UNIVERZA NA PRIMORSKEM
FAKULTETA ZA MATEMATIKO, NARAVOSLOVJE IN
INFORMACIJSKE TEHNOLOGIJE

Magistrsko delo

Uporaba Eliptičnih Krivulj v Kriptografiji

(Use of Elliptic Curves in Cryptography)

Ime in priimek: Luca Basiaco
Študijski program: Matematične znanosti, 2. stopnja
Mentor: izr. prof. dr. Štefko Miklavič

Koper, september 2014

Ključna dokumentacijska informacija

Ime in PRIIMEK: Luca BASIACO

Naslov zaključne naloge: Uporaba Eliptičnih Krivulj v Kriptografiji

Kraj: Koper

Leto: 2014

Število listov: 63 Število slik: 3 Število referenc: 26

Mentor: izr. prof. dr. Štefko Miklavič

Ključne besede: eliptične krivulje, eliptične krivulje definirane nad končnimi polji, problem diskretnega logaritma, simetrično šifriranje, asimetrično šifriranje, kriptografija eliptičnih krivulj.

Math. Subj. Class. (2010): 14H52, 94A60.

UDK: 517.5(043.2).

Izvleček:
Glavni in najpomembnejši cilj magistrske naloge je predstavitev uporabe eliptičnih krivulj v kriptografiji. Osredotočili se bomo na kriptosisteme, ki temeljijo predvsem na problemu diskretnega logaritma eliptičnih krivulj in na digitalne podpise.
Magistrska naloga je sestavljena iz šestih poglavij. Prvo poglavje je namenjeno uvodu. V drugem poglavju preučujemo temeljne pojme teorije eliptičnih krivulj, ter v tretjem poglavju analiziramo eliptične krivulje definirane nad končnimi polji. Četrto poglavje je namenjeno problemu diskretnega logaritma, v petem poglavju pa preučujemo kriptografijo eliptičnih krivulj. Zadnje poglavje je namenjeno zaključku.

Key words documentation

Name and SURNAME: Luca BASIACO

Title of final project paper: Use of Elliptic Curves in Cryptography

Place: Koper

Year: 2014

Number of pages: 63 Number of figures: 3 Number of references: 26

Mentor: Assoc. Prof. Štefko Miklavič, PhD

Keywords: elliptic curves, elliptic curves over finite fields, the discrete logarithm problem, symmetric encryption, asymmetric encryption, elliptic curve cryptography.

Math. Subj. Class. (2010): 14H52, 94A60.

UDC: 517.5(043.2).

Abstract: The main goal of the thesis is to introduce the topic of elliptic curve cryptography. We will focus on cryptosystems based especially on the discrete logarithm problem for elliptic curves, and on digital signatures.
The thesis is divided in six chapters. We start with a short introduction. In the second chapter we introduce the fundamental concepts of elliptic curve theory, and in the third chapter we focus on elliptic curves over finite fields. In the fourth and fifth chapters we present the discrete logarithm problem and the topic of elliptic curve cryptography, respectively. The conclusion follows.

Zahvala

Iskreno se zahvaljujem mentorju izr. prof. dr. Štefku Miklaviču za pomoč in za nasvete, ki mi jih je nudil pri realizaciji magistrskega dela, ter za potrpežljivost.

Najlepša hvala Assoc. Prof. Johanu Pederu Hansenu iz Aarhus Univerze na Danskem, ki me je s svojo strastjo do teorije eliptičnih krivulj močno navdušil.

Iskrena hvala tudi profesorici Elen Zrinski, ki mi je pomagala pri lektoriranju magistrskega dela.

Kazalo vsebine

Seznam slik

Poglavje 1

Uvod

Algoritem H. W. Lenstra za faktorizacijo, ki deluje na osnovi eliptičnih krivulj, je bila prva aplikacija eliptičnih krivulj v kriptografiji [17]. Takoj za tem sta leta 1985 N. Koblitz [15] in V. Miller [20] (neodvisno eden od drugega) predlagala uporabo grupe točk eliptične krivulje, definirane nad končnim poljem, v kriptosistemu, ki temelji na problemu diskretnega logaritma.

Najbolj pomembna prednost sistemov, ki delujejo na osnovi eliptičnih krivulj, v primerjavi s sistemi, ki delujejo na faktorizaciji celih števil ali na problem diskretnega logaritma za multiplikativne grupe končnih polj, je ta, da z manj uporabljenega prostora zagotovijo enako varnost. Z drugimi besedami je implementacija teh sistemov hitrejša, velikost pasovne širine in velikost ključev pa so bistveno manjše. Te lastnosti so ključnega pomena pri varnostnih aplikacijah tistih naprav, kjer sta računska moč ter fizični prostor omejena [14]. Za primer lahko podamo pametne kartice ter mobilne telefone.

Glavni cilj magistrske naloge je predstavitev določenih aplikacij eliptičnih krivulj v kriptografiji.

Vsebina magistrske naloge je razdeljena na sledeči način.

V sledečem poglavju bomo predstavili osnovne definicije in izreke teorije eliptičnih krivulj. Te so ključnega pomena pri nadaljnjih poglavjih. Začeli bomo z Weierstrassovimi enačbami, sledi zakon grupe, endomorfizmi, torzijske točke in Weilovo prirejanje.

Glavna tematika tretjega poglavja bodo eliptične krivulje nad končnimi polji. Začeli bomo z dvema enostavnima primeroma, nato pa sledi eden od najpomembnejših izrekov v teoriji eliptičnih krivulj: Hassejev izrek. Obravnavali bomo tudi Frobeniusov endomorfizem, red grupe $E(\mathbf{F}_q)$ in red točke $P \in E(\mathbf{F}_q)$, kjer je $\mathbf{F}_q$ polje s q elementi, ter supersingularne krivulje.

V četrtem poglavju bomo predstavili problem diskretnega logaritma. Analizirali bomo določene metode za reševanje omenjenega problema, kot na primer *index calculus*, Baby Step, Giant Step, Pollardovi λ in ρ metodi in MOV napad.

Peto poglavje je namenjeno kriptografiji eliptičnih krivulj. Spoznali bomo tako Diffie-Hellmanovo izmenjavo ključev, Massey-Omuravo šifriranje, ElGamalovo šifriranje z javnim ključem, ElGamalov digitalni podpis, itd.

Zadnje poglavje je namenjeno zaključku.

Da bi lažje in učinkovitejše razumeli vsebino magistrske naloge, je priporočljivo imeti dobro predznanje o teoriji polj. Da bi osvežili temeljne pojme omenjene teorije, predlagam knjigo [16], za osnovne kriptografske pojme pa knjigo [21].

Vsebina in poglavja magistrske naloge sledijo knjigi [26].

Poglavje 2

Eliptične krivulje

V tem poglavju bomo predstavili osnovne definicije, izreke in trditve o eliptičnih krivuljah, ki so bistvenega pomena za nadaljno vsebino tega dela. Začeli bomo z Weierstrassovimi enačbami, nato sledi zakon grupe, endomorfizmi, torzijske točke in Weilovo prirejanje.

2.1 Weierstrassove enačbe

Naj bo K poljubno polje (na primer racionalna števila $\mathbf{Q}$, realna števila $\mathbf{R}$, kompleksna števila $\mathbf{C}$ ali končna polja $\mathbf{F}_q$, kjer je $q = p^k$ $(k \geq 1)$ in p praštevilo) in $A, B \in K$. Eliptična krivulja E je graf enačbe

$$y^2 = x^3 + Ax + B. \tag{2.1}$$

Tovrstna oblika enačbe eliptične krivulje se imenuje **Weierstrassova enačba**.

Če je K polje in $A, B \in K$, potem pravimo, da je E **definirana nad** K. Točke s koordinatami v polju $L \supseteq K$, ki ustrezajo enačbi (2.1), bomo označili z $E(L)$. Po definiciji je v tej množici tudi posebna točka, ki jo bomo označili z ∞ (več o tem v nadaljevanju), namreč

$$E(L) = \{\infty\} \cup \{(x, y) \in L \times L \mid y^2 = x^3 + Ax + B\}. \tag{2.2}$$

Grafa eliptične krivulje si ne moremo smiselno predstavljati, zato, da bi lažje razumeli koncept, si ga lahko ponazorimo tako, da ga definiramo nad realnimi števili. Glavni obliki sta dve (Slika 2.1): graf (a), ki ima tri različne realne ničle in graf (b), ki ima eno realno ničlo.

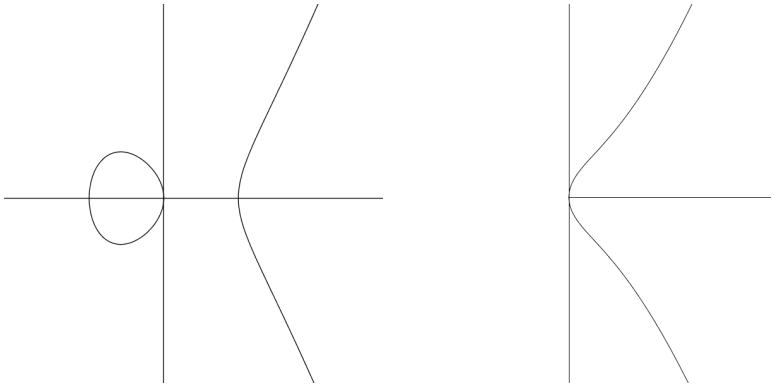
Možnosti večkratnih ničel ne dopustimo. Predpostaviti moramo namreč, da je

$$4A^3 + 27B^2 \neq 0. \tag{2.3}$$

Če so ničle kubične enačbe r_1, r_2 in r_3, potem se da pokazati, da je diskriminanta enačbe

$$((r_1 - r_2)(r_1 - r_3)(r_2 - r_3))^2 = -(4A^3 + 27B^2). \tag{2.4}$$

Če je torej $4A^3 + 27B^2 \neq 0$, so ničle paroma različne.



Slika 2.1: Grafa (a) $y^2 = x^3 - x$ in (b) $y^2 = x^3 + x$.

Posplošeni enačbi oblike

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

kjer so $a_1, \ldots, a_6$ konstante vrednosti, pravimo **posplošena Weierstrassova enačba**. Uporabljamo jo, ko je eliptična krivulja E definirana nad poljem karakteristike 2 ali 3. Če karakteristika polja ni enaka 2, potem lahko delimo z 2, da dobimo:

$$\left(y + \frac{a_1x}{2} + \frac{a_3}{2}\right)^2 = x^3 + \left(a_2 + \frac{a_1^2}{4}\right)x^2 + \left(a_4 + \frac{a_1a_3}{2}\right)x + \left(\frac{a_3^2}{4} + a_6\right),$$

kar se lahko zapiše kot

$$y_1^2 = x^3 + a_2'x^2 + a_4'x + a_6', \tag{2.6}$$

kjer je $y_1 = y + \frac{a_1x}{2} + \frac{a_3}{2}$ in a_2', a_4', a_6' so konstantne vrednosti. V kolikor karakteristika ni 3, bomo za $x_1 = x + \frac{a_2'}{3}$ dobili

$$y_1^2 = x_1^3 + Ax_1 + B,$$

za neki konstanti A in B.

Da bi si poenostavili stvari, bomo od sedaj naprej privzeli (v kolikor ni drugače zapisano), da je eliptična krivulja podana v Weierstrassovi obliki.

Zaradi tehničnih razlogov je izjemnega pomena dodati eliptični krivulji točko ∞. Glavni in najbolj pomemben razlog, da to počnemo, bo razviden v Izreku 2.2. Ta pa mora upoštevati določena pravila, katera bomo v nadaljevanju definirali.

2.2 Zakon grupe

Da bi lažje in učinkovitejše razumeli pojem eliptičnih krivulj, bomo privzeli, da je E definirana nad poljem $\mathbf{R}$. Pozneje bomo naša opažanja posplošili na poljubno polje.

V množici $E(\mathbf{R})$ lahko iz dveh točk oziroma iz ene točke dobimo novo točko. V nadaljevanju bomo natančneje analizirali ta proces.

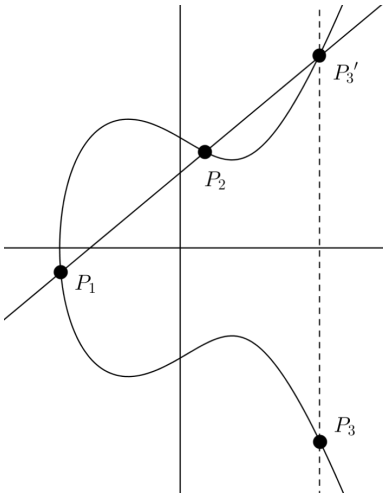
Naj bosta

$$P_1 = (x_1, y_1), \quad P_2 = (x_2, y_2)$$

točki eliptične krivulje E, ki je podana z enačbo $y^2 = x^3 + Ax + B$. Definirali bomo sedaj novo točko P_3 na sledeči način. Privzemimo najprej, da je $x_1 \neq x_2$. Potegnimo premico L skozi točki P_1 in P_2. Opazimo, da L seka E v še eni točki. Prezrcalimo dobljeno točko P_3' preko x-osi, da dobimo točko P_3. Definirajmo

$$P_1 + P_2 = P_3.$$

Opozoriti moramo, da tovrstno seštevanje ni enako seštevanju koordinat točk.



Slika 2.2: Seštevanje točk P_1 in P_2 na eliptični krivulji.

Poiščimo sedaj koordinate točke $P_3 = P_1 + P_2$.

Potegnimo premico L skozi P_1 in P_2. Njen smerni koeficient je

$$m = \frac{y_2 - y_1}{x_2 - x_1}.$$

Enačba premice L je

$$y = m(x - x_1) + y_1.$$

Sledi

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

Če preuredimo, dobimo

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

Ničle kubične enačbe so x-kordinate presečnih točk premice L in krivulje E. V splošnem je reševanje kubične enačbe zahteven proces, vendar imamo pomembno prednost, saj že poznamo dve ničli. Da se pokazati, da v kolikor imamo kubično enačbo x^3+ax^2+bx+c z ničlami r, s, t, potem je

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

Opazimo torej, da je

$$r + s + t = -a.$$

Ker poznamo dve ničli $r = x_1, s = x_2$, potem lahko pridobimo tretjo ničlo kot $x_3' = -a - x_1 - x_2$.

V našem primeru dobimo

$$x_3' = m^2 - x_1 - x_2$$

in

$$y_3' = m(x_3' - x_1) + y_1.$$

Prezrcalimo sedaj točko preko x-osi, da dobimo točko $P_3 = (x_3, y_3)$:

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

V primeru, ko je $x_1 = x_2$ in $y_1 \neq y_2$ je premica, ki gre skozi P_1 in P_2 vertikalna in seka E samo v točkah P_1 in P_2. V tem primeru definiramo $P_1 + P_2 = \infty$.

Predpostavimo sedaj, da je $P_1 = P_2 = (x_1, y_1)$. V tem primeru bomo za premico L vzeli tangento na krivuljo E v točki P_1. Z uporabo implicitnega odvajanja lahko najdemo smerni koeficient m premice L:

$$2y\frac{dy}{dx} = 3x^2 + A, \quad \text{torej} \quad m = \frac{dy}{dx} = \frac{3x_1^2 + A}{2y_1}.$$

Če je $y_1 = 0$, potem je premica vertikalna in definiramo, da je $P_1 + P_1 = \infty$. (*Tehnična opomba*: če je $y_1 = 0$, potem je števec $3x_1^2 + A \neq 0$. Glej [26, Exercise 2.5].) Predpostavimo torej, da je $y_1 \neq 0$. Enačba premice L je

$$y = m(x - x_1) + y_1.$$

Dobimo kubično enačbo

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

V tem primeru poznamo le eno ničlo oziroma x_1, ki pa je dvojna ničla. Iz tega sledi

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

Za konec predpostavimo, da je $P_2 = \infty$. Premica, ki gre skozi P_1 in ∞ je vertikalna in seka E v P_1', ki pa je zrcalna točka točke P_1. Poenostavljeno

$$P_1 + \infty = P_1$$

za vsako točko P_1 iz E. Enako velja za točko ∞, namreč $\infty + \infty = \infty$.

Dobljene rezultate bolj pregledno izpostavimo:

Definicija 2.1 (Zakon grupe)**.** Naj bo E eliptična krivulja definirana kot $y^2 = x^3 + Ax + B$. Naj bosta $P_1 = (x_1, y_1)$ in $P_2 = (x_2, y_2)$ točki v $E(L)$ in $P_1, P_2 \neq \infty$. Seštevanje v množici $E(L)$, i.e. $P_1 + P_2 = P_3 = (x_3, y_3)$, definiramo na naslednji način.

1. Če je $x_1 \neq x_2$, potem naj bo
$$x_3 = m^2 - x_1 - x_2, \quad y_3 = m(x_1 - x_3) - y_1, \quad \text{kjer je } m = \frac{y_2 - y_1}{x_2 - x_1}.$$
2. Če je $x_1 = x_2$ in $y_1 \neq y_2$, potem je $P_1 + P_2 = \infty$.
3. Če je $P_1 = P_2$ in $y_1 \neq 0$, potem naj bo
$$x_3 = m^2 - 2x_1, \quad y_3 = m(x_1 - x_3) - y_1, \quad \text{kjer je } m = \frac{3x_1^2 + A}{2y_1}.$$
4. Če je $P_1 = P_2$ in $y_1 = 0$, potem naj bo $P_1 + P_2 = \infty$.

Dodatno definiramo

$$P + \infty = P$$

za poljubno točko $P \in E(L)$.

Opazimo, da če sta $P_1, P_2 \in E(L)$, potem je tudi $P_1 + P_2 \in E(L)$. Sledi, da je $E(L)$ zaprta za zgoraj definirano seštevanje točk.

Pomembno je izpostaviti naslednje dejstvo: dobljeni rezultati ne veljajo le za eliptične krivulje definirane nad $\mathbf{R}$, ampak za poljubno polje K!

Iz definicije postaja jasno, da je točka ∞ ključnega pomena. O tem se bomo prepričali v naslednjem izreku.

Izrek 2.2. *Naj bo E eliptična krivulja $y^2 = x^3 + Ax + B$ nad poljem K. Seštevanje točk v $E(L)$ zadošča naslednjim lastnostim:*

1. *(komutativnost)* $P_1 + P_2 = P_2 + P_1$ *za poljubni točki* $P_1, P_2 \in E(L)$.
2. *(obstoj nevtralnega elementa)* $P + \infty = P$ *za poljubno točko* $P \in E(L)$.
3. *(obstoj inverzov) Za poljuno točko* $P \in E(L)$ *obstaja točka* $P' \in E(L)$*, tako da je* $P + P' = \infty$. P' *bomo poimenovali* $-P$.
4. *(asociativnost)* $(P_1+P_2)+P_3 = P_1+(P_2+P_3)$ *za poljubne točke* $P_1, P_2, P_3 \in E(L)$.

Z drugimi besedami, točke množice $E(L)$ *za tako definirano operacijo* $+$ *tvorijo aditivno abelovo grupo z nevrtralnim elementom* ∞.

Dokaz. Komutativnost je očitna, saj sledi neposredno iz formul ali iz dejstva, da je premica skozi P_1 in P_2 enaka premici, ki gre skozi P_2 in P_1. Točka (2) drži po definiciji. Za inverzne elemente pa naj bo P' zrcalna točka točke P preko x-osi. Potem je $P+P' = \infty$.
Asociativnost seštevanja lahko preverimo tako, da za poljubne točke $P_1, P_2, P_3 \in E(L)$ preverimo, da je $P_1+(P_2+P_3) = (P_1+P_2)+P_3$. Zaradi elementarnega in dolgotrajnega računaja, bomo dokaz enačbe izpustili. □

Opomba 2.3. Za Weierstrasovo enačbo velja, da če je $P = (x, y)$, potem je $-P = (x, -y)$. Za posplošeno Weierstrassovo enačbo (2.5) pa v splošnem ta lastnost ne velja. Če je $P = (x, y)$ na krivulji oblike (2.5), potem je

$$-P = (x, -a_1x - a_3 - y),$$

(glej [26, Exercise 2.9]).

Če je P točka na eliptični krivulji in je k pozitivno celo število, potem je $kP = P + P + \cdots + P$ (k krat). Če je $k < 0$, potem je $kP = (-P) + (-P) + \cdots + (-P)$ ($|k|$ krat). Da bi na hiter način izračunali kP, si lahko pomagamo s posebno metodo. Za primer lahko izračunamo $19P$:

$$2P, \quad 4P = 2P + 2P, \quad 8P = 4P + 4P, \quad 16P = 8P + 8P, \quad 19P = 16P + 2P + P.$$

Ta metoda nam pomaga, da rezultat dobimo v relativno kratkem času. Težava nastane takrat, ko delamo z racionalnimi ali realnimi števili, saj koordinate točk narastejo relativno hitro. Težava izgine, ko delamo s končnim poljem, na primer $\mathbf{F}_p$, saj računamo po modulu p.

Omenjeno metodo lahko posplošimo na sledeči način:

Definicija 2.4. Naj bo k pozitivno celo število in naj bo P točka na eliptični krivulji. Sledeči postopek nam izračuna kP.

1. Začnemo z $a = k$, $B = \infty$, $C = P$.

2. Če je a sod, potem je $a = a/2$, $B = B$ in $C = 2C$.

3. Če je a lih, potem je $a = a - 1$, $B = B + C$ in $C = C$.

4. Če je $a \neq 0$, pojdimo nazaj na korak 2.

5. Output B.

Output B je enak kP (glej [26, Exercise 2.8]).

Po drugi strani, če je eliptična krivulja definirana nad končnim poljem in so nam podane točke P in kP, potem se izkaže, da je zelo težko izračunati vrednost števila k. Ta proces se imenuje **problem diskretnega logaritma** eliptičnih krivulj in predstavlja temelj kriptografskih aplikacij. Več o tem v naslednjih poglavjih.

2.3 Endomorfizmi

Naj bo $\overline{K}$ algebraično zaprtje polja K in naj bosta $R_1(x, y), R_2(x, y)$ racionalni funkciji (kvocienta polinomov) s koeficienti iz polja $\overline{K}$.

Endomorfizem krivulje E je homomorfizem $\alpha : E(\overline{K}) \to E(\overline{K})$, ki deluje na naslednji način:

$$\alpha(x, y) = (R_1(x, y), R_2(x, y)),$$

za poljubno točko $(x, y) \in E(\overline{K})$.

Ker je α homomorfizem, velja, da $\alpha(P_1 + P_2) = \alpha(P_1) + \alpha(P_2)$ za poljubni točki $P_1, P_2 \in E(\overline{K})$ in da je $\alpha(\infty) = \infty$. Predpostavili bomo, da je α netrivialen oziroma da obstaja (x, y), tako da je $\alpha(x, y) \neq \infty$. Trivialni endomorfizem, ki preslika vsako točko v ∞, bomo označili z 0.

Primer 2.5. Naj bo eliptična krivulja E, definirana nad poljem $\overline{K}$, podana kot $y^2 = x^3 + Ax + B$ in naj bo $\alpha : E(\overline{K}) \to E(\overline{K})$ definiran z $\alpha(P) = 2P$. Potem je α homomorfizem grupe $E(\overline{K})$ v grupo $E(\overline{K})$ in

$$\alpha(x, y) = (R_1(x, y), R_2(x, y)),$$

kjer je

$$R_1(x, y) = \left(\frac{3x^2 + A}{2y}\right)^2 - 2x$$
$$R_2(x, y) = \left(\frac{3x^2 + A}{2y}\right)\left(3x - \left(\frac{3x^2 + A}{2y}\right)^2\right) - y.$$

Ker je α homomorfizem, podan z racionalnimi funkcijami, je α endomorfizem krivulje E. ◊

Izkaže se, da je zelo uporabno imeti določeno standardno obliko za racionalne funkcije. Naj bo $R(x,y)$ poljubna racionalna funkcija. Ker je $y^2 = x^3 + Ax + B$ za poljuben $(x,y) \in E(\overline{K})$, lahko zapišemo vsako sodo potenco od y s polinomom v x in vsako liho potenco od y z y krat nek polinom v x, da bi dobili racionalno funkcijo, ki je identična funkciji $R(x,y)$ na točkah v $E(\overline{K})$. Predpostavimo lahko torej, da je

$$R(x,y) = \frac{p_1(x) + p_2(x)y}{p_3(x) + p_4(x)y}.$$

Še več, imenovalec racionaliziramo lahko tako, da pomnožimo števec in imenovalec s $p_3 - p_4 y$ in nato zapišemo y^2 v obliki $x^3 + Ax + B$. Sledi

$$R(x,y) = \frac{q_1(x) + q_2(x)y}{q_3(x)}. \tag{2.7}$$

Poglejmo sedaj endomorfizem podan kot

$$\alpha(x,y) = (R_1(x,y), R_2(x,y)).$$

Ker je α homomorfizem, velja

$$\alpha(x,-y) = \alpha(-(x,y)) = -\alpha(x,y).$$

To pomeni, da je

$$R_1(x,-y) = R_1(x,y) \quad \text{in} \quad R_2(x,-y) = -R_2(x,y).$$

Torej, to pomeni, da če je R_1 zapisan v obliki (2.7), potem je $q_2(x) = 0$, in če je R_2 zapisan v obliki (2.7), potem je pripadajoč $q_1(x) = 0$. Zato lahko privzememo, da je

$$\alpha(x,y) = (r_1(x), r_2(x)y)$$

z racionalnimi funkcijami $r_1(x), r_2(x)$.

Kaj se pa zgodi, ko ena od racionalnih funkcij ni definirana na določeni točki? Zapišimo

$$r_1(x) = p(x)/q(x), \tag{2.8}$$

tako da polinoma $p(x)$ in $q(x)$ nimata skupnega faktorja. Če je $q(x) = 0$ za določeno točko (x,y), potem privzememo, da je $\alpha(x,y) = \infty$. Če je $q(x) \neq 0$, potem lahko iz [26, Exercise 2.19] opazimo, da je $r_2(x)$ definiran.

Naj bosta polinoma $p(x), q(x)$ kot v enačbi (2.8) in naj bo $\deg p(x)$ oziroma $\deg q(x)$, stopnja polinoma $p(x)$ oziroma $q(x)$. **Stopnjo** endomorfizma α definiramo kot

$$\deg(\alpha) = \max\{\deg p(x), \deg q(x)\},$$

če je α netrivialen. Ko je $\alpha = 0$, naj bo $\deg(0) = 0$. Pravimo, da je $\alpha \neq 0$ **separabilen** endomorfizem, ko je odvod od $r_1'(x) \neq 0$. To je ekvivalentno trditvi: vsaj eden od $p'(x)$ in $q'(x)$ ni enak 0. Glej [26, Exercise 2.22]. (V karakteristiki 0 bo nekonstantni polinom imel neničeln odvod. V karakteristiki $p > 0$ so polinomi z ničelnimi odvodi natanko tisti, ki so oblike $g(x^p)$.)

Primer 2.6. Nadaljevali bomo z naslednjim primerom, kjer je $\alpha(P) = 2P$. Kot smo videli zgoraj, velja

$$R_1(x, y) = \left(\frac{3x^2 + A}{2y}\right)^2 - 2x.$$

Z dejstvom, da je $y^2 = x^3 + Ax + B$ in algebraičnim računanjem dobimo

$$r_1(x) = \frac{x^4 - 2Ax^2 - 8Bx + A^2}{4(x^3 + Ax + B)}.$$

Opazimo, da je $\deg(\alpha) = 4$. Polinom $q'(x) = 4(3x^2 + A)$ ni enak 0 (niti v karakteristiki 3, saj velja, da če je $A = 0$, potem ima $x^3 + B$ večkratne ničle, kar je v nasprotju s predpostavko). Sledi, da je α separabilen. ◊

Pomemben primer endomorfizma je **Frobeniusova preslikava**. Predpostavimo, da je krivulja E definirana nad končnim poljem $\mathbf{F}_q$. Naj bo

$$\phi_q : \overline{\mathbf{F}}_q \to \overline{\mathbf{F}}_q, \quad \phi_q(x, y) = (x^q, y^q).$$

Frobeniusova preslikava ϕ_q ima zelo pomembno vlogo pri teoriji eliptičnih krivulj nad $\mathbf{F}_q$.

V nadaljevanju sledita lema in trditev, katerih ne bomo dokazali zaradi enostavnega in dolgotrajnega računanja. Kljub temu pa sta dokaza na lep način opisana v [26, stran 53–54].

Lema 2.7. *Naj bo krivulja E definirana nad poljem $\mathbf{F}_q$. Potem je ϕ_q endomorfizem krivulje E stopnje q, ter ϕ_q ni separabilen.*

Naslednja trditev bo ključnega pomena pri dokazu Hassejevega izreka v naslednjem poglavju.

Trditev 2.8. *Naj bo $\alpha \neq 0$ separabilen endomorfizem eliptične krivulje E. Potem je*

$$\deg \alpha = \#Ker(\alpha),$$

kjer je $Ker(\alpha)$ jedro homomorfizma $\alpha : E(\overline{K}) \to E(\overline{K})$ in je $\#Ker(\alpha)$ število elementov jedra $Ker(\alpha)$.

Če $\alpha \neq 0$ ni separabilen, potem je

$$\deg \alpha > \#Ker(\alpha).$$

Izrek 2.9. *Naj bo E eliptična krivulja definirana nad poljem K. Naj bo $\alpha \neq 0$ endomorfizem krivulje E. Potem je preslikava $\alpha : E(\overline{K}) \to E(\overline{K})$ surjektivna.*

Opomba 2.10. Obravnavanje eliptične krivulje nad $\overline{K}$ (in ne nad K) je izrednega pomena. Namreč, izkaže se, da množenje z 2 ne more biti surjetktivno nad $E(\mathbf{Q})$, če obstaja točka v $E(\mathbf{Q})$ z neskončnim redom. Intuitivno, obravnava eliptične krivulje nad zaprtim algebraičnim poljem nam porodi možnost reševanje enačb, ki so definirane z α, z namenom, da bi dobili prasliko točke.

Dokaz. Pokazali bomo, da za poljubno točko $(a, b) \in E(\overline{K})$ obstaja točka $(x, y) \in E(\overline{K})$, tako da je $\alpha(x, y) = (a, b)$.

Ker je $\alpha(\infty) = \infty$, lahko privzememo, da je $(a, b) \neq \infty$. Naj bo $r_1(x) = p(x)/q(x)$. Če $p(x) - aq(x)$ ni konstantni polinom, potem ima ničlo x_0. Ker p in q nimata skupne ničle, je $q(x_0) \neq 0$. Naj bo y_0 eden od dveh korenov elementa $x_0^3 + Ax_0 + B$. Potem je $\alpha(x_0, y_0)$ enak (a, b') za nek b' ([26, Exercise 2.19]). Ker $b'^2 = a^3 + Ax + B = b^2$, velja, da je $b = \pm b'$. Če je $b' = b$, potem smo končali. Če je $b' = -b$, potem je $\alpha(x_0, -y_0) = (a, -b') = (a, b)$.

Sedaj bomo obravnavali primer, ko je $p - aq$ konstanta. Ker je $E(\overline{K})$ neskončna in je jedro endomorfizma α končno, sledi, da se samo končno število točk v $E(\overline{K})$ lahko preslikajo v točko z dano x-koordinato. Ker $p(x)$ in $q(x)$ ne moreta biti hkrati konstanti, sledi, da $p(x)$ ali $q(x)$ ni konstanta. Če sta p in q dva nekonstantna polinoma, potem obstaja največ ena konstanta a, tako da je $p - aq$ konstanta (če je a' poleg a tudi tako število, potem je $(a' - a)q = (p - aq) - (p - a'q)$ konstanta in je $(a' - a)p = a'(p - aq) - a(p - a'q)$ konstanta, kar pomeni, da sta p in q konstanti). Sklepamo, da obstajata največ dve točki, (a, b) in $(a, -b)$ za nek b , ki ne pripadata sliki endomorfizma α. Naj bo (a_1, b_1) poljubna druga točka. Potem je $\alpha(P_1) = (a_1, b_1)$ za nek P_1. Izberemo lahko (a_1, b_1), tako da je $(a_1, b_1) + (a, b) \neq (a, \pm b)$, torej obstaja P_2, za katero velja, da je $\alpha(P_2) = (a_1, b_1) + (a, b)$. Sledi, da je $\alpha(P_2 - P_1) = (a, b)$ in $\alpha(P_1 - P_2) = (a, -b)$. Sklepamo, da je α surjektivna. □

Prišli smo do trenutka, ko moramo določiti bolj pregleden in učinkovit kriterij za separabilnost. Naj bo (x, y) poljubna točka, ki zadošča enačbi $y^2 = x^3 + Ax + B$. Potem lahko odvajamo y glede na x, da dobimo

$$2yy' = 3x^2 + A.$$

Podobno lahko odvajamo racionalno funkcijo $f(x, y)$ glede na x:

$$\frac{d}{dx} f(x, y) = f_x(x, y) + f_y(x, y)y',$$

kjer sta f_x in f_y parcialna odvoda.

Lema 2.11. *Naj bo E eliptična krivulja $y^2 = x^3 + Ax + B$. Naj bo $(u, v) \in E(\overline{K})$. Zapišimo*

$$(x, y) + (u, v) = (f(x, y), g(x, y)),$$

kjer sta $f(x,y)$ in $g(x,y)$ racionalni funkciji spremenljivk x, y (koeficienti so odvisni od (u,v)) in obravnavajmo y kot funkcijo v spremenljivki x, ki zadošča $dy/dx = (3x^2 + A)/(2y)$. Potem je

$$\frac{\frac{d}{dx}f(x,y)}{g(x,y)} = \frac{1}{y}.$$

Dokaz. Formule za seštevanje nam dajo

$$\begin{aligned} f(x,y) &= \left(\frac{y-v}{x-u}\right)^2 - x - u \\ g(x,y) &= \frac{-(y-v)^3 + x(y-v)(x-u)^2 + 2u(y-v)(x-u)^2 - v(x-u)^3}{(x-u)^3} \\ \frac{d}{dx}f(x,y) &= \frac{2y'(y-v)(x-u) - 2(y-v)^2 - (x-u)^3}{(x-u)^3}. \end{aligned}$$

Z elementarnim in dolgotrajnim računanjem in z uporabo dejstva, da je $2yy' = 3x^2 + A$, dobimo

$$\begin{aligned} &(x-u)^3(y\frac{d}{dx}f(x,y) - g(x,y)) = \\ &v(Au + u^3 - v^2 - Ax - x^3 + y^2) + y(-Au - u^3 + v^2 + Ax + x^3 - y^2). \end{aligned}$$

Ker sta točki $(u,v), (x,y) \in E(\overline{K})$, dobimo $v^2 = u^3 + Au + B$ in $y^2 = x^3 + Ax + B$. Zato zgornja enačba postane

$$v(-B + B) + y(B - B) = 0.$$

Sledi, da je $y\frac{d}{dx}f(x,y) = g(x,y)$. □

Lema 2.12. *Naj bodo $\alpha_1, \alpha_2, \alpha_3$ neničelni endomorfizmi eliptične krivulje E, za katere velja $\alpha_1 + \alpha_2 = \alpha_3$. Zapišimo*

$$\alpha_j(x,y) = (R_j(x), yS_j(x)).$$

Privzemimo, da obstajata taki konstanti c_1, c_2, da je

$$\frac{R_1'(x)}{S_1(x)} = c_1, \quad \frac{R_2'(x)}{S_2(x)} = c_2.$$

Potem je

$$\frac{R_3'(x)}{S_3(x)} = c_1 + c_2.$$

Dokaz. Naj bo $(x,y) \in E(\overline{K})$. Zapišimo

$$(x_1, y_1) = \alpha_1(x,y), \quad (x_2, y_2) = \alpha_2(x,y)$$

in

$$(x_3, y_3) = (x_1, y_1) + (x_2, y_2).$$

Potem sta x_3 in y_3 racionalni funkciji od x_1, y_1, x_2, y_2. x_1, y_1 in x_2, y_2 pa so racionalne funkcije od x, y. Po Lemi 2.11 in s predpostavko, da je $(u, v) = (x_2, y_2)$, velja

$$\frac{\partial x_3}{\partial x_1} + \frac{\partial x_3}{\partial y_1}\frac{dy_1}{dx_1} = \frac{y_3}{y_1}.$$

Podobno,

$$\frac{\partial x_3}{\partial x_2} + \frac{\partial x_3}{\partial y_2}\frac{dy_2}{dx_2} = \frac{y_3}{y_2}.$$

Zaradi predpostavke je

$$\frac{dx_j}{dx} = c_j\frac{y_j}{y}$$

za $j = 1, 2$. Zaradi verižnega pravila je

$$\begin{aligned}\frac{dx_3}{dx} &= \frac{\partial x_3}{\partial x_1}\frac{dx_1}{dx} + \frac{\partial x_3}{\partial y_1}\frac{dy_1}{dx_1}\frac{dx_1}{dx} + \frac{\partial x_3}{\partial x_2}\frac{dx_2}{dx} + \frac{\partial x_3}{\partial y_2}\frac{dy_2}{dx_2}\frac{dx_2}{dx}\\ &= \frac{y_3}{y_1}\frac{y_1}{y}c_1 + \frac{y_3}{y_2}\frac{y_2}{y}c_2\\ &= (c_1 + c_2)\frac{y_3}{y}.\end{aligned}$$

Za konec delimo z $\dfrac{y_3}{y}$ in dobimo želeni rezultat. □

Opomba 2.13. Da se pokazati, da poljuben neničelni endomorfizem α zadošča hipotezi Leme 2.12. Vendar bomo dokaz izpustili.

Trditev 2.14. *Naj bo E eliptična krivulja definirana nad poljem K, in naj bo n neničelno celo število. Predpostavimo, da je množenje z n na krivulji E podano kot*

$$n(x, y) = (R_n(x), yS_n(x))$$

za poljuben $(x, y) \in E(\overline{K})$, kjer sta R_n in S_n racionalni funkciji. Potem je

$$\frac{R_n'(x)}{S_n(x)} = n.$$

Sledi, da je množenje z n separabilno natanko tedaj, ko n ni večkratnik karakteristike p polja K.

Dokaz. Ker je $R_{-n} = R_n$ in $S_{-n} = -S_n$, sklepamo lahko, da je $R'_{-n}/S_{-n} = -R'_n/S_n$.

Opaziti moramo, da prvi del trditve trivialno velja za $n = 1$. Če velja za n, potem Lema 2.12 implicira, da velja za $n + 1$, kar je seštevek od n in 1. Sledi, $\frac{R_n'(x)}{S(x)} = n$ za poljuben n.

Velja, da je $R_n'(x) \neq 0$ natanko takrat, ko je $n = R_n'/S_n(x) \neq 0$, kar je ekvivalentno trditi, da p ne deli n. Po definiciji separabilnosti je $R_n' \neq 0$; s tem pa smo dokazali še drugi del trditve. □

Predstavili bomo sedaj, s pomočjo Leme 2.12, še zadnjo trditev v tem podpoglavju, ki bo v nadaljevanju pomembna pri dokazu Hassejevega izreka.

Trditev 2.15. *Naj bo E eliptična krivulja definirana nad poljem $\mathbf{F}_q$, kjer je q potenca praštevila p. Naj bosta r in s celi števili, ki nista hkrati enaki 0. Endomorfizem $r\phi_q + s$ je separabilen natanko takrat, ko $p \nmid s$.*

Dokaz. Zapišimo množenje z r kot

$$r(x, y) = (R_r(x), yS_r(x)).$$

Potem je

$$\begin{aligned}(R_{r\phi_q}(x), yS_{r\phi_q}(x)) &= (\phi_q r)(x, y) = (R_r^q(x), y^q S_r^q(x)) \\ &= \left(R_r^q(x), y(x^3 + Ax + B)^{(q-1)/2} S_r^q(x)\right).\end{aligned}$$

Torej,

$$c_{r\phi_q} = R'_{r\phi_q}/S_{r\phi_q} = qR_r^{q-1}R'_r/S_{r\phi_q} = 0.$$

Iz Trditve 2.14 velja, da je $c_s = R'_s/S_s = s$. Po Lemi 2.12 je

$$R'_{r\phi_q+s}/S_{r\phi_q+s} = c_{r\phi_q+s} = c_{r\phi_q} + c_s = 0 + s = s.$$

Torej je $R'_{r\phi_q+s} \neq 0$ natanko tedaj, ko $p \nmid s$. □

2.4 Torzijske točke

Naj bo E eliptična krivulja nad poljem K. Torzijske točke eliptične krivulje E so točke končnega reda. Te imajo pomembno vlogo pri študiju eliptičnih krivulj. Kot bomo videli v nadeljevanju, za poljubno eliptično krivuljo nad končnim poljem velja, da so vse njene točke torzijske.

Naj bo E eliptična krivulja definirana nad poljem K. Naj bo n pozitivno celo število. Množico torzijskih točk reda n definiramo kot

$$E[n] = \{P \in E(\overline{K}) \mid nP = \infty\}$$

(spomnimo se, da je $\overline{K}$ algebraično zaprtje polja K). S tem želimo poudariti, da $E[n]$ vsebuje točke s koordinatami polja $\overline{K}$ in ne samo iz polja K.

Primer 2.16. Naj bo E eliptična krivulja nad poljem K. Poiščimo $E[2]$.

Naj bo karakteristika polja K različna od 2. Sledi, da enačbo krivulje E lahko spremenimo v obliko (2.6). Naj bo

$$y^2 = (x - e_1)(x - e_2)(x - e_3),$$

kjer so $e_1, e_2, e_3 \in \overline{K}$. Točka P zadošča $2P = \infty$ natanko tedaj, ko je tangentna premica na krivulji E v točki P vertikalna. Z drugimi besedami je $y = 0$ in sledi

$$E[2] = \{\infty, (e_1, 0), (e_2, 0), (e_3, 0)\}.$$

Ta grupa je izomorfna grupi $\mathbf{Z}_2 \oplus \mathbf{Z}_2$, kjer je $\oplus$ direktna vsota dveh grup.

Naj bo sedaj karakteristika polja K enaka 2. Sledi, da lahko E spremenimo v eno izmed teh dveh oblik (glej [26, Section 2.8]):

1. $y^2 + xy + x^3 + a_2x^2 + a_6 = 0$ ali
2. $y^2 + a_3y + x^3 + a_4x + a_6 = 0$.

V prvem primeru je $a_6 \neq 0$ in v drugem primeru je $a_3 \neq 0$ (sicer bi krivulje bile singularne[1]). Če je $P = (x, y)$ točka reda 2, potem mora tangenta na krivulji E v točki P biti vertikalna, kar pomeni, da mora parcialni odvod na y biti enak 0. To pomeni, da v prvem primeru je $x = 0$. Substituiramo sedaj $x = 0$ v prvem primeru in dobimo $0 = y^2 + a_6 = (y + \sqrt{a_6})^2$. Sledi, da je $(0, \sqrt{a_6})$ edina točka reda 2 (kvadratni koreni so enolično določeni v polju karakteristike 2), in tako

$$E[2] = \{\infty, (0, \sqrt{a_6})\}.$$

Ta grupa je izomorfna grupi $\mathbf{Z}_2$.

V drugem primeru je parcialni odvod na y enak $a_3 \neq 0$. Sledi, da ne obstaja točka reda 2, in tako

$$E[2] = \{\infty\}.$$

$\Diamond$

Poglejmo sedaj posplošitev za $E[n]$.

Izrek 2.17. *Naj bo E eliptična krivulja nad poljem K in n pozitivno celo število. Če karakteristika polja K ne deli n, ali je enaka 0, potem je*

$$E[n] \simeq \mathbf{Z}_n \oplus \mathbf{Z}_n,$$

kjer je $\oplus$ direktna vsota dveh grup. Če je karakteristika polja K $p > 0$ in $p|n$, potem napišimo $n = p^r n'$, kjer $p \nmid n'$. Sledi, da je

$$E[n] \simeq \mathbf{Z}_{n'} \oplus \mathbf{Z}_{n'} \quad \text{ali} \quad \mathbf{Z}_n \oplus \mathbf{Z}_{n'}.$$

Dokaz izreka najdemo v [26, Section 3.2].

Pravimo, da je eliptična krivulja E nad poljem K s karakteristiko p navadna, če je $E[p] \simeq \mathbf{Z}_p$. Pravimo ji pa **supersingularna**, če je $E[p] \simeq \{\infty\}$.

Opomba 2.18. Besedi *supersingularen* in *singularen* nista smiselno povezani.

[1]Točka (a, b) eliptične krivulje $f(x, y) = 0$ je singularna natanko tedaj, ko sta oba parcialna odvoda funkcije f enaka 0 v točki (a, b), sicer je nesingularna. Eliptična krivulja je singularna natanko tedaj, ko ima singularno točko in je nesingularna natanko tedaj, ko so vse njene točke nesingularne. Če je eliptična krivulja nesingularna, potem nima večkratnih ničel.

2.5 Weilovo prirejanje

Naj bo E eliptična krivulja nad poljem K in n tako celo število, da ni deljivo s karakteristiko polja K. Potem je $E[n] \simeq \mathbf{Z}_n \oplus \mathbf{Z}_n$. Naj bo

$$\mu_n = \{x \in \overline{K} \mid x^n = 1\}$$

grupa n-tih korenov enote v polju $\overline{K}$. Ker karakteristika polja K ne deli n, sledi, da enačba $x^n = 1$ nima večkratnih ničel oziroma je število n-tih korenov v $\overline{K}$ enako n. Torej je μ_n ciklična grupa reda n. Elementu $\zeta \in \mu_n$ pravimo **primitivni n-ti koren enote**, če velja, da je $\zeta^k = 1$ natanko tedaj, ko n deli k. Z drugimi besedami je ζ generator grupe μ_n.

Izrek 2.19. *Naj bo E eliptična krivulja definirana nad poljem K in naj bo n pozitivno celo število. Predpostavimo, da karakteristika polja K ne deli n. Potem obstaja prirejanje*

$$e_n : E[n] \times E[n] \to \mu_n,$$

*ki ga imenujemo **Weilovo prirejanje** in zadošča naslednjim lastnostim:*

1. *e_n je bilinearen za obe spremenljivki. To pomeni, da je*

$$e_n(S_1 + S_2, T) = e_n(S_1, T)e_n(S_2, T)$$

   in

$$e_n(S, T_1 + T_2) = e_n(S, T_1)e_n(S, T_2)$$

   za poljubne $S, S_1, S_2, T, T_1, T_2 \in E[n]$.

2. *e_n je nedegeneriran za obe spremenljivki. To pomeni, da če je $e_n(S, T) = 1$ za vsak $T \in E[n]$, potem je $S = \infty$ in tudi, da če $e_n(S, T) = 1$ za vsak $S \in E[n]$, potem je $T = \infty$.*

3. *$e_n(T, T) = 1$ za poljuben $T \in E[n]$.*

4. *$e_n(T, S) = e_n(S, T)^{-1}$ za poljubna $S, T \in E[n]$.*

5. *$e_n(\sigma S, \sigma T) = \sigma(e_n(S, T))$ za poljuben avtomorfizem σ polja $\overline{K}$, za katerega velja, da je σ identična preslikava na koeficientih krivulje E (če je enačba krivulje E v Weierstrassovi obliki, to pomeni, da je $\sigma(A) = A$ in $\sigma(B) = B$).*

6. *$e_n(\alpha(S), \alpha(T)) = e_n(S, T)^{\deg(\alpha)}$ za poljuben separabilen endomorfizem α krivulje E. Če koeficienti krivulje E pripadajo končnemu polju $\mathbf{F}_q$, potem trditev velja tudi, ko je α Frobeniusov endomorfizem ϕ_q. (V bistvu trditev velja za poljuben endomorfizem α, separabilen ali ne. Glej [8].)*

Dokaz izreka lahko najdemo v [26, Chapter 11], vendar ga mi ne bomo obravnavali. Sledijo zanimive posledice izreka.

Naj bo n pozitivno celo število, ki ni deljivo s karakteristiko polja K. Naj bo $\{T_1, T_2\}$ **baza** množice $E[n] \simeq \mathbf{Z}_n \oplus \mathbf{Z}_n$. To pomeni, da poljuben element množice $E[n]$ lahko zapišemo kot $m_1T_1 + m_2T_2$, kjer sta $m_1, m_2 \in \mathbf{Z}$. m_1 in m_2 sta enolično določena po modulu n.

Posledica 2.20. *Naj bo $\{T_1, T_2\}$ baza množice $E[n]$. Potem je $e_n(T_1, T_2)$ primitivni n-ti koren enote.*

Dokaz. Predpostavimo, da je $e_n(T_1, T_2) = \zeta$ in $\zeta^d = 1$. Potem je $e_n(T_1, dT_2) = 1$. Velja tudi, da je $e_n(T_2, dT_2) = e_n(T_2, T_2)^d = 1$ (iz točke (1) in (3)). Naj bo $S \in E[n]$. Potem je $S = aT_1 + bT_2$ za neki celi števili a, b. Sledi

$$e_n(S, dT_2) = e_n(T_1, dT_2)^a e_n(T_2, dT_2)^b = 1.$$

Ker to velja za poljubno točko $S \in E[n]$, točka (2) implicira, da je $dT_2 = \infty$. Ker je $dT_2 = \infty$ natanko tedaj, ko $n|d$, sledi, da je ζ primitiven n-ti koren enote. □

Posledica 2.21. *Če je $E[n] \subseteq E(K)$, potem je $\mu_n \subset K$.*

Opomba 2.22. Spomnimo se, da imajo lahko točke v $E[n]$ koordinate iz polja $\overline{K}$. Hipoteza posledice je ta, da imajo vse te točke koordinate iz polja K.

Dokaz. Naj bo σ poljuben avtomorfizem polja $\overline{K}$, za katerega velja, da je σ identiteta na polju K. Naj bosta T_1, T_2 baza za množico $E[n]$. Ker predpostavimo, da imata T_1 in T_2 koordinate iz polja K, dobimo, da je $\sigma T_1 = T_1$ in $\sigma T_2 = T_2$. Iz točke (5) sledi, da je

$$\zeta = e_n(T_1, T_2) = e_n(\sigma T_1, \sigma T_2) = \sigma(e_n(T_1, T_2)) = \sigma(\zeta).$$

Fundamentalni izrek Galoisove teorije nam pove, da če je element $x \in \overline{K}$ fiksiran za poljuben tak avtomorfizem σ, potem $x \in K$. Sledi, da $\zeta \in K$. Ker iz Posledice 2.20 velja, da je ζ primitivnen n-ti koren enote, sledi, da je $\mu_n \subset K$. □

Posledica 2.23. *Naj bo E eliptična krivulja definirana nad poljem $\mathbf{Q}$. Potem $E[n] \nsubseteq E(\mathbf{Q})$ za $n \geq 3$.*

Dokaz. Če je $E[n] \subseteq E(\mathbf{Q})$, potem je $\mu_n \subset \mathbf{Q}$, kar ne velja za $n \geq 3$. □

Opomba 2.24. Ko je $n = 2$, obstaja možnost, da je $E[2] \subseteq E(\mathbf{Q})$. Na primer, če je krivulja E podana kot $y^2 = x(x-1)(x+1)$, potem je

$$E[2] = \{\infty, (0,0), (1,0), (-1,0)\}.$$

Če je $n = 3, 4, 5, 6, 7, 8, 9, 10, 12$, potem obstajajo eliptične krivulje E definirane nad $\mathbf{Q}$, ki imajo točke z racionalnimi koordinatami in so reda n. Zgornja posledica pa nam pove, da ni možno, da bi vse točke reda n imele racionalne koordinate za n.

Prišli smo do točke, ko bomo s pomočjo Weilovega prirejanja obravnavali dve trditvi, ki bosta bistvenega pomena pri dokazu Hassejevega izreka v naslednjem poglavju.

Naj bo n pozitivno celo število, ki ni deljivo s karakteristiko polja K in naj bo $\{T_1, T_2\}$ baza množice $E[n] \simeq \mathbf{Z}_n \oplus \mathbf{Z}_n$. Naj bo $\alpha : E(\overline{K}) \to E(\overline{K})$ homomorfizem. Potem α slika iz $E[n]$ v $E[n]$. Torej obstajajo $a, b, c, d \in \mathbf{Z}_n$, takšni, da je

$$\alpha(T_1) = aT_1 + cT_2, \quad \alpha(T_2) = bT_1 + dT_2.$$

Delovanje homomorfizma α na $E[n]$ glede na bazo $\{T_1, T_2\}$ lahko predstavimo s pomočjo 2×2 matrike

$$\alpha_n = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Kompozitum homomorfizmov ustreza množenju pripadajočih matrik.

Trditev 2.25. *Naj bo α endomorfizem eliptične krivulje E definirana nad poljem K. Naj bo n pozitivno celo število, ki ni deljivo s karakteristiko polja K. Potem* $\det(\alpha_n) \equiv \deg(\alpha) \pmod{n}$.

Dokaz. Naj bo $\{T_1, T_2\}$ baza množice $E[n]$. Iz Posledice 2.20 sledi, da je $\zeta = e_n(T_1, T_2)$ primitiven n-ti koren enote. Iz točke (6) Izreka 2.19 in zaradi lastnosti Weilovega prirejanja velja, da je

$$\begin{aligned} \zeta^{\deg(\alpha)} &= e_n(\alpha(T_1), \alpha(T_2)) = e_n(aT_1 + cT_2, bT_1 + dT_2) \\ &= e_n(T_1, T_1)^{ab} e_n(T_1, T_2)^{ad} e_n(T_2, T_1)^{cb} e_n(T_2, T_2)^{cd} \\ &= \zeta^{ad-bc}. \end{aligned}$$

Ker je ζ primitiven n-ti koren enote, sledi, da je $\deg(\alpha) \equiv ad - bc \pmod{n}$. □

Sedaj bomo obravnavali Trditev 2.26, ki velja za poljubne endomorfizme, vendar bomo dokaz omejili le na separabilne endomorfizme in na vse endomorfizme oblike $r + s\phi_q$ s poljubnimi celimi števili r, s.

Naj bosta α in β endomorfizma krivulje E in a, b celi števili. Endomorfizem $a\alpha + b\beta$ je definiran kot

$$(a\alpha + b\beta)(P) = a\alpha(P) + b\beta(P).$$

$a\alpha(P)$ pomeni množenje $\alpha(P)$ s številom a na krivulji E. Rezultatu nato prištejemo še $b\beta(P)$. $a\alpha + b\beta$ je posledično tudi endomorfizem.

Trditev 2.26.

$$\deg(a\alpha + b\beta) = a^2 \deg \alpha + b^2 \deg \beta + ab(\deg(\alpha + \beta) - \deg \alpha - \deg \beta).$$

Dokaz. Naj bo n tako celo število, ki ni deljivo s karakteristiko polja K. Naj matriki α_n in β_n določata endomorfizma α in β (na podlagi določene baze množice $E[n]$). Potem endomorfizem $a\alpha_n + b\beta_n$ določa delovanje endomorfizma $a\alpha + b\beta$ na množici $E[n]$. S pomočjo elementarnega in dolgotrajnega računanja dobimo

$$\deg(a\alpha_n + b\beta_n) = a^2 \deg \alpha_n + b^2 \deg \beta_n + ab(\deg(\alpha_n + \beta_n) - \deg \alpha_n - \deg \beta_n)$$

za poljubno matriko α_n in β_n (glej [26, Exercise 3.4]). Sklepamo torej, da je

$$\begin{aligned}&\deg(a\alpha + b\beta) \equiv \\ &a^2 \deg \alpha + b^2 \deg \beta + ab(\deg(\alpha + \beta) - \deg \alpha - \deg \beta) \pmod{n}.\end{aligned}$$

Ker to velja za vsa števila n, sledi, da mora zgornja kongruenca postati enakost. □

Poglavje 3

Eliptične krivulje nad končnimi polji

V tem poglavju bomo obravnavali eliptične krivulje definirane nad končnim poljem $\mathbf{F}$. Predstavili bomo zanimive izreke in lastnosti, ki bodo izjemnega pomena pri obravnavi kasnejših kriptografskih aplikacij.

Najprej se moramo zavedati naslednjega dejstva. Ker obstaja končno mnogo parov (x, y), kjer $x, y \in \mathbf{F}$, potem je grupa $E(\mathbf{F})$ končna.

Primer 3.1. Naj bo eliptična krivulja E, definirana nad poljem $\mathbf{F}_5$, podana kot $y^2 = x^3 + x + 1$. Koliko je $\#E(\mathbf{F}_5)$?

Problem rešimo enostavno tako, da preverimo, katera $x, y \in \mathbf{F}_5$ ustrezata zgornji enačbi. Dobimo, da je

$$E(\mathbf{F}_5) = \{\infty, (0,1), (4,2), (2,1), (3,4), (3,1), (2,4), (4,3), (0,4)\}.$$

Ker je eliptična krivulja grupa za operacijo seštevanja točk, potem velja, da je $E(\mathbf{F}_5)$ izomorfna grupi $\mathbf{Z}_9$ ali $\mathbf{Z}_3 \oplus \mathbf{Z}_3$.

Izračunajmo sedaj $2(0,1) = (0,1) + (0,1)$. S pomočjo Definicije 2.1 dobimo, da je seštevek enak $(4,2)$.

Izračunajmo sedaj $3(0,1) = (4,2) + (0,1)$. Dobimo, da je seštevek enak $(2,1)$.

Ker red točke deli red grupe, mora biti red točke $(0,1)$ enak 9. To pomeni, da je $E(\mathbf{F}_5)$ izomorfna grupi $\mathbf{Z}_9$. Še več, $E(\mathbf{F}_5)$ je ciklična grupa generirana s točko $(0,1)$. $\Diamond$

Primer 3.2. Naj bo eliptična krivulja E, definirana nad poljem $\mathbf{F}_7$, podana kot $y^2 = x^3 + 2$. Potem je

$$E(\mathbf{F}_7) = \{\infty, (0,3), (0,4), (3,1), (3,6), (5,1), (5,6), (6,1), (6,6)\}.$$

Z elementarnim računanjem se da pokazati, da za poljubno točko $P \in E(\mathbf{F}_7)$ velja, da je $3P = \infty$. Sledi, da je $E(\mathbf{F}_7)$ izomorfna grupi $\mathbf{Z}_3 \oplus \mathbf{Z}_3$. $\Diamond$

Sledita dva pomembna izreka.

Izrek 3.3. *Naj bo eliptična krivulja E definirana nad končnim poljem $\mathbf{F}_q$. Potem je*

$$E(\mathbf{F}_q) \simeq \mathbf{Z}_n \text{ ali } \mathbf{Z}_{n_1} \oplus \mathbf{Z}_{n_2}$$

za neko celo število $n \geq 1$, ali za neki celi števili $n_1, n_2 \geq 1$, kjer n_1 deli n_2.

Dokaz. Končna abelova grupa je izomorfna direktni vsoti cikličnih grup

$$\mathbf{Z}_{n_1} \oplus \mathbf{Z}_{n_2} \oplus \cdots \oplus \mathbf{Z}_{n_r},$$

kjer $n_i | n_{i+1}$ za $i \geq 1$. Za poljuben i ima grupa $\mathbf{Z}_{n_i}$ n_1 elementov, za katere velja, da njihov red deli n_1. Iz tega sledi, da ima eliptična krivulja $E(\mathbf{F}_q)$ n_1^r elementov, za katere velja, da njihov red deli n_1. Iz Izreka 2.17 vemo, da obstaja največ n_1^2 tovrstnih točk (tudi če dopustimo možnost, da so koordinate iz polja $\overline{\mathbf{F}}_q$). Sledi, da je $r \leq 2$. □

Izrek 3.4 (Hasse)**.** *Naj bo eliptična krivulja E definirana nad končnim poljem $\mathbf{F}_q$. Potem velja*

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

Dokaz tega izreka bomo podali v naslednjem podpoglavju.

3.1 Frobeniusov endomorfizem

Naj bo $\mathbf{F}_q$ končno polje z algebraičnim zaprtjem $\overline{\mathbf{F}}_q$ in naj bo

$$\begin{array}{rccc} \phi_q : \overline{\mathbf{F}}_q & \longrightarrow & \overline{\mathbf{F}}_q, \\ x & \mapsto & x^q \end{array}$$

Frobeniusova preslikava za polje $\mathbf{F}_q$.

Naj bo eliptična krivulja E definirana nad poljem $\mathbf{F}_q$. Potem ϕ_q preslika točke iz krivulje $E(\overline{\mathbf{F}}_q)$ na naslednji način:

$$\phi_q(x, y) = (x^q, y^q), \quad \phi_q(\infty) = \infty.$$

Lema 3.5. *Naj bo krivulja E definirana nad poljem $\mathbf{F}_q$ in naj bo $(x, y) \in E(\overline{\mathbf{F}}_q)$. Potem*

1. *$\phi_q(x, y) \in E(\overline{\mathbf{F}}_q)$;*
2. *$(x, y) \in E(\mathbf{F}_q)$ natanko tedaj, ko je $\phi_q(x, y) = (x, y)$.*

Dokaz. Pri dokazu bomo uporabili dejstvo, da je $(a + b)^q = a^q + b^q$, kjer je q potenca karakteristike polja. Pomembno je tudi dejstvo, da je $a^q = a$ za poljuben $a \in \mathbf{F}_q$.

Dokaz je identičen za Weierstrassovo enačbo, kot tudi za posplošeno Weierstrassovo enačbo. Uporabili bomo zadnjo omenjeno obliko. Dobimo torej

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

kjer $a_i \in \mathbf{F}_q$. Potenciramo enačbo na q-to potenco, da bi dobili

$$(y^q)^2 + a_1(x^qy^q) + a_3(y^q) = (x^q)^3 + a_2(x^q)^2 + a_4(x^q) + a_6.$$

To pomeni, da (x^q, y^q) pripada krivulji E. Dokazali smo (1).

Spomnimo se sedaj, da $x \in \mathbf{F}_q$ natanko tedaj, ko je $\phi_q(x) = x$. Podobno velja za y. Sledi

$$\begin{aligned}(x,y) \in E(\mathbf{F}_q) &\Leftrightarrow x, y \in \mathbf{F}_q \text{ in } (x,y) \in E(\mathbf{F}_q)\\ &\Leftrightarrow \phi_q(x) = x,\ \phi_q(y) = y \text{ in } (x,y) \in E(\mathbf{F}_q)\\ &\Leftrightarrow \phi_q(x,y) = (x,y) \text{ in } (x,y) \in E(\mathbf{F}_q).\end{aligned}$$

□

Lema 3.6. *Naj bo eliptična krivulja E definirana nad poljem $\mathbf{F}_q$. Potem je endomorfizem ϕ_q krivulje E stopnje q, ki ni separabilen.*

Lema je enaka Lemi 2.7.

Jedro endomorfizma ϕ_q je trivialno. To je povezano z dejstvom, da ϕ_q ni separabilen. Glej Trditev 2.8.

Naslednja trditev je ključnega pomena pri izračunanju števila točk eliptičnih krivulj nad končnimi obsegi. Ker je ϕ_q endomorfizem krivulje E, sta potem to tudi $\phi_q^2 = \phi_q \circ \phi_q$ oziroma $\phi_q^n = \phi_q \circ \phi_q \circ \cdots \circ \phi_q$, za poljuben $n \geq 1$. Ker je množenje z -1 tudi endomorfizem, sledi, da je vsota $\phi_q^n - 1$ endomorfizem eliptične krivulje E.

Trditev 3.7. *Naj bo eliptična krivulja E definirana nad poljem $\mathbf{F}_q$ in naj bo $n \geq 1$. Potem velja:*

1. *$Ker(\phi_q^n - 1) = E(\mathbf{F}_{q^n})$;*
2. *$\phi_q^n - 1$ je separabilen endomorfizem, zato je $\#E(\mathbf{F}_{q^n}) = \deg(\phi_q^n - 1)$.*

Dokaz. Ker je ϕ_q^n Frobeniusova preslikava za polje $\mathbf{F}_{q^n}$, potem (1) sledi iz Leme 3.5. Dejstvo, da je preslikava $\phi_q^n - 1$ separabilna, smo dokazali v Trditvi 2.15. Zato (2) sledi iz Trditve 2.8. □

Dokaz Hassejevega izreka. Sedaj lahko dokažemo Hassejev izrek (Izrek 3.4). Naj bo

$$a = q + 1 - \#E(\mathbf{F}_q) = q + 1 - \deg(\phi_q - 1). \tag{3.1}$$

Želimo pokazati, da je $|a| \leq 2\sqrt{q}$. Potrebujemo naslednje:

Lema 3.8. *Naj bosta r, s celi števili z* $\gcd(s, q) = 1$. *Potem je* $\deg(r\phi_q - s) = r^2 q + s^2 - rsa$.

Dokaz. Trditev 2.26 implicira, da je

$$\deg(r\phi_q - s) = r^2 \deg(\phi_q) + s^2 \deg(-1) + rs(\deg(\phi_q - 1) - \deg(\phi_q) - \deg(-1)).$$

Ker je $\deg(\phi_q) = q$ in $\deg(-1) = 1$, rezultat sledi iz (3.1). □

Opomba 3.9. Predpostavka, da je $\gcd(s, q) = 1$ ni potrebna. Vključimo jo, ker Trditve 2.26 nismo dokazali v splošnem, ampak samo v primeru, ko so endomorfizmi separabilni ali oblike $r + s\phi_q$ s poljubnimi celimi števili r, s.

Sedaj lahko zaključimo dokaz Hassejevega izreka. Ker je $\deg(r\phi_q - s) \geq 0$, Lema 3.8 implicira, da je

$$q\left(\frac{r}{s}\right)^2 - a\left(\frac{r}{s}\right) + 1 \geq 0$$

za poljubna r, s, kjer velja $\gcd(s, q) = 1$. Množica racionalnih števil r/s, kjer je $\gcd(s, q) = 1$, je gosta v $\mathbf{R}$. Sledi

$$qx^2 - ax + 1 \geq 0$$

za vsa realna števila x. Torej mora biti diskriminanta pripadajoče kvadratne funkcije negativna ali 0, kar pomeni, da je $a^2 - 4q \leq 0$. Torej je $|a| \leq 2\sqrt{q}$. S tem smo zaključili dokaz Hassejevega izreka. □

Obstaja več opornih točk, s katerimi smo izpeljali zgornji dokaz. Ena od teh je identificiranje $E(\mathbf{F}_q)$ z jedrom endomorfizma $\phi_q - 1$. Druga je ta, da je $\phi_q - 1$ separabilen, iz katerega sledi, da je red jedra enak stopnji endomorfizma $\phi_q - 1$. Tretja oporna točka je Weilovo prirejanje, še posebej točka (6) Izreka 2.19 in njegova posledica, Trditev 2.26.

Iz Trditve 3.7 lahko izpeljemo naslednjo uporabno posledico.

Izrek 3.10. *Naj bo eliptična krivulja E definirana nad poljem $\mathbf{F}_q$. Naj bo a tak, kot v enačbi (3.1). Potem je*

$$\phi_q^2 - a\phi_q + q = 0$$

in a je enolično določeno celo število k, tako da je

$$\phi_q^2 - k\phi_q + q = 0.$$

Z drugimi besedami, če $(x, y) \in E(\overline{\mathbf{F}}_q)$, potem je

$$\left(x^{q^2}, y^{q^2}\right) - a(x^q, y^q) + q(x, y) = \infty,$$

in je a enolično določeno celo število, za katero enakost velja za poljuben $(x, y) \in E(\overline{\mathbf{F}}_q)$. Še več, a je enolično določeno celo število, za katero velja, da je

$$a \equiv \mathrm{Trace}((\phi_q)_m) \pmod{m},$$

za poljuben m z $\gcd(m, q) = 1$.

Dokaz. Če $\phi_q^2 - a\phi_q + q = 0$ ni ničelni endomorfizem, potem je jedro končno (Trditev 2.8). Pokazali bomo, da je jedro neskončno, torej, da je endomorfizem ničelni.

Naj bo $m \geq 1$ celo število z $\gcd(m, q) = 1$. Spomnimo se, da lahko predstavimo endomorfizem ϕ_q s pomočjo matrike $(\phi_q)_m$. Ta opisuje delovanje endomorfizma ϕ_q na $E[m]$. Naj bo

$$(\phi_q)_m = \begin{pmatrix} s & t \\ u & v \end{pmatrix}.$$

Ker je $\phi_q - 1$ separabilen po Trditvi 2.15, Trditvi 2.8 in 2.25 implicirata, da je

$$\begin{aligned} \#\mathrm{Ker}(\phi_q - 1) = \deg(\phi_q - 1) &\equiv \det((\phi_q)_m - I) \\ &= sv - tu - (s + v) + 1 \pmod{m}. \end{aligned}$$

Iz Trditve 2.25 dobimo, da $sv - tu = \det((\phi_q)_m) \equiv q \pmod{m}$. Iz (3.1) je $\#\mathrm{Ker}(\phi_q - 1) = q + 1 - a$. Zato je

$$\mathrm{Trace}((\phi_q)_m) = s + v \equiv a \pmod{m}.$$

Po Cayley-Hamiltonovem izreku iz linearne algebre, ali z elementarnim in dolgotrajnim računanjem, dobimo

$$(\phi_q)_m^2 - a(\phi_q)_m + qI \equiv 0 \pmod{m},$$

kjer je I identična matrika velikosti 2×2. (Opaziti moramo, da je $X^2 - aX + q$ karakteristični polinom matrike $(\phi_q)_m$.) To pomeni, da je endomorfizem $\phi_q^2 - a\phi_q + q$ ničelni na množici $E[m]$. Ker obstaja neskončno mnogo izbir za m, je jedro endomorfizma $\phi_q^2 - a\phi_q + q$ neskončno, kar pomeni, da je endomorfizem ničelni.

Predpostavimo, da za $a_1 \neq a$ velja $\phi_q^2 - a_1\phi_q + q = 0$. Potem je

$$(a - a_1)\phi_q = (\phi_q^2 - a_1\phi_q + q) - (\phi_q^2 - a\phi_q + q) = 0.$$

Po Izreku 2.9 je endomorfizem $\phi_q : E(\overline{\mathbf{F}}_q) \to E(\overline{\mathbf{F}}_q)$ surjektiven. Torej je $(a - a_1)(x, y) = \infty$, za poljuben $(x, y) \in E(\overline{\mathbf{F}}_q)$. Še več, $(a - a_1)$ je ničelni endomorfizem na množici $E[m]$, za poljuben $m \geq 1$. Ker obstajajo točke v množici $E[m]$ reda m, ko je $\gcd(m, q) = 1$, dobimo, da je $a - a_1 \equiv 0 \pmod{m}$, za takšne m. Sledi, da je $a - a_1 = 0$ oziroma da je a enolično določeno število. □

Izpostavimo še rezultat, ki smo ga dokazali med dokazovanjem Izreka 3.10.

Trditev 3.11. *Naj bo eliptična krivulja E definirana nad poljem $\mathbf{F}_q$ in naj bo $(\phi_q)_m$ matrika, ki določa delovanje Frobeniusove funkcije ϕ_q na množici $E[m]$. Naj bo $a = q + 1 - \#E(\mathbf{F}_q)$. Potem je*

$$\mathrm{Trace}((\phi_q)_m) \equiv a \pmod{m}, \qquad \det((\phi_q)_m) \equiv q \pmod{m}.$$

Polinomu $X^2 - aX + q$ pravimo **Frobeniusov karakteristični polinom**.

3.2 Določanje reda grupe

Hassejev izrek nam poda zgornjo in spodnjo mejo pri določanju reda grupe eliptične krivulje, ki je definirana nad končnim poljem. V tem podpoglavju bomo pravzaprav predstavili metodo za določanje reda grupe.

Včasih je podana eliptična krivulja E definirana nad relativno majhnim končnim poljem $\mathbf{F}_q$ in nato želimo izvedeti red krivulje $E(\mathbf{F}_{q^n})$, za določen n. Red krivulje $E(\mathbf{F}_{q^n})$, ko je $n = 1$, lahko določimo tako, da preprosto pregledamo vse možne točke, ali s pomočjo druge osnovne metode. Z naslednjim izrekom pa lahko določimo red grupe za poljuben n.

Izrek 3.12. *Naj bo $\#E(\mathbf{F}_q) = q + 1 - a$. Zapišimo $X^2 - aX + q = (X - \alpha)(X - \beta)$. Potem je*

$$\#E(\mathbf{F}_{q^n}) = q^n + 1 - (\alpha^n + \beta^n),$$

za poljuben $n \geq 1$.

Dokaz. Najprej moramo dokazati, da je $\alpha^n + \beta^n$ celo število. Pri tem nam bo pomagala naslednja lema.

Lema 3.13. *Naj bo $s_n = \alpha^n + \beta^n$. Potem je $s_0 = 2$, $s_1 = a$, in $s_{n+1} = as_n - qs_{n-1}$, za poljuben $n \geq 1$.*

Dokaz. Za s_0 in s_1 preverimo neposredno. Privzemimo sedaj, da lema velja za $n \in \mathbf{N}$ in pokažimo, da velja tudi za $n + 1$.

Pomnožimo z α^{n-1} enačbo $\alpha^2 - a\alpha + q = 0$, da dobimo $\alpha^{n+1} = a\alpha^n - q\alpha^{n-1}$. Enako naredimo z β. Seštejemo enačbi in dobimo zgornjo lemo. □

Neposredno iz leme sledi, da je $\alpha^n + \beta^n$ celo število, za poljuben $n \geq 0$.

Naj bo

$$f(X) = (X^n - \alpha^n)(X^n - \beta^n) = X^{2n} - (\alpha^n + \beta^n)X^n + q^n.$$

Potem $X^2 - aX + q = (X - \alpha)(X - \beta)$ deli $f(X)$. Neposredno iz standardnega algoritma za deljenje polinomov sledi, da ima kvocientni polinom $Q(X)$ za koeficiente cela števila

(to sledi iz tega, da je vodilni koeficient polinoma $X^2 - aX + q$ enak 1 in da imata ta polinom in polinom $f(X)$ za koeficiente cela števila). Zato je

$$(\phi_q^n)^2 - (\alpha^n + \beta^n)\phi_q^n + q^n = f(\phi_q) = Q(\phi_q)(\phi_q^2 - a\phi_q + q) = 0,$$

saj je po Izreku 3.10 $\phi_q^2 - a\phi_q + q = 0$. Seveda velja tudi, da je $\phi_q^n = \phi_{q^n}$. Po Izreku 3.10 obstaja enolično določeno celo število k, tako da je $\phi_{q^n}^2 - k\phi_{q^n} + q^n = 0$, kjer je $k = q^n + 1 - \#E(\mathbf{F}_{q^n})$. Zato je

$$\alpha^n + \beta^n = q^n + 1 - \#E(\mathbf{F}_{q^n}).$$

S tem smo dokončali dokaz Izreka 3.12. □

Primer 3.14. [26, Exercise 4.2] Naj bo eliptična krivulja E, definirana nad poljem $\mathbf{F}_2$, podana kot $y^2 + y = x^3$. Pokažimo, da je

$$\#E(\mathbf{F}_{2^n}) = \begin{cases} 2^n + 1 & \text{če je } n \text{ lih} \\ 2^n + 1 - 2(-2)^{n/2} & \text{če je } n \text{ sod.} \end{cases}$$

Poglejmo najprej red krivulje $E(\mathbf{F}_2)$. Če je $x = 0$, potem je $y^2 + y = 0$, kar pomeni, da je $y_1 = 0$ in $y_2 = 1$. Če je $x = 1$, potem je $y^2 + y = 1$, kar pomeni, da y nima rešitve. Sklepamo torej, da je

$$\#E(\mathbf{F}_2) = \#\{\infty, (0,0), (0,1)\} = 3.$$

Zapišimo torej $\#E(\mathbf{F}_2)$ v obliki $\#E(\mathbf{F}_q) = q + 1 - a$. Dobimo $\#E(\mathbf{F}_2) = 3 = 2 + 1 - a$, kar pomeni, da je $a = 0$. Sledi, da je $X^2 + 2 = (X - i\sqrt{2})(X + i\sqrt{2})$. Po Izreku 3.12 sledi, da je

$$E(\mathbf{F}_{2^n}) = 2^n + 1 - ((i\sqrt{2})^n + (-i\sqrt{2})^n).$$

Predpostavimo, da je n lih, i.e. $n = 2k + 1$, kjer $k \in \mathbf{N}_0$. Potem je

$$\#E(\mathbf{F}_{2^n}) = 2^n + 1 - ((i\sqrt{2})^n + (-i\sqrt{2})^n) = 2^n + 1.$$

Predpostavimo sedaj, da je n sod, i.e. $n = 2k$, kjer $k \in \mathbf{N}$. Potem je

$$\#E(\mathbf{F}_{2^n}) = 2^n + 1 - ((i\sqrt{2})^n + (-i\sqrt{2})^n) = 2^n + 1 - 2(-2)^{n/2}.$$

♢

3.3 Red točke

Naj bo $P \in E(\mathbf{F}_q)$. Red točke P je najmanjše pozitivno celo število k, za katero velja, da je $kP = \infty$. Iz teorije grup vemo, da red točke deli red grupe $E(\mathbf{F}_q)$. Velja tudi, da za celo število n velja, da je $nP = \infty$ natanko tedaj, ko red točke P deli n. Po

Hassejevem izreku leži $\#E(\mathbf{F}_q)$ v intervalu dolžine $4\sqrt{q}$. To pomeni, da če najdemo točko, katere red je večji od $4\sqrt{q}$, potem obstaja le en večkratnik tega reda, ki leži v zgoraj omenjenem intervalu. Ta večkratnik mora biti ravno $\#E(\mathbf{F}_q)$.
Tudi če je red točke manjši od $4\sqrt{q}$, sledi, da je število možnosti za $\#E(\mathbf{F}_q)$ majhno. V ta namen nam pride prav, če uporabimo več točk, kar bo dodatno zmanjšalo število možnosti, dokler ne dobimo enolično rešitev za $\#E(\mathbf{F}_q)$.

Primer 3.15. Naj bo krivulja E, definirana nad $\mathbf{F}_{101}$, podana kot $y^2 = x^3 + 7x + 1$. Da se pokazati, da je red točke $(0, 1)$ enak 116, kar pomeni, da je $\#E(\mathbf{F}_{101})$ večratnik števila 116. Hassejev izrek nam pove, da je

$$101 + 1 - 2\sqrt{101} \leq \#E(\mathbf{F}_{101}) \leq 101 + 1 + 2\sqrt{101},$$

kar pomeni, da je $82 \leq \#E(\mathbf{F}_{101}) < 122$. Edini večkratnik števila 116 v tem intervalu je 116, kar pomeni, da je $\#E(\mathbf{F}_{101}) = 116$. Še več, sklepamo lahko, da je grupa ciklična in generirana s točko $(0, 1)$. ◊

V tem poglavju si bomo ogledali metodo za izračun reda poljubne točke eliptične krivulje.

Naj bo $P \in E(\mathbf{F}_q)$. Najti moramo najmanjše tako celo število k, za katero velja, da je $kP = \infty$. Naj bo $\#E(\mathbf{F}_q) = N$. Po Lagrangevem izreku je $NP = \infty$. Obstaja možnost, da ne poznamo še N, ampak vemo, da je $q+1-2\sqrt{q} \leq N \leq q+1+2\sqrt{q}$. V tem intervalu poskusimo najti takšne N, za katere velja, da je $NP = \infty$. Potrebovali bomo torej $4\sqrt{q}$ korakov. Lahko pa tudi pospešimo postopek do približno $4q^{1/4}$ korakov s pomočjo naslednjega, tako imenovanega **Baby Step, Giant Step** algoritma.

1. Izračunajmo $Q = (q + 1)P$.
2. Izberimo celo število m, kjer je $m > q^{1/4}$. Izračunajmo in shranimo točke jP za $j = 0, 1, 2, \ldots, m$.
3. Izračunajmo točke

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

   dokler točka $Q+k(2mP)$ ni enaka točki jP ali točki $-jP$ iz shranjenega seznama $(j = 0, 1, \ldots, m)$.
4. Zaključimo, da je $(q + 1 + 2mk \mp j)P = \infty$. Naj bo $M = q + 1 + 2mk \mp j$.
5. Faktoriziramo M. Naj bodo $p_1, \ldots, p_r$ različni praštevilski faktorji števila M.
6. Izračunajmo $(M/p_i)P$ za $i = 1, \ldots, r$. Če je $(M/p_i)P = \infty$ za nek i, zamenjamo M z M/p_i in gremo nazaj na korak (5). Če je $(M/p_i)P \neq \infty$ za vse i, potem je M red točke P.

7. V kolikor nas zanima $\#E(\mathbf{F}_q)$, potem ponovimo korake (1)-(6) z naključno izbranimi točkami krivulje $E(\mathbf{F}_q)$, dokler najmanjši skupni večkratnik redov deli samo eno celo število N, kjer je $q+1-2\sqrt{q} \leq N \leq q+1+2\sqrt{q}$. Potem je $N = \#E(\mathbf{F}_q)$.

Preveriti moramo sicer dve stvari.

Prva: če predpostavimo, da se točka (3) algoritma konča, potem nam algoritem zagotovo vrne celo število k, za katero velja, da je $kP = \infty$. Vendar zakaj se točka (3) algoritma konča?

Lema 3.16. *Naj bo a celo število in $|a| \leq 2m^2$. Potem obstajata taki celi števili a_0 in a_1, kjer je $-m < a_0 \leq m$ in $-m \leq a_1 \leq m$, da je*

$$a = a_0 + 2ma_1.$$

Dokaz. Naj bo $a_0 \equiv a \pmod{2m}$, kjer je $-m < a_0 \leq m$ in $a_1 = (a - a_0)/2m$. Potem je

$$|a_1| \leq (2m^2 + m)/2m < m + 1.$$

Iz definicije a_1 sledi, da je $a = a_0 + 2ma_1$. □

Naj bo $a = a_0 + 2ma_1$ kot v lemi in $k = -a_1$. Potem je

$$\begin{aligned} Q + k(2mP) &= (q + 1 - 2ma_1)P \\ &= (q + 1 - a + a_0)P = NP + a_0P \\ &= a_0P = \pm jP, \end{aligned}$$

kjer je $j = |a_0|$. Sledi, da se točka (3) algoritma konča.

Druga: zakaj v točki (6) dobimo red točke P?

Lema 3.17. *Naj bo g element aditivno pisane abelske grupe $(G, +)$. Predpostavimo, da je $Mg = 0$, za neko naravno število M. Naj bodo $p_1, \ldots, p_r$ različni praštevilski faktorji števila M. Če je $(M/p_i)g \neq 0$ za vse i, potem je M red elementa g.*

Dokaz. Naj bo k red elementa g. Potem $k|M$. Predpostavimo, da je $k \neq M$. Naj bo p_i praštevilo, ki deli M/k. Potem $p_ik|M$, torej $k|(M/p_i)$. Zato je $(M/p_i)g = 0$, kar je v protislovju s predpostavko. Sledi, da je $k = M$. □

Iz tega sledi, da na koraku (6) zagotovo dobimo red točke P.

Algoritem je imenovan *Baby Step, Giant Step* (v slovenščini *Otroški korak, Velikanski korak*), ker je korak iz točke jP v $(j+1)P$ *otroški*, korak iz točke $k(2mP)$ v $(k+1)(2mP)$ pa *velikanski*.

Primer 3.18. Naj bo eliptična krivulja E, definirana nad poljem $\mathbf{F}_{557}$, podana kot $y^2 = x^3 - 10x + 21$. Naj bo točka $P = (2, 3)$. Sledimo sedaj algoritmu.

1. $Q = 558P = (418, 33)$.
2. Naj bo $m = 5$, kar je večje od $557^{1/4}$. Seznam točk jP je
$$\infty, (2, 3), (58, 164), (44, 294), (56, 339), (132, 364).$$
3. Ko je $k = 1$, dobimo $Q + k(2mP) = (2, 3)$; to točko pa imamo že v našem seznamu, to je, ko je $j = 1$.
4. Velja, da je $(q + 1 + 2mk - j)P = 567P = \infty$.
5. Faktoriziramo $567 = 3^4 \cdot 7$. Izračunamo $(567/3)P = 189P = \infty$. Število 189 postane tako prvi kandidat za red točke P.
6. Faktoriziramo $189 = 3^3 \cdot 7$. Izračunamo $(189/3)P = (38, 535) \neq \infty$ in $(189/7)P = (136, 360) \neq \infty$. Sklepamo torej, da je 189 red točke P.

V kolikor želimo izvedeti še $\#E(\mathbf{F}_{557})$, potem vemo, da je po Hassejevem izreku $511 \leq \#E(\mathbf{F}_{557}) \leq 605$. Edini večratnik števila 189 v tem intervalu je $3 \cdot 189 = 567$. Sklepamo torej, da je $\#E(\mathbf{F}_{557}) = 567$. ◊

3.4 Supersingularne krivulje

Naj bo E eliptična krivulja definirana nad poljem s karakteristiko p. Pravimo, da je krivulja E **supersingularna**, če je $E[p] = \{\infty\}$. Z drugimi besedami, ni točk reda p, tudi v primeru, ko so koordinate iz algebraično zaprtega polja. V nadaljevanju bomo predstavili nekaj zanimivih lastnostih supersingularnih krivulj.

Trditev 3.19. *Naj bo eliptična krivulja E definirana nad končnim poljem $\mathbf{F}_q$, kjer je q potenca praštevila p. Naj bo $a = q + 1 - \#E(\mathbf{F}_q)$. Potem je krivulja E supersingularna natanko tedaj, ko je $a \equiv 0 \pmod{p}$ oziroma natanko tedaj, ko je $\#E(\mathbf{F}_q) \equiv 1 \pmod{p}$.*

Dokaz. Zapišimo $X^2 - aX + q = (X - \alpha)(X - \beta)$. Iz Izreka 3.12 sledi, da je
$$\#E(\mathbf{F}_{q^n}) = q^n + 1 - (\alpha^n + \beta^n).$$
S pomočjo Leme 3.13 dobimo, da $s_n = \alpha^n + \beta^n$ zadošča rekurzivni enačbi
$$s_0 = 2, \quad s_1 = a, \quad s_{n+1} = as_n - qs_{n-1}.$$
Predpostavimo, da je $a \equiv 0 \pmod{p}$. Potem je $s_1 = a \equiv 0 \pmod{p}$ in $s_{n+1} \equiv 0 \pmod{p}$, za poljuben $n \geq 1$. Sledi
$$\#E(\mathbf{F}_{q^n}) = q^n + 1 - s_n \equiv 1 \pmod{p},$$

kar pomeni, da ni točk reda p na krivulji $E(\mathbf{F}_{q^n})$, za poljuben $n \geq 1$. Ker je

$$\overline{\mathbf{F}}_q = \bigcup_{n \geq 1} \mathbf{F}_{q^n},$$

sledi, da ni točk reda reda p v krivulji $E(\overline{\mathbf{F}}_q)$. To pomeni, da je krivulja E supersingularna.

Predpostavimo sedaj, da je $a \not\equiv 0 \pmod{p}$. Iz rekurzijske enačbe sledi, da je $s_{n+1} \equiv as_n \pmod{p}$, za poljuben $n \geq 1$. Ker je $s_1 = a$, dobimo, da je $s_n \equiv a^n \pmod{p}$, za poljuben $n \geq 1$. Sledi

$$\#E(\mathbf{F}_{q^n}) = q^n + 1 - s_n \equiv 1 - a^n \pmod{p}.$$

Po malem Fermatovem izreku je $a^{p-1} \equiv 1 \pmod{p}$. Zato je red krivulje $E(\mathbf{F}_{q^{p-1}})$ deljiv s p, kar pomeni, da vsebuje točko reda p. Sledi, da krivulja E ni supersingularna.

Da bi dokazali še zadnji del trditve, opazimo, da je

$$\#E(\mathbf{F}_q) = q + 1 - a \equiv 1 - a \pmod{p},$$

torej je $\#E(\mathbf{F}_q) \equiv 1 \pmod{p}$ natanko tedaj, ko je $a \equiv 0 \pmod{p}$. □

Posledica 3.20. *Predpostavimo, da je praštevilo $p \geq 5$ in da je krivulja E definirana nad poljem $\mathbf{F}_p$. Potem je E supersingularna natanko tedaj, ko je $a = 0$ oziroma natanko tedaj, ko je $\#E(\mathbf{F}_p) = p + 1$.*

Dokaz. Če je $a = 0$, potem je krivulja E supersingularna po zgornji trditvi.

Predpostavimo sedaj, da je krivulja E supersingularna in da je $a \neq 0$. Potem iz dejstva, da je $a \equiv 0 \pmod{p}$ sledi $|a| \geq p$. Po Hassejevem izreku je $|a| \leq 2\sqrt{p}$, torej velja $p \leq 2\sqrt{p}$. To pomeni, da je $p \leq 4$. □

Ko je $p = 2$ ali $p = 3$, obstajajo primeri supersingularnih krivulj z $a \neq 0$.

Primer 3.21. Naj bo eliptična krivulja E, definirana nad poljem $\mathbf{F}_2$, podana kot $y^2 + y = x^3 + x$. Pokazimo, da je $\#E(\mathbf{F}_2) = 5$ in da je E supersingularna.

Naj bo $x = 0$. Potem opazimo, da je y enak 0 ali 1. Enako velja za $x = 1$. Število točk je enako 4. Če dodamo še točko ∞, dobimo

$$\#E(\mathbf{F}_2) = 5.$$

To pomeni, da je $a = p + 1 - \#E(\mathbf{F}_p) = 2 + 1 - 5 = -2 \equiv 0 \pmod{2}$. ◊

V Primeru 2.16 smo opazili, da je eliptična krivulja $y^2 + a_3y = x^3 + a_4x + a_6$, definirana nad poljem karakteristike 2, supersingularna. Velja, da je tudi krivulja $y^2 = x^3 + a_2x^2 + a_4x + a_6$, definirana nad poljem karakteristike 3, supersingularna natanko tedaj, ko je $a_2 = 0$.

Predstavili bomo sedaj način konstrukcije supersingularnih krivulj, ki so definirane nad polji z različnimi karakteristikami.

Trditev 3.22. *Predpostavimo, da je q liho število in da je $q \equiv 2 \pmod 3$. Naj bo $B \in \mathbf{F}_q^\times = \mathbf{F}_q \backslash \{0\}$. Potem je eliptična krivulja E, podana kot $y^2 = x^3 + B$, supersingularna.*

Dokaz. Naj bo $\psi : \mathbf{F}_q^\times \to \mathbf{F}_q^\times$ homomorfizem, definiran kot $\psi(x) = x^3$. Ker $q - 1$ ni večkratnik števila 3, sledi, da ni elementov reda 3 v grupi $\mathbf{F}_q^\times$, kar pomeni, da je jedro preslikave ψ trivialno. Torej je homomorfizem ψ injektiven in tudi surjektiven, saj je grupa $\mathbf{F}_q^\times$ končna.

Za poljuben $y \in \mathbf{F}_q$ obstaja enoličen $x \in \mathbf{F}_q$, tako da (x, y) pripada krivulji E oziroma je x edini kubični koren od $y^2 - B$. Ker obstaja q vrednosti za y, to pomeni, da imamo q točk na krivulji $E(\mathbf{F}_q)$. Če prištejemo še točko ∞, dobimo, da je

$$\#E(\mathbf{F}_q) = q + 1.$$

Sledi, da je krivulja E supersingularna. □

Poglavje 4

Problem diskretnega logaritma

Naj bo p praštevilo in a, b taki celi števili, ki nista kongruenti 0 po modulu p. Privzemimo, da obstaja tak k, za katerega velja

$$a^k \equiv b \pmod{p}.$$

Klasični **problem diskretnega logaritma** je računanje vrednosti k pri danih a, b, p. Ker je $k + (p-1)$ tudi rešitev, sledi, da lahko k zapišemo po modulu $(p-1)$, ali po modulu d, kjer $d|p-1$, če je $a^d \equiv 1 \pmod{p}$.

V splošnem naj bo G poljubna multiplikativno pisana grupa in $a, b \in G$. Privzemimo, da velja $a^k = b$ za neko celo število k. V tem primeru je problem diskretnega logaritma računanje števila k pri danih a, b. Kot primer je lahko G multiplikativna grupa $\mathbf{F}_q^\times$ končnega polja.

V kolikor delamo z aditivno pisanimi grupami, se stvari nekako spremenijo. Kot primer vzamemo kar eliptične krivulje.

Naj bo $E(\mathbf{F}_q)$ poljubna eliptična krivulja in naj bosta $(x, y), (z, w) \in E(\mathbf{F}_q)$. Privzemimo, da velja $k(x, y) = (z, w)$ za nek k. Problem diskretnega logaritma je računanje vrednosti k.

V naslednjem poglavju bomo spoznali različne kriptografske aplikacije, ki temeljijo na problemu diskretnega logaritma. Varnost teh kriptosistemov je neposredno odvisna od težavnosti reševanja problema diskretnega logaritma.

Napad s surovo silo je eden od načinov, s katerim lahko rešimo problem diskretnega logaritma. Z drugimi besedami, vzamemo poljuben k in preverimo, ali k ustreza enačbi $k(x, y) = (z, w)$. Proces ponovimo, dokler ne najdemo pravilnega k. Izkaže se, da je ta način reševanja nepraktičen in dolgotrajen, še posebej, ko je k celo število z več stotimi ciframi (to pa je običajna velikost števil v kiptografiji). Torej potrebujemo boljše metode.

V tem poglavju bomo obravnavali metodo *index calculus*, ki jo lahko uparabimo na

grupi $\mathbf{F}_q^\times$ oziroma na multiplikativni grupi poljubnega končnega polja. Pozor: zavedati se moramo, da te metode ne moremo uporabljati na poljubni grupi. Sledi Baby step, Giant step metoda, Pollardovi ρ in λ metodi in Pohlig-Hellmanova metoda. Te metode delujejo za poljubne končne grupe, še posebej za eliptične krivulje. Za konec bomo pokazali, da za supersingularne krivulje lahko poenostavimo problem diskretnega logaritma (na multiplikativni grupi $\mathbf{F}_q^\times$ končnega polja).

4.1 Index calculus

Naj bo p praštevilo in naj bo g primitivni koren mod p, kar pomeni, da je g generator ciklične grupe $\mathbf{F}_p^\times$. Z drugimi besedami velja, da poljuben $h \not\equiv 0 \pmod{p}$ lahko zapišemo v obliki $h \equiv g^k$ za neko celo število k, ki je enolično določeno po modulu $p-1$. Naj bo $k = L(h)$ diskretni logaritem vrednosti h, za katerega velja

$$g^{L(h)} \equiv h \pmod{p}.$$

Naj bosta $h_1, h_2 \in \mathbf{F}_p^\times$. Potem je

$$g^{L(h_1 h_2)} \equiv h_1 h_2 \equiv g^{L(h_1)+L(h_2)} \pmod{p},$$

kar pomeni, da je

$$L(h_1 h_2) \equiv L(h_1) + L(h_2) \pmod{p-1}.$$

Funkcija L spremeni množenje v seštevanje, kot klasična logaritemska funkcija.

Index calculus je metoda za izračunanje vrednosti diskretne logaritemske funkcije L. Glavna ideja je ta, da vzamemo veliko število relativno majhnih praštevil l, izračunamo njihov $L(l)$, nato pa uporabimo te informacije, da za poljuben h izračunamo $L(h)$. Da bi bolje razumeli koncept, bomo navedli primer.

Primer 4.1. Naj bo $p = 1217$ in $g = 3$. Izračunati želimo k, za katerega velja $3^k \equiv 37 \pmod{1217}$. Naj bo $B = \{2, 3, 5, 7, 11, 13\}$ množica majhnih praštevil. Najprej poskusimo najti tak x, za katerega velja

$$3^x \equiv \pm(\text{produkt nekih praštevil v } B) \pmod{1217}.$$

Najdemo naslednje:

$$\begin{aligned}
3^1 &\equiv 3 \pmod{1217} \\
3^{24} &\equiv -2^2 \cdot 7 \cdot 13 \\
3^{25} &\equiv 5^3 \\
3^{30} &\equiv -2 \cdot 5^2 \\
3^{54} &\equiv -5 \cdot 11 \\
3^{87} &\equiv 13
\end{aligned}$$

Te lahko spremenimo v kongruence po modulu $p-1 = 1216$. Ker vemo, da je $3^{(p-1)/2} \equiv -1 \pmod{p}$, sledi, da je $L(-1) = 608$.

$$\begin{aligned} 1 &\equiv L(3) \pmod{1216} \\ 24 &\equiv 608 + 2L(2) + L(7) + L(13) \\ 25 &\equiv 3L(5) \\ 30 &\equiv 608 + L(2) + 2L(5) \\ 54 &\equiv 608 + L(5) + L(11) \\ 87 &\equiv L(13) \end{aligned}$$

Iz prve kongruence je razvidno, da je $L(3) \equiv 1 \pmod{1216}$. Iz tretje kongruence je $L(5) \equiv 819 \pmod{1216}$. Iz šeste kongruence je $L(13) \equiv 87 \pmod{1216}$. Iz četrte kongruence dobimo

$$L(2) \equiv 30 - 608 - 2 \cdot 819 \equiv 216 \pmod{1216}.$$

Iz pete kongruence dobimo, da je $L(11) \equiv 54 - 608 - L(5) \equiv 1059 \pmod{1216}$. Iz druge dobimo

$$L(7) \equiv 24 - 608 - 2L(2) - L(13) \equiv 113 \pmod{1216}.$$

Sedaj poznamo diskretni logaritem poljubnega elementa množice B. Spomnimo se, da želimo izračunati $3^k \equiv 37 \pmod{1217}$. Izračunamo $3^j \cdot 37 \pmod{p}$ za naključno izbrano vrednost j, dokler ne dobimo tako celo število, ki je produkt praštevil množice B. V našem primeru dobimo, da je

$$3^{16} \cdot 37 \equiv 2^3 \cdot 7 \cdot 11 \pmod{1217}.$$

Zato je

$$L(37) \equiv 3L(2) + L(7) + L(11) - 16 \equiv 588 \pmod{1216},$$

in $3^{588} \equiv 37 \pmod{1217}$. ◊

Izbira moči množice B je izjemnega pomena. Če je množica B premajhna, potem bo zelo težko najti potence elementa g, ki so produkt praštevil množice B. Po drugi strani, če je množica B prevelika, bomo z lahkoto dobili take potence, ampak bo reševanje dobljenega sistema kongruenc postalo izredno zahtevno in nepraktično: kot zanimiv podatek lahko omenimo primer, ki sta ga leta 2001 rešila A. Joux in R. Lercier [12]. Za množico B sta vzela prvih milijon praštevil, nato pa sta, za izračunanje diskretne logaritme, uporabila 120-števk dolgo praštevilo.

Časovna zahtevnost metode *index calculus* je približno konstanta krat $\exp(\sqrt{2 \ln p \ln \ln p})$ (glej [19, stran 129]). V naslednjem podpoglavju je časovna zahtevnost algoritmov

približno $\sqrt{p} = \exp(\frac{1}{2}\ln p)$ [26]. Sledi, da je *index calculus*, v primeru, ko ga lahko uporabimo, hitrejši.

Ta metoda je močno odvisna od dejstva, da lahko cela števila zapišemo kot produkt praštevil. To pomeni, da ta metoda ni uporabna v poljubni grupi.

4.2 Napadi na problem diskretnega logaritma

V tem podpoglavju bomo predstavili napade na problem diskretnega logaritma. Te metode lahko uporabimo za poljubno grupo. Ker nas najbolj zanimajo eliptične krivulje, bo grupa G aditivno pisana.

Naj bosta $P, Q \in G$. Želimo izračunati tako število k, da velja $kP = Q$ (predpostavili bomo vedno, da tak k obstaja). Naj bo N moč grupe G. Po navadi je N podan. Da bi poenostavili stvari, bomo privzeli, da P generira grupo G.

4.2.1 Baby Step, Gian Step

Metodo je razvil D. Shanks [24]. Njena časovna zahtevnost je približno $\sqrt{N}$, količina shranjenih podatkov pa približno $\sqrt{N}$. Iz tega lahko sklepamo, da ta metoda deluje učinkovito za relativno majhna števila N.

1. Izberimo celo število $m \geq \sqrt{N}$.
2. Izračunajmo iP $(0 \leq i \leq m)$ in nato shranimo rezultat.
3. Izračunajmo točke $Q - jmP$ $(0 \leq j \leq m-1)$, dokler točka $Q - jmP$ ni enaka točki iP iz shranjenega seznama $(0 \leq i < m)$.
4. Če je $iP = Q - jmP$, dobimo, da je $Q = kP$, kjer je $k \equiv i + jm \pmod{N}$.

Zakaj ta metoda deluje? Ker je $m^2 \geq N$, lahko privzememo, da rezultat k zadošča neenačbi $0 \leq k < m^2$. Zapišimo $k = k_0 + mk_1$, kjer je $k_0 \equiv k \pmod{m}$ in $0 \leq k_0 < m$, in naj bo $k_1 = (k - k_0)/m$. Potem je $0 \leq k_1 < m$. Ko je $i = k_0$ in je $j = k_1$, dobimo, da je

$$Q - k_1 mP = kP - k_1 mP = k_0 P,$$

torej se točka (3) algoritma res konča.

Točko iP izračunamo tako, da prištejemo točko P (*otroški korak*) k točki $(i-1)P$. Točko $Q - jmP$ izračunamo tako, da prištejemo točko $-mP$ (*velikanski korak*) k točki $Q - (j-1)mP$.

Pomembno dejstvo pri tej metodi je to, da ni potrebno vedeti točne vrednosti moči grupe G. Potrebujemo le zgornjo mejo za N. V kolikor delamo z eliptičnimi krivuljami, definiranimi nad poljem $\mathbf{F}_q$, sledi, da je $m^2 \geq q + 1 + 2\sqrt{q}$ (po Hassejevem izreku).

Metodo lahko izboljšamo tako, da izračunamo in shranimo le točke iP za $0 \leq i \leq m/2$ in nato preverimo ali je $Q - jmP = \pm iP$ (glej [26, Exercise 5.1]).

Primer 4.2. Naj bo krivulja E podana kot $y^2 = x^3+2x+1$ in naj bo grupa $G = E(\mathbf{F}_{41})$. Naj bo $P = (0, 1)$ in $Q = (30, 40)$. Po Hassejevem izreku vemo, da je red grupe G največ 54, torej bomo vzeli za m vrednost 8. Točke iP, za $0 \leq i \leq 8$, so

$$\infty, (0, 1), (1, 39), (8, 23), (38, 38), (23, 23), (20, 28), (26, 9), (10, 18).$$

Izračunajmo $Q - jmP$ za $j = 0, 1, 2$ in dobimo

$$(30, 40), (9, 25), (26, 9),$$

nakar se ustavimo, ker je točka $(26, 9)$ enaka točki $7P$. Sledi, da je $j = 2$ oziroma

$$(30, 40) = (7 + 2 \cdot 8)P = 23P.$$

Dobimo, da je $k = 23$. ◊

4.2.2 Pollardovi ρ in λ metodi

Zaradi velike količine shranjenih podatkov Baby Step, Giant Step metoda ni najbolj primerna. Pollardovi ρ in λ metodi [23] in Baby Step, Giant Step metoda imajo približno enake časovne zahtevnosti, ampak prvi dve omenjeni metodi porabita veliko manj prostora za shranjevanje podatkov. Najprej bomo predstavili ρ metodo, nato pa njeno posplošitev oziroma λ metodo.

Naj bo grupa G končna z močjo N. Izberimo funkcijo $f : G \to G$, ki preslika elemente na naključen način. Izberimo naključen element P_0 in nato izračunamo iteracije $P_{i+1} = f(P_i)$. Ker je G končna množica, potem obstajata taka indeksa $i_0 < j_0$, da je $P_{i_0} = P_{j_0}$. Potem je

$$P_{i_0+1} = f(P_{i_0}) = f(P_{j_0}) = P_{j_0+1},$$

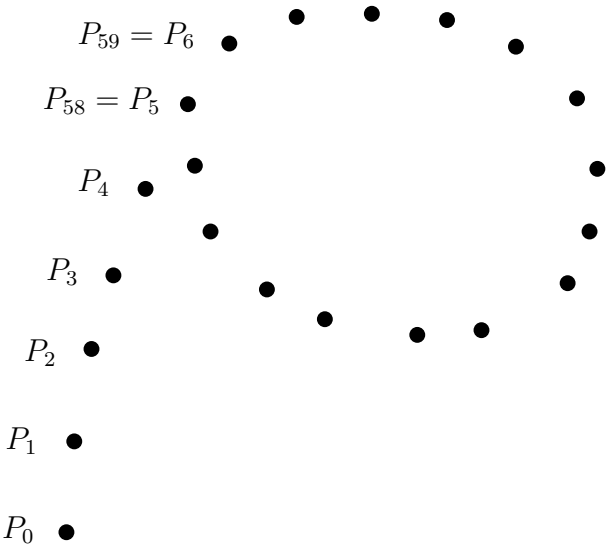
in podobno, $P_{i_0+\ell} = P_{j_0+\ell}$, za poljuben $\ell \geq 0$. Sledi, da je zaporedje P_i periodično s periodo $j_0 - i_0$ (ali z deljiteljem števila $j_0 - i_0$). Proces lahko ponazorimo s pomočjo Slike 4.1, na kateri je $i_0 = 5, j_0 = 58$. Kot vidimo iz slike, ime metode izhaja iz oblike grške črke ρ.

To metodo lahko implementiramo tako, da shranimo vse točke P_i, dokler se neka točka ne ponovi. Izkaže se, da je časovna zahtevnost te implementacije približno enaka $\sqrt{N}$ (kot pri metodi Baby Step, Giant Step). Kot je R. W. Floyd [9, 13] izpostavil, časovno zahtevnost metode lahko izboljšamo tako, da izpeljemo nekaj več izračunov. Glavna ideja je sledeča. Ko pride do ponovitev točk za dva indeksa, ki se razlikujeta za d, sledi, da bodo vse naslednje točke, za katere velja, da se indeksi razlikujejo za d,

enake. Sledi, da lahko izračunamo pare (P_i, P_{2i}) za $i = 1, 2, \ldots$, pri tem pa shranimo le trenutne pare, ne pa prejšnje. Pare lahko izračunamo tako:

$$P_{i+1} = f(P_i), \quad P_{2(i+1)} = f(f(P_{2i})).$$

Predpostavimo, da je $i \geq i_0$ in da je i večkratnik števila d. Potem se indeksa $2i$ in i razlikujeta za nek večratnik števila d oziroma je $P_i = P_{2i}$. Ker je $d \leq j_0$ in je $i_0 < j_0$, sledi, da za $i \leq j_0$ pride do ponovitev točk. Izkaže se, da je število korakov do ponovitev dveh točk največ konstanta krat $\sqrt{N}$.



Slika 4.1: Pollardova ρ metoda.

Uporabimo pa lahko še eno drugo metodo. Ta temelji na shranjevanju samo tistih točk P_i, ki zadoščajo določeni lastnosti. Na primer, zahtevamo lahko, da so zadnji k biti binarne reprezentacije koordinate x enake 0. Izkaže se, da v povprečju shranimo le eno izmed 2^k točk P_i. Privzemimo, da pride do ponovitev točk pri $P_i = P_j$ in da P_i ni shranjena v seznamu. Pričakujemo, da bo $P_{i+\ell}$ v shranjenem seznamu, za nek ℓ $(1 \leq \ell \leq 2^k)$. Potem bo $P_{j+\ell} = P_{i+\ell}$, kar pomeni, da bomo, s samo nekaj dodatnimi koraki, našli dve točki, ki se ponovita v shranjenem seznamu.

Glavni problem je izbira primerne funkcije f. Predstavili bomo način, kako to doseči. Grupo G razdelimo na s disjunktnih podmnožic $S_1, S_2, \ldots, S_s$, ki imajo približno enako moč. Izkaže se, da je število 20 (približno) primerno za s. Izberimo naključno $2s$ celih števil a_i, b_i po modulu N. Naj bo

$$M_i = a_i P + b_i Q.$$

Definiramo

$$f(g) = g + M_i \quad \text{če } g \in S_i.$$

Da bi lažje razumeli delovanje funkcije f, si lahko zamislimo, da se po naključju sprehodimo v grupi G tako, da elementi M_i predstavljajo naše možne korake.

Za konec izberimo naključni celi števili a_0, b_0 in naj bo $P_0 = a_0P + b_0Q$ začetni korak našega sprehoda v grupi G. Izračunajmo točke P_j in hkrati shranimo števili a_j in b_j. Če je $P_j = u_jP + v_jQ$ in je $P_{j+1} = P_j + M_i$, potem je $P_{j+1} = (u_j + a_i)P + (v_j + b_i)Q$, torej je $(u_{j+1}, v_{j+1}) = (u_j, v_j) + (a_i, b_i)$. Ko dobimo ponovitev $P_{j_0} = P_{i_0}$, potem dobimo

$$u_{j_0}P + v_{j_0}Q = u_{i_0}P + v_{i_0}Q \quad \text{oziroma} \quad (u_{i_0} - u_{j_0})P = (v_{j_0} - v_{i_0})Q.$$

Če je $\gcd(v_{j_0} - v_{i_0}, N) = d$, dobimo, da je

$$k \equiv (v_{j_0} - v_{i_0})^{-1}(u_{i_0} - u_{j_0}) \pmod{N/d}.$$

To nam poda d možnosti za k. Po navadi je število d majhno, tako da lahko izračunamo vse možnosti, dokler ne dobimo $Q = kP$.

V kriptografskih aplikacijah je N po navadi praštevilo, kar pomeni, da je d enak 1 ali N. Če je $d = N$, potem sta koeficienta točk P in Q večkratnika števila N, kar pomeni, da moramo začeti znova. Če pa je $d = 1$, dobimo k.

Primer 4.3. Naj bo eliptična krivulja E podana kot $y^2 = x^3 + x + 1$ in naj bo $G = E(\mathbf{F}_{1093})$. Za s vzamemo število 3. Naj bo $P = (0, 1)$ in $Q = (413, 959)$. Izkaže se, da je red točke P enak 1067. Želimo najti tak k, za katerega velja, da je $kP = Q$. Naj bo

$$P_0 = 3P + 5Q, \quad M_0 = 4P + 3Q, \quad M_1 = 9P + 17Q, \quad M_2 = 19P + 6Q.$$

Naj bo $f : E(\mathbf{F}_{1093}) \to E(\mathbf{F}_{1093})$ definirana kot

$$f(x, y) = (x, y) + M_i \quad \text{če je } x \equiv i \pmod 3.$$

x je celo število, za katero velja, da je $0 \leq x < 1093$. Nato ga reduciramo po modulu 3. Za primer je

$$f(P_0) = P_0 + M_2 = (727, 589),$$

saj je $P_0 = (326, 69)$ in je $326 \equiv 2 \pmod 3$.

V kolikor želimo, lahko definiramo $f(\infty)$ kot ∞. Po drugi strani, če srečamo $f(\infty)$, potem sledi, da je $aP + bQ = \infty$, kar pomeni, da k lahko najdemo na enostaven način. Z drugimi besedami, z ∞ nimamo nobenih težav.

Če izračunamo $P_0, P_1 = f(P_0), P_2 = f(P_1), \ldots$, dobimo

$$P_0 = (326, 69), P_1 = (727, 589), P_2 = (560, 365), P_3 = (1070, 260),$$
$$P_4 = (473, 903), P_5 = (1006, 951), P_6 = (523, 938), \ldots,$$
$$P_{57} = (895, 337), P_{58} = (1006, 951), P_{59} = (523, 938), \ldots.$$

Ponovitev točk dobimo pri točki $P_5 = P_{58}$. Če sproti shranjujemo koeficiente točk P in Q med izračunanjem, dobimo, da je

$$P_5 = 88P + 46Q \quad \text{in} \quad P_{58} = 685P + 620Q.$$

Zato je

$$\infty = P_{58} - P_5 = 597P + 574Q.$$

Ker je red točke P enak 1067, sledi, da je

$$-574^{-1}597 \equiv 499 \pmod{1067}.$$

Zato je $Q = 499P$ oziroma je $k = 499$.

Shranjevali smo vse točke $P_0, P_1, \ldots, P_{58}$, dokler ni prišlo do ponovitev točk.

Dajmo sedaj ponoviti izračune tako, da si pomagamo s pari (P_i, P_{2i}). Pomembno je to, da shranimo samo trenutni par, ne pa tudi prejšnje pare. Sledi, da sta za par (P_{53}, P_{106}) P_{53} in P_{106} enaka. To pomeni, da je

$$620P + 557Q = P_{53} = P_{106} = 1217P + 1131Q.$$

Sledi, da je $597P + 574Q = \infty$, kar pomeni, da je $k = 499$. ◊

Pollardova λ metoda uporablja funkcijo f, tako kot ρ metoda. Razlika je ta, da začnemo z več naključno izbranimi točkami $P_0^{(1)}, \ldots, P_0^{(r)}$. Tako dobimo zaporedja definarana kot

$$P_{i+1}^{(\ell)} = f(P_i^{(\ell)}), \quad 1 \leq \ell \leq r, \quad i = 0, 1, 2, \ldots.$$

S pomočjo več računalnikov lahko vzporedno izračunamo ta zaporedja. Točke, ki zadoščajo določeni lastnosti, pošljemo glavnemu računalniku. Ko pride do ponovitev točk med inputi različnih računalnikov, lahko rešimo problem diskretnega logaritma (kot pri ρ metodi). Ko pride do prve ponovitve dveh točk med dvemi zaporedji, se bodo vse naslednje točke teh dveh zaporedji ponovile. Pozorni moramo biti samo na točke, ki zadoščajo določeni lastnosti, saj se bodo te pojavile takoj po prvi ponovitvi točk.

V kolikor imamo samo dve naključni začetni točki, sledi, da imamo dva sprehoda v grupi G. Prej ali slej bosta ta dva sprehoda imela skupno točko, nato pa bosta nadaljevala po isti poti. Ime metode izhaja iz ponazoritve procesa v obliki grške črke λ.

Število korakov, da pride do prve ponovitve točk, je največ konstanta krat $\sqrt{N}$. Časovna zahtevnost se v primeru, da začnemo vzporedno z več naključnimi točkami, bistveno izboljša.

Za koncec bomo izpostavili razliko med Baby Step, Giant Step metodo in ρ oziroma λ metodi. Baby Step, Giant Step je **deterministična** metoda, kar pomeni, da se bo zagotovo končala v največ $l\sqrt{N}$ korakov, kjer je l neka konstanta. Po drugi strani sta ρ in λ **verjetnostni** metodi, kar pomeni, da obstaja velika verjetnost, da se bosta ti dve metodi končali pred napovedanim časom. Vendar tega ne moremo zagotoviti.

4.2.3 Pohlig-Hellmanova metoda

Naj točki P in Q pripadata grupi G. Želimo izračunati $kP = Q$, kjer je k celo število. Poznamo M (red točke P) in poznamo njegovo praštevilsko faktorizacijo

$$M = \prod_i q_i^{e_i}.$$

Glavna ideja pri Pohlig-Hellmananovi metodi je najti $k \pmod{q_i^{e_i}}$, za poljuben i, nato pa uporabiti Kitajski izrek o ostankih, da bi dobili $k \pmod{M}$.

Naj bo q praštevilo in naj bo q^e taka potenca števila q, da deli M. Zapišimo k kot

$$k = k_0 + k_1 q + k_2 q^2 + \dots,$$

kjer je $0 \leq k_i < q$. Naprej bomo izračunali $k_0, k_1, \dots, k_{e-1}$, nato pa bomo izračunali $k \pmod{q^e}$. Postopek je naslednji.

1. Izračunajmo $T = \left\{ j \left(\frac{M}{q} P\right) \mid 0 \leq j \leq q-1 \right\}$.
2. Izračunajmo $\frac{M}{q} Q$. Ta točka bo element $k_0 \left(\frac{M}{q} P\right)$ množice T.
3. Če je $e = 1$, se ustavimo, sicer nadaljujemo.
4. Naj bo $Q_1 = Q - k_0 P$.
5. Izračunajmo $\frac{M}{q^2} Q_1$. Ta točka bo element $k_1 \left(\frac{M}{q} P\right)$ množice T.
6. Če je $e = 2$, se ustavimo, sicer nadaljujemo.
7. Privzemimo, da smo izračunali $k_0, k_1, \dots, k_{r-1}$ in $Q_1, \dots, Q_{r-1}$.
8. Naj bo $Q_r = Q_{r-1} - k_{r-1} q^{r-1} P$.
9. Izračunajmo k_r tako, da je $\frac{M}{q^{r+1}} Q_r = k_r \left(\frac{M}{q} P\right)$.
10. Če je $r = e - 1$, se ustavimo, sicer pojdimo na korak (7).

Sledi, da je

$$k \equiv k_0 + k_1 q + \dots + k_{e-1} q^{e-1} \pmod{q^e}.$$

Zakaj ta metoda deluje? Imamo namreč

$$\frac{M}{q} Q = \frac{M}{q}(k_0 + k_1 q + \dots) P =$$
$$k_0 \frac{M}{q} P + (k_1 + k_2 q + \dots) MP = k_0 \frac{M}{q} P,$$

saj je $MP = \infty$. Sledi, da iz koraka (2) dobimo k_0. Potem je

$$Q_1 = Q - k_0 P = (k_1 q + k_2 q^2 + \dots) P,$$

torej je

$$\frac{M}{q^2}Q_1 = (k_1 + k_2 q + \cdots)\frac{M}{q}P =$$
$$k_1\frac{M}{q}P + (k_2 + k_3 q + \cdots)MP = k_1\frac{M}{q}P.$$

Dobili smo torej k_1. Podobno dobimo $k_2, k_3, \ldots$. Po $r = e - 1$ se moramo ustaviti, ker M/q^{e+1} ni celo število. Namreč, ne moremo pomnožiti Q_e s številom M/q^{e+1}, ki ni celo. Še več, ni potrebno nadaljevati, ker sedaj poznamo k mod q^e.

Primer 4.4. Naj bo eliptična krivulja E podana kot $y^2 = x^3 + 1$ in naj bo grupa $G = E(\mathbf{F}_{599})$. Naj bo $P = (60, 19)$ in $Q = (277, 239)$. Izkaže se, da je red točke P enak $M = 600$. Najti želimo tak k, za katerega velja, da je $kP = Q$. Praštevilska faktorizacija števila M je

$$600 = 2^3 \cdot 3 \cdot 5^2.$$

Izračunali bomo k mod 8, mod 3 in mod 25. Nato bomo s pomočjo Kitajskega izreka o ostankih izračunali k mod 600.

a) k **mod** 8. Dobimo, da je $T = \{\infty, (598, 0)\}$. Ker je

$$(M/2)Q = \infty = 0 \cdot \left(\frac{M}{2}P\right),$$

dobimo, da je $k_0 = 0$. Zato je

$$Q_1 = Q - 0P = Q.$$

Ker je $(M/4)Q_1 = 150Q_1 = (598, 0) = 1 \cdot \frac{M}{2}P$, dobimo, da je $k_1 = 1$. Zato je

$$Q_2 = Q_1 - 1 \cdot 2 \cdot P = (35, 243).$$

Ker je $(M/8)Q_2 = 75Q_2 = \infty = 0 \cdot \frac{M}{2}P$, dobimo, da je $k_2 = 0$. Zato je

$$k = 0 + 1 \cdot 2 + 0 \cdot 4 \equiv 2 \pmod 8.$$

b) k **mod** 3. Dobimo, da je $T = \{\infty, (0, 1), (0, 598)\}$. Ker je

$$(M/3)Q = (0, 598) = 2 \cdot \frac{M}{3}P,$$

dobimo, da je $k_0 = 2$. Zato je

$$k \equiv 2 \pmod 3.$$

c) k **mod** 25. Dobimo, da je

$$T = \{\infty, (84, 179), (491, 134), (491, 465), (84, 420)\}.$$

Ker je $(M/5)Q = (84, 179)$, dobimo, da je $k_0 = 1$. Potem je

$$Q_1 = Q - 1 \cdot P = (130, 129).$$

Ker je $(M/25)Q_1 = (491, 465)$, dobimo, da je $k_1 = 3$. Zato je

$$k = 1 + 3 \cdot 5 \equiv 16 \pmod{25}.$$

Sedaj imamo tri kongruence:

$$\begin{cases} x \equiv 2 \pmod 8 \\ x \equiv 2 \pmod 3 \\ x \equiv 16 \pmod{25} \end{cases}.$$

S pomočjo Kitajskega izreka o ostankih dobimo, da je $k \equiv 266 \pmod{600}$ oziroma je $k = 266$. ◊

Pohlig-Hellmanova metoda deluje učinkovito, če so vsa praštevila, ki delijo M, relativno majhna. Po drugi strani, če je q relativno veliko praštevilo, ki deli M, potem ni enostavno dobiti q elementov množice T. Vrednosti k_i lahko dobimo tudi tako, da ne določimo elemente množice T. Zavedati pa se moramo, da v kolikor bi radi dobili k_i, potem moramo najprej rešiti problem diskretnega logaritma v grupi, ki je generirana z elementom $(M/q)P$ reda q. Če je red velikosti števila q enak številu M (na primer $q = M$ ali $q = M/2$), potem Pohlig-Hellmanova metoda ni učinkovita. Iz tega sledi, da če kriptografski sistem temelji na problemu diskretnega logaritma, potem mora red grupe vsebovati relativno veliko praštevilo.

Če M vsebuje relativno majhna praštevila, potem s pomočjo Pohlig-Hellmanove metode lahko dobimo samo del informacij, ki nam bodo pomagale pri določitvi vrednosti k. Z drugimi besedami, dobili bomo kongruenco po modulu nekega produkta teh relativno majhnih praštevil. Izkaže se, da za nekatere kriptograske sisteme to ni zaželeno, kar pomeni, da je v veliko primerih red grupe G relativno veliko praštevilo. To izpeljemo tako, da začnemo z grupo, katere red vsebuje relativno veliko praštevilo q. Izberemo naključno točko P_1 in izračunamo njen red. Obstaja velika verjetnost (vsaj $1-1/q$; glej Opombo 4.6), da vrednost q deli red točke P_1. To pomeni, da lahko v nekaj poskusih dobimo točko P_1. Zapišimo red točke P_1 kot qm. Potem je red točke $P = mP_1$ enak q. V primeru, da je q relativno veliko število, bodo problemi diskretnega logaritma v ciklični grupi generirani s točko P učinkovito zdržali Pohlig-Hellmanov napad.

4.3 Napad z Weilovimi prirejanji

Ena od strategij za reševanje problema diskretnega logaritma temelji na reduciranje tega istega problema na enostavnejši problem diskretnega logaritma. Ta proces lahko izpeljemo z Weilovimi prirejanji. Ti pretvorijo problem diskretnega logaritma na eliptični krivulji v problem diskretnega logaritma v multiplikativni grupi končnega polja.

MOV napad (Menezes, Okamoto in Vanstone [18]) uporablja Weilovo prirejanje, da pretvori problem diskretnega logaritma v eliptični krivulji $E(\mathbf{F}_q)$ v problem diskretnega logaritma v $\mathbf{F}_{q^m}^{\times}$.

Spomnimo se, da probleme diskretnega logaritma v končnih poljih lahko napademo z medodo index calculus. V kolikor moč polja $\mathbf{F}_{q^m}$ ni precej večja od moči polja $\mathbf{F}_q$, se izkaže, da se te probleme, v primerjavi s problemi diskretnega logaritma na eliptični krivulji, da rešiti hitreje. Za supersingularne krivulje je lahko $m = 2$, kar pomeni, da je za to vrsto eliptičnih krivulj problem diskretnega logaritma hitreje rešljiv. To pa iz kriptografskega vidika ni zaželeno, tudi zato, ker je računanje s supersingularnimi eliptičnimi krivuljami, zaradi njihovih lepih lastnostih, enostavnejše (glej Podpoglavje 3.4).

Spomnimo se, da je za eliptično krivuljo E, definirano nad poljem $\mathbf{F}_q$, $E[N]$ množica tistih točk, za katerih velja, da njihov red deli N. Koordinate teh točk pripadajo algebraičnemu zaprtju polja $\mathbf{F}_q$. Če je $\gcd(q, N) = 1$ in točki $S, T \in E[N]$, potem je Weilovo prirejanje $e_N(S, T)$ N-ti koren enote. Računanje tega korena je enostavno in hitro. Prirejanje je bilinearno, in velja, da če je $\{S, T\}$ baza za $E[N]$, potem je $e_N(S, T)$ primitivni N-ti koren enote. Za poljuben S velja, da je $e_N(S, S) = 1$.

Naj bo eliptična krivulja E definirana nad poljem $\mathbf{F}_q$. Naj točki $P, Q \in E(\mathbf{F}_q)$. Naj bo N red točke P. Predpostavimo, da je

$$\gcd(N, q) = 1.$$

Želimo najti tak k, za katerega velja, da je $Q = kP$. Najprej pa se bomo prepričali, kdaj tak k res obstaja.

Lema 4.5. *Obstaja tak k, za katerega velja, da je $Q = kP$ natanko tedaj, ko je $NQ = \infty$ in je Weilovo prirejanje $e_N(P, Q) = 1$.*

Dokaz. Če je $Q = kP$, potem je $NQ = kNP = \infty$. Velja tudi, da je

$$e_N(P, Q) = e_N(P, P)^k = 1^k = 1.$$

Po drugi strani, če je $NQ = \infty$, potem točka $Q \in E[N]$. Ker je $\gcd(N, q) = 1$ velja, da je po Izreku 2.17 $E[N] \simeq \mathbf{Z}_N \oplus \mathbf{Z}_N$. Izberimo tako točko R, za katero velja, da je

$\{P, R\}$ baza množice $E[N]$. Potem je

$$Q = aP + bR$$

za neka cela števila a, b. Iz Posledice 2.20 sledi, da je $e_N(P, R) = \zeta$ primitivni N-ti koren enote. Ker je $e_N(P, Q) = 1$, dobimo

$$1 = e_N(P, Q) = e_N(P, P)^a e_N(P, R)^b = \zeta^b.$$

To implicira, da je $b \equiv 0 \pmod{N}$, torej je $bR = \infty$. Sledi, da je $Q = aP$, kot smo želeli. □

Idejo, s katero smo dokazali prejšnjo lemo, uporabimo za MOV napad na probleme diskretnega logaritma pri eliptičnih krivuljah. Izberimo m, tako da je

$$E[N] \subseteq E(\mathbf{F}_{q^m}).$$

Ker koordinate poljubne točke množice $E[N]$ pripadajo polju $\overline{\mathbf{F}}_q = \cup_{j \geq 1} \mathbf{F}_{q^j}$, potem število m res obstaja. Po Posledici 2.21 je grupa N-tih korenov enote μ_N vsebovana v polju $\mathbf{F}_{q^m}$. To pomeni, da bodo vsi naši izračuni izpeljani v polju $\mathbf{F}_{q^m}$. Algoritem je sledeči.

1. Izberimo naključno točko $T \in E(\mathbf{F}_{q^m})$.
2. Izračunajmo red M točke T.
3. Naj bo $d = \gcd(M, N)$ in naj bo $T_1 = (M/d)T$. Potem je red točke T_1 enak d in velja, da d deli N. Sledi, da $T_1 \in E[N]$.
4. Izračunajmo $\zeta_1 = e_N(P, T_1)$ in $\zeta_2 = e_N(Q, T_1)$. Potem ζ_1 in ζ_2 pripadata množici $\mu_d \subseteq \mathbf{F}_{q^m}^{\times}$.
5. Rešimo problem diskretnega logaritma $\zeta_2 = \zeta_1^k$ v $\mathbf{F}_{q^m}^{\times}$. Dobili bomo $k \pmod{d}$.
6. Ponovimo proces z naključnimi točkami T, dokler ni najmanjši skupni večratnik različnih vrednosti d enak N. Dobimo torej $k \pmod{N}$.

Opomba 4.6. Na prvi pogled bi lahko trdili, da se bo vrednost $d = 1$ pogosto pojavila. Vendar se zaradi strukture grupe $E(\mathbf{F}_{q^m})$ to ne zgodi. Spomnimo se, da je

$$E(\mathbf{F}_{q^m}) \simeq \mathbf{Z}_{n_1} \oplus \mathbf{Z}_{n_2}$$

za neki celi števili n_1, n_2, kjer $n_1 | n_2$ (po možnosti je $n_1 = 1$, kar pomeni, da je grupa ciklična). Potem $N | n_2$, ker je n_2 največji možni red točke v grupi. Naj bosta B_1, B_2 točki reda n_1 oziroma n_2 in naj B_1, B_2 generirata grupo $E(\mathbf{F}_{q^m})$. Potem je $T = a_1 B_1 + a_2 B_2$. Naj bo ℓ^e potenca praštevila, ki deli N. Potem $\ell^f | n_2$, kjer je $f \geq e$. Če

$\ell \nmid a_2$, potem ℓ^f deli M, kjer je M red točke T. Zato je $\ell^e | d = \gcd(M, N)$. Ker je verjetnost, da $\ell \nmid a_2$ enaka $1 - 1/\ell$, sledi, da je ta verjetnost vsaj tako velika, da ℓ^e deli d. Po določenih ponovitvah procesa z naključno izbranimi točkami T dobimo želeni rezultat. Ker nismo zajeli prispevka izraza $a_1 B_1$, je naša ocena verjetnosti nizka. Sledi, da po nekaj iteracij algoritma dobimo k.

Če je celo število m relativno veliko, potem bo po težavnosti problem diskretnega logaritma v grupi $\mathbf{F}_{q^m}^{\times}$, moči $q^m - 1$, primerljiv z originalnim problemom diskretnega logaritma v manjši grupi $E(\mathbf{F}_q)$, reda približno q (po Hassejevem izreku). Kot bomo videli v nadaljevanju, bomo za supersingularne krivulje vzeli vrednost $m = 2$.

Naj bo eliptična krivulja E definirana nad poljem $\mathbf{F}_q$, kjer je q potenca praštevila p. Potem je

$$\#E(\mathbf{F}_q) = q + 1 - a$$

za neko celo število a. Vemo, da je krivulja **supersingularna**, če je $a \equiv 0 \pmod{p}$. Iz Posledice 3.20 vemo, da je za $q = p \geq 5$, $a = 0$.

Trditev 4.7. *Naj bo eliptična krivulja E definirana nad poljem $\mathbf{F}_q$ in privzemimo, da je $a = q+1-\#E(\mathbf{F}_q) = 0$. Naj bo N pozitivno celo število. Če obstaja točka $P \in E(\mathbf{F}_q)$ reda N, potem je $E[N] \subseteq E(\mathbf{F}_{q^2})$.*

Dokaz. Frobeniusov endomorfizem ϕ_q zadošča enačbi $\phi_q^2 - a\phi_q + q = 0$. Ker je $a = 0$, potem sledi, da je

$$\phi_q^2 = -q.$$

Naj bo $S \in E[N]$. Ker je $\#E(\mathbf{F}_q) = q + 1$ in ker obstaja točka reda N, dobimo, da $N | q + 1$ ali $-q \equiv 1 \pmod{N}$. Zato je

$$\phi_q^2(S) = -qS = 1 \cdot S.$$

Iz Leme 3.5 sledi, da $S \in E(\mathbf{F}_{q^2})$. □

Kot vidimo se lahko problem diskretnega logaritma za supersingularne krivulje, definirane nad poljem $\mathbf{F}_q$ in z $a = 0$, prevede v problem diskretnega logaritma v $\mathbf{F}_{q^2}^{\times}$. Ta problem je veliko enostavnejši.

Ko je E supersingularna in $a \neq 0$, potem zgornji koncepti še vedno delujejo, ampak je $m = 3, 4$ ali 6 (glej [18] in [26, Exercise 5.12]). Ker so števila m majhna, je problem diskretnega logaritma še vedno relativno hitro rešljiv.

Poglavje 5

Kriptografija eliptičnih krivulj

V tem poglavju bomo predstavili nekaj aplikacij eliptičnih krivulj v kriptografiji. Te temeljijo predvsem na problemu diskretnega logaritma eliptičnih krivulj. Osredotočili se bomo na kriptosisteme in na digitalne podpise.

Zakaj sploh uporabljamo eliptične krivulje v kriptografiji? Izkaže se, da te zagotavljajo enako varnost kot klasični kriptografski sistemi, ampak uporabljajo manj bitov pri zapisu. Na primer, ocenjeno je v [3], da ključ z velikostjo 4096 bitov za RSA nam zagotovi enako varnost kot ključ z velikostjo 313 bitov v kriptografskem sistemu z eliptičnimi krivuljami. Iz tega sledi, da implementacije kriptografskih sistemov z eliptičnimi krivuljami uporabljajo manj fizičnega prostora, energije, itd. S pomočjo 3Com's PalmPilot naprave sta Daswani in Boneh [5] izvedla določene eksperimente. Ugotovila sta, da sta za ustvarjanje 512-bitnega RSA ključa porabila 3.4 minute, medtem ko sta za 163-bitnega ECC-DSA ključa porabila 0.597 sekunde. Čeprav so bili nekateri postopki, kot na primer preverjanje podpisa, nekoliko hitrejše pri RSA, so metode, ki uporabljajo eliptične krivulje, kot na primer ECC-DSA, v veliko primerih bistveno hitrejše.

5.1 Kratek uvod

Alenka želi poslati sporočilo Petru. Takemu sporočilu pravimo **čistopis**. Sara je radovedna in bi rada prebrala sporočilo. Ker si Alenka tega ne želi, mora svoje sporočilo šifrirati s pomočjo **šifrirnega ključa**. Takemu šifriranemu sporočilu pravimo **tajnopis**. Ko Peter dobi šifrirano sporočilo, ga dešifrira s pomočjo **dešifrirnega ključa**. Jasno je, da Sara ne sme pridobiti dešifrirnega ključa.

Obstajata dve vrsti šifriranja. V **simetričnem šifriranju** sta šifrirni in dešifrirni ključ enaka oziroma z lahkoto pridobimo enega iz drugega. Za primer simetričnega šifriranja lahko omenimo Data Encryprion Standard (DES) in Advanced Encryprion Standard (AES). V tem primeru se morata Alenka in Peter dogovoriti za ključ. Na

primer, nekaj dni prej lahko Peter pošlje Alenki človeka, ki ji bo predal ključ. Jasno je, da je v veliko primerih tak način nepraktičen.

Drugi način šifriranja je **javni šifrirni ključ** oziroma asimetrično šifriranje. V tem primeru Alenka in Peter ne potrebujeta nobenih predhodnih stikov. Peter objavi javni šifrirni ključ, katerega bo Alenka uporabila. Peter ima tudi zasebni dešifrirni ključ, s katerim si pomaga dešifrirati tajnopis. Zavedati se moramo, da je šifrirni ključ zasnovan tako, da bi moralo biti nemogoče pridobiti dešifrirni ključ iz šifrirnega ključa. Najbolj poznan sistem, ki temelji na javnem šifrirnem ključu, je RSA. Ta bazira na težavnosti faktorizacije celih števil v praštevila. ElGamalov sistem je tudi dobro poznan. Ta temelji na težavnosti problema diskretnega logaritma.

V splošnem so sistemi, ki temeljijo na javnem šifrirnem ključu, počasnejši v primerjavi z dobrim simetričnim sistemom. Iz tega razloga se po navadi uporablja asimetrični sistem za definicijo ključa, katerega bomo uporabili v simetričnem sistemu. Izboljšanje hitrosti je bistvenega pomena, še posebej, ko pošiljamo veliko količino podatkov.

5.2 Diffie-Hellmanova izmenjava ključev

Alenka in Peter se želita dogovoriti za ključ, katerega bosta uporabila za simetrično enkripcijsko shemo (na primer DES ali AES). Primer Alenke in Petra lahko apliciramo na primer dveh bank, ki si želita izmenjati finančne podatke. Izkaže se, da je pošiljanje ključa preko kurirja nepraktično in dolgotrajno. Privzemimo, da Alenka in Peter nista imela predhodnih stikov in da je javni kanal edini komunikacijski kanal med njima. Da bi si ustvarila ključ, si lahko pomagata s sledečo Diffie-Hellmanovo metodo.

1. Alenka in Peter izbereta tako eliptično krivuljo E, definirano nad poljem $\mathbf{F}_q$, za katero velja, da je problem diskretnega logaritma v grupi $E(\mathbf{F}_q)$ težek. Izbereta tudi tako točko $P \in E(\mathbf{F}_q)$, za katero velja, da je red točke P, relativno velik (po navadi izberemo eliptično krivuljo in točko P tako, da bo red točke P veliko praštevilo).

2. Alenka izbere zasebno celo število a, izračuna $P_a = aP$ in pošlje rezultat Petru.

3. Peter izbere zasebno celo število b, izračuna $P_b = bP$ in pošlje rezultat Alenki.

4. Alenka izračuna $aP_b = abP$.

5. Peter izračuna $bP_a = baP$.

6. Alenka in Peter se po javnem kanalu dogovorita za metodo, ki jo bosta uporabila za pridobitev ključa iz končnega rezultata abP. Za primer lahko vzameta kot ključ zadnjih 256 bitov x-koordinate točke abP. Druga možnost je ta, da uporabita zgoščevalno funkcijo na x-koordinati točke abP.

Edine informacije, ki so lahko javno dostopne, so krivulja E, končno polje $\mathbf{F}_q$, točke P, aP in bP. To pomeni, da v kolikor želi Sara dešifrirati Alenkino sporočilo, mora rešiti naslednji problem:

DIFFIE-HELLMANOV PROBLEM

Dani so P, aP, bP in $E(\mathbf{F}_q)$. Izračunajmo abP.

Če Sara lahko reši problem diskretnega logaritma v grupi $E(\mathbf{F}_q)$, potem lahko uporabi točki P in aP, da najde število a. To pomeni, da lahko izračuna $a(bP) = abP$.

Ni znano ali obstaja kakšen način za računanje abP, ne da bi predhodno rešili problem diskretnega logaritma.

Podajmo sedaj nekoliko drugačno vprašanje:

ODLOČITEV ZA DIFFIE-HELLMANOV PROBLEM

Dani so P, aP, bP in $E(\mathbf{F}_q)$. Dana je tudi točka $Q \in E(\mathbf{F}_q)$. Preverimo ali je $Q = abP$.

Diffie-Hellmanov problem in Odločitev za Diffie-Hellmanov problem lahko uporabimo za poljubno grupo. Prvotno sta bili uporabljeni za multiplikativne grupe $\mathbf{F}_q^\times$ končnih polj.

V nekaterih primerih eliptičnih krivulj lahko za rešitev Odločitve za Diffie-Hellmanov problem uporabljamo Weilovo prirejanje. Sedaj bomo predstavili primer.

Naj bo eliptična krivulja E definirana nad poljem $\mathbf{F}_q$, kjer je $q \equiv 2 \pmod 3$ in podana kot $y^2 = x^3 + 1$. Po Trditvi 3.22 je krivulja E supersingularna. Naj bo $\omega \in \mathbf{F}_{q^2}$ primitivni tretji koren enote. Velja, da $\omega \notin \mathbf{F}_q$, ker je red grupe $\mathbf{F}_q^\times$ enak $q - 1$; ta pa ni večkratnik števila 3.

Definirajmo preslikavo

$$\beta : E(\overline{\mathbf{F}}_q) \to E(\overline{\mathbf{F}}_q), \quad (x, y) \mapsto (\omega x, y), \quad \beta(\infty) = \infty.$$

S pomočjo elementarnega in dolgotrajnega računanja se izkaže, da je β izomorfizem (glej [26, Exercise 6.1]).

Privzemimo, da je red točke $P \in E(\overline{\mathbf{F}}_q)$ enak n. Potem je red točke $\beta(P)$ tudi enak n. Naj bo e_n standardno Weilovo prirejanje in $P_1, P_2 \in E[n]$. Definirajmo modificirano Weilovo prirejanje kot

$$\tilde{e}_n(P_1, P_2) = e_n(P_1, \beta(P_2)).$$

Lema 5.1. *Privzemimo, da $3 \nmid n$. Če je red točke $P \in E(\mathbf{F}_q)$ enak n, potem je $\tilde{e}_n(P, P)$ primitivni n-ti koren enote.*

Dokaz. Predpostavimo, da za neki celi števili u, v velja $uP = v\beta(P)$. Potem je

$$\beta(vP) = v\beta(P) = uP \in E(\mathbf{F}_q).$$

Če je $vP = \infty$, potem je $uP = \infty$, kar pomeni, da je $u \equiv 0 \pmod{n}$. Če $vP \neq \infty$, potem zapišimo $vP = (x, y)$, kjer sta $x, y \in \mathbf{F}_q$. Potem je

$$(\omega x, y) = \beta(vP) \in E(\mathbf{F}_q).$$

Ker $\omega \notin \mathbf{F}_q$, sledi, da je $x = 0$. Zato je $vP = (0, \pm 1)$, kar pomeni, da je reda 3. To je nemogoče, ker smo privzeli, da $3 \nmid n$. Sledi, da je edina rešitev, ki zadošča enačbi $uP = v\beta(P)$, enaka $u, v \equiv 0 \pmod{n}$, kar pomeni, da točki P in $\beta(P)$ tvorita bazo množice $E[n]$. Iz Posledice 2.20 sledi, da je $\tilde{e}_n(P, P) = e_n(P, \beta(P))$ primitivni n-ti koren enote. □

Privzemimo sedaj, da poznamo P, aP, bP, Q in bi želeli preveriti ali je $Q = abP$. Najprej moramo, s pomočjo standardnega Weilovega prirejanja, preveriti ali je točka Q večkratnik točke P. Po Lemi 4.5 je Q večkratnik točke P, natanko tedaj, ko je $e_n(P, Q) = 1$.

Privzemimo, da je to res oziroma da je $Q = tP$ za neko celo število t. Dobimo

$$\tilde{e}_n(aP, bP) = \tilde{e}_n(P, P)^{ab} = \tilde{e}_n(P, abP) \quad \text{in } \tilde{e}_n(Q, P) = \tilde{e}_n(P, P)^t.$$

Privzemimo, da $3 \nmid n$. Potem je $\tilde{e}_n(P, P)$ primitivni n-ti koren enote, kar pomeni, da je

$$Q = abP \iff t \equiv ab \pmod{n} \iff \tilde{e}_n(aP, bP) = \tilde{e}_n(Q, P).$$

V tem primeru smo rešili Odločitev za Diffie-Hellmanov problem. Kot smo videli, ni bilo potrebe po reševanju nobenih diskretnih logaritmov. Uporabili smo le Weilovo prirejanje.

Zgornjo metodo sta izumila Joux in Nguyen. Več o Odločitvi Diffie-Hellmanovega problema v [4].

Joux [10] (glej tudi [25]) je podal dodatno aplikacijo modificiranemu Weilovemu prirejanju. Tej aplikaciji pravimo **Diffie-Hellmanova tristranska izmenjava ključev**. Privzemimo, da Alenka, Peter in Jan želijo ustvariti skupni ključ. Standardni Diffie-Hellmanov postopek zahteva dva interakcijska kroga. Modificirano Weilovo prirejanje nam skrajša število krogov na enega.

Naj bo eliptična krivulja E definirana nad poljem $\mathbf{F}_q$, kjer je $q \equiv 2 \pmod{3}$, in podana kot $y^2 = x^3 + 1$. Naj bo točka P reda n. Po navadi je n relativno veliko praštevilo. Alenka, Peter in Jan naredijo naslednje:

1. Alenka, Peter in Jan izberejo vsak svoje zasebno celo število $a, b, c \pmod{n}$.
2. Alenka objavi aP, Peter objavi bP in Jan objavi cP.
3. Alenka izračuna $\tilde{e}_n(bP, cP)^a$, Peter izračuna $\tilde{e}_n(aP, cP)^b$ in Jan izračuna $\tilde{e}_n(aP, bP)^c$.
4. Ker so vsi izračunali enako število, sledi, da lahko s pomočjo predhodno določene metode ustvarijo ključ.

Ker je eliptična krivulja E supersingularna, sledi, da lahko problem diskretnega logaritma za krivuljo E poenostavimo na problem diskretnega logaritma za grupo $\mathbf{F}_{q^2}^{\times}$. To pomeni, da moramo izbrati tak q, da bo problem diskretnega logaritma težek.

V kolikor bi se radi podrobneje seznanili s kriptografskimi aplikacijami prirejanj, glejte [11].

5.3 Massey-Omuravo šifriranje

Alenka želi poslati sporočilo Petru preko javnega kanala, ampak nista si še ustvarila zasebnih ključev. Sedaj bomo predstavili način, kako lahko to izvedeta. Alenka zaklene škatlo, v kateri je sporočilo, s svojo ključavnico in jo nato pošlje Petru. Peter zaklene škatlo s svojo ključavnico in jo pošlje nazaj Alenki. Alenka odstrani svojo ključavnico in pošlje škatlo Petru. Peter odklene škatlo in prebere sporočilo.

Ta postopek lahko matematično implementiramo kot v nadaljevanju.

1. Alenka in Peter se dogovorita za tako eliptično krivuljo E, definirano nad poljem $\mathbf{F}_q$, da bo problem diskretnega logaritma v grupi $E(\mathbf{F}_q)$ težek. Naj bo $N = \#E(\mathbf{F}_q)$.

2. Alenka predstavi svoje sporočilo kot točko $M \in E(\mathbf{F}_q)$. (V nadaljevanju bomo razložili kako to izvesti.)

3. Alenka izbere zasebno celo število m_A, za katero velja, da je $\gcd(m_A, N) = 1$, izračuna $M_1 = m_A M$ in pošlje M_1 Petru.

4. Peter izbere zasebno celo število m_B, za katero velja, da je $\gcd(m_B, N) = 1$, izračuna $M_2 = m_B M_1$ in pošlje M_2 Alenki.

5. Alenka izračuna $m_A^{-1} \in \mathbf{Z}_N$. Izračuna $M_3 = m_A^{-1} M_2$ in pošlje M_3 Petru.

6. Peter izračuna $m_B^{-1} \in \mathbf{Z}_N$. Izračuna $M_4 = m_B^{-1} M_3$. Sledi, da je $M_4 = M$ sporočilo.

Dokažimo, da je M_4 originalno sporočilo oziroma da je

$$M_4 = m_B^{-1} m_A^{-1} m_B m_A M = M.$$

Velja, da je $m_A^{-1} m_A \equiv 1 \pmod{N}$. To pomeni, da je $m_A^{-1} m_A = 1 + kN$, za nek k. Grupa $E(\mathbf{F}_q)$ je reda N. Po Lagrangeovem izreku sledi, da je $NR = \infty$, za poljuben $R \in E(\mathbf{F}_q)$. To pomeni, da je

$$m_A^{-1} m_A R = (1 + kN)R = R + k\infty = R.$$

Če zgornjo enačbo apliciramo na enačbo $R = m_B M$, dobimo, da je

$$M_3 = m_A^{-1} m_B m_A M = m_B M.$$

Podobno kot za m_A^{-1} in m_A velja tudi, da je $m_B^{-1} m_B R = R$. Dobimo torej, da je

$$M_4 = m_B^{-1} M_3 = m_B^{-1} m_B M = M.$$

Radovedna Sara pozna $E(\mathbf{F}_q)$, točke $m_A M, m_B m_A M$ in $m_B M$. Naj bo $a = m_A^{-1}, b = m_B^{-1}, P = m_A m_B M$. Iz tega sledi, da Sara pozna P, bP, aP in želi izvedeti abP. To je Diffie-Hellmanov problem (glej Podpoglavje 5.2).

Zgornji postopek velja za poljubno končno grupo. Izkaže se, da je ta metoda redko uporabljena v praksi.

Za konec moramo pokazati, kako predstaviti sporočilo kot točko eliptične krivulje. Uporabili bomo Koblitzevo metodo. Privzemimo, da je eliptična krivulja E, definirana nad poljem $\mathbf{F}_p$, podana kot $y^2 = x^3 + Ax + B$. Procedura za poljubno polje $\mathbf{F}_q$ je podobna. Naj bo sporočilo predstavljeno kot število m, kjer je $0 \leq m < p/100$. Naj bo $x_j = 100m + j$, za $0 \leq j < 100$. Za $j = 0, 1, 2, \ldots, 99$ izračunajmo $s_j = x_j^3 + Ax_j + B$. Če je $s_j^{(p-1)/2} \equiv 1 \pmod{p}$, potem je s_j kvadrat mod p. To pomeni, da ni potrebno izračunati ostalih vrednosti j. Ko je $p \equiv 3 \pmod 4$, je kvadratni koren vrednosti s_j enak $y_j \equiv s_j^{(p+1)/4} \pmod{p}$ (glej [26, Exercise 6.7]). Ko je $p \equiv 1 \pmod 4$, lahko izračunamo kvadratni koren vrednosti s_j, ampak je postopek zahtevnejši (glej [6]). Dobimo točko (x_j, y_j) na krivulji E. Da bi dobili nazaj vrednost m iz točke (x_j, y_j), bomo izračunali $[x_j/100]$ (= največje celo število, ki je manjše ali enako vrednosti $x_j/100$). Ker je s_j naključen element grupe $\mathbf{F}_p^\times$ (ta je ciklična in sodega reda), je verjetnost, da bo s_j kvadrat, približno enaka $1/2$. Iz tega sledi, da je verjetnost, da ne bi našli točko za število m, po stotih poskušenih vrednostih enaka 2^{-100}.

5.4 ElGamalovo šifriranje z javnim ključem

Alenka želi poslati sporočilo Petru. Najprej mora Peter ustvariti svoj javni ključ na sledeči način. Izbere tako eliptično krivuljo E, definirano nad poljem $\mathbf{F}_q$, da je problem diskretnega logaritma v grupi $E(\mathbf{F}_q)$ težek. Izbere tudi točko P na krivulji E (po navadi je red točke P relativno veliko praštevilo). Izbere zasebno celo število s in izračuna $B = sP$. Eliptična krivulja E, končno polje $\mathbf{F}_q$ in točki P in B predstavljajo Petrov javni ključ. Objavljeni so v javnosti. Zasebni ključ Petra je število s.

Če želi Alenka poslati sporočilo Petru, mora izvesti naslednji algoritem:

1. Zabeleži si Petrov javni ključ.

2. Predstavi sporočilo kot točko $M \in E(\mathbf{F}_q)$.

3. Izbere zasebno celo število k in izračuna $M_1 = kP$.

4. Izračuna $M_2 = M + kB$.

5. Pošlje M_1 in M_2 Petru.

Peter dešifrira sporočilo tako, da izračuna

$$M = M_2 - sM_1.$$

Dešifriranje deluje, ker je

$$M_2 - sM_1 = (M + kB) - s(kP) = M + k(sP) - skP = M.$$

Radovedna Sara pozna Petrov javni ključ in točki M_1 in M_2. Če ji uspe rešiti problem diskretnega logaritma, potem lahko uporabi točki P in B, da dobi celo število s, kar pomeni, da lahko dešifrira sporočilo. Še več, lahko uporabi P in M_1, da najde k. Iz tega sledi, da lahko izračuna $M = M_2 - kB$. Izkaže se, vendar tega ne moremo dokazati, da je reševanje problema diskretnega logaritma edina metoda, ki nam pomaga do originalnega sporočila.

Pomembno je izpostaviti naslednje. Alenka mora vsakič, ko pošlje sporočilo Petru, izbrati različen in naključen k. Privzemimo, da Alenka uporabi enak k za M in M'. Sara opazi, da je $M_1 = M_1'$ in izračuna $M_2' - M_2 = M' - M$. Privzemimo, da je sporočilo M objavljeno v javnosti nasledji dan. To pomeni, da bo Sara poznala M in izračunala nato $M' = M - M_2 + M_2'$. Z drugimi besedami, če Sara pozna vsebimo prvotnega sporočila, bo z lahkoto razumela vsebino drugega sporočila.

Izkaže se, da ElGamalovo šifriranje z javnim ključem, v primerjavi z ElGamalovim digitalnim podpisom iz naslednjega podpoglavja, ni pogosto uporabljeno.

5.5 ElGamalov digitalni podpis

Alenka želi podpisati dokument. V kolikor je dokument v papirnati obliki, se Alenka podpiše na klasični način. Kaj pa, če je dokument v digitalni obliki? Ena rešitev je lahko ta, da pretvorimo Alenkin klasični podpis v digitalno obliko in ga nato priložimo k digitalnemu dokumentu. Ta rešitev ni primerna, ker lahko nagajiva Sara kopira podpis in ga nato priloži k drugemu dokumentu. Ker si Alenka tega ne želi, moramo najti način, kako priložiti podpis k dokumentu, upoštevajoč dejstva, da se podpis ne more več uporabiti. Po drugi strani mora obstajati možnost, da preverimo avtentičnost podpisa in da se prepričamo, da je prav Alenka podpisala dokument. Ta problem lahko rešimo s pomočjo problema diskretnega logaritma. Algoritem je bil prvotno zasnovan za multiplikativne grupe končnih polj. V resnici ga lahko uporabimo za poljubno končno grupo. Predstavimo ga sedaj za eliptične krivulje.

Alenka mora najprej ustvariti javni ključ. Izbere tako eliptično krivuljo E, definirano nad poljem $\mathbf{F}_q$, da je problem diskretnega logaritma v grupi $E(\mathbf{F}_q)$ težek. Nato izbere točko $A \in E(\mathbf{F}_q)$. Po navadi sta eliptična krivulja E in točka A izbrani tako, da je red N točke A relativno veliko praštevilo. Alenka izbere tudi zasebno celo število a in izračuna $B = aA$. Za konec izbere še tako funkcijo f, za katero velja, da je

$$f : E(\mathbf{F}_q) \to \mathbf{Z}.$$

Na primer, če je $\mathbf{F}_q = \mathbf{F}_p$, potem je lahko $f(x, y) = x$, kjer je x celo število, za katero velja $0 \leq x < p$. Funkcija f ne potrebuje posebnih lastnostih. Veljati mora le, da je zaloga vrednosti relativno velika in da se samo majhno število inputov preslika v dani output (na primer - največ dve točki (x, y) se za $f(x, y) = x$ lahko preslikata v isti x).

Alenkin javni ključ je $E, \mathbf{F}_q, f, A$ in B. Celo število a je skrito javnosti. Ni potrebno, da je celo število N objavljeno. Zavedati se moramo, da tajnost števila N ne vpliva na varnost kriptosistema.

V kolikor Alenka želi podpisati dokument, mora slediti sledečemu algoritmu:

1. Dokument predstavi kot celo število m (če je $m > N$, izbere eliptično krivuljo z večjim končnim poljem ali uporabi zgoščevalno funkcijo (več o tem v nadaljevanju)).

2. Izbere naključno celo število k, za katero velja, da je $\gcd(k, N) = 1$ in izračuna $R = kA$.

3. Izračuna $s \equiv k^{-1}(m - af(R)) \pmod{N}$.

Podpisano sporočilo je (m, R, s). m in s sta celi števili, točka R pa pripada krivulji E. Dokument m ni skrit javnosti. Če želimo, da postane, moramo dokument zašifrirati.

Peter preveri avtentičnost podpisa na sledeči način:

1. Zabeleži si Alenkin javni ključ.

2. Izračuna $V_1 = f(R)B + sR$ in $V_2 = mA$.

3. Če $V_1 = V_2$, potem je podpis avtentičen.

Če je podpis avtentičen, potem $V_1 = V_2$, ker

$$V_1 = f(R)B + sR = f(R)aA + skA = f(R)aA + (m - af(R))A = mA = V_2.$$

Uporabili smo dejstvo, da je $sk \equiv m - af(R) \pmod{N}$ oziroma da je $sk = m - af(R) + zN$, za neko celo število z. Zato je

$$skA = (m - af(R))A + zNA = (m - af(R))A + \infty = (m - af(R))A.$$

Sedaj lahko razumemo, zakaj smo pri kongruenci, kjer smo definirali s, uporabili mod N.

Če Sara reši problem diskretnega logaritma, lahko uporabi točki A in B, da dobi število a. V tem primeru bo lahko priložila Alenkin podpis k poljubnemu dokumentu. Lahko pa Sara uporabi A in R, da dobi število k. Ker pozna $s, f(R), m$, lahko uporabi kongruenco $ks \equiv m - af(R) \pmod{N}$, da dobi a. Če je $d = \gcd(f(R), N) \neq 1$, potem ima $af(R) \equiv m - ks \pmod{N}$ d rešitev za število a. Če je d majhno število, se izkaže, da bo Sara dobila a zelo hitro.

Pomembno je, da Alenka ne objavi števil a in k. Poleg tega je pomembno, da uporabi naključno in različno število k za vsak posamezen podpis. Privzemimo, da Alenka podpiše dokumenta m in m' z enakim številom k. Tako dobi dva podpisana dokumenta (m, R, s) in (m', R, s'). Sara takoj opazi, da je Alenka uporabila enaka k, ker je točka R enaka za oba podpisa. Dobimo torej kongruenci

$$ks \equiv m - af(R) \pmod{N}$$
$$ks' \equiv m' - af(R) \pmod{N}.$$

Če odštejemo kongruenci, dobimo $k(s - s') \equiv m - m' \pmod{N}$. Naj bo $d = \gcd(s - s', N)$. Obstaja d možnih vrednosti za k. Z nekaj poskusi lahko hitro dobimo k, kjer je $R = kA$. Enkrat, ko dobimo k, lahko najdemo a (glej zgoraj).

Izkaže se, da v nekaterih primerih ni potrebno, da Sara reši problem diskretnega logaritma z namenom, da priloži Alenkin podpis k poljubnemu dokumentu m. Pomembno je le, da ustvari taka R in s, da enačba za preverjanje $V_1 = V_2$ drži. To pomeni, da mora najti taka $R = (x, y)$ in s, da je

$$f(R)B + sR = mA.$$

Če izbere neko točko R (ni potrebno izbrati celega števila k), mora rešiti problem diskretnega logaritma $sR = mA - f(R)B$ za neko celo število s. V kolikor pa izbere število s, mora nato rešiti določeno enačbo za $R = (x, y)$. Reševanje te enačbe in problem diskretnega logaritma imata približno enako težavnost, čeprav enačba ni bila do sedaj še temeljito analizirana. Še več, nihče še ni izključil možnosti, da bi lahko z določenim postopkom izračunali R in s hkrati.

Obstajajo načini, kako s pomočjo avtentično podpisanih sporočil ustvarijo nova avtentično podpisana sporočila (glej [26, Exercise 6.2]). Vendar ustvarjena sporočila ne bodo načeloma imela smiselne vsebine.

Obstaja splošno prepričanje, da sta varnosti ElGamalovega sistema in problema diskretnih logaritmov za grupo $E(\mathbf{F}_q)$ prebližno enako močni.

Pomankljivost ElGamalovega sistema je ta, da je podpisano sporočilo (m, R, s) prebližno trikrat daljše kot originalno sporočilo (ni potrebno shraniti y-koordinato točke R, saj obstajata le dve vrednosti y za dani x). Pomagamo si pa lahko z bolj primerno

metodo. Ta temelji na zgoščevalni funkciji H. Metoda poteka tako, da najprej izberemo javno zgoščevalno funkcijo H, nato pa podpišemo $H(m)$. **Kriptografska zgoščevalna funkcija** je funkcija, ki vzame za input sporočilo poljubne dolžine (na primer sporočilo z več milijard bitov) in vrne kot output vrednosti fiksne dolžine (na primer 160 bitov), ki jih bomo imenovali zgoščevalne vrednosti (v angl. *hash values*). Zgoščevalna funkcija H mora zadoščati naslednjim lastnostim:

1. V kolikor je podano sporočilo m, mora biti vrednost $H(m)$ izračunana v relativno hitrem času.

2. V kolikor je podana vrednost y, mora biti računsko neizvedljivo najti m, kjer je $H(m) = y$.

3. Mora biti računsko neizvedljivo najti različni sporočili m_1 in m_2, kjer je $H(m_1) = H(m_2)$.

Točki (2) in (3) sta zelo pomembni, ker Sari preprečujeta ustvariti sporočila z določeno zgoščevalno vrednostjo ali ustvariti dve sporočili z enako zgoščevalno vrednostjo. S tem preprečujemo ponarejanje sporočil. Najbolj znani zgoščevalni funkciji sta MD5 (izumil jo je Rivest; ta ustvari output dolžine 128 bitov) in Secure Hash Algorithm (od NIST-a; ta ustvari output dolžine 160 bitov). Več o tem v [19]. Wang, Yin in Yu so nedavno našli nekaj šibkosti v teh dveh funkcijah, zato je njuna uporaba trenutno pod vprašajem.

Če Alenka uporabi zgoščevalno funkcijo, je podpisano sporočilo

$$(m, R_H, s_H),$$

kjer je $(H(m), R_H, s_H)$ veljavno sporočilo. Da bi preveril, če je podpis (m, R_H, s_H) avtentičen, mora Peter izvesti naslednji algoritem:

1. Zabeleži si Alenkin javni ključ.

2. Izračuna $V_1 = f(R_H)B + s_H R_H$ in $V_2 = H(m)A$.

3. Če je $V_1 = V_2$, potem je podpis avtentičen.

Prednost tega sistema je ta - če imamo nekaj milijard bitov dolgo sporočilo m sledi, da podpis potrebuje le nekaj tisoč dodatnih bitov. Če je problem diskretnega logaritma v grupi $E(\mathbf{F}_q)$ težek, sledi, da bo za Saro nemogoče uporabiti Alenkin podpis za poljubno drugo sporočilo. Pomembno je omeniti, da uporaba zgoščevalne funkcije ščiti tudi pred nekaterimi drugimi ponarejanji (glej [26, Exercise 6.2]).

Van Duin je ustvaril različico sheme ElGamalovega podpisa, ki je zelo učinkovita v nekaterih primerih. Za primer, računanje vrednosti k^{-1} ni prisotno in verifikacijski postopek zahteva le dva izračuna pri množenju celega števila in točke. Privzemimo, da

želi Alenka podpisati dokument m. Najprej izbere eliptično krivuljo E, ki je definirana nad končnim poljem $\mathbf{F}_q$ in točko $A \in E(\mathbf{F}_q)$ z relativno velikim praštevilskim redom N. Izbere tudi kriptografsko zgoščevalno funkcijo H, zasebno celo število a in izračuna $B = aA$. Njen javni ključ je (E, q, N, H, A, B). Alenka podpiše m tako, da sledi naslednjemu algoritmu:

1. Izbere naključno celo število k mod N in izračuna $R = kA$.
2. Izračuna $t = H(R, m)k + a \pmod{N}$.

Podpisani dokument je (m, R, t).

Peter preveri Alenkin podpis tako, da si zabeleži njen javni ključ in kontrolira, če velja enačba

$$tA = H(R, m)R + B.$$

Če enačba drži, je podpis avtentičen, sicer pa ni.

5.6 Algoritem za digitalni podpis

Standard za Digitalni Podpis (v angl. *Digital Signature Standard*) [1, 22] temelji na Algoritmu za Digitalni Podpis (v angl. *Digital Signature Algorithm (DSA)*). Originalna verzija je uporabljala multiplikativne grupe končnih polj, posodobitvena verzija (ECDSA) pa uporablja eliptične krivulje. Algoritem je neka varianta sheme ElGamalovega podpisa z nekaj spremembami. Sedaj bomo predstavili algoritem.

Alenka želi podpisati dukument m, kjer je m celo število (Alenka dejansko podpiše zgoščevalno vrednost dokumenta m, kot v Podpoglavju 5.5). Alenka izbere tako eliptično krivuljo, definirano nad poljem $\mathbf{F}_q$, da je $\#E(\mathbf{F}_q) = fr$, kjer je r relativno veliko praštevilo in f majhno celo število; po navadi $1, 2$ ali 4 (število f mora biti majhno zato, da bo algoritem učinkovit). Alenka nato izbere točko $G \in E(\mathbf{F}_q)$ reda r. Za konec izbere še zasebno celo število a in izračuna $Q = aG$. Alenka objavi sledeče podatke:

$$\mathbf{F}_q, \quad E, \quad r, \quad G, \quad Q.$$

(Ni potrebno, da je število f skrito javnosti; dobimo ga iz vrednosti q in r s pomočjo Hassejevega izreka - poslužimo se iste tehnike kot v Primeru 3.15). Alenka podpiše sporočilo m na sledeči način:

1. Izbere naključno število k, kjer je $1 \leq k < r$ in izračuna $R = kG = (x, y)$.
2. Izračuna $s = k^{-1}(m + ax) \pmod{r}$.

Podpisani dokument je

$$(m, R, s).$$

Peter preveri podpis tako:

1. Izračuna $u_1 = s^{-1}m \pmod r$ in $u_2 = s^{-1}x \pmod r$.
2. Izračuna $V = u_1G + u_2Q$.
3. Če je $V = R$, potem je podpis overjen.

Če je podpis sporočila avtentičen, potem bo enačba za preverjanje avtentičnosti držala:

$$V = u_1G + u_2Q = s^{-1}mG + s^{-1}xQ = s^{-1}(mG + xaG) = kG = R.$$

Največja razlika med ECDSA in ElGamalovim sistemom je postopek za preverjanje avtentičnosti. V ElGamalovem sistemu enačba za preverjanje avtentičnosti $f(R)B+sR = mA$ zahteva tri račune pri množenju celega števila s točko. Ti računi so najbolj dolgotrajni deli algoritma. V ECDSA izvedemo le dva taka računa. V kolikor je potrebno veliko preverjanja, potem je lahko ECDSA primernejši v primerjavi z ElGamalovim sistemom. Ta vrsta izboljšave je enaka van Duinovi izboljšavi, katero smo omenili na koncu prejšnjega podpoglavja.

5.7 ECIES

Elliptic Curve Integrated Encryption Scheme (ECIES) sta izumila Bellare in Rogaway [2]. To je shema za šifriranje z javnim ključem.

Alenka želi poslati sporočilo m Petru. Najprej Peter ustvari svoj javni ključ tako, da izbere tako eliptično krivuljo E, definirano nad poljem $\mathbf{F}_q$, da je problem diskretnega logaritma v $E(\mathbf{F}_q)$ težek. Nato izbere tako točko A na krivulji E, da bo red točke A relativno veliko praštevilo N. Izbere še celo število s in izračuna $B = sA$. Javni ključ Petra je (q, E, N, A, B). Njegov zasebni ključ je s.

Algoritem potrebuje tudi dve kriptografski zgoščevalni funkciji H_1 in H_2 in simetrično šifrirno funkcijo E_k (ta je odvisna od ključa k). Funkcije so predhodno določene preko javnega kanala.

Alenka želi zašifrirati in poslati svoje sporočilo Petru. Slediti mora sledečemu algoritmu:

1. Zabeleži si Petrov javni ključ.
2. Izbere si naključno celo število k, kjer je $1 \leq k \leq N - 1$.
3. Izračuna $R = kA$ in $Z = kB$.
4. Zapiše si output funkcije $H_1(R, Z)$ kot $k_1 \parallel k_2$ (to je k_1 - sledi mu k_2), kjer imata k_1 in k_2 določeni dolžini.
5. Izračuna $C = E_{k_1}(m)$ in $t = H_2(C, k_2)$.

6. Pošlje (R, C, t) Petru.

Peter želi dešifrirati sporočilo. Slediti mora sledečemu algoritmu:

1. Izračuna $Z = sR$.
2. Izračuna $H_1(R, Z)$ in si zapiše output kot $k_1 \parallel k_2$.
3. Izračuna $H_2(C, k_2)$. Če rezultat ni enak t, se ustavi in zavrne tajnopis, sicer nadaljuje.
4. Izračuna $m = D_{k_1}(C)$, kjer je D_{k_1} dekripcijska funkcija za E_{k_1}.

Avtentikacijski postopek je na koraku (3) pri dekripciji velikega pomena. V mnogih kriptosistemih lahko napadalec izbere različne tajnopise in prisili Petra, da jih dešifrira. S temi dekripcijami lahko napademo sistem. V našem sistemu lahko napadalec generira tajnopise tako, da izbere C in k_2' in nato izračuna $t' = H_2(C, k_2')$. Zavedati pa se moramo, da napadalec ne pozna Z, kar pomeni, da ne more uporabiti enake vrednosti k_2, katero Peter dobi od $H_1(R, Z)$. Zato obstaja zelo majhna verjetnost, da bo $t' = H_2(C, k_2')$ enak $t = H_2(C, k_2)$. To pomeni, da bo z veliko verjetnostjo Peter enostavno zavrnil tajnopis.

V našem sistemu smo za avtentikacijo uporabili zgoščevalne funkcije. Zavedati se moramo, da obstajajo tudi drugi načini za avtentikacijo sporočila.

Ena od prednosti sheme ECIES, v primerjavi z Massey-Omuravo in ElGamalovo metodo z javnimim ključem, je ta, da sporočilo ni predstavljeno kot točka na eliptični krivulji. Še več, ni potrebno izpeljati novih računov z eliptičnimi krivuljami za vsak posamezen blok sporočila, ker za pošiljanje čistopisa uporabljamo simetrično šifriranje.

Poglavje 6

Zaključek

Glavni cilj magistrske naloge je bila predstavitev določenih aplikacij eliptičnih krivulj v kriptografiji. V kolikor bi želeli poglobiti vaše znanje na tem področju, priporočam [7] in [26], kjer so predstavljene tudi druge aplikacije, kot na primer *A Public Key Scheme Based on Factoring* in *A Cryptosystem Based on the Weil Pairing*. Zanimivi sta tudi aplikaciji za faktorizacijo števil in za testiranje praštevilskosti.

Poglavje 7

Literatura

[1] MFIPS 186-2, *Digital signature standard*, Federal Information Processing Standards Publication 186, U. S. Dept. of Commerce/National Institute of Standards and Technology, 2000.

[2] M. Abdalla, M. Bellare, P. Rogaway, The Oracle Diffie-Hellman assumption and an analysis of DHIES, *Topics in cryptology - CT RSA 01*, Lecture Notes in Computer Science, **2020** (2001), Springer, Berlin, 143-158.

[3] I. F. Blake, G. Seroussi, N. P. Smart, *Elliptic curves in cryptography*, London Mathematical Society Lecture Note Series, **265** (2000), Cambridge University Press, Cambridge.

[4] D. Boneh, The decision Diffie-Hellman problem - *Algorithmic number theory (Portland, OR, 1998)*, Lecture Notes in Comput. Sci., **1423** (1998), Springer-Verlag, Berlin, 48-63.

[5] D. Boneh, N. Daswani, Experimenting with electronic commerce on the PalmPilot - *Financial Cryptography '99*, Lecture Notes in Comput. Sci., **1648** (1999), Springer-Verlag, Berlin, 1-16.

[6] H. Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, **138** (1993), Springer-Verlag, Berlin.

[7] H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen, F. Vercauteren, *Handbook of Elliptic and Hyperelliptic Curve Cryptography*, Chapman & Hall/CRC, Boca Raton, 2005.

[8] A. Enge, *Elliptic curves and their applications to cryptography: An introduction*, Kluwer Academic Publishers, Dordrecht, 1999.

[9] R. W. Floyd, Non-deterministic Algorithms, *JACM*, **14** (1967), 636–644.

[10] A. Joux, A one round protocol for tripartite Diffie-Hellman - *Algorithmic Number Theory (Leiden, The Netherlands, herefore maps2000)*, Lecture Notes in Comput. Sci., **1838** (2000), Springer-Verlag, Berlin, 385-394.

[11] A. Joux, The Weil and Tate pairings as building blocks for public key cryptosystems - *Algorithmic number theory (Sydney, Australia, 2002)*, Lecture Notes in Comput. Sci., **2369** (2002), Springer-Verlag, Berlin, 20-32.

[12] A. Joux, R. Lercier, Discrete logarithms in GF(p) (120 decimal digits) - April 2001. Elektronska pošta za poštni seznam NMBRTHRY, `http://perso.univ-rennes1.fr/reynald.lercier/file/nmbrJL01a.html`, avgust 2014.

[13] Donald E. Knuth, *The Art of Computer Programming, II: Seminumerical Algorithms*, Addison-Wesley Publishing Company, Reading, Massachusetts, 1969.

[14] A. Hibner Koblitz, N. Koblitz, A. Menezes, Elliptic curve cryptography: the serpentine course of a paradigm shift - *Journal of Number Theory*, **131** (2011), 781–814.

[15] N. Koblitz, Elliptic curve cryptosystems - *Mathematics of Computation*, **48** (1987), 203-209.

[16] N. Lauritzen, *Concrete Abstract Algebra - From Numbers to Gröbner Bases*, Cambridge University Press, Cambridge, 2003.

[17] H. W. Lenstra, Jr., Factoring integers with elliptic curves, *Annals of Mathematics*, **126** (1987), 649-673.

[18] A. J. Menezes, T. Okamoto, S. A. Vanstone, Reducing elliptic curve logarithms to logarithms in a finite field, *IEEE Trans. Inform. Theory*, **39** (1993), 1639-1646.

[19] A. J. Menezes, P. C. van Oorschot, S. A. Vanstone, *Handbook of applied cryptography*, CRC Press Series on Discrete Mathematics and its Applications, CRC Press, Boca Raton, FL, 1997.

[20] V. Miller, Uses of elliptic curves in cryptography - *Advances in Cryptology — CRYPTO '85*, Lecture Notes in Computer Science, **218** (1986), 417-426.

[21] Richard A. Mollin, *An Introduction to Cryptography, Second Edition*, Chapman & Hall/CRC, Boca Raton, 2007.

[22] IEEE P1363-2000, *Standard specifications for public key cryptography.*

[23] J. M. Pollard, Monte Carlo methods for index computation (mod p), *Math. Comp.*, **32** (1978), 918-924.

[24] D. Shanks, Class number, a theory of factorization, and genera - *1969 Number Theory Institute (Proc. Sympos. Pure Math., Vol. XX, State Univ. New York, Stony Brook, NY, 1969)*, Amer. Math. Soc., Providence, RI, 1971, 415-440.

[25] E. Verheul, Evidence that XTR is more secure than supersingular elliptic curve cryptosystems, *Eurocrypt 2001*, Lecture Notes in Computer Science, **2045** (2001), Springer-Verlag, Berlin, 195-210.

[26] Lawrence C. Washington, *Elliptic curves - Number Theory and Cryptography, Second Edition*, Chapman & Hall/CRC, Boca Raton, 2008.