičke krivulje u svoje standarde. Jedna od nekoliko preporučenih krivulja je i tzv. pseudoslučajna eliptička krivulja s oznakom B-163, zadana nad poljem \mathbb{F}_q , $q = 2^{163}$. Vezano uz polje dani su ireducibilni polinom (za polinomijalnu reprezentaciju), te tip normalne baze (za reprezentaciju preko normalne baze). Elementi polja zapisuju se kodirani u prirodne brojeve zapisane heksadecimalno. U slučaju da se radi o polinomijalnoj bazi, kôd elementa dobije se tako da polinom iz $\mathbb{F}_2[x]$ pridružen elementu polja shvatimo kao prirodni broj u binarnom zapisu

$$x^3 + x + 1 = \underline{1} \cdot x^3 + \underline{0} \cdot x^2 + \underline{1} \cdot x + \underline{1} \mapsto 1011_2 = 11,$$

odnosno da se u polinom (sad gledan nad $\mathbb{Z}[x]$) uvrsti broj 2. Na sličan način dobivamo i reprezentaciju elemenata u normalnoj bazi.

Polje $\mathbb{F}_{2^{163}}$ zadano je polinomom (pentanomom)

$$f(x) = x^{163} + x^7 + x^6 + x^3 + 1.$$

Sva binarna polja iz FIPS186-2 standarda (\mathbb{F}_{163} , \mathbb{F}_{233} , \mathbb{F}_{283} , \mathbb{F}_{409} , \mathbb{F}_{571}) su prostog (neparnog) stupnja proširenja što predložene krivulje nad njima čini otpornim na sve dosad otkrivene napade na ECDLP.

Predložene krivulje (nad binarnim poljima) zadane su jednadžbama oblika

$$E : y^2 + xy = x^3 + x^2 + a_6.$$

Sve su zadane krivulje kofaktora 2, što znači da su im redovi oblika $2 \cdot r$, gdje je r veliki prosti broj. Za krivulju B-163, r je

$$r = 5846006549323611672814742442876390689256843201587,$$

a koeficijent a_6 krivulje B-163 (u standardu označen sa b) kodiran obzirom na zadani ireducibilni polinom zapisan je heksadecimalno

$$b = 20a601907b8c953ca1481eb10512f78744a3205fd.$$

Standard također predlaže baznu točku $G = (G_x, G_y)$ reda r , mada se može uzeti bilo koja točka reda r :

$$G_x = 3f0eba16286a2d57ea0991168d4994637e8343e36$$

$$G_y = 0d51fbc6c71a0094fa2cdd545b11c5c0c797324f1$$

U standardu se isti elementi nalaze kodirani i u normalnoj bazi.

Literatura

- [BSS99] I. F. Blake, G. Seroussi, and N. P. Smart. *Elliptic Curves in Cryptography*. Cambridge University Press, 1999.
- [Hus87] Dale Husemöller. *Elliptic Curves*. Springer Verlag New York Inc., 1987.
- [Knu84] Donald E. Knuth. *The T_EXbook*. Addison-Wesley, 1984.
- [Kob94] Neal Koblitz. *A Course in Number Theory and Cryptography*. Springer Verlag New York Inc., 1994.
- [Kob98] Neal Koblitz. *Algebraic Aspects of Cryptography*. Springer Verlag New York Inc., 1998.
- [LN94] Rudolf Lidl and Harald Niederreiter. *Introduction to finite fields and applications*. Cambridge University Press, 1994.
- [Men93] Alfred Menezes. *Elliptic Curve Public Key Cryptosystems*. Kluwer Academic Publishers, 1993.
- [NZM91] Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery. *An Introduction to the Theory of Numbers*. John Wiley and Sons, Inc., fifth edition, 1991.
- [Sch95] Rene Schoof. Counting points on elliptic curves over finite fields. *J. Theorie des Nombres, Bordeaux*, 7:219–254, 1995.
- [Sil86] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Springer Verlag New York, 1986.
- [Sma01] Nigel P. Smart. How secure are curves over composite fields? *Advances in Cryptology, Eurocrypt 2001*, pages 30–39, 2001.
- [ST91] Joseph H. Silverman and John Tate. *Rational Points on Elliptic Curves*. Springer Verlag New York Inc., 1991.

Indeks

- anomalne krivulje, [14](#)
- apsolutni trag, [9](#)
- diskretni logaritam, [3](#)
- diskriminanta, [11](#)
- dopustiva zamjena varijabli, [11](#)
- ECDLP, [4](#)
- Frobeniusov endomorfizam, [17](#)
- Frobeniusov trag, [14](#)
- izomorfne krivulje, [11](#)
- j -invarijanta, [11](#)
- karakteristična jednadžba, [17](#)
- kompleksno množenje, [16](#)
- konjugati, [9](#)
- linearni trag, [9](#)
- m -torziona podgrupa, [18](#)
- normalna baza, [8](#)
- normalna forma, [11](#)
- svojstvena vrijednost, [25](#)
- Weierstrassova jednadžba, [11](#)

