Tampereen yliopisto

Mikko Paananen

Elliptiset käyrät ja alkulukutestaus

Informaatioteknologian ja viestinnän tiedekunta
Pro gradu -tutkielma
Matematiikka
Huhtikuu 2022

TIIVISTELMÄ

Mikko Paananen: Elliptiset käyrät ja alkulukutestaus
Pro gradu -tutkielma
Tampereen yliopisto
Matematiikan ja tilastotieteen tutkinto-ohjelma
Huhtikuu 2022

Tässä tutkielmassa perehdytään kirjallisuuskatsauksen omaisesti elliptisiä käyriä hyödyntävään alkulukutestaukseen. Tämä tarkoittaa menetelmiä, joilla voidaan testata, onko positiivinen kokonaisluku alkuluku vai ei hyödyntämällä äärellisten kuntien suhteen määriteltyjen elliptisten käyrien ominaisuuksia. Erityisesti tavoitteena on perehtyä Shafi Goldwasserin ja Joe Kilianin vuonna 1986 julkaisemaan Goldwasser–Kilian-algoritmina tunnettuun testiin, joka on toiminut pioneerina elliptisiä käyriä hyödyntäville alkulukutesteille ja jonka pohjalta on kehitetty eräitä nykypäivän tehokkaimpia alkulukutestejä.

Tutkielmassa käydään ensin läpi Goldwasser–Kilian-algoritmissa tarvittava teoreettinen pohja lukuteoriasta ja elliptisistä käyristä, minkä jälkeen voidaan esittää Goldwasser–Kilian-algoritmi kokonaisvaltaisesti tarjoten työkalut algoritmin jokaista vaihetta varten. Ensimmäisessä varsinaisessa luvussa, luvussa 2, käsitellään lukuteoriaa. Erityisesti käydään läpi neliöjäännöksiin liittyvää teoriaa ja esitellään joitakin tunnettuja lukuteoreettisia algoritmeja kuten Miller–Rabin-satunnaisalkulukutesti sekä Tonelli–Shanks-algoritmi modulaarisen neliöjuuren laskemiseen.

Kolmannessa luvussa käsitellään elliptisiä käyriä yleisesti kunnan suhteen sekä jäännösluokkarenkaan ja äärellisen kunnan suhteen määriteltynä. Goldwasser–Kilian-algoritmin kannalta erityisen olennainen käsiteltävä asia on elliptisen käyrän pisteiden lukumäärän laskeminen, kun kyseinen käyrä on määritelty äärellisen kunnan tai jäännösluokkarenkaan suhteen.

Itse Goldwasser–Kilian-algoritmi esitellään neljännessä luvussa. Tämä käydään läpi vaiheittain tarjoten esimerkit jokaisesta olennaisesta vaiheesta, minkä jälkeen luku päätetään analysoimalla hieman Goldwasser–Kilian-algoritmin suoriutumista. Tutkielman viidennessä ja samalla viimeisessä luvussa perehdytään pintapuolisesti tapoihin, joilla Goldwasser–Kilian-algoritmin suorituskykyä on saatu optimoitua. Erityisesti esitellään ECPP-algoritmi, joka on yksi nykypäivän tehokkaimmista alkulukutesteistä.

Avainsanat: elliptiset käyrät, alkulukutestaus
Tämän julkaisun alkuperäisyys on tarkastettu Turnitin OriginalityCheck -ohjelmalla.

Sisällys

1 Johdanto

Alkulukutestauksella tarkoitetaan menetelmiä, joilla voidaan testata, onko luonnollinen luku alkuluku vai ei. Tämä laskennallisen lukuteorian alue on merkittävässä roolissa nykypäivän informaatiota tulvillaan olevassa yhteiskunnassa, jossa tarve tiedon salaamiselle sekä turvalliselle lähettämiselle on suurempi kuin koskaan aikaisemmin. Tehokas alkulukutestaus on nimittäin mahdollistanut suuria alkulukuja hyödyntävät tiedonsalausmenetelmät, joita käytetään laajalti nykypäivänä erilaisissa tiedonsalausta vaativissa tilanteissa.

Alkulukutestauksen voidaan katsoa juontavansa juurensa antiikin Kreikan aikaan, jolloin filosofi Eratosthenes kehitti kirjoitetun historian ensimmäisen alkulukutestin: Eratostheneen seulan. Tämän jälkeen olennaisia muutoksia alalla tapahtui vasta 1600-luvulla, kun Fermat alkoi tutkimaan lukuteoriaa ja tuottamaan alkulukuihin liittyvää teoriaa. Hänen työtään lukuteorian ja alkulukujen parissa jatkoivat 1700- sekä 1800-luvuilla nimekkäät matemaatikot, kuten esimerkiksi Euler, Legendre sekä Gauss. Yhdessä he tuottivat 1900-lukuun mennessä merkittävän pohjan lukuteorialle ja olennaisesti alkulukutestaukselle, jonka aikakausi voidaan katsoa toden teolla alkaneeksi 1970-luvulla, vaikka toki aikaisemminkin oli joitakin alkulukutestejä kehitetty.

1970-luvun merkittäviin saavutuksiin kuuluvat muun muassa Millerin (1976) sekä Solovay–Strassenin (1977) kehittämät polynomiaikaiset alkulukutestit. Näistä Solovay–Strassenin testi on niin kutsuttu satunnaisalkulukutesti, toisin sanoen testi, joka osoittaa alkuluvun aina alkuluvuksi ja suurella todennäköisyydellä yhdistetyn luvun yhdistetyksi luvuksi. Millerin testi sen sijaan oli deterministinen testi, eli testi, joka osoittaa luvun joko alkuluvuksi tai yhdistetyksi luvuksi. Tämä kuitenkin nojautuu kuuluisaan laajennettuun Riemannin hypoteesiin, jota ei ole vielä tähän päivään mennessä saatu todistettua, joten Millerin testiä ei voida vielä pitää täysin luotettavana. Kuitenkin myöhemmin, vuonna 1980, Rabin hyödynsi Millerin ideoita ja kehitti niin kutsutun Miller–Rabin-testin, joka on Solovay–Strassenin testin tapaan satunnaisalkulukutesti ja joka suoriutuu myös polynomiajassa sekä hyvin pienellä virhemarginaalilla, kuten tullaan tässä tutkielmassa huomaamaan. 1980-luvun muita merkittäviä testejä ovat muun muassa Adlemanin ja Huangin vuonna 1983 kehittämä lähes polynomiajassa suoriutuva Jacobin summia hyödyntävä deterministinen testi, jota Cohen ja Lenstra kehittivät eteenpäin julkaisten vuonna 1984 Cohen–Lenstra-testinä tunnetun deterministisen testin. Jälkimmäisenä mainitun testin kompleksisuus kasvaa testattavan luvun suhteen niin hitaasti, että sitä pidetään käytännössä polynomiaikaisena algoritmina. Vasta 20 vuotta myöhemmin syntyi ensimmäinen varsinainen polynomiaikainen deterministinen alkulukutesti, kun Agrawal, Kayal ja Saxena julkaisivat vuonna 2004 AKS-algoritmina tunnetun alkulukutestin, jonka he osoittivat suoriutuvan mielivaltaisesta syöteluvusta deterministisesti polynomiajassa ilman, että testi riippui mistään todistamattomasta matematiikan hypoteeseista [1].

Alkulukutestaukseen liittyy olennaisesti myös sen todistaminen, että alkuluku on todella alkuluku. Erityisesti matemaatikkoja on kiinnostanut, voidaanko alkuluvulle tuottaa lyhyt todistus, joka voidaan tarkistaa polynomiajassa. Tällaista lyhyttä todistusta kutsutaan tässä tutkielmassa alkuluvun sertifikaatiksi, ja itse asiassa Pratt osoitti vuonna 1975, että jokaiselle alkuluvulle tälläinen sertifikaatti on aina löydettävissä, vaikkakaan käytännöllistä sekä geneeristä menetelmää tähän ei löydetty seuraavaan kymmeneen vuoteen.

Vuonna 1986 Shafi Goldwasser sekä Joe Kilian julkaisivat ensimmäisinä maailmassa elliptisiä käyriä hyödyntävän alkulukutestin, joka ei oleta testattavan luvun olevan mitään tiettyä muotoa. Tämä testi tunnetaan Goldwasser–Kilian-algoritmina. Tämä ei toki ollut ensimmäinen kerta kun elliptisiä käyriä hyödynnettiin lukuteorian ongelmissa, sillä muun muassa Lenstra kehitti vuonna 1985 elliptisiä käyriä hyödyntävän tekijöihinjakoalgoritmin ja samana vuon-

na Bosma kehitti elliptisiä käyriä hyödyntävän alkulukutestin, joka toimii vain tiettyä muotoa oleville luvuille. Tästä huolimatta Goldwasser–Kilian-algoritmi oli merkittävä saavutus alkulukutestauksen ja ylipäänsä lukuteorian maailmassa. Goldwasser–Kilian-algoritmista on nimittäin kehitetty muun muassa eräitä nykypäivän tehokkaimmista alkulukutesteistä, joten voidaan puhua eräänlaisesta matematiikan läpimurrosta. Goldwasser–Kilian-algoritmi etsii sille syötetylle alkuluvulle polynomiajassa sertifikaatin, joka voidaan tarkastaa polynomiajassa. Täten tämä oli vastaus Prattin vuoden 1975 tuloksesta alkaneeseen tehokkaan alkuluvun sertifikaatin tuottavan menetelmän etsintään.

Goldwasser–Kilian-algoritmin esittäminen on tämän tutkielman päätavoite. Tätä ei ole mahdollista tehdä täydellisesti pro gradu -tutkielman puitteissa, sillä Goldwasser ja Kilian hyödyntävät algoritmissaan useita muiden kehittämiä menetelmiä, joista osassa riittäisi sisältö jo itsessään pro gradu -tutkielmaa varten. Täten tutkielman asiasisältö on pyritty rajaamaan siten, että itse Goldwasser–Kilian-algoritmin esittäminen onnistuu edelleen mielekkäästi, vaikka joitakin asioita joudutaan jättämään esittämättä. Tutkielma rakenne koostuu johdannon lisäksi neljästä luvusta, joista luvussa 2 esitellään tutkielman kannalta olennaisia lukuteorian käsitteitä sekä tuloksia, perehdytään kahteen erilaiseen alkulukutestiin ja käsitellään modulaarisen neliöjuuren laskemista. Tutkielman laajimmassa osassa, luvussa 3, perehdytään elliptisiin käyriin liittyvään teoriaan yleisesti sekä Goldwasser–Kilian-algoritmia silmällä pitäen. Luvussa 4 esitellään itse Goldwasser–Kilian-algoritmi ja analysoidaan hieman sen suoriutumista. Viimeinen luku käytetään Goldwasser–Kilian-algoritmista kehitettyjen tehokkaampien algoritmien lyhyeeseen katsaukseen.

Tutkielman matemaattinen sisältö on sekoitus lukuteoriaa, algebraa sekä algebrallista geometriaa. Täten lukijalta odotetaan ainakin hyvää lukuteorian sekä algebran ymmärrystä. Tutkielma sisältää myös useita algoritmeja, joten lisäksi odotetaan, että lukija ymmärtää perusteet vaativuusteoriasta sekä algoritmeista.

2 Lukuteoriaa

Tämän luvun tavoitteena on esitellä joitakin lukuteorian tuloksia sekä algoritmeja, joita tarvitaan tutkielman myöhemmissä luvuissa tai jotka toimivat johdantona muun muassa alkulukutestaukseen. Alaluvussa 2.1 perehdytään joihinkin tunnettuihin lukuteorian käsitteisiin sekä tuloksiin, ja alaluvussa 2.2 perehdytään kahteen erilaiseen alkulukutestiin: Poclingtonin testiin sekä Miller–Rabin–testiin. Alaluku 2.3 käsittelee modulaarisen neliöjuuren laskemiseen käytettävää Tonelli–Shanks-algoritmia.

2.1 Joitakin peruskäsitteitä

Tämä alaluku käsittelee pääasiassa primitiivijuuria sekä neliöjäännöksiä, joista neliöjäännöksillä on tärkeä rooli tutkielman myöhemmissä luvuissa ja primitiivijuuria tarvitaan lähinnä neliöjäännöksiin liittyvän Eulerin kriteerin todistamisessa. Tämän alaluvun teoria pohjautuu useisiin lähteisiin, jotka mainitaan erikseen tekstissä.

Määritelmä 2.1. [4] (Primitiivijuuri) Olkoon p pariton alkuluku. Tällöin lukua $g \in \mathbb{Z}/p\mathbb{Z}$ kutsutaan *primitiivijuureksi* modulo p, mikäli se virittää kunnan $\mathbb{Z}/p\mathbb{Z}$ kertolaskuryhmän. Toisin sanoen jos $a \in (\mathbb{Z}/p\mathbb{Z})^*$, niin tällöin on olemassa $t \in \mathbb{N}$, $t < p$, jolla

$$a \equiv g^t \pmod{p}.$$

Huomautus. Primitiivijuuren yksi olennainen ominaisuus on se, että se tuottaa eri alkion jokaisella eksponentilla $0 \leq t < p$.

Lause 2.2. *Olkoon p pariton alkuluku. Tällöin primitiivijuuri modulo p on aina olemassa.*

Todistus. Riittää osoittaa, että ryhmä $(\mathbb{Z}/p\mathbb{Z})^*$ on syklinen, sillä tällöin on olemassa joukon $(\mathbb{Z}/p\mathbb{Z})^*$ virittäjä, joka toteuttaa samalla primitiivijuuren ehdot. Todistuksen syklisyydelle voi löytää muun muassa Serren teoksesta [16, s. 4]. □

Seuraavaa merkintää tullaan käyttämään useaan otteeseen tutkielmassa.

Merkintä 2.3. Olkoot a ja b, $b \neq 0$, kokonaislukuja. Tällöin merkinnällä a mod b tarkoitetaan pienintä positiivista kokonaislukua t, jolla pätee

$$t \equiv a \pmod{b}.$$

Olennaisesti luku a mod b on jakojäännös, joka syntyy kun luku a jaetaan luvulla b.

Huomautus. Merkintää mod tullaan tutkielman aikana käyttämään kahdessa eri tarkoituksessa: jakojäännöksen yhteydessä sekä kongruenssiyhtälön moduluksen määrittämisessä. Vaikka nämä käsitteet ovatkin hyvin lähellä toisiaan, on syytä pitää mielessä, että jakojäännöksen yhteydessä mod ei ole sulkeiden sisällä ja kongruenssiyhtälön tapauksessa se taas on.

Määritelmä 2.4. [14, s. 220] (Neliöjäännös) Olkoot p pariton alkuluku ja $a \in \mathbb{Z}$. Sanotaan, että a on *neliöjäännös* modulo p, mikäli on olemassa $b \in \mathbb{Z}$, jolla

$$b^2 \equiv a \pmod{p}.$$

Muussa tapauksessa a on *neliöepäjäännös*.

Huomautus. Nollasta poikkeavien neliöjäännösten modulo p lukumäärä on tällöin $\frac{p-1}{2}$. Tämä johtuu siitä, että kaikki neliöjäännökset saadaan laskemalla $a^2 \bmod p$ kaikilla kyseisen kunnan kertolaskuryhmän alkioilla a, joiden lukumäärä on $p-1$. Edelleen tiedetään, että $x^2 \equiv a^2 \pmod{p}$, jos ja vain jos $x = a$ tai $x = -a$, joten vain puolet joukon $(\mathbb{Z}/p\mathbb{Z})^*$ alkioista tuottaa yksikäsitteisen arvon neliöidessä. Täten nollasta poikkeavien neliöjäännösten modulo p määrä on täsmälleen $\frac{p-1}{2}$.

Seuraava Eulerin kriteerinä tunnettu tulos antaa välttämättömän ehdon sille, milloin luku on neliöjäännös modulo pariton alkuluku.

Lause 2.5. [14, s. 220–221] *Olkoot p pariton alkuluku ja $a \in \mathbb{Z}$, joilla* $\mathrm{syt}(a, p) = 1$. *Tällöin*

$$a^{(p-1)/2} \equiv 1 \pmod{p},$$

jos ja vain jos a on neliöjäännös modulo p.

Todistus. Oletettiin, että $\mathrm{syt}(a, p) = 1$, joten Fermat'n pienen lauseen nojalla

$$a^{p-1} \equiv 1 \pmod{p}.$$

Toisaalta p on alkuluku, joten tämän määräämässä jäännössysteemissä

$$a^{(p-1)/2} \equiv 1 \quad \text{tai} \quad a^{(p-1)/2} \equiv -1 \pmod{p}.$$

Voidaan huomata, että näistä ensin mainittu toteutuu, jos on olemassa primitiivijuuri g, jolla

$$a \equiv g^{2n} \pmod{p},$$

sillä tässä tapauksessa

$$a^{(p-1)/2} \equiv g^{(p-1)n} \equiv 1^n = 1 \pmod{p}.$$

Tällöin lisäksi g^n on kongruenssiyhtälön

$$x^2 \equiv a \pmod{p}$$

ratkaisu, joten a on neliöjäännös modulo p. Näin ollen primitiivijuuren parilliset potenssit tuottavat aina neliöjäännöksen modulo p, mikä kattaa $\frac{p-1}{2}$ kunnan $\mathbb{Z}/p\mathbb{Z}$ kertolaskuryhmän alkiota. Edelleen tiedetään, että täsmälleen $\frac{p-1}{2}$ tämän joukon alkiota ovat neliöjäännöksiä, joten primitiivijuuren parilliset potenssit tuottavat kaikki neliöjäännökset modulo p. Täten väite seuraa. □

Seuraavaksi esiteltävä *Legendren symboli* antaa käytännöllisen kokonaislukuarvon tiedolle siitä, onko luku neliöjäännös modulo pariton alkuluku vai ei. Tätä lukuarvoa hyödynnetään muun muassa myöhemmin tässä tutkielmassa esiteltävässä elliptisen käyrän pisteiden lukumäärän laskemisessa.

Määritelmä 2.6. [4] (Legendren symboli) Olkoot p pariton alkuluku ja $a \in \mathbb{Z}$. Tällöin *Legendren symboli* $\left(\frac{a}{p}\right)$ määritellään seuraavasti:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{jos } p \nmid a \text{ ja } a \text{ on neliöjäännös modulo } p, \\ 0, & \text{jos } p \mid a, \\ -1, & \text{jos } p \nmid a \text{ ja } a \text{ on neliöepäjäännös modulo } p. \end{cases}$$

Huomautus. Legendren symbolin laskemisessa voidaan hyödyntää esimerkiksi lauseessa 2.5 esitettyä Eulerin kriteeriä.

Päätetään tämä alaluku esittelemällä *Kiinalainen jäännöslause*, jota hyödynnetään tässä tutkielmassa vain Schoofin algoritmin yhteydessä alaluvussa 3.4.

Lause 2.7. [8] *(Kiinalainen jäännöslause) Olkoon* $N = n_1 n_2 \cdots n_s$*, missä* $n_1, \ldots, n_s \in \mathbb{Z}_{\geq 1}$ *ja* $\text{syt}(n_i, n_j) = 1$ *kaikilla* $i \neq j$*. Jos nyt* $a, u_1, \ldots, u_s \in \mathbb{Z}$*, niin tällöin on olemassa yksikäsitteinen kokonaisluku* u*, jolla*

$$a \leq u < a + N \quad ja \quad u \equiv u_i \pmod{n_i}$$

kaikilla $i = 1, \ldots, s$*.*

Todistus. Aloitetaan yksikäsitteisyyden todistamisella. Oletetaan, että on olemassa kokonaisluvut x ja y, joilla $a \leq x, y < a + N$ sekä $x \equiv u_i \pmod{n_i}$ ja $y \equiv u_i \pmod{n_i}$ kaikilla $i = 1, \ldots, s$. Tällöin siis $x \equiv y \pmod{n_i}$, eli $n_i \mid (x - y)$ kaikilla $i = 1, \ldots, s$. Edelleen $\text{syt}(n_i, n_j) = 1$ kaikilla $i \neq j$, joten $n_1 n_2 \cdots n_s = N \mid (x - y)$. Tämä on mahdollista vain, jos lukujen x ja y välinen etäisyys on luvun N monikerta. Kuitenkin välillä $[a, a + N[$ on vain N eri kokonaislukua, joten suurin mahdollinen etäisyys tällä välillä on $N - 1$. Täten on oltava $x - y = 0$, jolloin $x = y$.
Osoitetaan vielä, että lauseen ehdot toteuttava luku u on olemassa. Kun u käy läpi N eri kokonaislukua $a \leq u < a + N$, niin tällöin $(u \bmod n_1, \ldots, u \bmod n_s)$ käy läpi N eri jonoa, kuten yllä osoitettiin. Nyt kuitenkin on olemassa täsmälleen $n_1 n_2 \cdots n_s = N$ eri jonoa $(v_1, \ldots, v_s)$, missä $0 \leq v_i < n_i$ kaikilla $1 \leq i \leq s$, joten on oltava olemassa jokin kokonaisluku u, jolla $a \leq u < a + N$ ja

$$(u \bmod n_1, \ldots, u \bmod n_s) = (u_1, \ldots, u_s).$$

Täten väite seuraa. □

2.2 Alkulukutestauksesta

Tämän alaluvun tavoitteena on avata hieman alkulukutestausta sekä esitellä kaksi erilaista alkulukutestiä: Pocklingtonin testi ja Miller–Rabin-testi. Näistä ensin mainittu pohjautuu Koblitzin teokseen [9, s. 187] ja jälkimmäinen Rabinin artikkeliin [13].

Lause 2.8. *(Pocklingtonin kriteeri) Olkoon* $N > 1$ *kokonaisluku. Oletetaan, että on olemassa kokonaisluvut* a *ja* p*, joilla*

$$a^{N-1} \equiv 1 \pmod{N} \tag{2.1}$$

$$p \text{ on alkuluku, } p \mid N - 1 \text{ ja } p > \sqrt{N} - 1 \tag{2.2}$$

$$\text{syt}(a^{(N-1)/p} - 1, N) = 1. \tag{2.3}$$

Tällöin N *on alkuluku.*

Todistus. Tehdään vastaoletus: Oletetaan, että N ei ole alkuluku. Täten on olemassa luvun N alkutekijä q, jolle pätee $q \leq \sqrt{N}$. Nyt $p > \sqrt{N} - 1 \geq q - 1$, joten $p > q - 1$, ja koska p on alkuluku, niin $\text{syt}(p, q - 1) = 1$. Täten luvulla p on käänteisalkio r modulo $q - 1$ eli $rp \equiv 1 \pmod{q - 1}$, joten Fermat'n pienen lauseen nojalla

$$a^{rp} \equiv a \pmod{q}.$$

Nyt koska $q \mid N$, niin

$$\begin{aligned} a^{N-1} \equiv 1 \pmod{q} &\Rightarrow a^{r(N-1)} \equiv 1 \pmod{q} \\ &\Rightarrow a^{rp((N-1)/p)} \equiv a^{(N-1)/p} \equiv 1 \pmod{q}. \end{aligned}$$

Täten $q \mid a^{(N-1)/p} - 1$ ja $q \mid N$, mikä on ristiriita, sillä $\text{syt}(a^{(N-1)/p} - 1, N) = 1$. □

Lauseen 2.8 suorana seurauksena saadaan kätevä alkulukutesti: Mikäli syötteelle N löydetään kokonaisluvut a ja p, joilla lauseen ehdot toteutuvat, voidaan tällöin todeta luvun N olevan alkuluku. Tässä lähestymistavassa on kuitenkin joitakin ongelmakohtia. Nimittäin, ensinnäkin luvulla $N - 1$ ei välttämättä ole alkutekijää p, jolla $p > \sqrt{N} - 1$. Esimerkiksi muotoa $2^{2^n} + 1$ olevat *Fermat'n alkuluvut*, kuten $65537 = 2^{2^4} + 1$, ovat alkulukuja, joilla ei tällaisia tekijöitä ole. Toisaalta jos $N - 1$ on hyvin suuri luku, on sen alkutekijöiden löytäminen haastavaa. Nämä ongelmakohdat voidaan kuitenkin kiertää yleistämällä lauseen 2.8 alkuluvun p etsintä sellaisen luvun $N - 1$ tekijän s etsintään, missä luvun s alkutekijät tunnetaan ja $s > \sqrt{N} - 1$. Tämän jälkeen tarkistetaan lauseen ehdot korvaamalla luku p erikseen kaikilla luvun s tekijöillä.

Yllä esitetty Pocklingtonin kriteeriä hyödyntävä testi on esimerkki deterministisestä alkulukutestistä, jolla voidaan osoittaa luku alkuluvuksi tai yhdistetyksi luvuksi nojautumatta satunnaisuuteen. Seuraavaksi esiteltävä Miller–Rabin-testi on sen sijaan esimerkki satunnaisuuteen perustuvasta testistä, jossa luvulle pyritään löytämään niin kutsuttu *yhdistyneisyyden todiste*, joka osottaisi, että kyseessä on yhdistetty luku. Jos yhdistyneisyyden todistetta ei löydetä riitävän monella iteraatiolla, niin tällöin kyseessä on todennäköisesti alkuluku. Loput tämän alaluvun sisällöstä pohjautuu lähteeseen [13]. Aloitetaan määrittelemällä yhdistyneisyyden todiste.

Määritelmä 2.9. (Yhdistyneisyyden todiste) Olkoot $N > 1$ ja b kokonaislukuja. Merkitään $W_N(b)$, jos luvulla b pätee seuraavat ominaisuudet:

1. $1 \leq b < N$ ja
2. $b^{N-1} \not\equiv 1 \pmod{N}$, tai on olemassa $i \in \mathbb{N}$, jolla

$$2^i \mid N - 1 \quad \text{ja} \quad 1 < \text{syt}(b^{(N-1)/2^i} - 1, N) < N.$$

Jos luvulla b pätee $W_N(b)$, niin sanotaan, että b on luvun N *yhdistyneisyyden todiste*.

Huomautus. Jos $W_N(b)$ pätee, niin N on yhdistetty luku. Nimittäin, jos $b^{N-1} \not\equiv 1 \pmod{N}$, niin Fermat'n pienen lauseen nojalla N ei voi olla alkuluku, ja toisaalta jos

$$1 < \text{syt}(b^{(N-1)/2^i} - 1, N) < N,$$

niin luvulla N on ei-triviaali tekijä eikä se silloinkaan ole alkuluku.

Seuraava tulos antaa alarajan yhdistetyn luvun N yhdistyneisyyden todistajien lukumäärälle.

Lause 2.10. *Jos* $4 < N$ *on yhdistetty luku, niin*

$$\frac{3(N-1)}{4} \leq |\{b \mid W_N(b)\}|.$$

Todistus. Todistuksen voi löytää Rabinin artikkelista [13]. □

Lauseen 2.10 välitön seuraus on se, että jos $N > 4$ on yhdistetty, niin korkeintaan $1/4$ luvuista $1 \leq b < N$ ei ole yhdistyneisyyden todisteita luvulle N. Täten, kun valitaan satunnaisesti tasaisella jakaumalla $1 \leq b < N$, niin korkeintaan $1/4$ todennäköisyydellä b ei ole luvun N yhdistyneisyyden todiste. Kun tämä toistetaan vielä k:lla eri satunnaisella luvulla, on virheen mahdollisuus korkeintaan $1/4^k = 1/2^{2k}$, mikä tarkoittaa riittävän isolla luvulla k erittäin hyvää todennäköisyyttä todisteen löytymiselle, mikäli sellainen on ylipäänsä olemassa. Tämä luo pohjan Miller–Rabin-testinä tunnetulle satunnaisalkulukutestille, joka esitellään seuraavaksi.

Algoritmi 1. MR(N, k)
Oletetaan, että $N > 4$ on pariton ja $k \geq 1$.

1. Etsi positiiviset kokonaisluvut l ja m, missä m on pariton, joilla $N - 1 = 2^l m$.
2. Valitse satunnaisesti $b_1 \ldots, b_k \in \{1, \ldots, N - 1\}$.
3. Kaikilla $i = 1, \ldots, k$:
   (a) Aseta $b \leftarrow b_i$ ja laske $b^m \bmod N$.
   (b) Laske $b^{2^j m} \bmod N$ kaikilla $j = 1, \ldots, l$.
   (c) Jos $b^{N-1} = b^{2^l m} \not\equiv 1 \pmod N$, niin $W_N(b)$ pätee, joten palauta FALSE.
   (d) Laske syt$(b^{2^j m} - 1, N)$ kaikilla $j = 1, \ldots, l$. Jos jokin näistä arvoista ei ole 1 tai N, niin $W_N(b)$ pätee, joten palauta FALSE.
4. Yhdistyneisyyden todistetta ei löytynyt, joten palauta TRUE.

Huomautus. Vaiheessa 1 luvut l ja m voidaan löytää esimerkiksi seuraavasti: Tiedetään, että N on pariton, joten $N - 1$ on parillinen. Siispä $2^l \mid (N - 1)$ jollakin $l \geq 1$, jolloin toistuvasti puolittamalla voidaan helposti löytää sellainen l, jolla $2^l \mid (N - 1)$ ja $\dfrac{N-1}{2^l} = m$ on pariton.

2.3 Modulaarinen neliöjuuri

Tämän alaluvun tavoitteena on perehtyä modulaarisen neliöjuuren laskemiseen, mikä tarkoittaa käytännössä neliöjuuren laskemista kokonaisluvun, erityisesti alkuluvun, määräämässä jäännössysteemissä. Lukuisia menetelmiä on kehitetty tätä tehtävää varten, mutta tässä tutkielmassa perehdytään vain yhteen näistä, nimittäin Tonelli–Shanks-algoritmiin. Kyseinen algoritmi on käytetyin ja samalla yksi tehokkaimmista menetelmistä modulaarisen neliöjuuren laskemiseen, mistä syystä se on valikoitunut esitettäväksi tässä tutkielmassa. Tämän alaluvun lähteinä toimivat Cohenin [3] ja Humphreysin [6] teokset.

Oletetaan tässä alaluvussa, että N on pariton alkuluku ja $a \in \mathbb{Z}/N\mathbb{Z}$ on neliöjäännös modulo N. Tavoitteena on nyt löytää sellainen $x \in \mathbb{Z}/N\mathbb{Z}$, jolla

$$x^2 \equiv a \pmod N.$$

Tätä varten tarvitaan Sylowin p-aliryhmän käsite sekä Sylowin ensimmäisenä lauseena tunnettu tulos.

Määritelmä 2.11. [6, s. 98–99] (Sylowin p-aliryhmä) Olkoon G äärellinen kertalukua $p^e q$ oleva ryhmä, missä p on alkuluku, e ja q ovat positiivisia kokonaislukuja, sekä $p \nmid q$. Tällöin ryhmän G *Sylowin p-aliryhmä* on aliryhmä, jossa on p^e alkiota.

Huomautus. Jos G on lisäksi syklinen ryhmä, niin ryhmäteoriasta tiedetään, että tällöin Sylowin p-aliryhmä on syklisen ryhmän aliryhmänä myös syklinen.

Sylowin ensimmäinen lause osoittaa, että Sylowin p-aliryhmä on aina olemassa. Tämä lause esitetään seuraavaksi, mutta tämän todistus joudutaan kuitenkin sivuuttamaan.

Lause 2.12. [6, s. 98–99] *(Sylowin ensimmäinen lause) Olkoon G äärellinen kertalukua $p^e q$ oleva ryhmä, missä p on alkuluku, joka ei jaa lukua q. Tällöin ryhmällä G on ainakin yksi Sylowin p-aliryhmä.*

Todistus. Todistus sivuutetaan, mutta tämän voi löytää esimerkiksi Humphreysin teoksesta [6, s. 98–99]. □

Olkoon nyt $N = 2^e q + 1$, missä e ja q ovat epänegatiivisia kokonaislukuja sekä q on pariton. Tällöin kertolaskuryhmän $(\mathbb{Z}/N\mathbb{Z})^*$ kertaluku on $2^e q$, missä $2 \nmid q$, joten lauseen 2.12 nojalla on olemassa Sylowin 2-aliryhmä G, jonka kertaluku on 2^e. Lisäksi kertolaskuryhmä $(\mathbb{Z}/N\mathbb{Z})^*$ on tunnetusti syklinen, joten aliryhmän G on myös oltava syklinen. Oletetaan siis, että z on ryhmän G virittäjä. Tällöin ryhmän G neliöt ovat luvun z parillisia potensseja. Toisaalta neliöitä ovat myös alkiot, joiden kertaluku jakaa luvun 2^{e-1}. Ensimmäinen väittämä johtuu siitä, että jokainen alkio on muotoa z^n, missä n on epänegatiivinen kokonaisluku, jolloin jokainen neliö on muotoa $(z^n)^2 = z^{2n}$. Jälkimmäinen väittämä on seurausta tunnetusta Lagrangen lauseesta. Nyt koska a on neliöjäännös modulo N, niin

$$1 \equiv a^{(N-1)/2} = a^{(2^e q)/2} = (a^q)^{2^{e-1}} \pmod{N}.$$

Täten $a^q \bmod N$ on neliö ryhmässä G, joten on oltava olemassa parillinen k, jolla $0 \leq k < 2^e$ ja

$$a^q z^k = 1 \text{ ryhmässä } G. \tag{2.4}$$

Tällöin asettamalla

$$x = a^{(q+1)/2} z^{k/2}$$

saadaan ratkaisu kongruenssiyhtälölle $x^2 \equiv a \pmod{N}$, nimittäin

$$x^2 = \left(a^{(q+1)/2} z^{k/2}\right)^2 = a^{q+1} z^k = a \underbrace{\left(a^q z^k\right)}_{\equiv 1} \equiv a \pmod{N}.$$

Ennen Tonelli–Shanks-algoritmin esittämistä tarvitaan vielä seuraava aputulos.

Lemma 2.13. *Olkoot G Sylowin 2-aliryhmä kuten yllä, $z \in G$ ja n kokonaisluku, jolla*

$$z \equiv n^q \pmod{N}.$$

Tällöin z virittää ryhmän G, jos ja vain jos n on neliöepäjäännös modulo N.

Todistus. Jos z virittää ryhmän G, niin tällöin ryhmässä G pätee

$$1 = (n^q)^{2^e} = n^{2^e q} = n^{N-1}.$$

Toisaalta virittäjyydestä seuraa edelleen, että $n^{(N-1)/2} = -1$ ryhmässä G, joten $n^{(N-1)/2} \equiv -1 \pmod{N}$ ja siten n on Eulerin kriteerin nojalla neliöepäjäännös.
Jos n on neliöepäjäännös modulo N, niin tällöin

$$n^{(N-1)/2} \equiv -1 \pmod{N},$$

joten ryhmässä G pätee

$$n^{(2^e q)/2} = (n^q)^{2^{e-1}} = z^{2^{e-1}} = -1,$$

jolloin z on ryhmän G virittäjä. □

Näin ollen Tonelli–Shanks -algoritmin olennaiset vaiheet ovat seuraavat: Ensin etsitään alkio z, joka virittää Sylowin 2-aliryhmän G, ja tämän jälkeen etsitään yhtälöä 2.4 vastaava eksponentti k. Ensimmäisessä vaiheessa riittää lemman 2.13 nojalla generoida satunnaisesti kokonaisluku n, joka on neliöepäjäännös modulo N, minkä jälkeen saadaan virittäjä $z = n^q \bmod N$. Toisessa vaiheessa ei varsinaisesti etsitä eksponenttia k, vaan määritetään suoraan luvun

$$x = a^{(q+1)/2} z^{k/2}$$

arvo, joka on algoritmin lopputulos. Algoritmi saa syötteenä luvun a, joka on neliöjäännös modulo N ja jonka neliöjuuri lasketaan, sekä alkuluvun N.

Algoritmi 2. [3, s. 32–33] NELIÖJUURI(a, N)
Olkoot $N = 2^e q + 1$ alkuluku, missä q on pariton, ja a neliöjäännös modulo N.

1. Jos $a = 0$, niin palauta 0.
2. Generoi satunnaisesti tasaisella jakaumalla lukuja $n \in (\mathbb{Z}/N\mathbb{Z})^*$, kunnes $\left(\frac{n}{N}\right) = -1$. Aseta sitten $z \leftarrow n^q \bmod N$.
3. Aseta
$$\begin{aligned} y &\leftarrow z, \\ r &\leftarrow e, \\ x &\leftarrow a^{(q+1)/2} \bmod N \text{ ja} \\ b &\leftarrow a^q \bmod N. \end{aligned}$$
4. Jos $b \equiv 1 \pmod N$, niin palauta x. Muuten, etsi pienin kokonaisluku $m \geq 1$, jolla
$$b^{2^m} \equiv 1 \pmod N.$$
5. Aseta
$$\begin{aligned} t &\leftarrow y^{2^{r-m-1}} \bmod N, \\ y &\leftarrow t^2 \bmod N, \\ r &\leftarrow m, \\ x &\leftarrow xt \bmod N \text{ ja} \\ b &\leftarrow by \bmod N \end{aligned}$$
ja palaa vaiheeseen 3.

Huomautus. Vaiheen 3 alussa pätevät aina seuraavat ekvivalenssit:

$$\begin{aligned} ab &\equiv x^2 \pmod N, \\ y^{2^{r-1}} &\equiv -1 \pmod N \text{ ja} \\ b^{2^{r-1}} &\equiv 1 \pmod N. \end{aligned}$$

Tällöin y virittää ryhmän G Sylowin 2-aliryhmän G_r, jossa on 2^r alkiota ja jossa b on tällöin neliö. Jälkimmäisestä ehdosta seuraa, että $b^{2^m} = 1$ pätee viimeistään arvolla $m = r - 1$, joten luvun r arvo pienee jokaisella iteraatiolla. Tämä takaa sen, että algoritmi päättyy aina kunhan satunnaisella valinnalla löydetään neliöepäjäännös modulo N.

3 Elliptiset käyrät

Tässä luvussa käsitellään elliptisiä käyriä. Tämä tehdään luvussa 4 käsiteltävää alkulukutestausta silmällä pitäen, joten painoarvoa on annettu erityisesti äärellisten kuntien suhteen määritellyille elliptisille käyrille sekä näihin kuuluvien pisteiden lukumäärälle. Ensimmäisessä alaluvussa 3.1 käsitellään lyhyesti algebrallista geometriaa, sillä ovathan elliptiset käyrät alkujaan algebrallisen geometrian käsite. Tämän jälkeen alaluvussa 3.2 käsitellään elliptisiä käyriä yleisesti kunnan suhteen määriteltynä ja alaluvussa 3.3 käsitellään elliptisiä käyriä jäännösrenkaan suhteen määriteltynä. Tämän luvun viimeinen alaluku 3.4 on varattu äärellisen kunnan suhteen määriteltyjen elliptisien käyrien koon laskemiseen käytettyjen menetelmien tutkimiseen.

3.1 Algebrallista geometriaa

Kuten mainittua, ovat elliptiset käyrät algebrallisen geometrian käsite. Tästä syystä on mielekästä antaa lyhyt pohjustus tähän aihealueeseen antamalla määritelmät affiinille sekä projektiiviselle avaruudelle, joista jälkimmäisessä on elliptiset käyrät algebrallisessa geometriassa määritelty. Tämä alaluku pohjautuu täysin lähteen [17] luvun I alaluvuissa 2 ja 3 esitettyyn materiaaliin.

Määritelmä 3.1. (Affiini avaruus) Olkoon k kunta. Määritellään tällöin *affiini avaruus*

$$\mathbb{A}^n(k) := k^n.$$

Voidaan käyttää myös merkintää $\mathbb{A}^n$, mikäli vastaavasta kunnasta ei ole epäselvyyttä.

Affiinin avaruuden $\mathbb{A}^n$ origosta poikkeavien pisteiden välille voidaan muodostaa ekvivalenssirelaatio. Tämä relaatio, jolle käytetään merkintää $\sim$, määritellään seuraavasti: Kun $(0,\ldots,0) \neq (x_1,\ldots,x_n), (y_1,\ldots,y_n) \in \mathbb{A}^n$, niin $(x_1,\ldots,x_n) \sim (y_1,\ldots,y_n)$, mikäli on olemassa $\lambda \in k^*$, jolla

$$(y_1,\ldots,y_n) = \lambda(x_1,\ldots,x_n) = (\lambda x_1,\ldots,\lambda x_n).$$

On selvää, että kyseinen relaatio on ekvivalenssirelaatio. Pisteen $(x_1,\ldots,x_n)$ määräämää ekvivalenssiluokkaa merkitään muodossa $(x_1 : \ldots : x_n)$, missä ekvivalenssirelaationa toimii yllä määritelty relaatio $\sim$.

Määritelmä 3.2. (Projektiivinen avaruus) Olkoon k kunta. Määritellään tällöin *projektiivinen avaruus* $\mathbb{P}^n(k)$ affiinin avaruuden $\mathbb{A}^{n+1}$ pisteiden ekvivalenssiluokkien joukkona seuraavasti:

$$\mathbb{P}^n(k) := \{(x_0 : \ldots : x_n) \mid (x_0,\ldots,x_n) \in \mathbb{A}^{n+1},\ (x_0,\ldots,x_n) \neq (0,\ldots,0)\}.$$

Kuten affiinin avaruudenkin tapauksessa, voidaan projektiivista avaruutta merkitä myös muodossa $\mathbb{P}^n$, mikäli kunnasta ei ole epäselvyyttä.

Huomautus. Tämän tutkielman kannalta olennaisia projektiivisia avaruuksia ovat muotoa $\mathbb{P}^2$ olevat avaruudet, joita kutsutaan *projektiivisiksi tasoiksi*.

Projektiivisissa avaruuksissa ollaan kiinnostuneita erityisesti projektiivisista varistoista, jotka ovat niin kutsuttujen homogeenisten ideaalien määräämiä algebrallisia joukkoja eli vastaavien homogeenisten ideaalien polynomien nollakohtien joukkoja. Vaikka projektiivisten varistojen ominaisuuksia ei tulla tässä tutkielmassa montaa kertaa hyödyntämään, on niiden esittäminen silti mielekästä, sillä elliptiset käyrät ovat projektiivisen tason tietynlaisia projektiivisia varistoja. Ennen projektiivisen variston määrittelyä tarvitaan kuitenkin vielä homogeenisen polynomin ja homogeenisen ideaalin määritelmät sekä projektiivisen algebrallisen joukon määritelmä.

Määritelmä 3.3. (Homogeeninen polynomi) Olkoon $f \in k[X_0, \ldots, X_n]$. Tällöin f on astetta d oleva *homogeeninen polynomi*, mikäli

$$f(\lambda X_0, \ldots, \lambda X_n) = \lambda^d f(X_0, \ldots, X_n)$$

kaikilla $\lambda \in k$.

Huomautus. Polynomin homogeenisyys takaa, että projektiivisen avaruuden pisteet ovat hyvin määriteltyjä, sillä homogeeninen polynomi säilyttää ekvivalenssiluokan jonojen yhteyden toisiinsa. Nimittäin jos $(x_0, \ldots, x_n)$ ja $(y_0, \ldots, y_n)$ ovat saman ekvivalenssiluokan jonoja eli on olemassa $\lambda \in k^*$, jolla

$$(y_0, \ldots, y_n) = \lambda(x_0, \ldots, x_n) = (\lambda x_0, \ldots, \lambda x_n),$$

niin tällöin astetta d olevalla homogeenisellä polynomilla f pätee

$$f(y_0, \ldots, y_n) = f(\lambda x_0, \ldots, \lambda x_n) = \lambda^d f(x_0, \ldots, x_n).$$

Määritelmä 3.4. (Homogeeninen ideaali) Olkoon $I \subseteq k[X_0, \ldots, X_n]$ ideaali. Tällöin ideaali I on homogeeninen, mikäli se on homogeenisten polynomien virittämä.

Määritelmä 3.5. (Projektiivinen algebrallinen joukko) Olkoon $I \subseteq k[X_0, \ldots, X_n]$ homogeeninen ideaali. Tällöin ideaalin I määräämä *projektiivinen algebrallinen joukko* V_I on joukko

$$V_I = \{P \in \mathbb{P}^n \mid f(P) = 0 \text{ kaikilla } f \in I\}.$$

Toisaalta jos V on projektiivinen algebrallinen joukko, niin tämän homogeeninen ideaali $I(V)$ on renkaan $k[X_0, \ldots, X_n]$ ideaali, jonka virittää joukko

$$\{f \in k[X_0, \ldots, X_n] \mid f \text{ on homogeeninen ja } f(P) = 0 \text{ kaikilla } P \in V\}.$$

Määritelmä 3.6. (Projektiivinen varisto) Olkoon V projektiivinen algebrallinen joukko. Sanotaan, että V on *projektiivinen varisto*, jos tämän homogeeninen ideaali on renkaan $k[X_0, \ldots, X_n]$ alkuideaali.

Määritellään tämän alaluvun lopuksi projektiivisten varistojen välinen rationaalikuvaus sekä morfismi, joiden avulla voidaan määritellä myöhemmin elliptisten käyrien välinen isogenia. Tätä varten tarvitsee määritellä rationaalifunktio ja funktiokunta.

Määritelmä 3.7. (Rationaalifunktio) Olkoon k kunta. Tällöin *rationaalifunktio* F on

$$F(X_0, \ldots, X_n) = \frac{f(X_0, \ldots, X_n)}{g(X_0, \ldots, X_n)},$$

missä $f, g \in k[X_0, \ldots, X_n]$ ovat samaa astetta olevia homogeenisiä polynomeja. Sanotaan, että rationaalifunktio F on *säännöllinen* projektiivisen avaruuden $\mathbb{P}^n$ pisteessä P, mikäli $g(P) \neq 0$.

Määritelmä 3.8. (Funktiokunta) Olkoot k kunta ja $V \subseteq \mathbb{P}^n$ projektiivinen varisto. Tällöin variston V *funktiokunta* $k(V)$ on sellaisten rationaalifunktioiden

$$F(X_0, \ldots, X_n) = \frac{f(X_0, \ldots, X_n)}{g(X_0, \ldots, X_n)}$$

joukko, joilla pätee

1. $g \notin I(V)$ sekä
2. $\dfrac{f}{g} = \dfrac{f'}{g'}$, jos $fg' - f'g \in I(V)$, kun $\dfrac{f'}{g'} \in k(V)$.

Huomautus. Ehdosta 1 seuraa, että jokainen funktiokunnan $k(V)$ rationaalifunktio on säännöllinen ainakin yhdessä variston V pisteessä.

Määritelmä 3.9. (Rationaalikuvaus) Olkoot V_1 ja V_2 projektiivisia varistoja. Tällöin näiden välinen *rationaalikuvaus* ϕ on osittainen kuvaus

$$\phi = (f_0, \ldots, f_n) \colon V_1 \to V_2,$$

missä $f_0, \ldots, f_n \in k(V_1)$ ovat rationaalifunktioita. Siis

$$\phi(P) = (f_0(P), \ldots, f_n(P)) \in V_2$$

kaikilla pisteillä $P \in V_1$, joissa $f_0, \ldots, f_n$ ovat säännöllisiä.

Määritelmä 3.10. (Säännöllisyys ja morfismi) Olkoot V_1 ja V_2 projektiivisia varistoja ja

$$\phi = (f_0, \ldots, f_n) \colon V_1 \to V_2$$

rationaalikuvaus. Sanotaan, että ϕ on *säännöllinen* pisteessä $P \in V_1$, jos on olemassa rationaalifunktio $g \in k(V_1)$, jolla

1. gf_i on säännöllinen pisteessä P kaikilla $i = 0, \ldots, n$ ja
2. $(gf_i)(P) \neq 0$ jollakin $i \in 0, \ldots, n$.

Mikäli tällainen g on olemassa, niin asetetaan

$$\phi(P) = ((gf_0)(P), \ldots, (gf_n)(P)).$$

Jos rationaalikuvaus ϕ on säännöllinen kaikissa pisteissä $P \in V_1$, niin kuvausta ϕ kutsutaan *morfismiksi*. Tätä varten on mahdollista, että joukon V_1 eri pisteille tarvitsee valita eri rationaalifunktio g.

3.2 Elliptiset käyrät yleisessä kunnassa

Nyt kun projektiivinen taso on määritelty, voidaan tässä alaluvussa siirtyä määrittelemään itse elliptisiä käyriä. Tässä alaluvussa määritelmät tapahtuvat yleisesti mielivaltaisen kunnan suhteen, vaikkakin karakteristikaa 2 tai 3 olevat kunnat jätetään pois käsittelystä teorian monimutkaistumisesta johtuen. Tärkeimpinä asioina määritellään elliptinen käyrä sekä yhteenlasku tämän pisteiden välillä. Tässä alaluvussa esitetyt asiat perustuvat lähteeseen [17] sekä tutkielman tekijän omiin päätelmiin, ellei toisin mainita.

Määritelmä 3.11. (Elliptinen käyrä) Olkoon k kunta, jonka karakteristika ei ole 2 tai 3. Tällöin *elliptisen käyrän* määrää pari (A, B), missä A ja B ovat sellaisia kunnan k alkioita, joilla $\Delta_E = -16(4A^3 + 27B^2) \neq 0$. Tällöin käyrän E pisteet kunnan k suhteen ovat ne projektiivisen tason $\mathbb{P}^2$ pisteet, jotka toteuttavat niin sanotun *Weierstrassin yhtälön*, eli yhtälön

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

Täten saadaan joukko

$$E = \{(x : y : z) \in \mathbb{P}^2 \mid y^2z = x^3 + Axz^2 + Bz^3\}.$$

Elliptistä käyrää $E = (A, B)$ voidaan vaihtoehtoisesti merkitä myös muodossa $E(A, B)$ ja sen pisteiden joukkoa kunnan k suhteen voidaan merkitä muodossa $E(k)$. Arvoa Δ_E kutsutaan elliptisen käyrän E diskriminantiksi.

Huomautus. Etenkin merkintää $E(k)$ tullaan käyttämään tässä tutkielmassa useaan otteeseen.

Huomautus. Kyseessä on avaruuden $\mathbb{P}^2$ projektiivinen varisto, jonka homogeeninen ideaali on

$$< Y^2Z - X^3 - AXZ^2 - BZ^3 > \subseteq k[X, Y, Z].$$

Tutkitaan nyt, millaisia pisteitä elliptiset käyrät kunnan suhteen sisältävät. Olkoon $E = (A, B)$ elliptinen käyrä kunnan k suhteen määriteltynä. Nyt ensimmäinen havainto käyrästä E on se, että sillä on vain yksi piste, jossa $z = 0$, nimittäin piste $O = (0:1:0)$, joka on saatu joukosta $E(k)$ sijoittamalla $z = 0$ yhtälöön $y^2z = x^3 + Axz^2 + Bz^3$. Tällä sijoituksella nimittäin saadaan yhtälö muotoon $x^3 = 0$, mistä seuraa $x = 0$, jolloin jäljelle jää enää muuttujan y tarkastelu. Kuitenkaan muuttujan y arvolla ei ole merkitystä, sillä sen sisältämä termi on 0 joka tapauksessa, joten saadaan projektiivisen tason $\mathbb{P}^2$ pisteet $(0 : y : 0)$, missä $y \in k$, mikä on siis piste $(0 : 1 : 0)$. Loput joukon $E(k)$ pisteistä ovat muotoa $(x : y : 1)$, missä x ja y toteuttavat Weierstrassin yhtälön $y^2z = x^3 + Axz^2 + Bz^3$, sillä jos oletetaan, että $(x : y : z) \in E(k)$, missä $z \neq 1$ (ja $z \neq 0$), niin tällöin

$$\begin{aligned} y^2z = x^3 + Axz^2 + Bz^3 &\Leftrightarrow \frac{y^2z}{z^3} = \frac{x^3}{z^3} + \frac{Axz^2}{z^3} + \frac{Bz^3}{z^3} \\ &\Leftrightarrow \left(\frac{y}{z}\right)^2 = \left(\frac{x}{z}\right)^3 + A\left(\frac{x}{z}\right) + B. \end{aligned}$$

Täten piste $\left(\frac{x}{z} : \frac{y}{z} : 1\right)$ toteuttaa Weierstrassin yhtälön ja $(x, y, z) = (z \cdot \frac{x}{z}, z \cdot \frac{y}{z}, z \cdot 1)$, joten päädytään tilanteeseen $(x : y : z) = \left(\frac{x}{z} : \frac{y}{z} : 1\right)$, eli olennaisesti päädytään joka tapauksessa pisteeseen, jossa $z = 1$. Tästä voidaan kääntäen päätellä, että jos piste $(x : y : 1)$ toteuttaa elliptisen käyrän Weierstrassin yhtälön, niin tällöin kaikki ekvivalenssiluokan $(x : y : 1)$ pisteet $(x', y', z) = (zx, zy, z)$ toteuttavat saman Weierstrassin yhtälön. Yllä määriteltyä pistettä $O = (0 : 1 : 0)$ sanotaan käyrän $E(k)$ *nollapisteeksi*. Useissa lähteissä tätä kutsutaan myös *äärettömyyspisteeksi*, mutta kuten hieman myöhemmin tullaan huomaamaan, saadaan joukolle $E(k)$ muodostettua Abelin ryhmän rakenne yhteenlaskun suhteen, missä piste O toimii neutraalialkiona, joten on nollapiste on sikäli mielekäs nimitys pisteelle O.

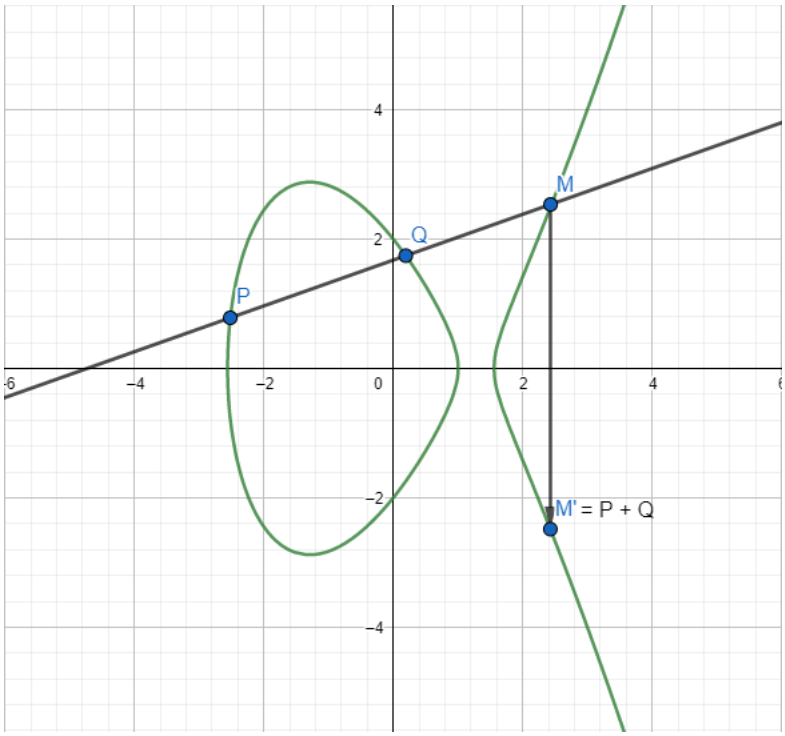
Lähdetään nyt muodostamaan Abelin ryhmää joukosta $E(k)$, missä k on kunta, jonka karakteristika ei ole 2 tai 3, ja $E = E(A, B)$ on elliptinen käyrä. Joukkona toimii siis $E(k)$, joka on määritelty jo yllä, joten tavoitteena on määritellä yhteenlasku tämän joukon pisteiden välille siten, että se toteuttaa Abelin ryhmän ehdot. Olkoon täten $P = (x_1 : y_1 : 1), Q = (x_2 : y_2 : 1) \in E(k)$ eli oletetaan, että $P, Q \neq O$. Ensinnäkin, määritellään $O + O = O$ ja $P + O = O + P = P$, jolloin voidaan todeta pisteen O olevan kyseisen ryhmän neutraalialkio. Toiseksi, asetetaan $P + Q = O$, jos ja vain jos $x_1 = x_2$ ja $y_1 = -y_2$, jolloin siis toisin sanoen saadaan määriteltyä vasta-alkio $-(x : y : 1) = (x : -y : 1)$ kaikilla $(x : y : 1) \in E(k)$. Muussa tapauksessa summan $S = (x_3 : y_3 : 1) = P + Q$ koordinaatit määritellään alkion $\lambda \in k$ avulla seuraavasti:

$$\begin{cases} x_3 = \lambda^2 - x_1 - x_2 \\ y_3 = \lambda(x_1 - x_3) - y_1, \end{cases}$$

missä $\lambda \in k$ on

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & \text{jos } x_2 \neq x_1 \\ \dfrac{3x_1^2 + A}{2y_1} & \text{muuten.} \end{cases}$$

Tämän niin kutsutun *tangentti ja jänne* -metodin intuitio voidaan selittää geometrisesti seuraavasti: Jos P ja Q ovat elliptisen käyrän pisteestä O poikkeavia pisteitä, niin tällöin kun asetetaan näiden pisteiden kautta kulkeva suora (tangentti tapauksessa $P = Q$), leikkaa tämä suora kyseisen käyrän kolmannessakin pisteessä M, jolloin summaksi saadaan tämän saadun pisteen M peilaus x-akselin suhteen. Piste M on joko P tai Q, mikäli kolmatta erillisitä leikkauspistettä ei ole.



Kuva 3.1: Elliptisen käyrän pisteiden P ja Q välisen summan geometrinen intuitio. Kuvan elliptinen käyrä on muodostettu Weierstrassin yhtälöstä $Y^2 = X^3 - 5X + 4$, jonka kuvaaja on piirretty tasossa $\mathbb{R}^2$. Pisteet P ja Q on valittu mielivaltaisesti kyseiseltä käyrältä.

Täten olemme saaneet määriteltyä yhteenlaskun joukolle $E(k)$, joten voimme vielä todeta, että kyseisellä laskutoimituksella saamme muodostettua juurikin Abelin ryhmän, niinkuin oli tarkoitus. Ensinnäkin, yhteenlasku on suljettu joukossa $E(k)$, mikä voidaan nähdä esimerkiksi yllä selostetusta geometrisesta tulkinnasta. Yhteenlaskun sulkeutuminen voitaisiin myös osoittaa algebrallisesti näyttämällä, että yllä määritelty piste $(x_3 : y_3 : 1)$ toteuttaa elliptisen käyrän Weierstrassin yhtälön, mutta tämä jätetään tutkielmasta pois sen työläisyyden takia. Neutraalialkion sekä vasta-alkioiden olemassaolot seuraavat suoraa määritelmästä ja kommutatiivisuus on myös sikäli selvä, että kahden pisteen välinen suora ei riipu näiden pisteiden järjestyksestä, jolloin ei näiden yhteenlaskun järjestyksellä ei myöskään ole merkitystä lopputuloksen kannalta. Assosiatiivisuuden osoittaminen voidaan tehdä geometrisesti tai algebrallisesti, mutta nämä ovat kuitenkin huomattavasti työläämpää kuin aiemmat kohdat, joten assosiatiivisyyden osoittaminen jätetään myös pois tästä tutkielmasta. Joitakin suuntaviivoja näiden sekä yhteenlaskun sulkeutumisen todistamiseen voi kuitenkin löytää muun muassa Silvermanin teoksesta [17].

Yllä elliptisen käyrän pisteet mielletään projektiivisen tason $\mathbb{P}^2$ pisteinä, mitä ne varsinaisesti ovatkin, sillä elliptiset käyrät ovat projektiivisia varistoja. Kuitenkin elliptisen käyrän pisteet voidaan aina palauttaa muotoon $(x : y : 1)$, joten tästä syystä pisteet voidaan mieltää käytännön kannalta myös pareina $(x, y) \in k^2$, missä x ja y toteuttavat yhtälön

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

ja elliptinen käyrä E kunnan k suhteen määriteltynä voidaan mieltää joukkona

$$E(k) = \{(x, y) \in k^2 \mid y^2 = x^3 + Ax + B\} \cup \{(0, 1)\}.$$

Tällä tavoin määriteltynä saadaan käytännöllisempi lähestymistapa elliptisiin käyriin, mikä on olennaista tutkielman myöhemmissä luvuissa käsiteltävien asioiden kannalta.

Esitellään tämän alaluvun lopuksi vielä elliptisen käyrän yhteenlasku- sekä monikerta-algoritmit. Näissä algoritmeissa, kuten kaikissa lopuissa tutkielman elliptisen käyrän pisteitä käsittelevissä algoritmeissa, elliptisten käyrien pisteitä käsitellään pareina (x, y) eikä ekvivalenssiluokkina $(x : y : 1)$.

Algoritmi 3. [5] SUMMA$((x_1, y_1), (x_2, y_2), (A, B))$

1. Jos $x_1 = x_2$ ja $y_1 = -y_2$, niin palauta O.

2. Jos $x_1 = x_2$ ja $y_1 = y_2$, niin aseta $\lambda \leftarrow \dfrac{3x_1^2 + A}{2y_1}$.
   Jos $x_1 \neq x_2$, niin aseta $\lambda \leftarrow \dfrac{y_2 - y_1}{x_2 - x_1}$.

3. Aseta
$$\begin{aligned} \beta &\leftarrow y_1 - \lambda x_1, \\ x_s &\leftarrow \lambda^2 - x_1 - x_2 \text{ ja} \\ y_s &\leftarrow -(\lambda x_s + \beta). \end{aligned}$$

4. Palauta (x_s, y_s).

Monikerta qP, missä q on positiivinen kokonaisluku, tapahtuu luonnollisesti toistamalla yllä määriteltyä yhteenlaskualgoritmia q kertaa pisteelle P. Tämä voidaan toteuttaa tehokkaasti seuraavalla rekursiivisella menettelyllä [5]:

$$qP = \begin{cases} P & \text{jos } q = 1 \\ \dfrac{q}{2}(P + P) & \text{jos } q \text{ on parillinen} \\ P + (q - 1)P & \text{jos } q \text{ on pariton.} \end{cases}$$

Tämä voidaan kirjoittaa myös algoritmin muodossa seuraavasti:

Algoritmi 4. MONIKERTA$(q, P, (A, B))$
Oletetaan, että $q \in \mathbb{Z}_{\geq 1}$.

1. Jos $q = 1$, niin palauta P.

2. Jos q on parillinen, niin palauta MONIKERTA$(q/2, P + P, (A, B))$.

3. Muussa tapauksessa palauta $(P +$ MONIKERTA$(q - 1, P, (A, B)))$.

3.3 Elliptiset käyrät jäännösluokkarenkaassa sekä äärellisessä kunnassa

Alaluvussa 3.2 käsiteltiin elliptisiä käyriä yleisellä tasolla jokseenkin mielivaltaisen kunnan suhteen. Tässä alaluvussa tullaan havaitsemaan, että elliptinen käyrä voidaan määritellä myös jäännösluokkarenkaan suhteen, mikä on olennaista erityisesti luvussa 4 käsiteltävää alkulukutestausta silmällä pitäen. Tärkeimmät tässä alaluvussa esiteltävät asiat ovat elliptisen käyrän määritteleminen jäännösluokkarenkaan suhteen, pseudosummana tunnetun laskutoimituksen määrittely ja Hassen lause, joka antaa ylä- ja alarajan äärellisen kunnan suhteen määritetyn elliptisen käyrän koolle. Tämä alaluku pohjautuu useisiin eri lähteisiin, jotka mainitaan erikseen tekstissä.

Määritelmä 3.12. [12] (Elliptinen käyrä renkaan $\mathbb{Z}/N\mathbb{Z}$ suhteen) Määritellään elliptinen käyrä $E = (A, B)$ renkaan $\mathbb{Z}/N\mathbb{Z}$ suhteen, missä N on positiivinen kokonaisluku ja $A, B \in \mathbb{Z}/N\mathbb{Z}$, joilla $4A^3 + 27B^2 \neq 0$. Käyrän E pisteiden joukko $E(\mathbb{Z}/N\mathbb{Z})$ on parien $(x, y) \in (\mathbb{Z}/N\mathbb{Z})^2$ joukko, joilla

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

Pisteiden välinen yhteenlasku tapahtuu algoritmin 5 kuvaamalla tavalla.

Huomautus. Kun elliptinen käyrä määritellään renkaan $\mathbb{Z}/N\mathbb{Z}$ suhteen, ei tällöin välttämättä saada Abelin ryhmän rakennetta joukolle $E(\mathbb{Z}/N\mathbb{Z})$. Nimittäin, pisteiden välisessä summassa tarvittavat käänteisalkiot eivät ole yleisesti olemassa ja toisaalta voi olla olemassa pisteet (x_1, y_1) ja (x_2, y_2), joilla

$$x_1 = x_2 \quad \text{ja} \quad y_1 \neq \pm y_2.$$

Kummassakaan tapauksessa summaa ei ole määritelty. Tämä ei kuitenkaan ole alkulukutestauksen kannalta ongelma, sillä mikäli Abelin ryhmän rakenne ei toteudu renkaalla $\mathbb{Z}/N\mathbb{Z}$, voidaan tällöin olla varmoja, että $\mathbb{Z}/N\mathbb{Z}$ ei ole kunta, jolloin N ei ole alkuluku.

Jos elliptinen käyrä $E = (A, B)$ määritellään yleisesti renkaan $\mathbb{Z}/N\mathbb{Z}$ suhteen, niin sen pisteiden välinen yhteenlasku voidaan toteuttaa myös alla esitetyllä PSEUDOSUMMA-nimisellä algoritmilla. Kyseisen algoritmin hyöty on siinä, että mikäli summassa vaadittavia käänteisalkioita ei löydy, niin algoritmi löytää tässä tapauksessa luvun N tekijän ja palauttaa tämän.

Algoritmi 5. [12] PSEUDOSUMMA$((x_1, y_1), (x_2, y_2), (A, B), N)$

1. Jos $x_1 = x_2$ ja $y_1 = -y_2$, niin palauta summa O.
2. Jos $x_1 \neq x_2$, niin:
   (a) Laske $d = \text{syt}(x_2 - x_1, N)$.
   (b) Jos $1 < d < N$, niin palauta tekijä d.
   (c) Jos $d = 1$, niin aseta $\lambda \leftarrow \dfrac{y_2 - y_1}{x_2 - x_1}$.
3. Jos $x_1 = x_2$ ja $y_1 = y_2$, niin:
   (a) Laske $d = \text{syt}(2y_1, N)$.
   (b) Jos $1 < d < N$, niin palauta tekijä d.
   (c) Jos $d = N$, niin palauta summa O.
   (d) Muuten aseta $\lambda \leftarrow \dfrac{3x_1^2 + A}{2y_1}$.

4. Aseta

$$\begin{aligned}\beta &\leftarrow y_1 - \lambda x_1,\\ x_s &\leftarrow \lambda^2 - x_1 - x_2 \text{ ja}\\ y_s &\leftarrow -(\lambda x_s + \beta).\end{aligned}$$

5. Palauta summa (x_s, y_s).

Olkoot $E = (A, B)$ elliptinen käyrä renkaan $\mathbb{Z}/N\mathbb{Z}$ suhteen ja $p > 3$ alkuluku, joka jakaa luvun N. Mikäli $4A^3 + 27B^2 \not\equiv 0 \pmod{p}$, niin käyrä E voidaan esittää myös moduloon p korvaamalla parin (A, B) parilla $(A_p, B_p) = (A \bmod p, B \bmod p) = E_p$. Jos $x \in \mathbb{Z}/N\mathbb{Z}$, niin merkitään $x_p = x \bmod p \in \mathbb{Z}/p\mathbb{Z}$ ja jos tällöin $P = (x, y) \in E(\mathbb{Z}/N\mathbb{Z})$, niin merkitään $P_p = (x_p, y_p) \in E_p(\mathbb{Z}/p\mathbb{Z})$. Seuraava tulos voidaan osoittaa, mikäli joukon $E(\mathbb{Z}/N\mathbb{Z})$ pisteiden P ja Q välinen summa on määritelty.

Lemma 3.13. [5] *Jos $E = (A, B)$ on elliptinen käyrä renkaan $\mathbb{Z}/N\mathbb{Z}$ suhteen ja $P, Q \in E(\mathbb{Z}/N\mathbb{Z})$, joilla $P + Q$ on määritelty, niin tällöin*

$$(P + Q)_p = P_p + Q_p.$$

Todistus. Esitetään todistus pääpiirteissään hahmotelman omaisesti. Mikäli $P = O$ tai $Q = O$, niin väite on triviaalisti tosi. Oletetaan siis, että $P, Q \neq O$, ja merkitään $P = (x_1, y_1)$ sekä $Q = (x_2, y_2)$. Pisteiden välisen summan lopputulos voidaan mieltää joukon $\mathbb{Z}/N\mathbb{Z}$ rationaalifunktiona ja tätä seikkaa hyödynnetään todistuksen edetessä. Jos nyt $R(x_1, x_2, \ldots, x_n)$ on rationaalifunktio joukon $\mathbb{Z}/N\mathbb{Z}$ suhteen, niin huomataan, että joko $R(x_1, x_2, \ldots, x_n)$ ei ole määritelty tai

$$(R(x_1, x_2, \ldots, x_n)_p)_p = R((x_1)_p, (x_2)_p, \ldots, (x_n)_p).$$

Laskiessa rationaalifunktiota $R((x_1)_p, (x_2)_p, \ldots, (x_n)_p)$ otetaan rationaalifunktion R kertoimet modulo p sen sijaan, että käytettäisiin niitä modulo N. Nyt pisteiden välinen summa ottaa huomioon kolme eri tapausta:

1. Jos $x_1 = x_2$ ja $y_1 = -y_2$, niin lopputulos on O.

2. Jos $P = Q$, niin summan lopputulos on

$$\left(\frac{F(x_1, x_2, y_1, y_2, A, B)}{(2y_1)^3}, \frac{G(x_1, x_2, y_1, y_2, A, B)}{(2y_1)^3}\right).$$

3. Jos $x_1 \neq x_2$, niin saadaan

$$\left(\frac{R(x_1, x_2, y_1, y_2, A, B)}{(x_2 - x_1)^3}, \frac{S(x_1, x_2, y_1, y_2, A, B)}{(x_2 - x_1)^3}\right)$$

Tässä F, G, R ja S ovat $\mathbb{Z}/N\mathbb{Z}$-kertoimisia polynomeja. Nyt jos (P, Q) ja (P_p, Q_p) päätyvät samaan tapaukseen kolmesta yllä määritellystä tapauksesta, niin tällöin SUMMA-algoritmi muodostaa saman rationaalifunktion luvuilla x_1, x_2, y_1 ja y_2 kuin mitä se tuottaa luvuilla $(x_1)_p, (x_2)_p, (y_1)_p$ ja $(y_2)_p$, jolloin lemman väite seuraa. Enää täytyy siis osoittaa, että jos (P, Q) ja (P_p, Q_p) päätyvät eri tapauksiin, niin tällöin $P + Q$ ei ole määritelty. Tämä voi tapahtua, jos joko

1. $x_1 = x_2$, mutta $y_1 \neq \pm y_2$, tai

2. $x_1 \neq x_2$, mutta $(x_1)_p = (x_2)_p$.

Ensimmäisessä tapauksessa summaa $P+Q$ ei ole määritelty. Jälkimmäisessä tapauksessa ehdosta $(x_1)_p = (x_2)_p$ seuraa $x_2 \equiv x_1 \pmod{p}$, jolloin $p \mid (x_2 - x_1)$, joten luvun $x_2 - x_1$ käänteisalkiota ei voida määrittää eli summaa $P + Q$ ei voida määritellä. Muita tapauksia ei ole, sillä tiedetään, että $a = b \Rightarrow a_p = b_p$ ja $a = -b \Rightarrow a_p = -b_p$. Täten jos $P + Q$ on määritelty, niin tämä tuottaa saman rationaalifunktion kuin $P_p + Q_p$ ja siten lemman väite seuraa. □

Tämän luvun loppuosassa tarkastellaan elliptisiä käyriä äärellisen kunnan suhteen määriteltyinä. Erityisenä mielenkiinnon kohteena on muotoa $\mathbb{Z}/N\mathbb{Z}$ olevat kunnat, missä N on alkuluku, sillä tällaiset kunnat ovat keskiössä Goldwasser–Kilian -algoritmia käsiteltäessä. Ensin tarvitaan kuitenkin määritelmät elliptisten käyrien väliselle isogenialle, endomorfismirenkaalle sekä tämän renkaan alkioiden astekuvaukselle. Loput tämän alaluvun esitettävistä asioista perustuu Silvermanin teokseen [17].

Määritelmä 3.14. (Isogenia) Olkoot E_1 ja E_2 elliptisiä käyriä. Näiden välinen *isogenia* on morfismi

$$\phi\colon E_1 \to E_2,$$

jolle pätee $\phi(O_1) = O_2$. Sanotaan, että E_1 ja E_2 ovat *isogeenisiä*, jos näiden välillä on olemassa isogenia ϕ, jolla $\phi(E_1) \neq \{O_2\}$.

Huomautus. Voitaisiin osoittaa, että jokainen isogenia on ryhmähomomorfismi elliptisten käyrien välillä, joka säilyttää pisteiden välisen yhteenlaskun. Tämän lisäksi voidaan itse asiassa osoittaa, että jokaisella isogenialla $\phi\colon E_1 \to E_2$ pätee aina joko $\phi(E_1) = \{O_2\}$ tai $\phi(E_1) = E_2$. Alaluvusta 3.1 muistetaan, että morfismi on rationaalikuvaus, joka on säännöllinen kaikissa käyrän E_1 pisteissä.

Määritelmä 3.15. (Endomorfismirengas) Olkoon E elliptinen käyrä. Tällöin elliptisen käyrän E *endomorfismirengas* $\mathrm{End}(E)$ on kaikkien isogenioiden $\phi\colon E \to E$ joukko, jossa yhteenlasku- ja kertolaskuoperaatiot määritellään seuraavasti:

1. $(\psi + \phi)(P) = \psi(P) + \phi(P)$ ja

2. $(\psi\phi)(P) = \psi(\phi(P))$.

Huomautus. Todistusta sille, että renkaan aksioomat toteutuvat, ei esitetä tässä tutkielmassa. Tämän todistuksen voi kuitenkin löytää Silvermanin teoksesta.

Seuraavaksi esiteltävä astekuvauksen määritelmä ei päde yleisesti kaikilla kunnilla, mutta jäännösluokkakunnassa se kuitenkin pätee, mikä riittää tämän tutkielman kannalta.

Määritelmä 3.16. (Astekuvaus) Olkoot N alkuluku ja E elliptinen käyrä kunnan $\mathbb{Z}/N\mathbb{Z}$ suhteen. Tällöin *astekuvaus* joukon $\mathrm{End}(E)$ alkioille on kuvaus

$$\deg\colon \mathrm{End}(E) \to \mathbb{Z},\ \phi \mapsto |\ker(\phi)|\,.$$

Alkion ϕ kuvaa tässä kuvauksessa kutsutaan alkion ϕ *asteeksi*.

Esimerkki 3.17. Olkoot N alkuluku, E kunnan $\mathbb{Z}/N\mathbb{Z}$ suhteen määritelty elliptinen käyrä ja $n \in \mathbb{N}$. Tällöin voidaan määritellä monikertaisogenia $[n] \in \mathrm{End}(E)$, jossa

$$[n](P) = \underbrace{P + \cdots + P}_{n \text{ kpl}}.$$

Tällöin pätee $\deg([n]) = n^2$. Yksi erikoistapaus tästä on isogenia $[0]$, jolla pätee $[0](P) = O$ kaikilla $P \in E$.

Todistus. Todistus asteen arvolle sivuutetaan tässä tutkielmassa sen työläisyyden vuoksi. Todistuksen voi tosin löytää Silvermanin teoksesta. □

Astekuvaus on hyödyllinen työkalu Hassen lauseen todistamisessa, sillä astekuvaus on niin kutsuttu positiivisesti määrätty neliömuoto, minkä takia sillä on joitakin hyödyllisiä ominaisuuksia todistusta ajatellen. Määritellään seuraavaksi positiivisesti määrätty neliömuoto.

Määritelmä 3.18. (Neliömuoto) Olkoon A Abelin ryhmä. Tällöin kuvaus

$$d\colon A \to \mathbb{R}$$

on *neliömuoto*, mikäli

1. $d(\alpha) = d(-\alpha)$ kaikilla $\alpha \in A$ ja
2. kuvaus
$$L\colon A \times A \to \mathbb{R}, \quad (\alpha, \beta) \mapsto d(\alpha + \beta) - d(\alpha) - d(\beta)$$
on bilineaarinen.

Jos lisäksi pätee

1. $d(\alpha) \geq 0$ kaikilla $\alpha \in A$ ja
2. $d(\alpha) = 0$, jos ja vain jos $\alpha = 0$,

niin neliömuoto d on *positiivisesti määrätty*.

Huomautus. Ehdosta 2 seuraa muun muassa yhtäsuuruus $d(m\alpha) = m^2 d(\alpha)$ kaikilla $\alpha \in A$ ja kokonaisluvuilla m. Nimittäin

$$\begin{aligned} L(m\alpha, -m\alpha) &= d(m\alpha - m\alpha) - d(m\alpha) - d(-m\alpha) \\ &= -2d(m\alpha) \end{aligned}$$

ja toisaalta bilineaarisuuden nojalla

$$L(m\alpha, -m\alpha) = m^2 L(\alpha, -\alpha) = -2m^2 d(\alpha),$$

joten $d(m\alpha) = m^2 d(\alpha)$.

Lemma 3.19. *Olkoot N alkuluku ja E kunnan $\mathbb{Z}/N\mathbb{Z}$ suhteen määritelty elliptinen käyrä. Tällöin astekuvaus*

$$\deg\colon \mathrm{End}(E) \to \mathbb{Z}$$

on positiivisesti määrätty neliömuoto.

Todistus. Todistuksen haastava osuus on bilineaarisuuden osoittaminen. Tähän tarvitaan isogenioiden, erityisesti monikertaisogenioiden, ominaisuuksia, joiden osoittaminen itsessään on jo työläs tehtävä. Tästä syystä todistus sivuutetaan tässä tutkielmassa, tosin todistuksen voi löytää Silvermanin teoksesta. □

Lemma 3.20. *Olkoot E elliptinen käyrä ja $\phi, \psi \in \mathrm{End}(E)$. Tällöin pätee*

$$|\deg(\phi - \psi) - \deg(\phi) - \deg(\psi)| \leq 2\sqrt{\deg(\phi)\deg(\psi)}.$$

Todistus. Olkoot $\phi, \psi \in \mathrm{End}(E)$ ja asetetaan

$$L(\psi, \phi) = \deg(\psi - \phi) - \deg(\phi) - \deg(\psi).$$

Nyt L on bilineaarinen, sillä deg on lemman 3.19 nojalla neliömuoto. Täten kaikilla kokonaisluvuilla m ja n pätee

$$\begin{aligned} mnL(\psi, \phi) = L(m\psi, n\phi) &= \deg(m\psi - n\phi) - \deg(n\phi) - \deg(m\psi) \\ &= \deg(m\psi - n\phi) - n^2 \deg(\phi) - m^2 \deg(\psi). \end{aligned}$$

Yhtäsuuruus $\deg(n\xi) = n^2 \deg(\xi)$ kaikilla $\xi \in \mathrm{End}(E)$ ja kokonaisluvuilla n on osoitettu määritelmän 3.18 huomautuksessa. Lemman 3.19 nojalla deg on lisäksi positiivisesti määrätty, joten

$$0 \leq \deg(m\psi - n\phi) = m^2 \deg(\psi) + mnL(\psi, \phi) + n^2 \deg(\phi),$$

jolloin asettamalla $m = -L(\psi, \phi)$ ja $n = 2\deg(\psi)$ saadaan

$$\begin{aligned} &0 \leq \deg(\psi)\big(4\deg(\psi)\deg(\phi) - L(\psi, \phi)^2\big) \\ &\Rightarrow L(\psi, \phi)^2 \leq 4\deg(\psi)\deg(\phi) \\ &\Rightarrow |L(\psi, \phi)| \leq 2\sqrt{\deg(\psi)\deg(\phi)} \\ &\Rightarrow |\deg(\phi - \psi) - \deg(\phi) - \deg(\psi)| \leq 2\sqrt{\deg(\psi)\deg(\phi)}. \end{aligned}$$

Yllä oletetaan, että $\deg(\psi) \neq 0$, vaikkakin epäyhtälö on triviaalisti tosi myös tapauksessa $\deg(\psi) = 0$. □

Ennen Hassen lauseen käsittelyä tarvitsee vielä määritellä Frobeniuksen endomorfismi.

Määritelmä 3.21. (Frobeniuksen endomorfismi) Olkoon E kunnan $\mathbb{Z}/N\mathbb{Z}$ suhteen määritelty elliptinen käyrä. Tällöin käyrän E N:s *Frobeniuksen endomorfismi* on kuvaus

$$\phi\colon E(\mathbb{Z}/N\mathbb{Z}) \to E(\mathbb{Z}/N\mathbb{Z}), \quad (x, y) \mapsto (x^N, y^N).$$

Nyt voidaan esittää ja todistaa itse Hassen lause. Tällä merkittävällä tuloksella on tärkeä rooli äärellisten kuntien suhteen määriteltyjen elliptisten käyrien teoriassa ja se on avainasemassa myös Goldwasser–Kilian-algoritmin toiminnassa. Se luo nimittäin pohjan Schoofin algoritmille sekä lauseelle 4.2, jotka molemmat ovat keskeisessä asemassa Goldwasser–Kilian-algoritmin muodostamisessa.

Lause 3.22. *(Hassen lause) Olkoot N alkuluku ja E elliptinen käyrä kunnan $\mathbb{Z}/N\mathbb{Z}$ suhteen. Tällöin*

$$\big||E(\mathbb{Z}/N\mathbb{Z})| - N - 1\big| \leq 2\sqrt{N}.$$

Todistus. Olkoon $\phi\colon E \to E$ N:s Frobeniuksen endomorfismi, toisin sanoen

$$\phi\colon E \to E, \quad (x, y) \mapsto (x^N, y^N).$$

Nyt Fermat'n pienen lauseen nojalla

$$x^N \equiv x \pmod{N},$$

jolloin kaikilla $P \in E(\mathbb{Z}/N\mathbb{Z})$ pätee $\phi(P) = P$, joten kuvaus ϕ pitää itse asiassa elliptisen käyrän E pisteet paikallaan. Nyt toisaalta

$$\phi(P) - P = O \Leftrightarrow (\phi - 1)(P) = 0 \Leftrightarrow P \in \ker(\phi - 1),$$

joten saadaan $E(\mathbb{Z}/N\mathbb{Z}) = \ker(\phi - 1)$, missä luvulla 1 merkitään monikertaisogeniaa [1], joka on käytännössä identtinen kuvaus $E \to E$. Täten erityisesti siis

$$|E(\mathbb{Z}/N\mathbb{Z})| = |\ker(\phi - 1)| = \deg(\phi - 1).$$

Lemman 3.20 nojalla kuitenkin

$$|\deg(\phi - 1) - \deg(\phi) - \deg(1)| \leq 2\sqrt{\deg(\phi)\deg(1)},$$

missä $\deg(\phi - 1) = |E(\mathbb{Z}/N\mathbb{Z})|$, $\deg(\phi) = N$ ja $\deg(1) = 1$, joten päästään haluttuun tulokseen

$$\big||E(\mathbb{Z}/N\mathbb{Z})| - N - 1\big| \leq 2\sqrt{N}.$$

□

Huomautus. Tämän tutkielman kannalta olennaista on, että lauseen 3.22 avulla saadaan joukon $E(\mathbb{Z}/N\mathbb{Z})$ pisteiden lukumäärälle yläraja

$$|E(\mathbb{Z}/N\mathbb{Z})| \leq N + 1 + 2\sqrt{N}.$$

3.4 Elliptisen käyrän koko äärellisen kunnan suhteen

Eräs kiinnostava ongelma elliptisiä käyriä tutkittaessa on joukon $E(\mathbb{Z}/N\mathbb{Z})$ koon laskeminen. Puhtaan mielenkiinnon lisäksi tälle on käytännön sovelluskohteita muun muassa elliptisiä käyriä hyödyntävissä kryptografian sekä alkulukutestauksen menetelmissä, joista jälkimmäisestä esimerkkinä käy juurikin tässä tutkielmassa esiteltävän Goldwasser–Kilian-algoritmin toiminta vaatii joukon $E(\mathbb{Z}/N\mathbb{Z})$ koon toistuvaa laskemista luvun p eri arvoilla. Tehokasta ratkaisua tähän ongelmaan ei ollut saatavilla ennen kuin René Schoof vuonna 1985 tarjosi artikkelissaan [15] teoreettisen polynomiajassa suoriutuvan niin kutsutun Schoofin algoritmin, joka mullisti äärellisten kuntien suhteen määriteltyjen elliptisten käyrien teoriaa. Tässä alaluvussa perehdytään joihinkin yksinkertaisiin menetelmiin joukon $E(\mathbb{Z}/N\mathbb{Z})$ koon laskemiseksi sekä riittävällä tasolla itse Schoofin algoritmiin. Tämä alaluku pohjautuu pääasiassa lähteeseen [15].

Oletetaan, että N on alkuluku.

Olkoon $E = (A, B)$ kunnan $\mathbb{Z}/N\mathbb{Z}$ suhteen määritelty elliptinen käyrä. Nyt halutaan siis määrittää eri pisteiden $(x, y) \in E(\mathbb{Z}/N\mathbb{Z})$ lukumäärä, jolloin mukaanluettuna äärettömyyspiste O saadaan joukon $E(\mathbb{Z}/N\mathbb{Z})$ koko. Ensimmäinen intuitiivinen idea on määrittää koko niin kutsutusti "raa'alla voimalla", eli käymällä läpi kaikki pisteet $(x, y) \in (\mathbb{Z}/N\mathbb{Z})^2$ ja testata, millä pisteillä pätee

$$y^2 \equiv x^3 + Ax + B \pmod{N}. \tag{3.1}$$

Tämä on yksinkertainen ja varmasti toimiva menetelmä. Kuitenkin varjopuolena joudutaan yhtälö 3.1 testaamaan kaikilla $x \in \mathbb{Z}/N\mathbb{Z}$ ja $y \in \mathbb{Z}/N\mathbb{Z}$, eli yhteensä N^2 kertaa. Täten, kyseessä on suhteellisen raskas ajassa $O(N^2)$ suoriutuva algoritmi, jolla ei ole juurikaan käyttöarvoa suurilla luvun N arvoilla.

Tätä on kuitenkin mahdollista optimoida. Nimittäin, jos tiedetään, että $z = x^3 + Ax + B$ on neliöjäännös modulo N, niin tällöin tiedetään, että neliöjuurella $\sqrt{z}$ on kaksi eri ratkaisua, mikäli $N \nmid z$, ja yksi ratkaisu, jos $N \mid z$. Tämän tiedon nojalla voidaan jokaisella luvun x arvolla laskea luvun y sopivien arvojen lukumäärä, jolloin riittää käydä läpi vain kaikki $x \in \mathbb{Z}/N\mathbb{Z}$. Täten saadaan

$$|E(\mathbb{Z}/N\mathbb{Z})| = 1 + \sum_{x \in \mathbb{Z}/N\mathbb{Z}} \left(\left(\frac{x^3 + Ax + B}{N} \right) + 1 \right),$$

missä luku 1 summan alussa viittaa äärettömyyspisteeseen ja $\left(\frac{x^3 + Ax + B}{N} \right)$ on Legendren symboli. Summa $\left(\frac{x^3 + Ax + B}{N} \right) + 1$ tuottaa aina neliöjuurien (eli luvun y arvojen) lukumäärän kyseisellä luvun x arvolla Legendren symbolin käyttäytymisestä johtuen. Legendren symbolin arvo taas voidaan määrittää hyödyntämällä lausetta 2.5. Siis jokaisella $x \in \mathbb{Z}/N\mathbb{Z}$ pahimmassa tapauksessa lasketaan vain jakojäännös $(x^3 + Ax + B)^{(N-1)/2} \bmod N$, mikä tapahtuu suhteellisen tehokkaasti toistuvalla neliöinnillä, joten tällä menettelyllä saadaan hieman intuitiivista menetelmää tehokkaammin suoriutuva algoritmi elliptisen käyrän koon laskemiseen.

Tämän alaluvun lopuksi käsitellään pääpiirteissään yhtä tehokkaimmista joukon $E(\mathbb{Z}/N\mathbb{Z})$ laskemiseen käytetyistä menetelmistä, nimittäin Schoofin algoritmia. Täsmällinen perehtyminen ei tämän tutkielman puitteissa ole mahdollista, sillä algoritmin vaatiman teorian esittäminen vaatisi huomattavan paljon työtä. Kuitenkin sen rooli Goldwasser–Kilian -algoritmissa on hyvin merkittävä, joten sen esittäminen on tästä syystä mielekästä. Aloitetaan määrittelemällä elliptisen käyrän l-torsiopisteet.

Määritelmä 3.23. (Elliptisen käyrän l-torsiopisteet) Olkoot E elliptinen käyrä kunnan $\mathbb{Z}/N\mathbb{Z}$ suhteen ja $l > 0$ kokonaisluku. Joukon $E(\mathbb{Z}/N\mathbb{Z})$ l-torsiopisteiden joukko $E[l]$ määritellään seuraavasti:

$$E[l] := \{P \in E(\mathbb{Z}/N\mathbb{Z}) \mid lP = O\}.$$

Määritelmä 3.24. (Jakopolynomit) Olkoon $\mathbb{Z}/N\mathbb{Z}$ kunta. *Jakopolynomit* $\psi_n \in (\mathbb{Z}/N\mathbb{Z})[X, Y]$, $n \in \mathbb{Z}_{\geq -1}$, määritellään rekursiivisesti seuraavalla tavalla:

$$\begin{aligned}
&\psi_{-1}(X,Y) = -1,\ \psi_0(X,Y) = 0,\ \psi_1(X,Y) = 1,\ \psi_2(X,Y) = 2Y,\\
&\psi_3(X,Y) = 3X^4 + 6AX^2 + 12BX - A^2,\\
&\psi_4(X,Y) = 4Y(X^6 + 5AX^4 + 20BX^3 - 5A^2X^2 - 4ABX - 8B^2 - A^3),\\
&\psi_{2n}(X,Y) = \psi_n(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2)/2Y,\\
&\psi_{2n+1}(X,Y) = \psi_{n+2}\psi_n^3 - \psi_{n+1}^3\psi_{n-1}.
\end{aligned}$$

Huomautus. Jakopolynomille ψ_l pätee $\psi_l(P) = 0$ täsmälleen elliptisen käyrän E l-torsiopisteillä P.

Määritellään vielä polynomi $f_n \in (\mathbb{Z}/N\mathbb{Z})[X]$ polynomista ψ_n seuraavasti: Eliminoidaan Y^2-termit Weierstrassin yhtälön

$$Y^2 = X^3 + AX + B$$

avulla. Tällöin jäljelle jäävä polynomi $\psi_n'(X,Y)$ kuuluu renkaaseen $(\mathbb{Z}/N\mathbb{Z})[X]$, jos n on pariton, ja renkaaseen $Y(\mathbb{Z}/N\mathbb{Z})[X]$, jos n on parillinen. Täten määritellään

$$f_n(X) = \begin{cases} \psi_n'(X,Y), & \text{jos } n \text{ on pariton,} \\ \psi_n'(X,Y)/Y, & \text{jos } n \text{ on parillinen.} \end{cases}$$

Lause 3.25. *Olkoot $P = (x,y) \in E(\mathbb{Z}/N\mathbb{Z})$ ja $n \in \mathbb{Z}_{\geq -1}$. Mikäli $nP \neq O$, niin*

$$nP = \left(x - \frac{\psi_{n-1}\psi_{n+1}}{\psi_n^2}, \frac{\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2}{4Y\psi_n^3} \right).$$

Tässä $\psi_k = \psi_k(x,y)$. Jos oletetaan lisäksi, että $P \notin E[2]$, niin tällöin $nP = O$, jos ja vain jos $f_n(x) = 0$.

Todistus. Sivuutetaan tässä tutkielmassa. Todistuksen voi löytää Taten vuonna 1974 julkaistusta artikkelista [18]. □

Olkoon E kunnan $\mathbb{Z}/N\mathbb{Z}$ suhteen määritelty elliptinen käyrä. Nyt lauseen 3.22 nojalla tiedämme, että $|E(\mathbb{Z}/N\mathbb{Z})| \leq N + 1 + 2\sqrt{N}$. Toisin ilmaistuna voidaan sanoa, että

$$|E(\mathbb{Z}/N\mathbb{Z})| = N + 1 - t,$$

missä t on kokonaisluku, jolla $|t| \leq 2\sqrt{N}$. Täten laskeakseen joukon $E(\mathbb{Z}/N\mathbb{Z})$ koon, riittää määrittää luvun t arvo. Tämä voidaan tehdä laskemalla jakojäännöksen $t \bmod l$ arvo riittävän monella pienellä alkuluvulla $l = 3, 5, 7, \ldots, L$, $l \neq N$, joille pätee

$$M = \prod_{l \leq L,\ l \neq 2, N} l > 4\sqrt{N},$$

jolloin lauseen 2.7 (kiinalainen jäännöslause) nojalla voidaan määrittää luvun $0 \leq t < M$ arvo yksikäsitteisesti. Tämä on Schoofin algoritmin perusajatus. Huomautettakoon vielä, että jakojäännökset $t \bmod l$ voidaan määrittää tietämättä luvun t arvoa.

Olennaisesti Schoofin algoritmissa tärkeimmäksi tehtäväksi muodostuu jakojäännöksen $t \bmod l$ laskeminen kaikilla luvun M alkutekijöillä l. Schoofin (1985) idea oli laskea, milloin yhtälö

$$\phi^2 - t'\phi + N = 0 \tag{3.2}$$

pätee käyrän E l-torsiopisteissä, kun $l = 3, 5, 7, 11, \ldots, L$ ja $t' \in \mathbb{Z}/l\mathbb{Z}$. Voidaan huomata, että tämä pätee vain sellaisilla luvun t' arvoilla, joilla $t' \equiv t \pmod{l}$, joten tällä menettelyllä saadaan määritettyä jakojäännökset $t \bmod l$. Seuraava aputulos antaa ehdon yhtälön 3.2 toteutumiselle.

Lemma 3.26. *Jos $l \in \{3, 5, 7, 11, \ldots, L\} \setminus \{N\}$ ja $t' \in \mathbb{Z}/l\mathbb{Z}$, niin*

$$\phi^2(x,y) + N(x,y) = t'\phi(x,y) \quad \textit{kaikilla } (x,y) \in E[l],$$

jos ja vain jos

$$(X^{N^2}, Y^{N^2}) + N'(X,Y) \equiv t'(X^N, Y^N) \pmod{\psi_l, Y^2 - X^3 - AX - B},$$

missä $N' = (N \bmod l)$.

Todistus. "⇒" Nyt pätee siis $(\phi^2 + N - t'\phi)(x, y) = 0$ kaikilla $(x, y) \in E[l]$. Toisaalta kaikilla $(x, y) \in E[l]$ pätee myös $\psi_l(x, y) = 0$ ja $(Y^2 - X^3 - AX + B)(x, y) = 0$, joten

$$\begin{aligned}(\phi^2 + N - t'\phi)(x, y) &= ((X^{N^2}, Y^{N^2}) + N'(X, Y) - t'(X^N, Y^N))(x, y) \\ &= (f\psi_l + g(Y^2 - X^3 - AX + B))(x, y)\end{aligned}$$

kaikilla $(x, y) \in E[l]$ ja joillakin $f, g \in (\mathbb{Z}/N\mathbb{Z})[X, Y]$.
"⇐" Tämä suunta on selvä, sillä nyt $(X^{N^2}, Y^{N^2}) + N'(X, Y) - t'(X^N, Y^N)$ voidaan esittää polynomien ψ_l ja $Y^2 - X^3 - AX + B$ lineaarikombinaationa, jolloin suoraan seuraa, että

$$\phi^2(x, y) + N(x, y) = t'\phi(x, y) \quad \text{kaikilla } (x, y) \in E[l].$$

□

Täten jokaisella alkuluvulla l ja luvulla $t' \in \mathbb{Z}/l\mathbb{Z}$ lasketaan (X^{N^2}, Y^{N^2}), $N'(X, Y)$ ja $t'(X^N, Y^N)$ moduloon ψ_l ja $Y^2 - X^3 - AX - B$ kunnes pätee

$$(X^{N^2}, Y^{N^2}) + N'(X, Y) \equiv t'(X^N, Y^N) \pmod{\psi_l, Y^2 - X^3 - AX - B}.$$

Jos tämä ehto pätee, on $(t \bmod l)$ löydetty, jolloin voidaan siirtyä seuraavaan alkuluvun l arvoon. Kun $t_l = (t \bmod l)$ on laskettu kaikilla $l = 3, 5, \ldots, L$, voidaan luvun t arvo laskea seuraavasti: Määritetään $M_l = \dfrac{M}{l}$ kaikilla $3 \leq l \leq L$, jolloin selvästi $\text{syt}(l, M_l) = 1$. Seuraavaksi ratkaistaan luvut N_l yhtälöistä

$$N_l M_l \equiv 1 \pmod{l}$$

kaikilla $3 \leq l \leq L$. Tällöin luvun t arvoksi saadaan

$$t \equiv t_3 N_3 M_3 + \cdots + t_L N_L M_L \pmod{M}. \tag{3.3}$$

Nimittäin, $t \equiv t_l N_l M_l \equiv t_l \pmod{l}$ kaikilla $3 \leq l \leq L$, sillä kaikki muut summan 3.3 termit $t_p N_p M_p$, $p \neq l$, sisältävät tekijän l, jolloin nämä termit eivät vaikuta jakojäännökseen jaettaessa luvulla l. Toisaalta $N_l M_l \equiv 1 \pmod{l}$ kaikilla $3 \leq l \leq L$, joten on t yksikäsitteinen modulo M. Täten saadaan Schoofin algoritmi:

Algoritmi 6. SCHOOF$((A, B), N)$
Oletetaan, että $N > 3$ on alkuluku.

1. Etsi alkuluvut $3, 5, \ldots, L$, joilla $3 \cdot 5 \cdot \cdots \cdot L > 4\sqrt{N}$, ja aseta
$$M \leftarrow \prod_{3 \leq l \leq L} l.$$
2. Laske $t_l = t \bmod l$ jokaisella $l = 3, 5 \ldots, L$.
3. Laske jokaisella $l = 3, 5 \ldots, L$ luvut M_l sekä N_l, joilla $N_l M_l \equiv 1 \bmod l$.
4. Laske $t = t_3 N_3 M_3 + \cdots + t_L N_L M_L \bmod M$.
5. Palauta $N + 1 - t$.

Huomautus. Algoritmin raskain osuus on vaihe 2. Tämän suorittaminen esitettiin yllä pääpiirteissään, mutta täsmällisempiä työkaluja siihen ei anneta, koska se vaatisi enemmän työtä, kuin mitä tutkielman kannalta olisi mielekästä tehdä.

4 Elliptiset käyrät alkulukutestauksessa

Tässä vaiheessa on käsitelty riittävän paljon teoriaa elliptisiin käyriin ja alkulukutestaukseen liittyen, jotta voidaan alkaa yhdistämään näitä kahta aihealuetta ja perehtyä elliptisten käyrien hyödyntämiseen alkulukutestauksessa. Tavoitteena on käsitellä Shafi Goldwasserin ja Joe Kilianin vuonna 1986 julkaisema Goldwasser–Kilian-algoritmina tunnettu alkulukutesti sekä analysoida hieman todennäköisyyttä, jolla tämä algoritmi suoriutuu syöteluvun alkuluvuksi todistamisesta. Ensin esitellään lause 4.2, joka luo pohjan koko Goldwasser–Kilian-algoritmille, jonka jälkeen siirrytään muodostamaan itse algoritmia pala kerrallaan esimerkkejä käyttäen. Tässä luvussa läpikäydyt esimerkit ovat tutkielman tekijän itse keksimiä, mutta muutoin tämän luvun sisältö perustuu lähteeseen [5], ellei toisin mainita.

4.1 Goldwasser–Kilian-algoritmi

Ennen Goldwasser–Kilian-algoritmin käsittelyä on syytä määritellä todennäköisen alkuluvun käsite, sillä tämä käsite tulee kulkemaan mukana koko loppu tutkielman ajan.

Määritelmä 4.1. (Todennäköinen alkuluku) Olkoon N positiivinen kokonaisluku. Sanotaan, että N on *todennäköinen alkuluku*, jos N läpäisee jonkin satunnaisalkulukutestin.

Nyt voidaan alkaa käsittelemään itse Goldwasser–Kilian-algoritmia aloittamalla tuloksesta, joka luo pohjan koko testin toiminnalle.

Lause 4.2. *Olkoot N kokonaisluku, joka ei ole jaollinen luvuilla 2 tai 3, $A, B \in \mathbb{Z}/N\mathbb{Z}$, joilla* $\text{syt}(4A^3 + 27B^2, N) = 1$*, $E = (A, B)$ on elliptinen käyrä sekä $O \neq P \in E(\mathbb{Z}/N\mathbb{Z})$. Jos nyt pätee $qP = O$ jollakin alkuluvulla q, jolle lisäksi pätee*

$$q > (\sqrt[4]{N} + 1)^2,$$

niin tällöin N on alkuluku.

Todistus. Todistetaan väite vastaoletuksella. Oletetaan siis, että N on yhdistetty luku. Tällöin on olemassa alkutekijä $p \leq \sqrt{N}$, jolle oletusten nojalla pätee $p \neq 2, 3$. Edelleen oletusten nojalla on myös oltava $4A^3 + 27B^2 \not\equiv 0 \pmod{p}$. Täten $P_p \in E(\mathbb{Z}/p\mathbb{Z})$ ja lemmaa 3.13 toistuvasti soveltaen saadaan $qP_p = O$. Siis pisteen P_p asteen on jaettava luku q, mikä tarkoittaa sitä, että kyseisen asteen oltava täsmälleen q. Tämä johtuu siitä, että $P_p \neq O$, joten pisteen P_p aste ei ole 1, ja toisaalta q on alkuluku, joten vain q voi toteuttaa halutut ehdot. Nyt kuitenkin pisteen P_p aste voi olla korkeintaan $|E(\mathbb{Z}/p\mathbb{Z})|$ ja lauseen 3.22 (Hassen lause) nojalla

$$|E(\mathbb{Z}/p\mathbb{Z})| \leq p + 2\sqrt{p} + 1 = (\sqrt{p} + 1)^2 \leq (\sqrt[4]{N} + 1)^2 < q,$$

joten päädytään ristiriitaan. □

Lauseen 4.2 hyödyllisyys ilmenee siinä, että se mahdollistaa niin kutsutun DOWNRUN-prosessin. Tämä prosessi toimii seuraavasti: Ensin muodostetaan jono todennäköisiä alkulukuja

$$(N_0, N_1, \ldots, N_n),$$

missä kaikilla $i = 0, \ldots, n-1$ pätee $N_i > N_{i+1}$ sekä implikaatio

$$N_{i+1} \text{ on alkuluku } \Rightarrow N_i \text{ on alkuluku.}$$

Tällöin osoittaakseen, että N_0 on alkuluku, riittää osoittaa, että luku N_n on alkuluku, minkä jälkeen lumipalloefektin omaisesti jokainen kyseisen jonon luku osoittautuu alkuluvuksi. Perusajatuksena on siis redusoida luvun alkuluvuksi osoittaminen jonkin huomattavasti pienemmän alkuluvun osoittamiseksi. Jos nyt tarkastellaan lausetta 4.2, niin tämän nojalla todistaakseen, että N on alkuluku, täytyy löytää todennäköinen alkuluku q, jolla

$$qP = O \text{ jollakin } P \in E(\mathbb{Z}/N\mathbb{Z}) \quad \text{ja} \quad q > (\sqrt[4]{N} + 1)^2.$$

Jos tämän jälkeen saadaan todistettua, että q on alkuluku, niin lauseen 4.2 nojalla N on alkuluku. Nyt todistaakseen, että q on alkuluku, voidaan soveltaa lausetta 4.2 uudestaan, jolloin täytyy etsiä luvulle q uusi todennäköinen alkuluku q', joka toteuttaa lauseen ehdot. Saadaan DOWNRUN-prosessi, sillä tätä todennäköisten alkulukujen ketjuttamista jatketaan niin kauan, kunnes päädytään riittävän pieneen lukuun q, joka voidaan todistaa nopeasti alkuluvuksi jollakin deterministisellä testillä. Tästä lauseen 4.2 nojalla seuraa, että alkuperäinen luku N on alkuluku. Tämä on Goldwasser–Kilian -algoritmin toimintaperiaate, joka voidaan esittää korkealla tasolla seuraavasti:

Algoritmi 7. [2] GK(N)

1. Muodosta elliptinen käyrä E renkaan $\mathbb{Z}/N\mathbb{Z}$ suhteen, jolla $|E(\mathbb{Z}/N\mathbb{Z})| = m = 2q$ jollakin alkuluvulla q.

2. Tarkista, päteekö lauseen 4.2 ehdot käyrällä E ja luvulla q. Jos ehdot pätee, niin N on alkuluku. Muussa tapauksessa N on yhdistetty luku.

3. Luku q osoitetaan alkuluvuksi rekursiivisesti algoritmilla GK.

Yllä määritellystä Goldwasser–Kilian -algoritmin korkean tason esityksestä voidaan huomata, että algoritmin olennaisia vaiheita ovat ensin sopivan elliptisen käyrän $E = (A, B)$ muodostaminen renkaan $\mathbb{Z}/N\mathbb{Z}$ suhteen ja tämän jälkeen sopivaan elliptisen käyrän pisteen $P \in E(\mathbb{Z}/N\mathbb{Z})$ etsiminen. Esitetään nämä vaiheet omina algoritmeinaan aloittaen ensin mainitusta.

Elliptisen käyrän muodostaminen tapahtuu GENEROI-KÄYRÄ -nimisellä algoritmilla, jossa pareja $(A, B) = E$ muodostetaan satunnaisesti tasaisella jakaumalla kunnes pätee

$$\text{syt}(4A^3 + 27B^2, N) = 1 \quad \text{ja} \quad |E(\mathbb{Z}/N\mathbb{Z})| = 2q$$

jollakin todennäköisellä alkuluvulla q. Algoritmi palauttaa elliptisen käyrän (A, B) ja todennäköisen alkuluvun q.

Algoritmi 8. GENEROI-KÄYRÄ(N)

1. Generoi satunnaisesti tasaisella jakaumalla pari $(A, B) \in (\mathbb{Z}/N\mathbb{Z})^2$, jolla $\text{syt}(4A^3 + 27B^2, N) = 1$. Tällöin saadaan elliptinen käyrä $E = (A, B)$.

2. Laske $m = |E|$ esimerkiksi Schoofin algoritmia käyttäen. Jos m on pariton, palaa vaiheeseen 1. Muussa tapauksessa aseta $q = \dfrac{m}{2}$.

3. Jos $2, 3 \mid q$, niin palaa vaiheeseen 1.

4. Tarkista, että luku q on todennäköisesti alkuluku käyttäen jotakin riittävän tehokasta satunnaisalkulukutestiä, kuten Miller–Rabin -testiä. Jos q osoittautuu yhdistetyksi luvuksi, niin palaa vaiheeseen 1.

5. Palauta $((A, B), q)$.

Huomautus. Luvun syt$(4A^3+27B^2, N)$ arvo voidaan laskea tehokkaasti Eukleideen algoritmilla.

Vaiheessa 2. voitaisiin sallia yleisempikin tilanne, missä $m = rq$ jollakin r ja riittävän suurella q. Tämä kuitenkin monimutkaistaisi algoritmin analysointia, joten tyydymme esittämään algoritmin arvolla $r = 2$, kuten Goldwasser ja Kilian ovat sen esittäneet.

Esimerkki 4.3. Olkoon $N = 107$. Generoidaan elliptinen käyrä syötteestä N algoritmilla 8.

1. Generoidaan satunnaisesti pari $(A, B) \in \mathbb{Z}/107\mathbb{Z}$. Saadaan $(A, B) = (60, 102)$. Eukleideen algoritmilla nähdään, että syt$(4 \cdot 60^3 + 27 \cdot 102^2, 107) = 1$, joten saadaan elliptinen käyrä $E = (60, 102)$.

2. Käyrän E pisteiden lukumääräksi saadaan $|E(\mathbb{Z}/107\mathbb{Z})| = 120 = 2 \cdot 60$. Kuitenkin $2 \mid 60$ (ja $3 \mid 60$), joten palataan etsimään uusi pari (A, B).

3. Viiden uudelleengeneroinnin jälkeen saadaan pari $E = (A, B) = (84, 33)$, jolla syt$(4 \cdot 84^3 + 27 \cdot 33^2, 107) = 1$ ja $|E(\mathbb{Z}/107\mathbb{Z})| = 106 = 2 \cdot 53$, missä $2, 3 \nmid 53$.

4. MR$(53, 12)$ palauttaa TRUE, joten 53 on todennäköisesti alkuluku. Luvun 53 esittämiseen tarvitaan kuusi bittiä, joten siitä syystä Miller–Rabin toistetaan $2 \cdot 6 = 12$ kertaa.

5. Palautetaan $((84, 33), 53)$.

Seuraava vaihe on VALITSE-PISTE-nimellä kutsuttu algoritmi, joka saa syötteenä luvut N ja q sekä elliptisen käyrän $E = (A, B)$. Tämä algoritmi etsii elliptisen käyrän $E = (A, B)$ pisteen P, jolle pätee $P \neq O$ ja $qP = O$.

Algoritmi 9. VALITSE-PISTE$(N, q, (A, B))$

1. Generoi satunnaisesti tasaisella jakaumalla $x \in \mathbb{Z}/N\mathbb{Z}$, jolla $z = x^3+Ax+B$ on neliöjäännös modulo N.

2. Laske $y = \sqrt{z}$ ja aseta $P \leftarrow (x, y)$.

3. Laske qP. Jos $qP \neq O$, niin palaa vaiheeseen 1.

4. Palauta P.

Huomautus. Vaiheessa 1 selvittääkseen, onko z neliö, riittää lauseen 2.5 nojalla tarkastaa, että

$$z^{(N-1)/2} \equiv 1 \pmod{N}.$$

Vaikka lause 2.5 vaatii, että N on alkuluku, voidaan sitä silti hyödyntää tietämättä, onko N alkuluku. Nimittäin, jos

$$z^{(N-1)/2} \not\equiv \pm 1 \pmod{N},$$

niin tämä osoittaisi, että N on yhdistetty luku, mikä on joka tapauksessa Goldwasser–Kilian-algoritmin kannalta hyödyllinen tieto. Vaiheen 2 neliöjuuren laskeminen voidaan toteuttaa esimerkiksi Tonelli–Shanks-algoritmia käyttäen.

Esimerkki 4.4. Jatketaan esimerkkiä 4.3 etsimällä elliptisen käyrän $E = (84, 33)$ piste P, jolla pätee $53P = O$.

1. Generoidaan satunnaisesti tasaisella jakaumalla $x \in \mathbb{Z}/107\mathbb{Z}$. Saadaan $x = 60$.

2. Lasketaan $z = x^3 + 84x + 33$ renkaassa $\mathbb{Z}/107\mathbb{Z}$. Tämän arvoksi saadaan $z = 11$.

3. Lasketaan $z^{(N-1)/2} \bmod N = 11^{53} \bmod 107$. Saadaan $z^{53} \equiv 1 \pmod{107}$, joten neliöjuuri $\sqrt{z}$ on olemassa.

4. Lasketaan siis $y = \sqrt{z} = \sqrt{11}$ renkaassa $\mathbb{Z}/107\mathbb{Z}$. Saadaan $y = 15$, joten saadaan piste $P = (x, y) = (60, 15)$.

5. Lasketaan $53P$. Havaitaan, että $53P = O$, joten pisteellä $P = (60, 15)$ pätee halutut ehdot.

6. Palautetaan $P = (60, 15)$.

Seuraavan algoritmin tarkoitus on vain nivoa yhteen kaksi edellistä algoritmia ja palauttaa niiden lopputulema, johon kuuluu siis elliptinen käyrä (A, B), tämän käyrän piste P ja todennäköinen alkuluku q.

Algoritmi 10. PÄÄVAIHE(N)

1. Laske $((A, B), q) \leftarrow$ GENEROI-KÄYRÄ(N).

2. Laske $P \leftarrow$ VALITSE-PISTE($N, q, (A, B)$).

3. Palauta $((A, B), P, q)$.

Nyt voidaan esitellä täsmällisemmin Goldwasser–Kilian-algoritmi. Algoritmin tavoitteena on siis muodostaa syöteluvulle N muotoa

$$((A_0, B_0), P_0, N_1), \ldots, ((A_{i-1}, B_{i-1}), P_{i-1}, N_i)$$

oleva sertifikaatti, josta voidaan nopeasti tarkastaa, että N on alkuluku. Kyseinen sertifikaatti koostuu käytännössä algoritmin 10 (PÄÄVAIHE) paluuarvoista $((A_j, B_j), P_j, N_{j+1})$, missä $j = 0, \ldots, i$, ja sen tarkastamiseen käytetään erikseen määriteltyä algoritmia, joka esitellään hieman myöhemmin.

Algoritmi 11. GK(N)
Oletetaan, että N ei ole jaollinen luvuilla 2 tai 3. Muutenhan se olisi yhdistetty luku eikä algoritmin suorittaminen olisi tarpeen.

1. Aseta $i \leftarrow 0$, $N_0 \leftarrow N$ ja $L \leftarrow M$, missä M on yläraja luvuille, jotka voidaan testata riittävän tehokkaasti vaiheen 3 testillä.

2. Kun $N_i > L$:

   (a) Laske $((A_i, B_i), P_i, N_{i+1}) \leftarrow$ PÄÄVAIHE(N_i).

   (b) Aseta $i \leftarrow i + 1$.

3. Testaa luku N_i jollakin ennalta määrätyllä deterministisellä testillä. Jos N_i ei ole alkuluku, niin palaa vaiheeseen 1.

4. Palauta $((A_0, B_0), P_0, N_1), \ldots, ((A_{i-1}, B_{i-1}), P_{i-1}, N_i)$.
   Mikäli vaiheen 1 aloittamisen jälkeen $k^{\log k}$ vaihetta on suoritettu, niin keskeytä algoritmi ja palaa vaiheeseen 1. Tässä edelleen k on syötteen N bittien lukumäärä.

Huomautus. Kyseessä on satunnaisuuteen perustuva testi, joten ei ole takeita siitä, kuinka nopeasti algoritmi muodostaa sertifikaatin luvulle N, mikäli se koskaan saa muodostettua sellaista.

Huomautus. Vaiheessa 3 toimii käytännössä mikä tahansa deterministinen alkulukutesti, joka ei oleta syöteluvun olevan jotain tiettyä muotoa. Yläraja L täytyy vain valita siten, että käytetty testi suoriutuu nopeasti tätä ylärajaa pienemmistä luvuista. Goldwasser ja Kilian käyttävät artikkelissaan vaiheessa 3 Cohen-Lenstra-testinä tunnettua determinististä testiä, joka suoriutuu ajassa $\mathcal{O}(k)$ kokoluokkaa

$$2^{k^{C/\log\log k}}$$

olevista syötteistä, missä C on positiivinen vakio. Tällöin alaraja L saataisiin muotoon

$$L = \max(2^{k^{C/\log\log k}}, 37)$$

[5].

Mikäli algoritmi 11 saa muodostettua sertifikaatin syötteelle N, täytyy tämä sertifikaatti vielä tarkastaa, jotta voidaan varmistaa, että syötetty luku N on alkuluku. Tämä tapahtuu seuraavalla algoritmilla.

Algoritmi 12. TARKASTA$(N, ((A_0, B_0), P_0, N_1), \ldots, ((A_{i-1}, B_{i-1}), P_{i-1}, N_i))$

1. Jos $N_i > L$, missä L on vastaava yläraja kuin Goldwasser–Kilian-algoritmissa, niin keskeytä algoritmi.
2. Testaa luku N_i deterministisesti.
3. Aseta $N_0 \leftarrow N$. Testaa, että jokaisella $j = 0, \ldots, i-1$ pätee
   (a) $2, 3 \nmid N_j$,
   (b) $\operatorname{syt}(4A_j^3 + 27B_j^2, N_j) = 1$,
   (c) $N_{j+1} > (\sqrt[4]{N_j} + 1)^2 = \sqrt{N_j} + 2\sqrt[4]{N_j} + 1$ ja
   (d) $P_j \neq O$ ja $N_{j+1}P_j = O$.

   Jos yksikin yllä mainituista ehdoista ei päde, niin keskeytä algoritmi. Muussa tapauksessa hyväksy luku N alkuluvuksi.

Lause 4.5. *TARKASTA-algoritmi hyväskyy aina algoritmin 11 palauttaman sertifikaatin. Jos algoritmi TARKASTA$(N, ((A_0, B_0), P_0, N_1), \ldots, ((A_{i-1}, B_{i-1}), P_{i-1}, N_i))$ hyväksyy luvun N alkuluvuksi, niin tällöin N on alkuluku.*

Todistus. Osoitetaan ensin lauseen ensimmäinen väittämä. Oletetaan siis, että syötteellä N algoritmi GK(N) palauttaa sertifikaatin

$$((A_0, B_0), P_0, N_1), \ldots, ((A_{i-1}, B_{i-1}), P_{i-1}, N_i).$$

Tällöin tiedetään, että $N_i \leq L$, sillä algoritmi GK on päättynyt, ja toisaalta tiedetään myös, että N_i on alkuluku, sillä se on testattu deterministisesti algoritmin GK vaiheessa 3. Täten algoritmin TARKASTA kaksi ensimmäistä vaihetta menevät läpi. Nyt jos $j \in \{0, \ldots, i-1\}$, niin algoritmi GK varmistaa sen, että $2, 3 \nmid N_j$. Vastaavasti algoritmissa GeneroiKäyrä varmistetaan ehdot

$$\operatorname{syt}(4A_j^3 + 27B_j^2, N_j) = 1 \quad \text{sekä} \quad N_{j+1} > (\sqrt[4]{N_j} + 1)^2$$

ja algoritmi VALITSE-PISTE varmistaa, että $P_j \neq O$ ja $N_{j+1}P_j = O$. Täten kaikilla $j = 0, \ldots, i-1$ algoritmin TARKASTA vaiheen 3 ehdot toteutuvat, joten TARKASTA hyväksyy luvun N sertifikaatilla

$$((A_0, B_0), P_0, N_1), \ldots, ((A_{i-1}, B_{i-1}), P_{i-1}, N_i).$$

Oletetaan nyt, että algoritmi TARKASTA hyväksyy syötteen

$$(N, ((A_0, B_0), P_0, N_1), \ldots, ((A_{i-1}, B_{i-1}), P_{i-1}, N_i)).$$

Tällöin selvästi luvun N_i on oltava alkuluku. Toisaalta jokaisella $j = 0, \ldots, i-1$ algoritmi on tarkastanut, että lauseen 4.2 ehdot toteutuvat, joten jos N_{j+1} on alkuluku, niin N_j on alkuluku kaikilla $j = 0, \ldots, i-1$. Täten siitä, että N_i on alkuluku, seuraa

$$\begin{aligned} N_i \text{ on alkuluku} &\Rightarrow N_{i-1} \text{ on alkuluku} \\ &\Rightarrow N_{i-2} \text{ on alkuluku} \\ &\vdots \\ &\Rightarrow N_0 = N \text{ on alkuluku.} \end{aligned}$$

Täten luvun N on oltava alkuluku. □

Käydään lopuksi läpi esimerkki, jossa muodostetaan seritifikaatti alkuluvulle $N = 107$ käyttämällä Goldwasser–Kilian-algoritmia.

Esimerkki 4.6. Osoitetaan luku $N = 107$ alkuluvuksi käyttäen Goldwasser–Kilian-algoritmia. Asetetaan $i \leftarrow 0$, $N_0 \leftarrow N$ ja $L \leftarrow 40$.

1. Lasketaan GENEROI-KÄYRÄ(N_0): Saadaan $((A_0, B_0), N_1) = ((17, 41), 59)$.
2. Lasketaan VALITSE-PISTE$(107, 59, (17, 41))$ = VALITSE-PISTE$(107, 59, (17, 41))$: Saadaan $P_0 = (11, 75)$, jolla $59P_0 = O$.
3. Otetaan talteen $((A_0, B_0), P_0, N_1) = ((17, 41), (11, 75), 59)$ ja asetetaan $i \leftarrow i + 1 = 1$.
4. Lasketaan GENEROI-KÄYRÄ($N_1 = 59$): Saadaan $((A_1, B_1), N_2) = ((52, 35), 37)$.
5. Lasketaan VALITSE-PISTE$(59, 37, (52, 35))$: Saadaan $P_1 = (39, 9)$, jolla $37P_1 = O$.
6. Otetaan talteen $((A_1, B_1), P_1, N_2) = ((52, 35), (39, 9), 37)$ ja asetetaan $i \leftarrow i + 1 = 2$.
7. Nyt $N_i = N_2 = 37 < L$, joten testataan luku 37 deterministisesti esimerkiksi kokeilemalla jakaa se kaikilla alkuluvuilla $2 \leq p \leq \sqrt{37}$.
8. Voidaan helposti huomata, että 37 on alkuluku, joten luvulle $N = 107$ on saatu muodostettua sertifikaatti

   $$((17, 41), (11, 75), 59), ((52, 35), (39, 9), 37),$$

   joka osoittaa luvun N olevan alkuluku. Täten algoritmi on päättynyt.

4.2 Analysointia

Tässä alaluvussa tutkitaan todennäköisyyttä, jolla Goldwasser–Kilian-algoritmi tulkitsee alkuluvun onnistuneesti alkuluvuksi. Tämä tapahtuu analysoimalla virheen tapahtumisen mahdollisuutta ensin algoritmissa 8, ja tämän jälkeen algoritmissa 9, jolloin näiden kahden yhteisvaikutuksesta saadaan siten Goldwasser–Kilian-algoritmin virheen mahdollisuus. Tämän luvun sisältö perustuu lähteeseen [5] sekä tutkielman tekijän havaintoihin.

Aloitetaan Goldwasser–Kilian-algoritmin analysointi algoritmin 8 (GENEROI-KÄYRÄ) tarkastelusta. Ensimmäinen vaihe tässä algoritmissa on etsiä pari $(A, B) \in (\mathbb{Z}/N\mathbb{Z})^2$, jolla $\text{syt}(4A^3 + 27B^2, N) = 1$. Todennäköisyys virheen tapahtumiselle tässä vaiheessa on häviävän pieni, sillä jos A on valittu satunnaisesti ja oletetaan, että N on alkuluku, niin tällöin luvulle B on korkeintaan kaksi huonoa vaihtoehtoa:

$$B = \pm\sqrt{\frac{-4A^3}{27}}.$$

Täten todennäköisyys sopivan parin (A, B) löytymiselle satunnaisesti generoimalla on vähintään $\frac{N-2}{N}$, joten tämä ei ole algoritmia suuresti rajoittava vaihe. Seuraavassa vaiheessa lasketaan muodostetun elliptisen käyrän pisteiden lukumäärä m Schoofin algoritmilla. Tässä vaiheessa halutaan, että $m = 2q$ jollakin alkuluvulla q, joten on syytä tutkia todennäköisyyttä, jolla halutut ominaisuudet omaava käyrä löydetään. Seuraavat kaksi tulosta antavat arvion tälle todennäköisyydellä:

Lause 4.7. *Olkoot $p > 5$ alkuluku ja*

$$S \subseteq [p + 1 - \lfloor\sqrt{p}\rfloor, p + 1 + \lfloor\sqrt{p}\rfloor].$$

Tällöin on olemassa sellainen positiivinen vakio c, että jos $E = (A, B)$ on kunnan $\mathbb{Z}/p\mathbb{Z}$ suhteen satunnaisesti tasaisella jakaumalla generoitu elliptinen käyrä, niin

$$P(|E| \in S) > \frac{c}{\ln p} \cdot \frac{|S| - 2}{2\lfloor\sqrt{p}\rfloor + 1},$$

missä $P(|E| \in S)$ on tapahtuman $|E| \in S$ todennäköisyys.

Todistus. Todistuksen voi löytää Lenstran artikkelista [11]. □

Seuraus 4.8. *Olkoot $p > 5$ alkuluku, E kunnan $\mathbb{Z}/p\mathbb{Z}$ suhteen määritelty satunnaisesti tasaisella jakaumalla generoitu elliptinen käyrä ja*

$$S(p) = \left\{ q \in \left[\frac{p + 1 - \lfloor\sqrt{p}\rfloor}{2}, \frac{p + 1 + \lfloor\sqrt{p}\rfloor}{2} \right] \,\middle|\, q \text{ on alkuluku} \right\}.$$

Jos nyt $|E| = m$, niin

$$P(m = 2q, \text{missä } q \text{ on alkuluku}) > \frac{c}{\ln p} \cdot \frac{|S(p)| - 2}{2\lfloor\sqrt{p}\rfloor + 1},$$

missä c on vakio.

Todistus. Määritellään

$$S = \{r \in [p + 1 - \lfloor\sqrt{p}\rfloor, p + 1 + \lfloor\sqrt{p}\rfloor] \mid r = 2q \text{ jollakin alkuluvulla } q\}.$$

Tällöin siis

$$S \subseteq [p + 1 - \lfloor\sqrt{p}\rfloor, p + 1 + \lfloor\sqrt{p}\rfloor].$$

Nyt voidaan muodostaa bijektio $S(p) \to S$, jossa $q \mapsto 2q$. Tämä on nimittäin selvästi injektio, ja toisaalta jos $r \in S$, niin on olemassa alkuluku q, jolla $r = 2q$ ja selvästi $q \in S(p)$, joten saadaan bijektio. Näin ollen $|S| = |S(p)|$, joten lauseen 4.7 nojalla

$$\begin{aligned} P(m = 2q, \text{missä } q \text{ on alkuluku}) = P(m \in S) &> \frac{c}{\ln p} \cdot \frac{|S| - 2}{2\lfloor\sqrt{p}\rfloor + 1} \\ &= \frac{c}{\ln p} \cdot \frac{|S(p)| - 2}{2\lfloor\sqrt{p}\rfloor + 1}. \end{aligned}$$

□

Siis todennäköisyys $P(m = 2q$, missä q on alkuluku) riippuu joukon $S(p)$ koosta sekä vakiosta c. Tämän tiedon hyöty ilmenee siinä, että joukon $S(p)$ koolle tiedetään arvio. Nimittäin, kuuluisan *alkulukulauseen* nojalla lukua N pienempien tai yhtä suurien alkulukujen lukumäärä on noin $\frac{N}{\ln N}$ [7, s. 3], jolloin joukon $S(p)$ koolle saadaan arvioksi

$$|S(p)| \approx \frac{U}{\ln U} - \frac{L}{\ln L},$$

missä $U = \frac{p + 1 + \lfloor \sqrt{p} \rfloor}{2}$ ja $L = \frac{p + 1 - \lfloor \sqrt{p} \rfloor}{2}$. Tässä vaiheessa on siis löydetty elliptinen käyrä, jonka koko on muotoa $2q$, joten algoritmin 8 lopuksi tarkistetaan vielä algoritmilla 1, että q on todennäköisesti alkuluku. Algoritmi 1 toistetaan $2k$ eri satunnaisella luvulla, missä k on luvun q bittien lukumäärä, joten lauseen 2.10 nojalla on virheen todennäkisyys tässäkin vaiheessa häviävän pieni, korkeintaan $1/2^{4k}$.

Seuraavaksi Goldwasser–Kilian-algoritmi etsii edellisessä vaiheessa muodostetun elliptisen käyrän pisteen P, jolla pätee $P \neq O$ ja $qP = O$. Toisin ilmaistuna halutaan löytää elliptisen käyrän piste, jonka kertaluku on q. Täten selvittääkseen todennäköisyyden, jolla kyseinen piste voidaan satunnaisesti generoimalla löytää, täytyy selvittää kertalukua q olevien pisteiden lukumäärä. Seuraavaa apulausetta voidaan hyödyntää tämän ongelman ratkaisemisessa.

Lemma 4.9. *Olkoot E kunnan $\mathbb{Z}/N\mathbb{Z}$ suhteen määritelty elliptinen käyrä, missä N on alkuluku. Tällöin on olemassa positiiviset kokonaisluvut m_1 ja m_2, joilla $m_1 \mid m_2$ ja*

$$E(\mathbb{Z}/N\mathbb{Z}) \cong (\mathbb{Z}/m_1\mathbb{Z})^+ \times (\mathbb{Z}/m_2\mathbb{Z})^+,$$

missä $(\mathbb{Z}/m_i\mathbb{Z})^+$ on joukon $\mathbb{Z}/m_i\mathbb{Z}$ yhteenlaskuryhmä.

Todistus. Tulos on esitetty Goldwasserin ja Kilianin artikkelissa [5], mutta todistusta tälle ei ole annettu, joten siitä syystä todistus sivuutetaan tässäkin tutkielmassa. □

Jos nyt oletetaan, että N on alkuluku ja aikaisemmin muodostettu elliptinen käyrä E on määritelty kunnan $\mathbb{Z}/N\mathbb{Z}$ suhteen siten, että $|E| = 2q$ jollakin alkuluvulla q, niin lemman 4.9 nojalla

$$|E(\mathbb{Z}/N\mathbb{Z})| = 2q = m_1 m_2,$$

missä $m_1 \mid m_2$. Nyt kuitenkin ainoa vaihtoehto on, että $m_1 = 1$ ja $m_2 = 2q$, sillä q on alkuluku, joten

$$E(\mathbb{Z}/N\mathbb{Z}) \cong (\mathbb{Z}/m_1\mathbb{Z})^+ \times (\mathbb{Z}/m_2\mathbb{Z})^+ \cong (\mathbb{Z}/2q\mathbb{Z})^+.$$

Ryhmästä $(\mathbb{Z}/2q\mathbb{Z})^+$ tiedetään, että siinä on täsmälleen $q - 1$ alkiota, jonka kertaluku on q. Nimittäin, jos oletetaan, että $r \in \mathbb{Z}/2q\mathbb{Z}$, jolla $rq = 0$, niin tällöin $2q \mid rq$. Nyt kuitenkin $2 \nmid q$, joten on oltava $2 \mid r$. Siis $r = 2m$ jollakin $m \in \mathbb{Z}/2q\mathbb{Z}$. Itse asiassa $2 \mid 2m$ kaikilla $m \in \mathbb{Z}/2q\mathbb{Z}$, joten kertalukua q olevia alkioita ovat kaikki parilliset nollasta poikkeavat luvut joukossa $\mathbb{Z}/2q\mathbb{Z}$ joita on täsmälleen $q - 1$ kappaletta. Nyt koska

$$E(\mathbb{Z}/N\mathbb{Z}) \cong (\mathbb{Z}/2q\mathbb{Z})^+,$$

on ryhmässä $E(\mathbb{Z}/N\mathbb{Z})$ myös $q - 1$ eri alkiota, jonka kertaluku on q. Lisäksi on selvää, että $q(x, y) = O$, jos ja vain jos $q(x, -y) = O$, joten on olemassa ainakin $(q - 1)/2$ vaihtoehtoa luvulle x siten, että saadaan muodostettua sopiva piste (x, y). Enää on siis selvitettävä todennäköisyys sille, että milloin $z = x^3 + Ax + B$ on neliöjäännös modulo N. Ensinnäkin havaitaan, että jos $r < N/2$, niin

$$(N - r)^2 = N^2 - 2Nr + r^2 \equiv r^2 \pmod{N},$$

joten kaikki mahdolliset neliöjäännökset modulo N ovat ekvivalentteja (modulo N) lukujen $1, \ldots, (N-1)/2$ neliöiden kanssa. Toisaalta on huomattu, että nämä neliöjäännökset ovat jakautuneet lähes tasaisella jakaumalla, joten z on neliöjäännös todennäköisyydellä

$$\frac{(N-1)/2}{N-1} = \frac{1}{2}.$$

Täten, luvun x satunnaisella valinnalla saadaan sopiva elliptisen käyrän piste vähintään todennäköisyydellä

$$\frac{1}{2} \cdot \frac{(q-1)/2}{N}.$$

Tässä tulon jälkimmäinen osa saadaan tiedosta, että sopivia vaihtoehtoja luvulle x on ainakin $(q-1)/2$ kappaletta, kun vaihtoehtoja joukossa $\mathbb{Z}/N\mathbb{Z}$ on N kappaletta.

5 Joitakin kehitysaskeleita

Tämä tutkielman viimeinen luku käsittelee otsikonsa mukaisesti joitakin kehitysaskeleita, joita Goldwasser–Kilian-algoritmista on otettu eteenpäin vuosien saatossa. Goldwasser–Kilian-algoritmin suurin heikkous on joukon $E(\mathbb{Z}/N\mathbb{Z})$ koon laskeminen Schoofin algoritmia käyttäen. Nimittäin, ensinnäkin sen implementointi on käytännön tasolla lähes mahdotonta [2]. Toiseksi, kuten Schoof artikkelissaan (1995) toteaa, että jos algoritmin implementoinnissa onnistutaan, on sen suorituskyky siltikin käytännössä heikko, sillä laskenta jakopolynomeilla renkaassa $(\mathbb{Z}/N\mathbb{Z})[X,Y]/\langle\psi_l, Y^2 - X^3 - AX - B\rangle$ varaa muistia huomattavan paljon. Esimerkiksi, jos $N \approx 10^{200}$, niin tällöin laskennassa tarvitaan alkulukuja $l > 250$, jolloin yhdenkin alkion esittämiseen renkaassa $(\mathbb{Z}/N\mathbb{Z})[X,Y]/\langle\psi_l, Y^2 - X^3 - AX - B\rangle$ tarvittaisiin vähintään 1,5 megatavua muistia [15].

Täten, yllä mainituista syistä johtuen Goldwasser–Kilian -algoritmin kehittämiseen on ainakin kaksi luontevaa vaihtoehtoa: Joukon $E(\mathbb{Z}/N\mathbb{Z})$ koon laskemisen optimointi tai sen laskemisen kiertäminen. Näistä ensimmäisessä vaihtoehdossa esimerkkinä käy tekijöidensä nimien mukaan nimetty Schoof-Elkies-Atkin -algoritmi, joka on Noam Elkiesin ja A. O. L. Atkinin Schoofin algoritmista kehittämä optimoitu algoritmi elliptisen käyrän pisteiden lukumäärän laskemiseen. Olennainen ero Schoofin algoritmiin on hyvien ja huonojen alkulukujen eroittelu määrittäessä alkulukujen joukkoa, jolla Schoofin algoritmi suoritetaan. Tästä voi lukea muun muassa Schoofin artikkelista [15]. Toinen vaihtoehto, joukon $E(\mathbb{Z}/N\mathbb{Z})$ koon laskemisen kiertäminen, on A. O. L. Atkinin ja F. Morainin kehittämä idea, jossa etsitään sellainen elliptinen käyrä, jonka koko on helppo laskea, jolloin vältytään tähän tehtävään tarkoitettujen raskaiden algoritmien käytöltä. Tämä menetelmä tunnetaan ECPP-algoritmina ja tutkielman viimeinen osio käytetään tämän pintapuoliseen käsittelyyn.

5.1 ECPP-algoritmi

Tässä alaluvussa perehdytään Atkinin ja Morainin kehittämään ECPP-algoritmina tunnettuun alkulukutestiin. Tämä algoritmi on saanut alkunsa samoihin aikoihin Goldwasser–Kilian-algoritmin kanssa Atkinin toimesta vuonna 1986, jonka jälkeen vuonna 1987 Morain kehitti oman versionsa algoritmista. Vuonna 1989 Atkin ja Morain tapasivat ja yhdistivät omat ideansa saaden aikaan ECPP-algoritmin, josta he julkaisivat kattavan artikkelin vuonna 1993 [2]. Kyseinen artikkeli toimii tämän luvun pääasiallisena lähteenä.

ECPP-algoritmi on yksi tehokkaimpia nykypäivän alkulukutestejä. Perusperiaate on kuitenkin sama kuin Goldwasser–Kilian-algoritmissa: Etsitään elliptinen käyrä E, jonka koko on $m = 2q$ jollakin todennäköisellä alkuluvulla q, jotta lauseen 4.2 ehdot toteutuvat. Tämän jälkeen toistetaan sama menettely luvulla q. Olennainen ero on kuitenkin siinä, että ECPP-algoritmissa etsitään sellainen käyrä, jonka koko voidaan helposti laskea eikä täten tarvita raskasta algoritmia, kuten Schoofin algoritmia, elliptisen käyrän pisteiden lukumäärän laskemiseen. Tämä onnistuu hyödyntämällä niin kutsutun kompleksisen kertolaskun omaavien elliptisten käyrien ominaisuuksia.

Olkoon nyt N testattava positiivinen kokonaisluku. Pääpiirteissään ECPP-algoritmi etenee siten, että ensin etsitään diskriminantti $-D$, missä D on positiivinen kokonaisluku, joka ei ole jaollinen minkään parittoman alkuluvun neliöllä, ja jolla toteutuu yhtälö

$$4N = U^2 + DV^2, \tag{5.1}$$

missä U ja V ovat kokonaislukuja. Tällöin saadaan imaginäärinen neliökunta $K = \mathbb{Q}(\sqrt{-D})$, jossa $N = \pi\overline{\pi}$, missä π kuuluu kunnan K kokonaisten alkioiden joukkoon, eli käytännössä joukkoon $\mathbb{Z}[\omega]$, missä

$$\omega = \begin{cases} \sqrt{-D/4} & \text{jos } D \equiv 0 \pmod 4, \\ \dfrac{1+\sqrt{-D}}{2} & \text{muuten.} \end{cases}$$

Nyt voidaan määrittää elliptisen käyrän E Weierstrassin yhtälö muodostamalla diskriminantista $-D$ riippuva niin kutsuttu Hilbertin luokkapolynomi $H_D(X) \in \mathbb{Z}[X]$ ja ratkaisemalla jokin yhtälön

$$H_D(X) \equiv 0 \pmod N$$

juuri j. Tämä juuri j on elliptisen käyrän E j-invariantti, jonka avulla Weierstrassin yhtälön kertoimet saadaan laskettua. Nimittäin Weierstrassin yhtälö on tällöin joko

$$Y^2 = X^3 + 3kX + 2k$$

tai

$$Y^2 = X^3 + 3kc^2X + 2kc^3,$$

missä c on mikä tahansa neliöepäjäännös modulo N ja

$$k = \frac{j}{1728 - j}$$

[10]. Tällä tavalla määriteltynä elliptisellä käyrällä E on kompleksinen kertolasku ja

$$|E(\mathbb{Z}/N\mathbb{Z})| = N + 1 - U,$$

kun U on sellainen yhtälön 5.1 ratkaisu, jolla $N+1-U = 2q$ jollakin todennäköisellä alkuluvulla q. Tämä menettely on kuvattu tarkemmin muun muassa Atkinin ja Morainin artikkelissa [2].

Algoritmi 13. ECPP(N)

1. Jos N on riittävän pieni, niin testaa se jollakin deterministisellä testillä ja palauta tämän lopputulos.
2. Etsi imaginäärinen neliökunta $K = \mathbb{Q}(\sqrt{-D})$, missä $-D$ on perusdiskriminantti, jolla

   $$4N = U^2 + DV^2, \tag{5.2}$$

   missä $U, V \in \mathbb{Z}$.
3. Laske $m = N + 1 - U$ kaikilla yhtälön 5.1 ratkaisuilla U. Jos jollakin näistä pätee $m = 2q$, missä q on todennäköinen alkuluku, niin ota talteen luvut m sekä q ja mene vaiheeseen 4. Muuten, palaa vaiheeseen 2 etsimään uusi imaginäärinen neliökunta.
4. Muodosta polynomi $H_D(X)$ ja ratkaise jokin juuri j yhtälöstä $H_D(X) \equiv 0 \pmod N$.
5. Muodosta elliptisen käyrän E yhtälö luvun j avulla, jolloin $|E(\mathbb{Z}/N\mathbb{Z})| = m$.
6. Etsi piste käyrältä E käyttämällä esimerkiksi algoritmia 9.
7. Toista rekursiivisesti ECPP(q) ja palauta tämän lopputulos.

Algoritmista 13 voidaan huomata, että kyseessä on pääpiirteissään Goldwasser–Kilian-algoritmi, jossa ainoana muutoksena on elliptisen käyrän muodostaminen. ECPP-algoritmissa tätä vaihetta lähestytään päinvastaisesta suunnasta Goldwasser–Kilian-algoritmiin verrattuna, sillä siinä missä Goldwasser–Kilian-algoritmi muodostaa ensin elliptisen käyrän ja sen jälkeen määrittää sen koon, niin ECPP-algoritmi määrittää ensin koon ja sen jälkeen muodostaa tätä kokoa vastaavan elliptisen käyrän. Täten vältytään käyrän koon laskemiselta esimerkiksi Schoofin algoritmia käyttäen, mikä tuo merkittävän parannuksen Goldwasser–Kilian-algoritmiin verrattuna etenkin suurilla syöteluvun N arvoilla. A. K. Lenstra ja H. W. Lenstra ovat atrikkelissaan [10] antaneet heuristisen analyysin pohjalta ECPP-algoritmin kompleksisuudeksi $O\left((\log N)^{6+\epsilon}\right)$ millä tahansa $\epsilon > 0$, missä raskaimmaksi tehtäväksi muodostuu Hilbertin polynomin $H_D(X)$ määrittäminen sekä yhtälön

$$H_D(X) \equiv 0 \pmod{N}$$

ratkaiseminen. Kertolaskua optimoimalla koko algoritmin kompleksisuus saadaan suuruusluokkaan $O\left((\log N)^{5+\epsilon}\right)$. Tästä suorituskykyä on saatu edelleen parannettua hyödyntämällä vain sellaisia diskriminantteja D, jotka voidaan esittää pienten alkulukujen tulona, jolloin modulaarisen neliöjuuren $\sqrt{N} \bmod N$ laskeminen palautuu pienten alkulukujen modulaarisen neliöjuuren laskemiseen. Tällöin saadaan ECPP-algoritmin kompleksisuudeksi $O\left((\log N)^{4+\epsilon}\right)$, mikä tarkoittaa huomattavaa parannusta tehokkuudessa verrattuna esimerkiksi Goldwasser–Kilian-algoritmiin, jonka vaativuus on suuruusluokkaa $O\left((\log N)^{9+\epsilon}\right)$. Merkittävän teoreettisen suorituskyvyn lisäksi on ECPP-algoritmi osoittautunut myös hyvin käytännölliseksi alkulukutestiksi, joten muun muassa näistä syistä ei ole yllättävää, että kyseessä on yksi nykypäivän tehokkaimmista menetelmistä löytää alkulukuja.

Kirjallisuutta

[1] Agrawal, M., Kayal, N. ja Saxena, N. *PRIMES is in P*. Annals of Mathematics, 160, 781–793, (2004).

[2] Atkin, A. O. L. ja Morain, F. *Elliptic curves and primality proving*. Mathematics of Computation 61:203, 29–68, (1993).

[3] Cohen, H. *A course in computational algebraic number theory*. Springer, Berlin / Heidelberg (2000).

[4] Cox, D. A. *Primes of the form* $x^2 + ny^2$. Wiley, New York (1989).

[5] Goldwasser, S. ja Kilian, J. *Primality testing using elliptic curves*. Proceedings of the 18th Annual ACM Symposium on Theory of Computing, ACM, New York (1986).

[6] Humphreys, J. F. *A course in group theory*. Oxford: Oxford University Press, (1996).

[7] Jameson, G. J. O. *The prime number theorem*. Vol. 53. New York: Cambridge University Press, (2003)

[8] Knuth, D. E. *The art of computer programming. Volume 2, Seminumerical algorithms*. Addison Wesley, (1997).

[9] Koblitz, N. *A course in number theory and cryptography*. Second Edition. Springer, New York, (1994)

[10] Lenstra, A. K. ja Lenstra, Jr., H. W. *Algorithms in number theory*. Handbook of Theoretical Computer Science (A): Algorithms and Complexity, Elsevier, (1990).

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

[12] Morain, F. *Implementation of Atkin-Goldwasser–Kilian primality testing algorithm*. (1995).

[13] Rabin, M. O. *Probabilistic algorithm for testing primality*. Journal of Number Theory 12(1), (1980).

[14] Schoender, M. R. *Number theory in science and comminucation*. Springer, Berlin Heidelberg, (2009).

[15] Schoof, R. *Counting points on elliptic curves over finite fields*. Journal de Théorie des Nombres de Bordeaux, vol. 7, 219– 254, (1995).

[16] Serre, J.-P. *A course in arithmetic*. Graduate texts in mathematics, vol. 7. Springer, New York, (1973).

[17] Silverman, J. H. *The arithmetic of elliptic curves*. Graduate texts in mathematics, vol. 106. Springer, New York (1986).

[18] Tate, J. T. *The arithmetic of elliptic curves*. Inventiones Mathematicae 23.3-4, 179–206. Springer, New York (1974).