TAMPEREEN YLIOPISTO
Pro gradu -tutkielma

Joni Mattila

Pollardin rho-hyökkäys elliptiseen käyrään perustuvaa kryptosysteemiä vastaan

Informaatiotieteiden yksikkö
Matematiikka
2016

Tampereen yliopisto
Informaatiotieteiden yksikkö
MATTILA, JONI: Pollardin rho-hyökkäys elliptiseen käyrään perustuvaa kryptosysteemiä vastaan
Pro gradu -tutkielma, 44 s.
Matematiikka
Toukokuu 2016

Tiivistelmä

Tämä tutkielma tarkastelee menetelmiä ratkaista diskreetin logaritmin ongelma yleisesti ryhmissä ja erityisesti elliptisillä käyrillä. Aluksi tutustutaan lyhyesti elliptisiin käyriin esitellen yhteenlasku elliptisen käyrän pisteille ja osoitetaan näin muodostuva rakenne Abelin ryhmäksi. Esitellään myös diskreetin logaritmin ongelma. Käydään läpi kryptografian perusteita ja esitetään syklisille ryhmille diskreetin logaritmin ongelmaan perustuvat Diffi-Hellman-avaimenvaihtoprotokolla, ElGamal-kryptosysteemi ja ElGamal-digitaalinen allekirjoitus. Käsitellään alkeellisia menetelmiä ratkaista diskreetin logaritmin ongelma ja Pohlig-Hellman reduktio, joka mahdollistaa diskreetin logaritmin ongelman redusoinnin pienempää kertalukua oleviin aliryhmiin, todistetaan tätä varten kiinalainen jäännöslause. Lopuksi tutustutaan Pollardin rho-menetelmään ja siihen tehtäviin yleisiin parannuksiin sekä parannuksiin ratkaistaessa diskreetin logaritmin ongelmaa elliptisillä käyrillä.

Sisältö

1 Johdanto

Tässä Pro gradu -tutkielmassa tutustutaan erityisesti julkisen avaimen kryptosysteemien taustalla olevan diskreetin logaritmin ongelman ratkaisuun. Pääpainona on Pollardin ρ-menetelmä, joka on menetelmä diskreetin logaritmin ongelman ratkaisuun. Käsitellään ρ-menetelmän parannuksia ja erityisesti ρ-menetelmän käyttöä, kun ryhmänä on elliptinen käyrä.

Luvussa 2 perehdytään elliptisten käyrien peruskäsitteisiin. Määritellään elliptisen käyrän pisteille yhteenlasku ja osoitetaan näin muodostettava rakenne Abelin ryhmäksi. Lisäksi tutkitaan elliptisen käyrän pisteitä, joiden kertaluku on joko 2 tai 3. Päälähteenä tässä luvussa on käytetty Washingtonin Elliptic Curves, Number Theory and Cryptography, second edition kirjaa[12] ja Hyryn luentoja kurssilta Kryptografian algebralliset menetelmät [8].

Luvussa 3 esitellään diskreetin logaritmin käsite ja diskreetin logaritmin ongelma. Lisäksi esitetään kahdenna ja lisää -algoritmi diskreetin logaritmin laskemiseksi ja parannus tuohon algoritmiin, joka on hyödyllinen erityisesti laskettaessa diskreettiä logaritmia elliptisillä käyrillä.

Luvussa 4 tutustutaan kryptografian perusteisiin. Esitellään kryptosysteemin käsite. Perehdytään erityisesti julkisen avaimen salaukseen. Esitellään Diffie-Hellman-avaimenvaihtoprotokolla, ElGamal-kryptosysteemi ja ElGamal-digitaalinen allekirjoitus. Tutustutaan myös näihin kohdistuviin hyökkäysmahdollisuuksiin. Päälähteenä tässä luvussa on Buchmannin Introduction to Cryptography, second edition [3].

Luvussa 5 käsitellään Pohlig-Hellman reduktiota, joka mahdollistaa diskreetin logaritmin ongelman redusoinnin pienempiin ryhmiin. Todistetaan tätä varten lisäksi kiinalainen jäännöslause.

Luvussa 6 tutustutaan Pollardin ρ-menetelmään. Tutkitaan siihen liittyviä parannuksia: Floydin syklinlöytö algoritmin avulla ei ole tarvetta säilyttää muistissa valtavia määriä informaatiota, rinnakkaisen ρ-menetelmän avulla voimme jakaa laskentaa useille koneille, Montgomeryn temppu mahdollistaa useamman käänteisalkion laskemisen samaan aikaan ja negaation avulla voimme siirtyä käyttämään etsinnässä ekvivalenssiluokkia. Negaation ongelmana on kuitenkin turhat syklit, jotka eivät anna tarpeellista informaatiota diskreetin logaritmin ongelman ratkaisemiseksi. Esitelläänkin tapa välttää näitä turhia syklejä. Päälähteenä tässä luvussa on Bersteinin, Langen ja Schwaben julkaisu On the correct use of the negation map in the Pollard rho method [2]. Käsiteltävä negaatio on nimenomaan parannus ρ-menetelmään ratkaistaessa diskreetin logaritmin ongelmaa, kun ryhmänä on elliptinen käyrä.

Lukijalta oletetaan algebran ja lukuteorian perusteiden hallintaa.

2 Johdatus elliptisiin käyriin

Tässä luvussa määritellään elliptinen käyrä yli kunnan K, esitellään käyrän pisteiden yhteenlasku ja osoitetaan näin muodostettava rakenne Abelin ryhmäksi. Lisäksi tarkastellaan elliptisten käyrien pisteitä, joiden kertalukuja ovat 2 tai 3.

2.1 Elliptinen käyrä

Määritellään aluksi elliptinen käyrä ja todistetaan tulos, joka toteaa, että elliptisen käyrän määritelmä ei salli moninkertaisia juuria.

Määritelmä 2.1. Ks. [12, s. 9]. Olkoon K kunta, jonka karakteristika ei ole 2 eikä 3. *Elliptinen käyrä* on joukko

$$E(K) = \left\{ (x, y) \in K^2 \mid y^2 = x^3 + ax + b \right\} \cup \{ \infty \},$$

missä $a, b \in K$. Lisäksi vaaditaan, että elliptisen käyrän *diskriminantille*

$$\Delta = 4a^3 + 27b^2$$

pätee, että $\Delta \neq 0$.

Huomautus. Oletetaan jatkossa, että kunnan K karakteristika eroaa luvuista 2 ja 3.

Huomautus. Käytetään elliptisestä käyrästä myös merkintää

$$E_{(a,b)}(K) = \left\{ (x, y) \in K^2 \mid y^2 = x^3 + ax + b \right\} \cup \{ \infty \}.$$

Esimerkki 2.1. Joukko $E_{(5,7)}(\mathbb{Z}_{73})$ muodostaa elliptisen käyrän, sillä 73 on alkuluku, joten $\mathbb{Z}_{73}$ on kunta. Lisäksi diskriminantti

$$\Delta = 4a^3 + 27b^2 = 4 * 5^3 + 27 * 7^2 = 71 \neq 0,$$

joten kyseessä on elliptinen käyrä.

Lause 2.1. *Jos $E(K)$ on elliptinen käyrä, niin polynomilla*

$$p = X^3 + aX + b \in K[X]$$

ei ole moninkertaista juurta.

Todistus. Vrt. [12, s. 9]. Olkoon $E(K)$ elliptinen käyrä ja

$$p = X^3 + aX + b \in K[X].$$

Tiedetään, että polynomilla p on kolme juurta kunnan K algebrallisessa sulkeumassa $\overline{K}$. Olkoot $r_1, r_2, r_3 \in \overline{K}$ polynomin p juuria. Tällöin pätee, että

$$\begin{aligned}
&X^3 + aX + b \\
&= (X - r_1)(X - r_2)(X - r_3) \\
&= (X^2 - r_2X - r_1X + r_1r_2)(X - r_3) \\
&= (X^2 - (r_1 + r_2)X + r_1r_2)(X - r_3) \\
&= X^3 - (r_1 + r_2)X^2 + r_1r_2X - r_3X^2 + (r_1r_3 + r_2r_3)X - r_1r_2r_3 \\
&= X^3 - (r_1 + r_2 + r_3)X^2 + (r_1r_2 + r_1r_3 + r_2r_3)X - r_1r_2r_3.
\end{aligned}$$

Nyt yhdistämällä kertoimet saadaan, että

$$\begin{cases} 0 = r_1 + r_2 + r_3, \\ a = r_1r_2 + r_1r_3 + r_2r_3 \text{ ja} \\ b = -r_1r_2r_3, \end{cases}$$

jos ja vain jos

$$\begin{cases} r_3 = -r_1 - r_2, \\ a = -(r_1^2 + r_1r_2 + r_2^2) \text{ ja} \\ b = r_1^2r_2 + r_1r_2^2. \end{cases}$$

Osoitetaan, että

$$((r_1 - r_2)(r_1 - r_3)(r_2 - r_3))^2 = -(4a^3 + 27b^2),$$

haluttu tulos seuraa tästä. Laskemalla saadaan, että

$$\begin{aligned}
&((r_1 - r_2)(r_1 - r_3)(r_2 - r_3))^2 \\
&= ((r_1 - r_2)(2r_1 + r_2)(r_1 + 2r_2))^2 \\
&= (r_1 - r_2)^2(2r_1 + r_2)^2(r_1 + 2r_2)^2 \\
&= (r_1^2 - 2r_1r_2 + r_2^2)(4r_1^2 + 4r_1r_2 + r_2^2)(r_1^2 + 4r_1r_2 + 4r_2^2) \\
&= 4r_1^6 + 12r_1^5r_2 - 3r_1^4r_2^2 - 26r_1^3r_2^3 - 3r_1^2r_2^4 + 12r_1r_2^5 + 4r_2^6.
\end{aligned}$$

Oletetaan tunnetuksi, että

$$(x + y + z)^3 = x^3 + y^3 + z^3 + 3(xy^2 + xz^2 + x^2y + yz^2 + x^2z + y^2z) + 6xyz,$$

missä $x, y, z \in K$. Nyt saadaan laskemalla myös, että

$$\begin{aligned}
-(4a^3 + 27b^2) &= 4(r_1^2 + r_1r_2 + r_2^2)^3 - 27(r_1^2r_2 + r_1r_2^2)^2 \\
&= 4(r_1^6 + r_1^3r_2^3 + r_2^6 + 3(r_1^4r_2^2 + r_1^2r_2^4 + r_1^5r_2^2 + r_1r_2^5 + r_1^4r_2^2 + r_1^2 + r_2^4) \\
&\quad + 6r_1^3r_2^3) - 27(r_1^4r_2^2 + 2r_1^3r_2^3 + r_1^2r_2^4) \\
&= 4r_1^6 + 12r_1^5r_2 - 3r_1^4r_2^2 - 26r_1^3r_2^3 - 3r_1^2r_2^4 + 12r_1r_2^5 + 4r_2^6.
\end{aligned}$$

Yhdistämällä nämä kaksi saadaan, että

$$((r_1 - r_2)(r_1 - r_3)(r_2 - r_3))^2 = -(4a^3 + 27b^2).$$

Tällöin juuret $r_1, r_2, r_3 \in \overline{K}$ ovat erillisiä, koska $4a^3 + 27b^2 \neq 0$. Siis polynomilla $p = X^3 + aX + b$ ei ole moninkertaista juurta. □

Todistetaan vielä hyödyllinen tulos moninkertaisten juurien tunnistamiseksi.

Lause 2.2. *Olkoon K kunta ja $f \in K[X]$ polynomi, jolla on juuri $\alpha \in K$. Tällöin α on polynomin f moninkertainen juuri, jos ja vain jos $f'(\alpha) = 0$.*

Todistus. Ks. [10, s. 124]. Oletetaan ensiksi, että α on polynomin f moninkertainen juuri. Tällöin $f = (X - \alpha)^m g$, missä $g \in K[X]$ ja $m > 1$. Derivoimalla f saadaan, että

$$f' = m(X - \alpha)^{m-1} g + g'(X - \alpha)^m.$$

Siis $f'(\alpha) = 0$.

Oletetaan sitten, että $f'(\alpha) = 0$. Tehdään vastaoletus, että α ei ole polynomin f moninkertainen juuri. Tällöin $f = (X - \alpha)g$, missä $g \in K[X]$ ja $g(\alpha) \neq 0$. Derivoidaan nyt f ja saadaan, että

$$f' = g + (X - \alpha)g'.$$

Nyt $f'(\alpha) = g(\alpha) \neq 0$, mikä on ristiriita, joten α on polynomin f moninkertainen juuri. □

2.2 Yhteenlaskukaavat ja käyrään liittyvä ryhmä

Samaan tapaan kuin Hyryn luennoilla [8], määritellään elliptisen käyrän $E(K)$ pisteiden P ja Q summa $P + Q$. Merkitään, että $P = (x_1, y_1)$ ja $Q = (x_2, y_2)$. Merkitään myös, että $P + Q = (x_3, y_3) \in E(K)$.

Tutkitaan aluksi tapausta $P \neq Q$ ja $x_1 \neq x_2$. Merkitään pisteiden P ja Q kautta kulkevan suoran kulmakerrointa seuraavasti $m = \frac{y_2 - y_1}{x_2 - x_1}$ ja suoraa

$$L = \left\{ (x, y) \in K^2 \mid y = m(x - x_1) + y_1 \right\}.$$

Tarkastellaan nyt leikkausta $E(K) \cap L$. Jos $(x, y) \in E(K) \cap L$, niin saadaan kaksi yhtälöä:

$$\begin{aligned} y &= m(x - x_1) + y_1 \text{ ja} \\ y^2 &= x^3 + ax + b. \end{aligned}$$

Sijoitetaan ensimmäinen jälkimmäiseen ja saadaan, että

$$(m(x - x_1) + y_1)^2 = x^3 + ax + b.$$

Merkitään, että

$$q = X^3 + aX + b - (m(X - x_1) + y_1)^2 \in K[X].$$

Tämä voidaan purkaa auki siten, että saadaan toisen asteen termin kertoimeksi $-m^2$. Kolmannen asteen polynomina tämä voidaan esittää juurien avulla

$$\begin{aligned} q &= (X - x_1)(X - x_2)(X - t) \\ &= X^3 - (x_1 + x_2 + t)X^2 + (x_1x_2 + x_1t + x_2t)X - x_1x_2t, \end{aligned}$$

mistä saadaan kertoimia vertaamalla, että

$$-m^2 = -(x_1 + x_2 + t),$$

jos ja vain jos

$$t = m^2 - x_1 - x_2.$$

Nyt on saatu pisteen $P+Q$ koordinaatti $x_3 = t$. Toinen koordinaateista saadaan peilaamalla x-akselin suhteen. Siis sijoitetaan $x = x_3$ suoran L yhtälöön

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

ja peilataan tämä x-akselin suhteen, jolloin

$$\begin{aligned} y_3 &= -(m(x_3 - x_1) + y_1) \\ &= m(x_1 - x_3) - y_1. \end{aligned}$$

Toisessa tapauksessa $P \neq Q$ ja $x_1 = x_2$ määritellään, että $P + Q = \infty$.
Tapauksessa, missä $P = Q$ ja $y_1 \neq 0$ tutkitaan polynomia

$$p = Y^2 - X^3 - aX - b \in K[X, Y].$$

Derivoidaan muuttujien X ja Y suhteen, jolloin

$$\frac{\partial}{\partial X}(Y^2 - X^3 - aX - b) = -3X^2 - a \text{ ja}$$

$$\frac{\partial}{\partial Y}(Y^2 - X^3 - aX - b) = 2Y.$$

Määritellään nyt elliptisen käyrän $E(K)$ tangentti pisteessä P seuraavasti:

$$\begin{aligned} L &= \left\{ (x, y) \in K^2 \mid (-3x_1^2 - a)(x - x_1) + 2y_1(y - y_1) = 0 \right\} \\ &= \left\{ (x, y) \in K^2 \mid y = \frac{3x_1^2 + a}{2y_1}(x - x_1) + y_1 \right\}. \end{aligned}$$

Merkitään vielä, että

$$m = \frac{3x^2 + a}{2y}.$$

Nyt elliptisen käyrän tangentti pisteessä P on

$$L = \left\{ (x, y) \in K^2 \mid y = m(x - x_1) + y_1 \right\}.$$

Tutkitaan sitten leikkausta $L \cap E(K)$. Merkitään, että

$$p = X^3 + aX + b - (m(X - x_1) + y_1)^2 \in K[X].$$

Jos $(x, y) \in L \cap E(K)$, niin

$$p(x) = x^3 + ax + b - (m(x - x_1) + y_1)^2 = 0.$$

Osoitetaan, että x_1 on polynomin p kaksoisjuuri. Nyt polynomin p derivaatta on

$$p' = 3X^2 + a - 2m(m(X - x_1) + y_1) \in K[X].$$

Tällöin

$$\begin{aligned} p'(x_1) &= 3x_1^2 - 2my_1 \\ &= 2x_1^2 + a - 2y_1 \frac{3x_1^2 + a}{2y_1} \\ &= 0. \end{aligned}$$

Nyt, koska $p(x_1) = 0$ ja $p'(x_1) = 0$, niin lauseen 2.2 nojalla on x_1 polynomin p kaksoisjuuri, joten koska $deg(p) = 3$, niin polynomin p juuret ovat x_1 ja r. Tällöin saadaan polynomin p termin X^2 kerrointen vertailusta, että

$$2x_1 + r = m^2.$$

Nyt siis $x_3 = r = m^2 - 2x_1$. Sijoitetaan saatu piste x_3 tangentin yhtälöön ja peilataan tämä x-akselin suhteen ja saadaan, että $y_3 = m(x_1 - x_3) - y_1$.

Tapauksessa $P = Q$ ja $y_1 = 0$ määritellään, että $P + Q = \infty$. Lisäksi määritellään, että $P + \infty = \infty + P = P$ ja $\infty + \infty = \infty$.

Yhdistetään tämä kaikki määritelmäksi.

Määritelmä 2.2. Ks. [12, s. 14]. Olkoon $E(K)$ elliptinen käyrä. Olkoon $P_1 = (x_1, y_1)$ ja $P_2 = (x_2, y_2)$ pisteitä elliptisellä käyrällä $E(K)$ siten, että $P_1, P_2 \neq \infty$. Määritellään pisteiden yhteenlasku $P_1 + P_2 = (x_3, y_3)$ seuraavasti:

1. Jos $x_1 \neq x_2$, niin $x_3 = m^2 - x_1 - x_2$ ja $y_3 = m(x_1 - x_3) - y_1$, missä $m = \frac{y_2 - y_1}{x_2 - x_2}$.
2. Jos $x_1 = x_2$ ja $y_1 \neq y_2$, niin $P_1 + P_2 = \infty$.
3. Jos $P_1 = P_2$ ja $y_1 \neq 0$, niin $x_3 = m^2 - 2x_1$ ja $y_3 = m(x_1 - x_3) - y_1$, missä $m = \frac{3x_1^2 + a}{2y_1}$.
4. Jos $P_1 = P_2$ ja $y_1 = 0$, niin $P_1 + P_2 = \infty$.

Lisäksi määritellään, että $P + \infty = \infty + P = P$ kaikilla käyrän E pisteillä P.

Lause 2.3. *Elliptinen käyrä $E(K)$ yhdessä edellä esitetyn yhteenlaskun kanssa muodostaa Abelin ryhmän.*

Todistus. Vrt. [12, s. 15]. Osoitetaan pari $(E(K), +)$ Abelin ryhmäksi.

1. Pisteiden P ja Q kautta kulkeva suora on yksikäsitteinen ja sisältää vain kolme leikkauspistettä elliptisen käyrän $E(K)$ kanssa, joten vaihdannaisuus on selvä. Muissa tapauksissa vaihdannaisuus tulee suoraan määritelmästä.

2. Yhteenlaskun määritelmän perusteella $P + \infty = P$ kaikilla $P \in E(K)$. Siis alkio ∞ toimii neutraali-alkiona.

3. Jos $P = (x_1, y_1)$, niin valitaan $-P = (x_1, -y_1)$. Nyt jos $y_1 \neq -y_1$, niin yhteenlaskun määritelmän perusteella $P + (-P) = \infty$. Jos $y_1 = -y_1$, niin $y_1 = 0$. Nimittäin jos pätisi, että $y_1 + y_1 = 0$ ja $y_1 \neq 0$, niin voitaisiin kertoa alkion y_1 käänteisalkiolla y_1^{-1} ja saada, että $1 + 1 = 0$, mikä ei ole mahdollista, koska kunnan K karakteristika ei ole 2, joten täytyy olla, että $y_1 = 0$. Siis yhteenlaskun määritelmän perusteella $P + (-P) = \infty$. Lisäksi tietenkin $\infty + \infty = \infty$. Nyt kaikilla $P \in E(K)$ on olemassa käänteisalkio.

4. Sivuutetaan liitännäisyyden todistaminen. Ks. [12, s. 20].

□

Esimerkki 2.2. Tutkitaan elliptistä käyrää

$$E(\mathbb{Z}_5) = \left\{ (x, y) \in \mathbb{Z}_5^2 \mid y^2 = x^3 + x \right\} \cup \{ \infty \}.$$

Nyt käyrän diskriminantti on

$$\Delta = 4 * 1^3 + 27 * 0^2 = 4 \neq 0,$$

joten kyseessä todella on elliptinen käyrä.

Käyrän pisteet on helppo selvittää, sillä $\mathbb{Z}_5$ on äärellinen 5-alkioinen kunta. Nyt siis kokeilemalla arvoja 0, 1, 2, 3 ja 4 yhtälöön $y^2 = x^3 + x$ saadaan, että

$$E(\mathbb{Z}_5) = \{ \infty, (0,0), (2,0), (3,0) \}.$$

Lasketaan esimerkiksi mitä on $(0,0) + (2,0)$. Sovelletaan yhteenlaskun määritelmän ensimmäistä kohtaa, koska $0 \neq 2$. Tällöin

$$m = \frac{y_2 - y_1}{x_2 - x_1} = \frac{0 - 0}{2 - 0} = 0,$$

$$x_3 = m^2 - x_1 - x_2 = 0^2 - 0 - 2 = 3$$

ja

$$y_3 \ = m(x_1 - x_3) = 0 * (0 - 3) = 0,$$

joten

$$(0,0) + (2,0) = (3,0).$$

Esimerkki 2.3. Olkoon E elliptinen käyrä. Tutkitaan seuraavaksi joukon

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

erikoistapausta, joukkoa $E[2]$(vrt. [12, s. 77]). Olkoon $p = x^3 + ax + b \in \overline{K}[X]$ polynomi. Polynomi p voidaan esittää muodossa $p = (X - e_1)(X - e_2)(X - e_3)$, missä $e_1, e_2, e_3 \in \overline{K}$. Tiedetään yhteenlaskun määritelmän perusteella, että jos $2P = \infty$, niin $P = (x, 0)$, jollain $x \in \overline{K}$. Tällöin

$$p(x) = x^3 + ax + b = (x - e_1)(x - e_2)(x - e_3) = 0.$$

Nyt siis $x = e_1$ tai $x = e_2$ tai $x = e_3$. Lisäksi tietenkin $2\infty = \infty$, joten $\infty \in E[2]$. Siis saadaan, että

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

Esimerkki 2.4. Vrt. [8]. Olkoon $E(K)$ elliptinen käyrä. Tutkitaan joukkoa $E[3]$. Olkoon $P \in E[3]$. Nyt siis $3P = \infty$. Selvästi $3\infty = \infty$, joten oletetaan, että $P \neq \infty$. Tällöin $3P = \infty$, jos ja vain jos $2P = -P$. Merkitään, että $P = (x, y)$ ja $P + P = (x_0, y_0)$. Huomataan nyt, että $2P = -P$, jos ja vain jos $x_0 = x$.

Yhteenlaskun määritelmästä saadaan, että

$$x_0 = (\frac{3x^2 + a}{2y})^2 - 2x = x \text{ ja}$$
$$y_0 = \frac{3x^2 + a}{2y}(x - x_0) - y = y.$$

Merkitään, että

$$f = X^3 + aX + b \in K[X].$$

Derivoidaan tämä kolmesti ja saadaan, että

$$f' = 3X^2 + a \in K[X],$$
$$f'' = 6X \in K[X] \text{ ja}$$
$$f''' = 6 \in K[X].$$

Siis voidaan antaa seuraava esitys alkiolle x_0:

$$x_0 = \frac{[f'(x)]^2}{4f(x)} - 2x.$$

Nyt $x_0 = x$, jos ja vain jos

$$\frac{[f'(x)]^2}{4f(x)} - 2x = x.$$

Mikä on yhtäpitävää sen kanssa, että

$$\frac{[f'(x)]^2}{4f(x)} = 3x = \frac{3}{6}f''(x),$$

joka taas on yhtäpitävää sen kanssa, että

$$[f'(x)]^2 = 2f(x)f''(x).$$

Merkitään nyt, että

$$g = (f')^2 - 2ff'' \in K[x].$$

Yhdistämällä edelliset yhtäpitävyydet saadaan, että $x_0 = x$, jos ja vain jos $g(x) = 0$.

Huomataan, että polynomin g aste on 4. Tutkitaan siis onko polynomilla g erilliset juuret vai löytyykö siltä moninkertainen juuri. Lauseen 2.2 nojalla $x \in \overline{K}$ on polynomin g moninkertainen juuri, jos ja vain jos $g(x) = 0$ ja $g'(x) = 0$. Derivoidaan siis g käyttämällä ketjusääntöä ja tulon derivoimissääntöä

$$\begin{aligned} g' &= 2f'f'' - 2f'f'' - 2ff''' \\ &= -2ff''' \\ &= -12f. \end{aligned}$$

Tällöin, jos $g(x) = 0$ ja $g'(x) = 0$, niin edellisen derivoinnin nojalla $f(x) = 0$ ja myös $f'(x) = 0$, mikä ei ole mahdollista sillä $E(K)$ on elliptinen käyrä, jolloin polynomilla f ei ole moninkertaista juurta.

Olkoot $r_1, r_2, r_3, r_4 \in \overline{K}$ polynomin g juuret. Oletetaan sitten, että $\mu_i^2 = f(r_i)$ indeksin i arvoilla 1, 2, 3 ja 4. Tällöin siis

$$E[3] = \{\, (r_i, \pm\mu_i) \mid i = 1, 2, 3, 4 \,\} \cup \{\, \infty \,\}.$$

3 Diskreetin logaritmin ongelma

3.1 Diskreetti logaritmi ja diskreetin logaritmin ongelma

Diskreetin logaritmin ongelma on monen salausjärjestelmän taustalla oleva vaikeana pidetty ongelma. Itse diskreetti logaritmi on ”helppo” laskea, mutta yleisesti pidetään ”vaikeana” ratkaista x yhtälöstä

$$xP = Q,$$

missä P ja Q ovat jonkin ryhmän G alkioita. Tietenkin ongelman vaikeuteen vaikuttavat luonnollisesti ryhmän G ja alkion P valinta.

Määritelmä 3.1. Ks. [7, s. 63]. Olkoon G ryhmä. Olkoot $P, Q \in G$. Sanotaan, että $k \in \mathbb{Z}$ on alkion Q P-kantainen *diskreetti logaritmi* jos $kP = Q$. Tilannetta, jossa k on tuntematon kutsutaan *diskreetin logaritmin ongelmaksi*.

Huomautus. Yllä oleva määritelmä sallii useamman arvon k olemassaolon. Yleensä jos G ryhmä ja $P, Q \in G$, niin tarkoitetaan diskreetillä logaritmilla pienintä sellaista $k \geq 0$, että $kP = Q$.

Ennen diskreetin logaritmin ongelman käsittelyä on hyvä kuitenkin käsitellä tapausta, jossa n ja P ovat tunnettuja, mutta Q tuntematon. Työläs tapa olisi laskea

$$nP = P + P + \cdots + P,$$

missä n kappaletta pisteitä P. Esitetään vähemmän työläs algoritmi, jonka avulla voidaan laskea arvo nP.

3.2 Kahdenna ja lisää -algoritmi

Olkoon G ryhmä ja $P \in G$. Esitetään algoritmi alkion nP laskemiseen, kun $n \in \mathbb{N} \setminus \{ 0 \}$.

Algoritmi 1 Kahdenna ja lisää -algoritmi

Input: $n > 0$ ja $P \in G$
Output: nP

Asetetaan aluksi:
$Q \leftarrow P$
$R \leftarrow 0$
while $n > 0$ **do**
  if $n \equiv 1 \mod 2$ **then**
    $R \leftarrow R + Q$
  end if
  $Q \leftarrow 2Q$
  $n \leftarrow \lfloor \frac{n}{2} \rfloor$
end while
return $R = nP$

Todistus. Vrt. [7, s. 292-293]. Luku n voidaan esittää binäärilukuna

$$n = n_0 + n_1 * 2 + n_2 * 2^2 + \cdots + n_r * 2^r,$$

missä $n_0, n_1, \ldots, n_r \in \{ 0, 1 \}$. Asetetaan nyt

$$Q_0 = P, Q_1 = 2Q_0, Q_2 = 2Q_1, \ldots, Q_r = 2Q_{r-1},$$

jolloin

$$Q_i = 2^i P.$$

Tällöin

$$\begin{aligned} nP &= (n_0 + n_1 * 2 + n_2 * 2^2 + \cdots + n_r * 2^r)P \\ &= n_0 P + n_1 * 2P + n_2 * 2^2 * P + \cdots + n_r 2^r P \\ &= n_0 Q_0 + n_1 Q_1 + \cdots + n_r Q_r. \end{aligned}$$

□

Esimerkki 3.1. Olkoon $E_{(-3,5)}(\mathbb{Z}_{73})$ elliptinen käyrä ja $P = (9, 14) \in E_{(-3,5)}(\mathbb{Z}_{73})$. Selvitetään, mitä on $37P$ käyttäen kahdenna ja lisää algoritmia.

Muunnetaan luku 37 binääriksi. Tällöin

$$37 = 1 * 2^0 + 1 * 2^2 + 1 * 2^5 = 100101_2.$$

Lasketaan siis pisteet $Q_0 = P$, $Q_1 = 2Q_0$, $Q_2 = 2Q_1$, $Q_3 = 2Q_2$, $Q_4 = 2Q_3$ ja $Q_5 = 2Q_4$. Nyt kyseessä pisteen tuplaus, joten sovelletaan kaikissa kohdissa yhteenlaskukaavoista sitä, missä tangentin avulla selvitetään uusi piste. Käydään läpi mitä on $2P$. Muut kohdat lasketaan samalla tavalla.

Selvitetään aluksi pisteen $P = (x_1, y_1) = (9, 14)$ kautta kulkevan tangentin kulmakerroin. Nyt

$$m = \frac{3x_1^2 + a}{2y_1} = \frac{3 * 9^2 - 3}{2 * 14} = \frac{21}{28} = 21 * 60 = 19.$$

Tällöin

$$x_3 = m^2 - 2x_1 = 19^2 - 2 * 9 = 51$$

ja

$$y_3 = m(x_1 - x_3) - y_1 = 19(9 - 51) - 14 = 64.$$

Siis

$$Q_1 = 2P = 2(9, 14) = (51, 54).$$

Pisteet Q_2, Q_3, Q_4 ja Q_5 lasketaan vastaavasti.

Lopulta saadaan, että

$$\begin{aligned} 37P &= (2^0 + 2^2 + 2^5)P \\ &= P + 2^2P + 2^5P \\ &= P + Q_2 + Q_5 \\ &= (9, 14) + (9, 59) + (51, 64) \\ &= \infty + (51, 64) \\ &= (51, 64). \end{aligned}$$

Negaation hyödyntäminen laskettaessa pistettä nP

Olkoon $E_{(a,b)}(K)$ elliptinen käyrä ja $P = (x, y) \in E_{(a,b)}(K)$. Nyt $-P = (x, -y)$. Pisteen $-P$ selvittäminen on siis erittäin helppoa. Tämän havainnon perusteella voidaan helpottaa kahdenna ja lisää -algoritmin laskemista.

Lause 3.1. *Olkoon n positiivinen kokonaisluku ja $k = \lfloor \log n \rfloor + 1$. Tällöin*

$$n = u_0 + u_1 * 2 + u_2 * 2^2 + u_3 * 2^3 + \cdots + u_k * 2^3,$$

missä u_0, u_1, $\cdots$, $u_k \in \{ -1, 0, 1 \}$.

Todistus. Vrt. [7, s. 295]. Esitetään luku n binäärissä. Siis

$$n = n_0 + n_1 * 2 + n_2 * 2^2 + \cdots + n_{k-1} * 2^{k-1},$$

missä $n_0, n_1, \cdots, n_{k_1} \in \{ 0, 1 \}$.

Oletetaan, että

$$n_s = n_{s+1} = \cdots = n_{s+t-1} = 1$$

ja $n_{s+t} = 0$, jollain $t > 0$ ja $s \in \{ 0, 1, \cdots, k - 2 \}$. Tällöin siis

$$2^s + 2^{s+1} + \cdots + s^{s+t-1} + 0 * 2^{s+t}$$

on osa luvun n binääriesitystä. Oleellinen havainto on nyt, että

$$\begin{aligned} 2^s + 2^{s+1} + \cdots + s^{s+t-1} + 0 * 2^{s+t} &= 2^s(1 + 2 + 3 + \cdots + 2^{t-1}) \\ &= 2^s(2^t - 1). \end{aligned}$$

Siis luku $2^s + 2^{s+1} + \cdots + s^{s+t-1} + 0 * 2^{s+t}$ voidaan korvata binääriesityksessä luvulla $2^s(2^t - 1)$. Käymällä binääriesitystä vasemmalta oikealle voidaan löytää kaikki tällaiset esiintymät ja suorittaa korvaukset. □

Esimerkki 3.2. Luvun 2016 binääriesitys on

$$2016 = 2^5 + 2^6 + 2^7 + 2^8 + 2^9 + 2^{10}.$$

Siis

$$\begin{aligned} 2^5 + 2^6 + 2^7 + 2^8 + 2^9 + 2^{10} &= 2^5(2^6 - 1) \\ &= -2^5 + 2^{11}. \end{aligned}$$

Siis $2016 = -2^5 + 2^{11}$.

Esimerkki 3.3. Jatketaan edellistä esimerkkiä. Olkoon $E_(a, b)(\mathbb{Z}_p)$ elliptinen käyrä ja $P \in E_(a, b)(\mathbb{Z}_p)$. Halutaan selvittää, mitä on $2016P$. Nyt kahdenna ja lisää -algoritmin avulla lasketaan alkuun

$$Q_0 = P, Q_1 = 2 * Q_0, \ldots, Q_{10} = 2 * Q_9,$$

ja lopuksi lasketaan, mitä on

$$2016P = Q_5 + Q_6 + Q_7 + Q_8 + Q_9 + Q_{10}.$$

Edellinen esimerkki kertoo, että $2016 = -2^5 + 2^{11}$. Jos vielä lasketaan

$$Q_{11} = 2Q_{10},$$

niin voidaan soveltaa algoritmin paranneltua versiota ja lopuksi tarvitsee vain laskea

$$2016P = -Q_5 + Q_{11}.$$

Jälkimmäinen tapa siis sopii hyvin elliptisten käyrien kanssa käytettäväksi, koska käänteisalkion selvittäminen on erittäin helppoa.

Diskreetin logaritmin ongelma

Esimerkki 3.4. Palataan diskreetin logaritmin ongelmaan. Jos G on ryhmä ja $P, Q \in G$ siten, että $nP = Q$, niin yksinkertaisin tapa ratkaista tämä ongelma on laskea yhteen alkioita P, kunnes summaksi saadaan Q. Seuraavissa luvuissa esitellään ratkaisumenetelmiä, jotka eivät ole näin työläitä.

Esimerkki 3.5. Tehtävänä ratkaista diskreetin logaritmin ongelma $5^x = 8$ ryhmässä $\mathbb{Z}_{13}^*$. Nyt

$$\begin{aligned} 5^0 &= 0, \\ 5^1 &= 5, \\ 5^2 &= 12 \text{ ja} \\ 5^3 &= 8. \end{aligned}$$

Siis $x = 8$. Tässä ratkaisu löytyi helposti, mutta jos ryhmänä on $\mathbb{Z}_p$, missä p on suuri alkuluku, niin ratkaisun löytyminen näin on aivan liian työlästä.

Esimerkki 3.6. Vrt. [12, Harjoitus 5.2 s. 166]. Esitetään esimerkki siitä, miksi ryhmän valinta on tärkeää diskreetin logaritmin ongelman vaikeuden kannalta. Tutkitaan ryhmää $(\mathbb{Z}_p, +)$ ja diskreetin logaritmin ongelmaa $nP = Q$. Edellisessä p on alkuluku. Nyt diskreetin logaritmin ongelman ratkaisuun riittää lineaarisen kongruenssin

$$nP \equiv Q \mod p$$

ratkaiseminen.

Tällöin $syt(P, p) = 1$, joten voidaan etsiä laajennetun Eukleideen algoritmin avulla alkiolle P käänteisalkio A.

Kerrotaan alkiolla A ja saadaan, että

$$n \equiv QA \mod p.$$

4 Kryptografiaa

Salauksen tarkoitus on pitää viesti tai data salassa. Erityisesti digitaalinen kehitys on luonut tarpeen salausjärjestelmien käyttöön. Esimerkiksi kaupankäynti tietoverkkojen kautta on täysin riippuvainen salausmenetelmistä, jos halutaan pitää asiakkaan tiedot, erityisesti maksutiedot, salassa. Lisäksi yksityisyyden säilyttäminen aikana, jolloin suuri osa sosiaalisesta elämästä tapahtuu tietoverkkojen kautta, vaatii vahvoja salausmenetelmiä. Niin rikolliset hakkerit kuin valtiolliset tahot ovat hyvinkin tietoisia mahdollisuuksista tiedon hankintaan suojaamattomista verkoista.

Tässä luvussa esitellään kryptografian perusteita keskittyen julkisen avaimen salauksiin. Päälähteenä tässä luvussa on Buchmannin Introduction to Cryptography [3].

4.1 Kryptosysteemi

Määritelmä 4.1. Ks. [3, s. 71-72]. *Kryptosysteemi* on 5-jono $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$, jolle pätevät seuraavat ehdot:

1. Joukko $\mathcal{P}$ on *selkotekstien* joukko.
2. Joukko $\mathcal{C}$ on *salatekstien* joukko.
3. Joukko $\mathcal{K}$ on *avainten* joukko.
4. Kokoelma $\mathcal{E} = \{ E_k \mid k \in \mathcal{K} \}$ on kokoelma *salauskuvauksia*
$$E_k : \mathcal{P} \to \mathcal{C}.$$
5. Kokoelma $\mathcal{D} = \{ D_k \mid k \in \mathcal{K} \}$ on kokoelma *salauksen purkukuvauksia*
$$D_k : \mathcal{C} \to \mathcal{P}.$$
6. Lisäksi jokaisella $e \in \mathcal{K}$ on olemassa $d \in \mathcal{K}$ siten, että kaikilla $p \in \mathcal{P}$ pätee, että $D_d(E_e(p)) = p$.

Kryptosysteemiä, jossa salausavain toimii salaamiseen ja salauksen purkamiseen sanotaan *symmetriseksi kryptosysteemiksi*. Jos avain salauksen purkamiseen on eri kuin salaamiseen käytetty on kyseessä *epäsymmetrinen kryptosysteemi* tai *julkisen avaimen kryptosysteemi*.

Esimerkki 4.1. Vrt. [3, s. 72]. Esitetään klassinen esimerkki symmetrisestä kryptosysteemistä, Caesarin salakirjoitus. Koodataan aakkosto $\{ a, b, \ldots, z \}$ numeroiksi siten, että $a = 0, b = 1, \ldots, z = 25$.

Olkoon $k \in \mathbb{Z}_{26}$. Määritellään salauskuvaus ja salauksen purkukuvaus nyt seuraavasti:

$$E_k(p) = (p + k) \mod 26 \text{ ja}$$
$$D_k(c) = (c - k) \mod 26.$$

Salataan nyt viesti *De vita Caesarum* käyttäen avaimena $k = 5$. Poistetaan viestistä välilyönnit ja muunnetaan isot kirjaimet pieniksi. Saadaan salattu viesti *ijanyfhfjxfwzr*.

Esimerkki 4.2. Vrt. [3, Harjoitus 3.16.3 s. 111]. Olkoon $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ kryptosysteemi, $k \in \mathcal{K}$ avain ja $E_k \in \mathcal{E}$ salauskuvaus. Osoitetaan, että salauskuvaus E_k on injektio.

Oletetaan, että $a, b \in \mathcal{P}$ ovat selkotekstejä siten, että $E_k(a) = E_k(b)$. Nyt kryptosysteemin määritelmän kuudennen kohdan nojalla on olemassa sellainen $d \in \mathcal{K}$, että jos $D_d \in \mathcal{D}$ on salauksen purkukuvaus, niin $D_d(E_k(a)) = a$ ja $D_d(E_k(b)) = b$. Siis soveltamalla kuvausta D_d yhtälön $E_k(a) = E_k(b)$ molemmille puolille saadaan, että $a = b$, joten salauskuvaus E_k on injektio.

Huomautus. Hoffstein, Pipher ja Silverman [7, s. 38] listaavat ominaisuuksia joita hyvän kryptosysteemin tulisi omata. Olkoon $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ kryptosysteemi.

1. Jos $k \in \mathcal{K}$ on avain ja $p \in \mathcal{P}$ selkoteksti, niin tulisi olla helppoa laskea salateksti $E_k(p)$.

2. Jos $k \in \mathcal{K}$ on avain ja $c \in \mathcal{C}$ on salateksti, niin tulisi olla helppoa laskea selkoteksti $D_k(c)$.

3. Jos $c_1, c_2, \ldots, c_n \in \mathcal{C}$ salattu avaimella $k \in \mathcal{K}$, niin tulisi olla vaikeaa selvittää $D_k(c_1)$, $D_k(c_2)$, $\ldots$, $D_k(c_n)$ ilman tietoa avaimesta k.

4. Jos (p_1, c_1), (p_2, c_2), $\ldots$, (p_n, c_n) lista toisiaan vastaavia pareja selkotekstejä ja salatekstejä, niin tulisi olla vaikeaa purkaa salaus listan ulkopuolisesta viestistä c ilman tietoa avaimesta $k \in \mathcal{K}$.

Lisäksi hyödyllinen sääntö on niin sanottu *Kerckhoffin periaate*[7, s. 38], joka sanoo, että kryptosysteemin tulisi riippua vain avaimen pitämisestä salassa. Itse algoritmien tulisi olla julkista tietoa, jotta mahdolliset ongelmat voidaan havainnoida.

4.2 Julkisen avaimen salaus

Julkisen avaimen kryptosysteemien on tarkoitus vastata erityisesti avaimen vaihtoa koskeviin ongelmiin. Jos kaksi tahoa haluaa keskustella keskenään salatusti, on heidän jossain vaiheessa päästävä sopimukseen käytettävästä avaimesta.

Tässä luvussa esitetyt julkisen avaimen kryptosysteemit pohjaavat diskreetin logaritmin ongelmaan.

4.2.1 Diffie-Hellman-avaimenvaihtoprotokolla

Esitetään Diffie-Hellman-avaimenvaihtoprotokolla sykliselle ryhmälle $G = \langle P \rangle$. Vrt. [3, s. 188-191]. Kyseessä ei ole varsinainen kryptosysteemi, vaan tapa sopia salausavain turvattomien viestintäyhteyksien yli. Nyt kaksi henkilöä Alice ja Bob haluavat sopia yhteisestä salausavaimesta. He ovat jo päässeet yhteisymmärrykseen syklisestä ryhmästä G ja sen virittäjästä P. Oletetaan, että $ord(P) = n$. Tällöin

1. Alice valitsee luvun $a \in \{ 1, 2, \ldots, n-1 \}$ ja laskee alkion $K = aP$ sekä lähettää tämän Bobille.

2. Vastaavasti Bob valitsee luvun $b \in \{ 1, 2, \ldots, n-1 \}$ ja laskee alkion $H = bP$ sekä lähettää tämän Alicelle.

3. Nyt Bob voi laskea arvon

$$bK = b(aP) = (ba)P = (ab)P$$

   ja Alice arvon

$$aH = a(bP) = (ab)P.$$

   Tämä yhteinen arvo voi toimia salausavaimena jatkossa.

Huomautus. Tässä tutkielmassa käytetään nimiä Bob ja Alice viittaamaan keskustelijoihin, jotka haluavat esimerkiksi sopia salausavaimesta käyttäen Diffie-Hellman avaimenvaihtoprotokollaa. Tahoon, jonka tarkoitus on selvittää näiden kahden viestintää, viitataan vain hyökkääjänä.

Määritelmä 4.2. Oletetaan, että hyökkääjä tuntee Alicen ja Bobin käyttämän ryhmän G, sen generoivan alkion P sekä alkiot aP ja bP. Tällöin hyökkääjä haluaa selvittää näillä tiedoilla salausavaimen abP. Kyseistä ongelmaa kutsutaan *Diffie-Hellman ongelmaksi*.

Huomautus. Selvästi hyökkääjä, joka pystyy ratkaisemaan diskreetin logaritmin ongelman $K = aP$ tai $H = bP$, pystyy näin myös ratkaisemaan Diffie-Hellman ongelman.

Esimerkki 4.3. Vrt. [7, Harjoitus 5.15 s. 341]. Olkoon $E_{(a,b)}(\mathbb{Z}_p)$ elliptinen käyrä. Tässä p on alkuluku. Oletetaan, että $Q \in E(\mathbb{Z}_p)$.

Nyt jos Bob haluaa lähettää Alicelle pisteen $rQ = (x_r, y_r)$, missä $r \in \mathbb{N}$, niin hänen tarvitsee lähettää vain arvo x_r ja bitti

$$B = \begin{cases} 0, \text{ jos } 0 \leq y_r < \frac{1}{2}p \\ 1, \text{ jos } \frac{1}{2}p \leq y_r < p. \end{cases}$$

Nimittäin Alice voi ratkaista yhtälöstä

$$y^2 = x_r^3 + ax_r + b$$

arvon y ja päätellä bitistä B kumman arvon Bob valitsi.

Esimerkki 4.4. Vrt. [3, s. 190]. Alice ja Bob haluavat luoda salausavaimen käyttäen Diffie-Hellmannia, mutta heidän epäonnekseen heidän käyttämäänsä keskustelukanavaan on asettunut hyökkääjä, joka on aina heidän viestiensä välissä.

Olkoon $G = \langle P \rangle$ syklinen ryhmä. Hyökkääjä teeskentelee olevansa Alice ja lähettää Bobille arvon aP ja vastaanottaa Bobilta arvon bP. Vastaavasti hyökkääjä teeskentelee olevansa Bob ja lähettää Alicelle arvon $a'P$ ja vastaanottaa tältä arvon $b'P$.

Nyt kun Alice haluaa lähettää Bobille viestin m, hän käyttää symmetristä salausta ja avainta $a'b'P$. Tällöin hyökkääjä vastaanottaa viestin $E_{a'b'P}(m)$, purkaa sen salauksen saaden selville sen sisällön, ja salaa viestin uudelleen käyttäen avainta abP. Nyt hän lähettää viestin $E_{abP}(m)$ Bobille, joka pystyy purkamaan sen omalla avaimellaan. Näin Alice ja Bob luulevat keskustelevansa vain toistensa kanssa vaikka oikeasti keskustelevat hyökkääjän kanssa, joka vain välittää viestejä heille toisiltaan.

Tällaista hyökkäystä kutsutaan *mies välissä -hyökkäykseksi*.

Huomautus. Diffie-Hellman-avaimenvaihtoprotokollan toimintaedellytyksenä käytännössä on tietenkin, että diskreetin logaritmin ongelma on vaikea ryhmässä G. Mahdollisia ryhmiä voisivat olla esimerkiksi elliptiset käyrät $E_{(a,b)}(\mathbb{Z}_p)$, missä p on suuri alkuluku.

4.2.2 ElGamal-kryptosysteemi

Vrt. [3, s. 191-195]. ElGamal-kryptosysteemi on esimerkki epäsymmetrisestä kryptosysteemistä. Tässä Alicen salausavain jakautuu kahteen osaan: julkiseen osaan, jonka avulla muut ihmiset voivat viestiä hänen kanssaan, ja salaiseen osaan, joka mahdollistaa hänelle lähetettyjen salattujen viestien purkamisen.

Avaimen luonti. Alice valitsee syklisen ryhmän G ja sen virittäjän P. Lisäksi hän valitsee satunnaisen luvun a joukosta $\{ 0, 1, \ldots, n-1 \}$, missä $n = ord(P)$. Tämän jälkeen hän laskee arvon $A = aP$. Tällöin hänen julkinen avaimensa on kolmikko (G, P, A).

Salaus. Selkotekstien joukko on tässä tapauksessa

$$\mathcal{P} = \{ 0, P, 2P, \ldots, (n-1)P \}.$$

Jos Bob haluaa kommunikoida Alicen kanssa, hän valitsee satunnaisen luvun b joukosta $\{ 0, 1, \ldots, n-1 \}$ ja laskee arvon $B = bP$. Nyt salatakseen viestin $M \in \mathcal{P}$ Bob lisää viestiin alkion bA saaden salatekstin $C = bA + M$. Tämän jälkeen Bob lähettää Alicelle parin (B, C).

Salauksen purku. Hyödynnetään Alicen tietoa luvusta a. Olkoon $x = n-a$. Nyt $ord(P) = n$, joten

$$\begin{aligned} xB + C &= (n-a)bP + bA + M \\ &= b(nP) - baP + bA + M \\ &= -baP + bA + M \\ &= -baP + baP + M = M. \end{aligned}$$

Hyökkäys. Jälleen, jos hyökkääjä kykenee ratkaisemaan diskreetin logaritmin ongelman $A = aP$, niin kykenee hän myös purkamaan salauksen.

Lause 4.1. *Olkoon $G = \langle P \rangle$ syklinen ryhmä siten, että $ord(P) = n$. Oletetaan, että on olemassa* oraakkeli*, joka pystyy purkamaan salauksen mistä tahansa ElGamal-kryptosysteemillä salatusta salatekstistä. Tällöin hyökkääjä, jolla on käytössään tällainen oraakkeli, kykenee ratkaisemaan Diffie-Hellman ongelman.*

Todistus. Vrt. [7, s. 71]. Diffie-Hellman ongelmassa hyökkääjän tarkoitus on selvittää alkio $(ab)P$, kun tiedossa ovat alkiot aP ja bP.

Nyt ovela hyökkääjä voi antaa oraakkelille tiedoksi julkisen avaimen kolmikon (G, P, aP) ja pyytää tätä selvittämään salatekstin $(bP, 0)$. Tällöin oraakkeli palauttaa takaisin alkion

$$(n-a)bP + 0 = b(nP) - abP = -abP,$$

jolloin hyökkääjän on helppoa selvittää alkion $-abP$ käänteisalkio abP ja näin myös helppoa ratkaista Diffie-Hellman ongelma.

Entä jos hyökkääjän käyttämä oraakkeli ei hyväksy arvoa 0? Tällöin hyökkääjä lähettää oraakkelille parin (bP, C). Hän vastaanottaa oraakkelilta

$$M = (n-a)bP + C = -abP + C.$$

Nyt selvittämällä alkion M käänteisalkio $-M$ saadaan, että

$$C - M = abP.$$

Näin on selvitetty Diffie-Hellman ongelma. □

4.2.3 ElGamal-digitaalinen allekirjoitus

Vrt. [12, s. 175-177]. Perinteisesti asiakirjan voi todentaa oikeaksi, jos sen luoja on allekirjoittanut sen. Tällöin jokainen, joka tunnistaa hänen allekirjoituksensa, kykenee vahvistamaan asiakirjan aitouden. Esitetään vastaava digitaalinen tapa.

Avaimen valinta. Olkoon $G = \langle P \rangle$ syklinen ryhmä. Oletetaan, että $ord(P) = n$. Suoritetaan avaimen valinta samaan tapaan, kuin ElGamal-kryptosysteemissä. Julkiseksi avaimeksi saadaan kolmikko (G, P, A), missä $A = aP$. Täydennetään tämä vielä nelikoksi valitsemalla kuvaus

$$f : G \to \mathbb{Z}.$$

Luku a jää jälleen salaiseksi tiedoksi.

Asiakirjan allekirjoitus. Esitetään asiakirja lukuna $m \in \mathbb{Z}$. On huomattava, että tässä sallitaan vain viestit $m < n$. Valitaan satunnainen u siten, että $syt(u, n) = 1$ ja lasketaan $R = uP$. Lopuksi lasketaan

$$s \equiv u^{-1}(m - af(R)) \mod n.$$

Nyt allekirjoitettu viesti on kolmikko (m, R, s).

Allekirjoituksen vahvistaminen. Lasketaan arvot $V_1 = f(R)A + sR$ ja $V_2 = mP$. Tällöin asiakirja on aito, jos $V_1 = V_2$. Nyt siis

$$s \equiv u^{-1}(m - af(R)) \mod n,$$

joten $su = m - af(R) + tn$, jollain $t \in \mathbb{Z}$. Siis saadaan, että

$$\begin{aligned} suP &= (m - af(R) + tn)P \\ &= (m - af(R))P + t(nP). \end{aligned}$$

Oletettiin, että $Ord(P) = n$, joten

$$suP = (m - af(R))P.$$

Siis on mahdollista vahvistaa asiakirjan aitous, sillä

$$\begin{aligned} V_1 &= f(R)A + sR \\ &= f(R)aP + suP \\ &= f(R)aP + (m - af(R))P \\ &= f(R)aP + mP - f(R)aP \\ &= mP = V_2. \end{aligned}$$

Hyökkäys. Tavalliseen tapaan, jos hyökkääjä pystyy ratkaisemaan diskreetin logaritmin ongelman $A = aP$, niin hän pystyy käyttämään arvoa a viestien allekirjoituksen väärentämiseen.

Vaihtoehtoisesti hyökkääjä voi ratkaista diskreetin logaritmin ongelman $R = uP$ ja hyödyntää tietoa arvosta u. Tällöin

$$us \equiv (m - af(R)) \mod n,$$

ja jos $syt(f(R), n) = d$, niin yhtälöllä

$$af(R) \equiv m - us \mod n$$

on d ratkaisua tuntemattomalle a. Nimittäin

$$a\frac{f(R)}{d} \equiv \frac{m - us}{d} \mod \frac{n}{d}.$$

Tällöin on olemassa $(\frac{f(R)}{d})^{-1} \mod \frac{n}{d}$, sillä $syt(\frac{f(R)}{d}, \frac{n}{d}) = 1$. Nyt mahdollinen arvo a löytyy joukosta

$$\left\{ (\frac{f(R)}{d})^{-1}(\frac{m - us}{d}) + i\frac{n}{d} \mid 0 \leq i \leq d \right\}.$$

Kolmas vaihtoehto on, että viestin allekirjoittaja on käyttänyt uudelleen samaa arvoa u kahden eri viestin allekirjoittamiseen. Tällöin hyökkääjällä on käytössään viestit (m, R, s) ja (m', R, s'). Tiedetään, että

$$\begin{cases} us \equiv (m - af(R)) \mod n \\ us' \equiv (m' - af(R)) \mod n. \end{cases}$$

Vähennetään nämä toisistaan ja saadaan yhtälö

$$u(s - s') \equiv (m - m') \mod n.$$

Jos $syt(s - s', n) = d$, niin saadaan d kokeiltavaa arvoa mahdolliseksi luvuksi u. Tämän jälkeen tiedetään $R = uP$ ja voidaan hyödyntää edellistä hyökkäystä luvun a selvittämiseksi. Siis on syytä pitää huolta siitä, että arvoa u ei käytetä uudelleen.

Esimerkki 4.5. Esitetään esimerkki viestin todentamisesta aidoksi käyttäen ElGamal-digitaalista allekirjoitusta. Olkoon $\mathbb{Z}_{23}^* = \langle \overline{5} \rangle$ ryhmä ja $f : \mathbb{Z}_{23}^* \to \mathbb{Z}$, $\overline{x} \mapsto x$ kuvaus. Tällöin siis $P = \overline{5}$. Käytetään salaisena lukuna lukua $a = 7$. Tällöin julkinen avain on nelikko $K_{pub} = (\mathbb{Z}_{23}^*, \overline{5}, \overline{17}, f)$.

Allekirjoitetaan viesti $m = 9$ käyttäen julkista avainta K_{pub}. Valitaan satunnainen luku $u = 13$ ja lasketaan alkio $R = P^u = \overline{5}^{13} = 21$. Nyt

$$\begin{aligned} s &\equiv u^{-1}(m - af(R)) \mod n \\ &\equiv 17 * (9 - 7 * 21) = 8 \mod 22. \end{aligned}$$

Tällöin allekirjoitettu viesti on kolmikko $(9, \overline{21}, 8)$.

Tarkistetaan allekirjoitetun viestin aitous. Nyt

$$\begin{aligned} V_1 &= A^{f(R)} * R^s = \overline{5}^{f(21)} * \overline{21}^8 = 11 \text{ ja} \\ V_2 &= P^m = \overline{5}^1 3 = 11. \end{aligned}$$

Siis viesti on aito.

Esimerkki 4.6. Jatketaan edellistä esimerkkiä. Oletetaan, että viesti $m' = 2$ on allekirjoitettu vahingossa käyttäen samaa arvoa u, kuin viesti $m = 9$.

Tällöin meillä on viestit $(9, \overline{21}, 8)$ ja $(2, \overline{21}, 21)$. Selvitetään nyt, mikä on salainen luku a. Ensiksi halutaan löytää kahdesti käytetty u.

Tiedetään, että $u * (8 - 21) \equiv (9 - 2) \mod 22$. Siis

$$9u \equiv 7 \mod 22.$$

Nyt $syt(9, 22) = 1$, joten on olemassa käänteisalkio alkiolle 9 mod 22. Siis $u \equiv 7 * 5 \equiv 13 \mod 22$.

Nyt tiedetään, että $R = P^u = \overline{5}^{13} = \overline{21}$. Tiedetään, että

$$af(R) \equiv m - us \mod n.$$

Siis $af(\overline{21}) \equiv 15 \mod 22$. Nyt $syt(21, 22) = 1$, joten on olemassa käänteisalkio. Saadaan, että $a \equiv 15 * 21 \equiv 7 \mod 22$, joka on etsitty ratkaisu diskreetin logaritmin ongelmaan. Hyökkääjämme voi nyt väärentää kyseisellä julkisella avaimella varmennettuja viestejä.

5 Pohlig-Hellman reduktio

Pohlig-Hellman reduktio on hyödyllinen tapa helpottaa diskreetin logaritmin ongelman $kP = Q$ ratkaisua syklisessä ryhmässä $G = \langle P \rangle$, jos $ord(P)$ jakautuu alkulukutekijöiksi siten, että siinä on vain pieniä alkulukuja. Tällöin voidaan diskreetin logaritmin ongelma jakaa pienempiin osiin ja soveltaa seuraavaksi käsiteltävää kiinalaista jäännöslausetta.

5.1 Kiinalainen jäännöslause

Aliluvussa esitellään kiinalainen jäännöslause todistuksineen. Lausetta sovelletaan myöhemmin ratkottaessa diskreetin logaritmin ongelmaa, mutta yksinäänkin se on hyödyllinen ratkaistaessa lineaarisia kongruenssi yhtälöryhmiä. Todistetaan aluksi kuitenkin kaksi lausetta auttamaan kiinalaisen jäännöslauseen todistuksessa.

Lause 5.1. *Jos $a_1, \ldots, a_l \in \mathbb{Z}$ keskenään jaottomia lukuja luvun $m \in \mathbb{Z}$ kanssa, niin samoin on luku $a_1 * \cdots * a_l$.*

Todistus. Vrt. [9, s. 34]. Todistetaan lause vastaoletuksella. Merkitään, että

$$L = a_1 * \cdots * a_l.$$

Oletetaan vastoin väitettä, että $syt(L, m) = d \neq 1$. Tunnetusti d voidaan esittää alkulukujen tulona. Olkoon p yksi luvun d alkulukuesityksen alkuluvuista. Tällöin $p \mid L$, joten $p \mid a_i$, jollain $i \in \{ 1, 2, \ldots, l \}$. Nyt pätee myös, että $p \mid m$, joten $syt(a_i, m) \neq 1$, mikä on ristiriita. Siis $syt(L, m) = 1$, joten luvut L ja m ovat keskenään jaottomia. □

Lause 5.2. *Oletetaan, että luvut $a_1, \ldots, a_l \in \mathbb{Z}$ jakavat luvun $n \in \mathbb{Z}$, ja että $syt(a_i, a_j) = 1$, kun $i \neq j$. Tällöin luku $a_1 * \cdots * a_l$ jakaa luvun n.*

Todistus. Vrt.[9, s. 34]. Todistetaan lause induktiolla indeksin l suhteen. Tapaus $l = 1$ on selvä. Oletetaan, että $l > 1$. Induktio-oletuksen nojalla

$$L' = a_1 * \cdots * a_{l-1}$$

jakaa luvun n. Edellisen lauseen nojalla $syt(L', a_l) = 1$. Laajennetun Eukleideen algoritmin avulla löydetään $r, s \in \mathbb{Z}$ siten, että

$$ra_l + sa_1 * \cdots * a_{l-1} = 1.$$

Kerrotaan molemmat puolet luvulla n ja saadaan, että

$$n = nra_l + nsa_1 * \cdots * a_{l-1}.$$

Induktio-oletuksen nojalla $a_1 * \cdots * a_{l-1}$ jakaa luvun n ja lauseen oletuksen nojalla a_l jakaa luvun n, joten luku n on jaollinen luvulla $a_1 * \cdots * a_l$. □

Lause 5.3. *(Kiinalainen jäännöslause) Olkoot* $m, m_1, m_2, \ldots m_t \in \mathbb{Z}_+$ *siten, että* $m = m_1 m_2 \cdots m_t$ *ja* $syt(m_i, m_j) = 1$*, kun* $i \neq j$*. Olkoot* $b_1, b_2, \ldots, b_t \in \mathbb{Z}$*. Tällöin kongruensseilla* $x \equiv b_1 \mod m_1$*,* $x \equiv b_2 \mod m_2$*, ...,* $x \equiv b_t \mod t$ *on ratkaisu. Lisäksi muut ratkaisut eroavat luvun* m *verran toisistaan.*

Todistus. Vrt. [9, s. 34]. Olkoon $n_i = m/m_i$ kaikilla $i \in \{ 1, 2, \ldots, t \}$. Nyt oletuksen nojalla $syt(m_i, m_j) = 1$, missä $i \neq j$ ja $i, j \in \{ 1, 2, \ldots, t \}$, joten lauseen 5.1 nojalla kaikilla $i \in \{ 1, 2, \ldots, t \}$ pätee, että $syt(m_i, n_i) = 1$, joten kaikilla $i \in \{ 1, 2, \ldots, t \}$ on olemassa $r_i, s_i \in \mathbb{Z}$ siten, että

$$r_i m_i + s_i n_i = 1,$$

missä r_i ja s_i voidaan löytää Eukleideen algoritmin avulla.

Olkoon $e_i = s_i n_i$ kaikilla $i \in \{ 1, 2, \ldots, t \}$. Tällöin

$$e_i \equiv 1 \mod m_i,$$

koska $s_i n_i - 1 = -r_i m_i$. Merkitään nyt, että

$$x_0 = \sum_{i=1}^{t} b_i e_i.$$

Nyt kaikilla $i \in \{ 1, 2, \ldots, t \}$

$$x_0 \equiv b_i e_i \mod m_i,$$

sillä $m_i \mid x_0 - b_i e_i$. Siis kaikilla $i \in \{ 1, 2, \ldots, t \}$

$$x_0 \equiv b_i \mod m_i,$$

sillä $e_i \equiv 1 \mod m_i$, joten x_0 on ratkaisu.

Tutkitaan vielä lauseen viimeistä kohtaa. Oletetaan, että on olemassa toinenkin ratkaisu x_1. Nyt kaikilla $i \in \{ 1, 2, \ldots, t \}$ pätee, että $x_1 - x_0 \equiv 0 \mod m_i$, joten $m_i \mid x_1 - x_0$. Nyt, koska $x_1 - x_0$ on jaollinen kaikilla m_i, niin se on lauseen 5.2 nojalla myös jaollinen luvulla m, joten x_1 ja x_0 eroavat toisistaan, jollain luvun m moninkerralla. □

Esimerkki 5.1. Sovelletaan kiinalaista jäännöslausetta etsittäessä ratkaisua kongruensseihin

$$\begin{aligned} x &\equiv 1 \mod 2, \\ x &\equiv 2 \mod 3 \text{ ja} \\ x &\equiv 3 \mod 5. \end{aligned}$$

Nyt

$$m = 2 * 3 * 5 = 30.$$

Merkitään, että $n_1 = 15$, $n_2 = 10$ ja $n_3 = 6$. Eukleideen algoritmin avulla saadaan, että

$$\begin{aligned} 1 * 15 - 7 * 2 &= 1, \\ 1 * 10 - 3 * 3 &= 1 \text{ ja} \\ 1 * 6 - 1 * 5 &= 1. \end{aligned}$$

Tällöin yksi kongruenssien yhteisistä ratkaisuista on

$$\begin{aligned} x_0 &\equiv 1 * 1 * 15 + 2 * 1 * 10 + 3 * 1 * 6 \\ &\equiv 53 \\ &\equiv 23 \mod 30. \end{aligned}$$

5.2 Pieni-askel suuri-askel

Esitetään ensimmäinen raakaa voimaa ”parempi” menetelmä diskreetin logaritmin ongelman ratkaisuun. Pieni-askel suuri-askel -menetelmää voidaan soveltaa esimerkiksi yhdessä Pohlig-Hellman reduktion kanssa.

Vrt. [3, s. 215]. Olkoon $G = \langle P \rangle$ syklinen ryhmä siten, että $ord(P) = n$. Oletetaan, että $kP = Q$, jollain $k \in \mathbb{N}$.

Asetetaan $m = \lceil \sqrt{n} \rceil$. Tällöin $k = qm + r$, jollain $0 \leq r < m$. Nyt oletuksen $kP = Q$ nojalla

$$kP = (qm + r)P = Q.$$

Siis

$$qmP + rP = Q,$$

mistä saadaan vähentämällä rP molemmilta puolilta, että

$$qmP = q(mP) = Q - rP.$$

Etsitään nyt diskreetin logaritmin ongelman ratkaisevat arvot q ja r. Lasketaan aluksi joukko

$$B = \{ \, (Q - rP, r) \mid 0 \leq r < m \, \}.$$

Jos $(0, r) \in B$, niin $Q - rP = 0$, joten $rP = Q$. Siis r on ratkaisu diskreetin logaritmin ongelmaan.

Muuten asetetaan, että $\delta = mP$ ja lasketaan arvoja $q\delta = q(mP)$, missä $q \in \mathbb{Z}_+$, kunnes löydetään törmäys $(q\delta, r) \in B$, jollain r siten, että $0 \leq r < m$. Tällöin

$$Q - rP = q\delta = q(mP).$$

Siis

$$Q = (qm + r)P,$$

jolloin $qm + r$ on ratkaisu diskreetin logaritmin ongelmaan $kP = Q$.

Yllä oleva ratkaisumenetelmä toimii, sillä esitys $k = qm + r$ on yksikäsitteinen ja se käy läpi kaikki mahdolliset arvot q ja r.

Esimerkki 5.2. Oletetaan tunnetuksi, että $\mathbb{Z}_{43}^* = \langle\overline{5}\rangle$. Ratkaistaan diskreetin logaritmin ongelma $\overline{5}^k = \overline{22}$ käyttäen pieni-askel iso-askel -menetelmää.

Nyt 43 on alkuluku, joten $ord(\overline{5}) = 42$. Asetetaan, että

$$m = \lceil\sqrt{42}\rceil = 7.$$

Lasketaan nyt $\overline{22} * \overline{5}^{-r}$ arvoilla $0 \leq r < 7$. Saadaan parit $(\overline{22}, 0)$, $(\overline{13}, 1)$, $(\overline{37}, 2)$, $(\overline{16}, 3)$, $(\overline{29}, 4)$, $(\overline{23}, 5)$ ja $(\overline{39}, 6)$. Pari $(0, r)$ ei kuulu tähän joukkoon, joten asetetaan, että

$$\delta = \overline{5}^7 = \overline{37}.$$

Nyt

$$\delta^1 = \overline{37}^1 = \overline{37},$$

joten löydetään törmäys.

Saadaan, että

$$\overline{22} * \overline{5}^{-2} = \overline{37} = \overline{5}^7,$$

mistä saadaan, että

$$\overline{5}^9 = \overline{22}.$$

Siis diskreetin logaritmin ongelman ratkaisu on $k = 9$.

Algebraa

Lause 5.4. *Olkoon G ryhmä ja $P \in G$ siten, että $ord(P) = n$. Olkoon $e \in \mathbb{Z}$. Tällöin $eP = 0$, jos ja vain jos n jakaa luvun e.*

Todistus. Vrt. [3, s. 41]. Jos n jakaa luvun e, niin pätee, että $e = kn$, jollain $k \in \mathbb{Z}$. Tällöin

$$eP = (kn)P = k(nP) = k * 0 = 0.$$

Toisaalta, jos $eP = 0$ ja $e = qn + r$, missä $0 \leq r < n$, niin

$$rP = (e - qn)P = eP - q(nP) = 0.$$

Nyt, koska $r < n$ ja $n = ord(P)$, niin $r = 0$. Siis $e = qn$, joten n jakaa luvun e. □

Lause 5.5. *Olkoon G ryhmä ja $P \in G$ siten, että $ord(P) = n$. Olkoot $l, k \in \mathbb{Z}$. Tällöin $lP = kP$, jos ja vain jos $l \equiv k \mod n$.*

Todistus. Vrt. [3, s. 41]. Olkoon $e = l - k$. Sovelletaan lausetta 5.4. Jos $lP = kP$, niin $eP = 0$. Lauseen 5.4 nojalla n jakaa luvun e. Siis $l \equiv k \mod n$. Jos

$$l \equiv k \mod n,$$

niin n jakaa luvun e. Lauseen 5.4 nojalla $eP = 0$. Siis $lP = kP$. □

5.3 Pohlig-Hellman reduktio

Vrt. [3, s. 222]. Olkoon $G = \langle P \rangle$ syklinen ryhmä. Oletetaan, että $ord(P) = n$ ja, että $kP = Q$, missä $k \in \mathbb{Z}$. Oletetaan lisäksi, että tunnetaan luvun n jako alkulukutekijöihin. Siis

$$n = \prod_{p|n} p^{e(p)}.$$

Redusoidaan diskreetin logaritmin laskeminen aliryhmiin joiden kertaluku on alkuluku potenssiin jotain. Merkitään kaikilla alkuluvuilla $p \mid n$, että

$$n_p = \frac{n}{p^{e(p)}}, P_p = n_p P \text{ ja } Q_p = n_p Q.$$

Tällöin $ord(P_p) = p^{e(p)}$ kaikilla alkuluvuilla $p \mid n$ ja $k_p P_p = Q_p$, joillain $k_p \in \mathbb{Z}$.

Lause 5.6. *Edellisiä merkintöjä käyttäen. Olkoon k_p alkion Q_p diskreetti logaritmi kannan P_p suhteen kaikilla alkuluvuilla p, joille pätee, että $p \mid n$. Olkoon lisäksi $k \in \{ 0, 1, \ldots, n-1 \}$ ratkaisu kongruensseihin*

$$k \equiv k_p \mod p^{e(p)}.$$

Tällöin k on ratkaisu diskreetin logaritmin ongelmaan $kP = Q$.

Todistus. Vrt. [3, s. 222]. Nyt

$$n_p(Q - kP) = n_p Q - n_p(kP) = Q_p - n_P Q = Q_p - Q_p = 0,$$

kaikilla alkuluvuilla p siten, että $p \mid n$. Tällöin lauseen 5.4 nojalla

$$ord(Q - kP) \mid n_p.$$

Merkitään, että $n = p_1^{e(p)} p_2^{e(p_2)} \cdots p_l^{e(p_l)}$. Tällöin selvästi $syt(n_{p_1}, \ldots, n_{p_l}) = 1$. Siis $Ord(Q - kP) = 1$, joten $kP = Q$ ja k on ratkaisu diskreetin logaritmin ongelmaan. □

Huomautus. Siis edellä mainittu diskreetin logaritmin ongelma voidaan ratkaista etsimällä ratkaisut diskreetin logaritmin ongelmiin $k_p P_p = Q_p$ ja soveltamalla ratkaisuihin kiinalaista jäännöslausetta. Tässä

$$ord(P_p) = ord(\frac{n}{p^e} P) = p^e,$$

sillä $ord(p) = n$.

Esimerkki 5.3. Oletetaan tunnetuksi, että $\mathbb{Z}_{151}^* = \langle \overline{7} \rangle$. Ratkaistaan diskreetin logaritmin ongelma $\overline{7}^k = \overline{40}$ käyttämällä Pohlig-Hellman reduktiota.

Nyt $ord(\overline{7}) = 150 = 2 * 3 * 5^2$, joten ongelma jakautuu kolmen diskreetin logaritmin ongelman ratkaisuun.

Merkitään, että $n_2 = \frac{150}{2} = 75$, $P_2 = \overline{7}^{75} = \overline{150}$ ja $Q_2 = \overline{40}^{75} = 1$. Tällöin $P_2^k = Q_2$, missä $k \mod 2$. Siis $k \equiv 0 \mod 2$.

Merkitään, että $n_3 = \frac{150}{3} = 50$, $P_3 = \overline{7}^{50} = \overline{32}$ ja $Q_3 = \overline{40}^5 0 = \overline{32}$. Tällöin $P_3^k = Q_3$, missä $k \mod 3$. Siis $k \equiv 1 \mod 3$.

Merkitään, että $n_{5^2} = \frac{150}{5^2} = 6$, $P_{5^2} = \overline{7}^6 = \overline{20}$ ja $Q_{5^2} = \overline{40}^6 = \overline{123}$. Tällöin $P_{5^2}^k = Q_{5^2}$, missä $k \mod 5^2$. Siis $k \equiv 16 \mod 5^2$.

Saadaan siis kongruenssit $k \equiv 0 \mod 2$, $k \equiv 1 \mod 3$ ja $k \equiv 16 \mod 5^2$. Vaihtoehtoisesti voidaan suoraan nähdä ratkaisu tai soveltaa kiinalaista jäännöslausetta ja saadaan, että $k \equiv 16 \mod 150$. Siis diskreetin logaritmin ongelmaan $\overline{7}^k = \overline{40}$ ratkaisu on $k = 16$.

Redusointi alkuluku kertaluvullisiin aliryhmiin

Vrt. [3, s. 223-224]. Olkoon $G = \langle P \rangle$ syklinen ryhmä. Oletetaan, että $ord(P) = p^e$, missä p on alkuluku ja $e \in \mathbb{Z}_+$. Näin voidaan olettaa edellisen reduktion perusteella. Halutaan ratkaista diskreetin logaritmin ongelma $kP = Q$. Kirjoitetaan luku k p-kantaisena lukuna

$$k = k_0 + k_1 p + \cdots + k_{e-1} p^{e-1},$$

missä $k_i \in \{ 0, 1, \ldots, p-1 \}$ kaikilla $i \in \{ 0, 1, \ldots, e-1 \}$. Kerrotaan yhtälö $kP = Q$ luvulla p^{e-1} ja saadaan, että

$$p^{e-1} kP = p^{e-1} Q.$$

Nyt luvun k p-kantaisen esityksen avulla saadaan, että

$$\begin{aligned} p^{e-1} kP &= p^{e-1}(k_0 + k_1 p + \cdots + k_{e-1} p^{e-1}) P \\ &= p^{e-1} k_0 P + (k_2 + k_3 p + \cdots + k_{e-1} p^{e-1})(p^e P). \end{aligned}$$

Tällöin $p^e P = 0$, sillä $ord(P) = p^e$. Saadaan, että

$$k_0(p^{e-1} P) = p^{e-1} Q. \tag{5.1}$$

Nyt ratkaisemalla tämä diskreetin logaritmin ongelma löydetään k_0. Loput luvut k_i etsitään rekursiivisesti. Oletetaan, että tunnetaan luvut $k_0, k_1, \ldots, k_{i-1}$. Etsitään nyt luku k_i kertomalla $kP = Q$ luvulla p^{e-i-1}. Saadaan vastaavasti kuin edellä, että

$$\begin{aligned} p^{e-i-1} Q &= p^{e-i-1}(kP) \\ &= p^{e-i-1}(k_0 + k_1 p + \cdots + k_{e-1} p^{e-1}) P \\ &= (p^{e-i-1} k_0 + p^{e-i} k_1 + \cdots + p^{e-1} k_i) P + (k_i + k_{i+1} p + \cdots + k_{e-1} p^{e-i-2})(p^e P) \\ &= (p^{e-i-1} k_0 + p^{e-i} k_1 + \cdots + p^{e-1} k_i) P, \end{aligned}$$

mistä saadaan siirtämällä kertoimen k_i sisältämä termi omalle puolelleen, että

$$k_i(p^{e-1} P) = p^{e-i-1}(Q - (k_0 + k_1 p + \cdots + k_{i-1} p^{i-1}) P). \tag{5.2}$$

Kyseessä diskreetin logaritmin ongelma, josta voidaan ratkaista k_i.

Huomautus. Edellisessä

$$ord(p^{e-1}P) = p,$$

sillä $ord(P) = p^e$.

Huomautus. Seuraus Pohlig-Hellman reduktiosta on, että jos halutaan tehdä diskreetin logaritmin ongelmasta hankalampi, on syytä tarkistaa ettei $ord(P)$ jakaudu pienten alkulukujen tekijöiksi.

Huomautus. Pohlig-Hellman reduktio ei itsessään ole ratkaisumenetelmä diskreetin logaritmin ongelmaan, vaan se vain redusoi ratkaisun etsimisen pienempiin ongelmiin. Näiden "helpompien" diskreetin logaritmin ongelmien ratkaisemiseen voidaan käyttää raa'an voiman menetelmää tai pieni-askel suuri-askel tapaa. Seuraavassa luvussa esitetään vielä yksi mahdollinen ratkaisumenetelmä: Pollardin ρ-menetelmä.

Esimerkki 5.4. Esitetään esimerkki diskreetin logaritmin ongelman ratkaisusta käyttäen Pohlig-Hellman reduktiota.

Oletetaan tunnetuksi, että $\mathbb{Z}_{4159}^* = \langle\overline{3}\rangle$. Ratkaistaan ongelma $\overline{3}^k = \overline{764}$. Nyt 4159 on alkuluku, joten

$$ord(\overline{3}) = 4158 = 2 * 3^3 * 7 * 11.$$

Lauseen 5.6 nojalla voidaan ensiksi ratkaista neljä diskreetin logaritmin ongelmaa aliryhmissä, joiden kertaluvut ovat $2, 3^3, 7$ ja 11. Tämän jälkeen ratkaisu saadaan näiden ratkaisujen avulla soveltamalla kiinalaista jäännöslausetta.

Merkitään, että

$$\begin{aligned} n_0 &= \frac{4158}{2} = 2079, \\ P_0 &= \overline{3}^{2079} = \overline{4158} \text{ ja} \\ Q_0 &= \overline{764}^{2079} = \overline{1}. \end{aligned}$$

Tällöin $P_0^{k_0} = Q_0$, jollain $k_0 \in \mathbb{Z}$. Selvästi $k_0 = 0$.

Merkitään, että

$$\begin{aligned} n_1 &= \frac{4158}{3^3} = 154 \\ P_1 &= \overline{3}^{154} = \overline{3838} \text{ ja} \\ Q_1 &= \overline{764}^{154} = \overline{3166}. \end{aligned}$$

Nyt $ord(\overline{3}) = 4158$, joten $ord(P_1) = ord(\overline{3}^{154}) = 3^3$. Merkitään vielä, että

$$k_1 = k_0' + k_1' * 3 + k_2' 3^2.$$

Sovelletaan aikaisemmin esitettyä reduktio tulosta, jonka mukaan lukujen $k_0^{'}, k_1^{'}$ ja $k_2^{'}$ löytäminen voidaan tehdä rekursiivisesti ratkaisemalla kolme diskreetin logaritmin ongelmaa. Sovelletaan tässä siis kaavoja 5.1 ja 5.2. Kaavan 5.1 avulla saadaan johdettua diskreetin logaritmin ongelma, josta voidaan ratkaista $k_0^{'}$. Saadaan siis yhtälö

$$(\overline{3838}^{3^2})^{k_0^{'}} = \overline{3166}^{3^2}.$$

Sievennetään tätä ja saadaan, että

$$\overline{1604}^{k_0^{'}} = \overline{1}.$$

Siis $k_0^{'} = 0$. Ratkaistaan seuraavaksi $k_1^{'}$ ja $k_2^{'}$ käyttäen rekursiokaavaa 5.2. Luvulle $k_1^{'}$ saadaan yhtälöksi

$$\overline{1604}^{k_1^{'}} = \overline{2554}.$$

Ratkaistaan tämä raa'alla voimalla ja saadaan, että $k_1^{'} = 2$. Jälleen rekursiokaavalla 5.2 saadaan yhtälö

$$\overline{1604}^{k_2^{'}} = \overline{1604}.$$

Siis $k_2^{'} = 1$. Lopuksi saadaan, että

$$k_1 = k_0^{'} + k_1^{'} * 3 + k_2^{'} * 3^2 = 0 + 2 * 3 + 1 * 3^2 = 15.$$

Merkitään, että

$$\begin{aligned} n_2 &= \frac{4158}{7} = 594, \\ P_2 &= \overline{3}^{594} = \overline{970} \text{ ja} \\ Q_2 &= \overline{764}^{594} = \overline{1}. \end{aligned}$$

Saadaan yhtälö $P_2^{k_2} = Q_2$, jollain $k_2 \in \mathbb{Z}$. Selvästi $k_2 = 0$.

Merkitään, että

$$\begin{aligned} n_3 &= \frac{4158}{11} = 378, \\ P_3 &= \overline{3}^{378} = \overline{2045} \text{ ja} \\ Q_3 &= \overline{764}^{378} = \overline{2874}. \end{aligned}$$

Saadaan yhtälö $P_3^{k_3} = Q_3$, jollain $k_3 \in \mathbb{Z}$. Ratkaistaan k_3 raa'alla voimalla ja saadaan, että $k_3 = 9$.

Meillä on nyt yhtälöt

$$\begin{aligned} k &\equiv k_0 \equiv 0 \mod 2, \\ k &\equiv k_1 \equiv 15 \mod 3^2, \\ k &\equiv k_2 \equiv 0 \mod 7 \text{ ja} \\ k &\equiv k_3 \equiv 9 \mod 11. \end{aligned}$$

Soveltamalla näihin kiinalaista jäännöslausetta saadaan, että

$$k \equiv 42 \mod 4158.$$

Siis diskreetin logaritmin ongelman $\overline{3}^k = \overline{764}$ ratkaisu on $k = 42$.

6 Pollardin ρ-menetelmä

Pollardin ρ-menetelmä on ratkaisumenetelmä diskreetin logaritmin ongelmaan ryhmässä G. Erityisesti se soveltuu kyseisen ongelman ratkaisuun elliptisillä käyrillä $E_{(a,b)}(\mathbb{Z}_p)$, missä p on alkuluku.

6.1 Pollardin ρ-menetelmä

Esitellään Pollardin ρ-menetelmä. Vrt. [3, s. 217-218]. Olkoon $G = \langle P \rangle$ syklinen ryhmä. Voidaan olettaa, että $ord(P) = q$, missä q on alkuluku. Näin voidaan olettaa, sillä Pohlig-Hellman reduktiolla diskreetin logaritmin ongelma voidaan redusoida alkuluku kertaluvullisiin ongelmiin. Halutaan ratkaista diskreetin logaritmin ongelma

$$kP = Q, \text{ missä } Q \in G.$$

Jaetaan joukko G kolmeen erilliseen joukkoon G_1, G_2 ja G_3. Siis

$$G = G_1 \cup G_2 \cup G_3.$$

Määritellään nyt kuvaus $f : G \to G$ seuraavasti:

$$f(W) = \begin{cases} P + W, \text{ kun } R \in G_1 \\ 2W, \text{ kun } R \in G_2 \\ Q + W, \text{ kun } R \in G_3. \end{cases}$$

Valitaan nyt satunnainen luku $a_0 \in \{ 1, \ldots, q \}$. Lasketaan tämän jälkeen arvo $W_0 = a_0 P$. Määritellään nyt jono $(W_i)_{i \in \mathbb{N}}$ rekursiivisesti,

$$W_{i+1} = f(R_i).$$

Nyt jonon jäsenet ovat muotoa $W_i = a_i P + b_i Q$, missä $i \in \mathbb{N}$. Tällöin jonoille $(a_i)_{i \in \mathbb{N}}$ ja $(b_i)_{i \in \mathbb{N}}$ saadaan seuraavat esitykset. Jos a_0 on kuten aikasemmin ja $b_0 = 0$, niin

$$a_{i+1} = \begin{cases} a_i + 1 \mod q, \text{ kun } R_i \in G_1 \\ 2a_i \mod q, \text{ kun } R_i \in G_2 \\ a_i \mod q, \text{ kun } R_i \in G_3 \end{cases}$$

ja

$$b_{i+1} = \begin{cases} b_i \mod q, \text{ kun } R_i \in G_1 \\ 2b_i \mod q, \text{ kun } R_i \in G_2 \\ b_i + 1 \mod q, \text{ kun } R_i \in G_3. \end{cases}$$

Nyt G on äärellinen ryhmä, joten jonossa $(W_i)_{i\in\mathbb{N}}$ toistuu alkioita. Siis saadaan, että

$$a_tP + b_tQ = a_{t+l}P + b_{t+l}Q,$$

joillain $t, l \in \mathbb{N} \setminus \{ 0 \}$, jolloin

$$(a_t - a_{t+l})P = (b_{t+l} - b_t)Q.$$

Tällöin lauseen 5.5 nojalla diskreetille logaritmille k pätee, että

$$(a_t - a_{t+l}) \equiv k(b_{t+l} - b_t) \mod q.$$

Nyt q on alkuluku, joten on olemassa käänteisalkio $(b_{t+l} - b_t)^{-1}$. Nyt

$$k \equiv (a_t - a_{t+l})(b_{t+l} - b_t)^{-1} \mod q.$$

Edellinen esitys ei ole vielä täydellinen törmäyksen $W_t = W_{t+l}$ löytämisen kannalta, sillä se vaatii tallettamaan alkioita mahdollisesti valtavia määriä muistiin.

Huomautus. Nimensä Pollardin ρ-menetelmä saa jonon $(W_i)_{i\in\mathbb{N}}$ graafista, joka muistuttaa ρ kirjainta.

6.2 Floydin syklinlöytö algoritmi

Aikaisemmin todettiin, että jos S äärellinen joukko, niin kuvauksen $f : S \to S$ avulla määritelty jono $(x_i)_{i\in\mathbb{N}}$, missä $x_{i+1} = f(x_i)$, päätyy sykliin. Esitetään algoritmi syklin löytämiseksi.

Määritelmä 6.1. Vrt. [1, s. 52]. Olkoon S äärellinen joukko, $x_0 \in S$ ja $f : S \to S$ kuvaus. Määritellään jono $(x_i)_{i\in\mathbb{N}}$ siten, että $x_{i+1} = f(x_i)$. Jos $x_0, x_1, \ldots x_{k-1}$ ovat jonon $(x_i)_{i\in\mathbb{N}}$ jäseniä siten, että $x_l \neq x_j$ kaikilla $l \neq j$ ja $l, j \in \{ 0, 1, \ldots, k-1 \}$, niin kutsutaan tätä jonon alkuosaa *jonon hännäksi*. Jos $x_k = x_{k+h}$ ja $x_l \neq x_j$ kaikilla $l \neq j$ ja $l, j \in \{ k, k+1, \ldots, k+h-1 \}$, niin kutsutaan alkioita $x_k, x_{k+1}, \ldots, x_{k+h-1}$ *sykliksi*.

Lause 6.1. *Olkoon S äärellinen joukko, $x_0 \in S$ ja $f : S \to S$ kuvaus. Oletetaan, että jonon $(x_i)_{i\in\mathbb{N}}$, missä $x_{i+1} = f(x_i)$ hännän pituus on t ja syklin pituus c. Tällöin on olemassa $i \in \mathbb{Z}_+$ siten, että $x_i = x_{2i}$ ja $t \leq i \leq t + c$.*

Todistus. Vrt. [1, s. 53 lause 2.10.a]. Nyt hännän pituus on t ja syklin pituus c, joten $x_t = x_{t+c}$. Tällöin myös $x_t = x_{t+kc}$ kaikilla $k \in \mathbb{N}$.

Huomataan, että jos $t \leq c$, niin $x_c = x_{c+kc}$. Nyt jos $k = 1$, niin $x_c = x_{2c}$. Jos $c < t$, niin valitaan sellainen $n \in \mathbb{N}$, että $t \leq nc$. Nyt $x_{nc} = x_{nc+knc}$, ja jos $k = 1$, niin $x_{nc} = x_{2nc}$.

Nyt jos $t \geq 1$, niin sopiva luku i löytyy väliltä $t \leq i \leq t+c-1$. Jos $t = 0$, niin voisi olla, että $i = 0$. Voidaan kuitenkin valita $i = c$, jolloin $0 < i \leq t + c$. □

Olkoon S äärellinen joukko, $x_0 \in S$ ja $f : S \to S$ kuvaus. Olkoon lisäksi $(x_i)_{i\in\mathbb{N}}$ jono siten, että $x_{i+1} = f(x_i)$. Edellisen lauseen nojalla on olemassa indeksi $j \in \mathbb{N}$ siten, että $x_j = x_{2j}$. Määritellään nyt toinen jono $(y_i)_{i\in\mathbb{N}}$ siten, että $y_0 = x_0$ ja $y_i = f(f(y_{i-1}))$. Siis $y_i = x_{2i}$. Etsitään nyt sellainen $i \in \mathbb{N}$, että $y_i = x_i$. Tällöin $x_i = y_i = x_{2i}$.

Esimerkki 6.1. Olkoon $f : \mathbb{Z}_{73} \to \mathbb{Z}_{73}$, $x \mapsto x^2$ kuvaus. Jos $x_0 = 3$ ja $y_0 = 3$, niin

$$\begin{aligned} &i = 0 : x_0 = 3, y_0 = 3 \\ &i = 1 : f(x_0) = 9 = x_1, f(f(y_0)) = 8 = y_1 \\ &i = 2 : f(x_1) = 8 = x_2, f(f(y_1)) = 8 = y_2. \end{aligned}$$

Siis $x_2 = x_4$.

Nyt voimme soveltaa Pollardin ρ-menetelmässä Floydin syklinlöytö algoritmia törmäyksen löytämiseksi.

6.3 Additiivinen kulku

Vrt. [2, Additive walks]. Olkoon G syklinen ryhmä siten, että $G = \langle P \rangle$ ja $ord(P) = q$, missä q on alkuluku. Oletetaan, että $kP = Q$, jollain $k \in \mathbb{Z}$. Seuraava oleellinen parannus Pollardin ρ-menetelmään on määritellä kuvaus $f : G \to G$ ja *additiivinen kulku seuraavasti*:

$$f(W) = W + R_{h(W)},$$

missä $h : G \to \{\, 0, 1, \ldots, r-1 \,\}$ kuvaus ja $R_0, R_1, \ldots, R_{r-1}$ ovat muotoa

$$R_i = a_i P + b_i Q,$$

missä $a_i, b_i \in \mathbb{Z}$ satunnaisesti valittuja. Jono $(W_i)_{i\in\mathbb{N}}$ määritellään siten, että $W_0 = b_0 P$, missä $b_0 \in \mathbb{Z}$ satunnainen kokonaisluku ja $W_{i+1} = f(W_i)$.

Esimerkki 6.2.

$$\begin{aligned} S_1 &= \{\, 0, 1, \ldots, 24 \,\}, \\ S_2 &= \{\, 25, 26, \ldots, 49 \,\} \text{ ja} \\ S_3 &= \{\, 50, 51, \ldots, 72 \,\}. \end{aligned}$$

Olkoon

$$\begin{aligned} R_1 &= 5^{38} * 70^{58} = 54, \\ R_2 &= 5^2 * 70^{12} = 25 \text{ ja} \\ R_3 &= 5^{59} * 70^{31} = 39. \end{aligned}$$

Määritellään nyt $f : \mathbb{Z}_{73}^* \to \mathbb{Z}_{73}^*$ seuraavasti:

$$f(W) = W * R_i,$$

missä $W \in S_i$ jollain $i = 1, 2, 3$. Olkoon $x_0 = 5^{34} * 70^5 = 36$. Käytetään nyt Floydin syklinlöytö algoritmia törmäyksen löytämiseen. Siis etsitään $x_i = x_{2i}$. Asetetaan $i = 0$, $x_0 = 36$ ja $y_0 = 36$. Lasketaan pareja $(f(x_i), f(f(y_i))$, kunnes löydetään törmäys. Saadaan seuraava jono pareja: $(36, 36)$, $(24, 55)$, $(55, 43)$, $(28, 23)$, $(43, 54)$, $(53, 9)$, $(23, 32)$, $(1, 29)$, $(54, 24)$, $(62, 28)$, $(9, 53)$, $(48, 1)$, $(32, 62)$, $(70, 48)$, $(29, 70)$ ja $(68, 68)$. Siis $x_{15} = x_{30}$.

Käydään jonoa uudelleen läpi ensimmäisestä alkiosta x_0 alkaen aina alkioon x_{30} asti, samalla pitäen muistissa eksponentit. Sovelletaan tässä Fermat'n pientä lausetta

$$a^{p-1} \equiv 1 \mod p \text{ kaikilla } a \in \mathbb{Z}_p^*,$$

jotta saadaan eksponentit pysymään pienenä. Saadaan jono $x_0 = 5^{34} * 70^5, \ldots, x_{15} = 5^{61} * 70^{32}, \ldots, x_{30} = 5^1 * 70^6$. Tällöin $x_{15} = x_{30}$, joten $5^{61} * 70^{32} \equiv 5^1 * 70^6 \mod 73$. Edelleen voidaan sieventää, että

$$5^{12} \equiv 70^{26} \mod 73.$$

Nyt $26 * k \equiv 12 \mod 72$, mutta $syt(26, 72) = 2$, joten 26 ei ole kääntyvä modulo 72. Jaetaan 2 siis pois ja saadaan, että $13k \equiv 6 \mod 36$, jolloin saadaan, että $k \equiv 6 * 25 \equiv 6 \mod 36$. Nyt etsitty ratkaisu on joko $k \equiv 6 \mod 72$ tai $k \equiv 6 + 36 \equiv 42 \mod 72$. Laskemalla todennetaan, että ratkaisu on

$$k \equiv 42 \mod 72.$$

6.4 Rinnakkainen ρ-menetelmä

Esitetään van Oorschotin ja Wienerin idea[11], kuinka jakaa törmäyksen etsiminen ρ-menetelmässä useammalle koneelle.

Olkoon $G = \langle P \rangle$ syklinen ryhmä ja $ord(P) = q$, missä q on alkuluku. Oletetaan, että $kP = Q$, jollain $k \in \mathbb{Z}$. Olkoon $f : G \to G, W \mapsto W + R_{h(W)}$ kuvaus, missä $h : G \to \{ 0, \ldots, n-1 \}$ kuvaus ja $R_i = a_i P + b_i Q$, $a_i, b_i \in \mathbb{Z}$ kaikilla $i \in \{ 0, \ldots, n-1 \}$. Olkoon lisäksi $D \subseteq G$ joukko helposti määriteltäviä erikoispisteitä.

Oletetaan, että käytössä on N kappaletta laskentayksiköitä. Jokainen laskentayksikkö aloittaa laskemaan jonoa $W_{i+1} = f(W_i)$ satunnaisesta pisteestä $W_0 = a_0 P + b_0 Q$. Laskenta pysähtyy, kun saavutetaan jokin erikoispisteistä $W_j \in D$. Tämän jälkeen laskentaa suorittava kone lähettää saavutettujen pisteiden listaa ylläpitävälle koneelle parin (W_0, W_j). Tämän jälkeen kone arpoo uuden aloituspisteen ja aloittaa laskennan alusta.

Jos saavutettujen pisteiden listalta löydetään pisteparit (W_h, W_t) ja (W_l, W_t) siten, että $W_h \neq W_l$, niin voidaan selvittää W_t muodossa $a_i P + b_i Q$ käymällä jonot uudelleen läpi aloituspisteestä erikoispisteeseen pitäen muistissa kertoimet

[2, Eliminating coefficients]. Oletetaan, että löydetty törmäys

$$a_i P + b_i Q = c_j P + d_j Q.$$

Siirretään termit omille puolilleen ja saadaan, että

$$(a_i - c_j)P = (d_j - b_i)Q.$$

Nyt lauseen 5.5 nojalla

$$(a_i - c_j) \equiv k(d_j - b_i) \mod q.$$

Tässä q alkuluku, joten luvuilla $\mod q$ on käänteisalkiot. Siis

$$k \equiv (a_i - c_j)(d_j - b_i)^{-1} \mod q.$$

Siis diskreetin logaritmin ongelman $kP = Q$ ratkaisu on löydetty.

Huomautus. On mahdollista, että algoritmi ei pysähdy. Nimittäin jos ryhmän kertaluku on valtava verrattuna erikoispisteiden määrään, saattaa käydä niin, että laskettavista jonoista ei löydy yhtään erikoispistettä.

Esimerkki 6.3. Olkoon $f : \mathbb{Z}_{23} \to \mathbb{Z}_{23}$, $x \mapsto x^2$. Valitaan erikoispisteiksi joukko $D = \{ 5, 16, 20 \}$. Suoritetaan laskentaa rinnakkain kolmella koneella ja taulukoidaan tuloksia kunnes löydetään kaksi jonoa, jotka päätyvät samaan erikoispisteeseen.

x_i	Kone 1	x_i	Kone 2	x_i	Kone 3
x_0	3	x_0	4	x_0	21
x_1	9	x_1	16	x_1	4
x_2	12	x_0	7	x_2	16

Löydetty siis parit $(4, 16)$ ja $(21, 16)$.

6.5 Montgomeryn temppu

Olkoon $p \in \mathbb{N}$ alkuluku. Esitetään algoritmi alkioiden $a_1, \ldots, a_n \in \mathbb{Z}_p^*$ käänteisalkioiden $b_1, \ldots, b_n \in \mathbb{Z}_p^*$ löytämiseksi käyttäen vain kerran laajennettua Eukleideen algoritmia.

Algoritmi 2 Montgomeryn temppu

Input: $a_1, \ldots, a_n \in \mathbb{Z}_p^*$

Output: $b_1, \ldots, b_n \in \mathbb{Z}_p^*$ siten, että $a_i b_i = 1$ kaikilla $i \in \{ 1, \ldots, n \}$.

1: Asetetaan aluksi:
2: $c_1 \leftarrow a_1$
3: $c_2 \leftarrow c_0 a_2 \mod p$.
4: $\vdots$
5: $c_n \leftarrow c_{n-1} a_n \mod p$
6: Sovelletaan käänteistä Eukleideen algoritmia luvun c_n käänteisalkion löytämiseksi. Oletetaan, että kyseinen käänteisalkio on $u \in \mathbb{Z}_p^*$.
7: Lasketaan lopuksi käänteisalkiot:
8: $i \leftarrow n$
9: **while** $i > 1$ **do**
10: $\quad b_i \leftarrow u c_{i-1} \mod p$
11: $\quad u \leftarrow u a_i \mod p$
12: $\quad i \leftarrow i - 1$
13: **end while**
14: $b_1 \leftarrow u$
15: **return** $b_1, \ldots, b_n$

Todistus. Vrt. [4, s. 481]. Nyt $c_n = a_1 \cdots a_n$. Tällöin $syt(c_n, p) = 1$, koska p alkuluku. Tällöin laajennettu Eukleideen algoritmi löytää luvut $u, m \in \mathbb{Z}$ siten, että

$$uc_n + mp = 1.$$

Nyt tietenkin

$$uc_n \equiv 1 \mod p,$$

joten u on alkion c_n käänteisalkio ryhmässä $\mathbb{Z}_p^*$. Nyt alkiosta u voidaan poimia yksitellen käänteisalkiot pois. Esimerkiksi, jos $i = n$, niin

$$b_n = uc_{n-1} = (a_1 \cdots a_n)^{-1} a_1 \ldots a_{n-1} = a_n^{-1}.$$

Asetetaan tämän jälkeen $u \leftarrow u a_n$. Siis $u = (a_1 \cdots a_{n-1})^{-1}$. Tätä toistamalla saadaan käänteisalkiot $b_n, \ldots, b_2$. Asetetaan lopuksi $b_1 = u$. □

Esimerkki 6.4. Etsitään alkioiden $2, 3, 5 \in \mathbb{Z}_{23}$ käänteisalkiot.

Nyt $c_1 = 2$, $c_2 = 6$ ja $c_3 = 7$. Tällöin

$$syt(7, 23) = 1 = 10 * 7 + (-3) * 23,$$

joten $m = 10$. Saadaan, että

$$b_3 = m * c_2 = 10 * 6 = 14$$

ja uusi

$$m = m * a_3 = 10 * 5 = 4.$$

Alkioksi

$$b_2 = m * c_1 = 4 * 2 = 8$$

ja

$$m = m * a_2 = 4 * 3 = 12.$$

Nyt $b_1 = 12$.

Siis

$$a_1 * b_1 = 2 * 12 = 1$$
$$a_2 * b_2 = 3 * 8 = 1$$
$$a_3 * b_3 = 5 * 14 = 1.$$

6.6 Pollardin ρ-menetelmä elliptisille käyrille

Tässä aliluvussa valitaan kunnaksi $K = \mathbb{Z}_p$, missä p on alkuluku. Tarkastellaan elliptistä käyrää $E(\mathbb{Z}_p)$. Oletetaan $P, Q \in E(K)$ siten, että $kP = Q$, jollain $k \in \mathbb{Z}$. Esitetään kuinka Pollardin ρ-menetelmää sovelletaan negaation kanssa. Oletetaan, että $ord(P) = q$, missä q on alkuluku.

Negaatio

Esimerkki 6.5. Olkoon G Abelin ryhmä. Tutkitaan kuvausta $f : G \to G$, $x \mapsto -x$. Tämä on selvästi bijektio. Oletetaan, että $a, b \in G$. Nyt

$$f(a + b) = -(a + b).$$

Ryhmille pätee tunnetusti, että $-(a + b) = -b - a$. Tällöin

$$f(a + b) = -b - a = -a - b = f(a) + f(b),$$

sillä G on Abelin ryhmä. Siis f on automorfismi.

Vrt. [5, osio 3]. Hyödynnetään sitä havaintoa, että jos $P = (x, y) \in E(K) \setminus \{ \infty \}$, niin $-P = (x, -y)$. Määritellään nyt relaatio $\sim$ elliptiselle käyrälle $E(K)$ siten, että $T \sim S$, jos ja vain jos $T = \pm S$ kaikilla $S, T \in E(K)$. Relaatio $\sim$ selvästi ekvivalenssirelaatio.

Nyt voidaan määritellä kuvaus $f : E(K)/\sim \to E(K)/\sim$ samalla tavalla, kuin Bernstein, Lange ja Schwabe [2, osio 3]. Siis f kuvaus siten, että

$$W \mapsto \left| W + R_{h(W)} \right|,$$

missä h kuvaus siten, että $W \mapsto \{ 0, 1, \ldots, r - 1 \}$, missä pisteet $R_i \in \langle P \rangle$. Sovitaan, että $|(x, y)| = (x, y)$ jos y on parillinen ja jos y on pariton, niin $|(x, y)| = (x, -y)$.

Määritellään nyt jono $(W_i)_{i \in \mathbb{N}}$ siten, että $W_0 = |b_0 Q|$, missä b_0 on satunnainen kokonaisluku ja $W_{i+1} = f(W_i)$. Olkoon $D \subseteq E(K)/\sim$ joukko erikoispisteitä. Nyt ratkaisu voidaan etsiä rinnakkaisella ρ-menetelmällä.

Turhat syklit

Vrt. [5]. Edellisen kaltainen siirtyminen laskemaan alkioita ekvivalenssiluokkien edustajien kautta ei ole ongelmaton, vaan aiheuttaa niin sanottuja *turhia syklejä*. Olkoon $W_l, W_{l+1}, \ldots, W_{l+k}, W_{l+k+1} = W_l$ sykli. Olkoot $\epsilon_l, \epsilon_{l+1}, \ldots, \epsilon_{l+k} \in \{ -1, 1 \}$. Arvot ϵ_i riippuvat siitä, valitaanko operaatiossa $|W|$ piste W vaiko W. Siis merkitään tässä, että $|W_{l+k}| = \epsilon_{l+k} W_{l+k}$. Tällöin, jos $W_{i+1} = |f(W_i)|$ ja f on määritelty kuten aikaisemmin, niin saadaan pisteelle W_{l+k+1} lausekkeeksi seuraava:

$$\begin{aligned} W_{l+k+1} &= \epsilon_{l+k}(W_{l+k} + R_{h(W_{l+k})}) \\ &= \epsilon_{l+k} W_{l+k} + \epsilon_{l+k} R_{h(W_{l+k})} \\ &= \epsilon_{l+k}\epsilon_{l+k-1}(W_{l+k-1} + R_{h(W_{l+k-1})}) + \epsilon_{l+k} R_{h(W_{l+k})} \\ &= \epsilon_{l+k}\epsilon_{l+k-1} W_{l+k-1} + \epsilon_{l+k}\epsilon_{l+k-1} R_{h(W_{l+k-1})} + \epsilon_{l+k} R_{h(W_{l+k})} \\ &\vdots \\ &= \epsilon_{l+k}\epsilon_{l+k-1} \ldots \epsilon_l W_l + \mathcal{T}, \end{aligned}$$

missä

$$\mathcal{T} = \epsilon_{l+k}\epsilon_{l+k-1} \ldots \epsilon_l R_{h(W_l)} + \cdots + \epsilon_{l+k} R_{h(W_{l+k})}.$$

Nyt jos $\mathcal{T} = 0$, niin täytyy olla, että $\epsilon_{l+k}\epsilon_{l+k-1} \ldots \epsilon_l = 1$, sillä $W_{l+k+1} = W_l$. Siis löydetty törmäys ei kerro oleellista informaatiota diskreetin logaritmin ongelman ratkaisusta ja tällaista sykliä sanotaankin *turhaksi sykliksi*.

Turhien syklien välttäminen

Määritelmä 6.2. Vrt. [6, s. 148]. Määritellään *leksikografinen järjestys* karteesiselle tulolle $\mathbb{Z}_p \times \mathbb{Z}_p$, missä p on alkuluku seuraavasti: $(x, y) \leq (x', y')$, jos ja vain jos $x < x'$ tai $x = x'$ ja $y \leq y'$.

Vrt. [2, s. osio 3]. Sovelletaan negaatiota Pollardin ρ-menetelmässä. Tällöin turhien syklien välttämiseksi laskennassa tarkastetaan tietyin väliajoin ollaanko päädytty 2-sykliin. Siis pisteen W_{i-1} laskemisen jälkeen tarkastetaan onko $W_{i-1} = W_{i-3}$. Jos näin on, niin määritellään, että $W_i = |2 \min \{ W_{i-1}, W_{i-2} \}|$, missä min leksikografinen minimi. Suoritetaan vastaavat tarkistukset 4-sykleille, 6-sykleille ja niin edelleen aina pienimpään parilliseen syklin pituuteen joka ylittää arvon $\frac{\log q}{\log r}$, missä r pisteiden R_i lukumäärä ja $q = ord(P)$.

Huomautus. On mahdollista, että tämä tapa ei johda turhan syklin välttämiseen. Nimittäin jos W_i, W_{i+1} on turha sykli tai siis

$$\begin{aligned} W_{i+2} &= \epsilon_2(W_{i+1} + R_{h(W_{i+1})}) \\ &= \epsilon_2(\epsilon_1(W_i + R_{h(W_i)}) + R_{h(W_{i+1})}) \\ &= \epsilon_2\epsilon_1 W_i + \epsilon_2\epsilon_1 R_{W_i} + \epsilon_2 R_{h(W_{i+1})}, \end{aligned}$$

missä

$$\epsilon_2\epsilon_1 R_{W_i} + \epsilon_2 R_{h(W_{i+1})} = 0$$

ja

$$\epsilon_2\epsilon_1 W_i = W_i.$$

Nyt $\epsilon_1 = \epsilon_2 = 1$ tai $\epsilon_2 = \epsilon_1 = -1$. Siis $R_{h(W_i)} = R_{h_{W_{i+1}}}$ tai $R_{h(W_i)} = -R_{h(W_{i+1})}$.

Jos $min\{ W_i, W_{i+1} \} = W_i$ ja $R_{h(W_i)} = W_i$, niin

$$\begin{aligned} |2min\{ W_i, W_{i+1} \}| &= |2W_i| \\ &= |W_i + W_i| \\ &= \left|W_i + R_{h(W_i)}\right| \\ &= \epsilon_1(W_i + R_{h(W_i)}) \\ &= W_{i+1}. \end{aligned}$$

Siis on mahdollista, että esitetty syklin välttämistapa ei aina toimi.

Lähteet

[1] L.M.Batten, *Public Key Cryptography Applications and Attacks*. John Wiley & sons, Inc, 2013.

[2] D.J.Bernstein, T.Lange, P.Schwabe, *On the correct use of the negation map in the Pollard rho method*. Public Key Cryptography - PKC 2011, 128-146.

[3] J.A.Buchmann, *Introduction to Cryptography, second edition*. Springer, 2001.

[4] H.Cohen, *A Course in Computational Algebraic Number Theory*. Springer, 1993.

[5] I.Duursma, P.Gaudry, F.Morain, *Speeding up the discrete log computation on curves with automorphisms*. Asiacrypt 1999, 103-121.

[6] H.-D.Ebbinghaus, J.Flum, W.Thomas, *Mathematical logic, second edition*. Springer, 1984.

[7] J.Hoffstein, J.Pipher, J.H.Silverman, *An Introduction to Mathematical Cryprography*. Springer, 2008.

[8] E.Hyry, luennot kurssilta *Kryptografian algebralliset menetelmät*, 2008.

[9] K.Ireland, M.Rosen, *A Classical Introduction to Modern Number Theory, second edition*. Springer, 1990.

[10] S.Lang, *Undergraduate algebra, third edition*. Springer, 2005.

[11] P.C.van Oorschot, M.J.Wiener, *Parallel Collision Search with Cryptanalytic Applications*. Journal of Cryptology 12 (1999), 1-28.

[12] L.C.Washington *Elliptic Curves, Number Theory and Cryptography, second edition*. Taylor and Francis Group, LLC, 2008.