Selkäreppusalauksista p-adisissa approksimaatiohiloissa

Pro Gradu
Lotta Makkonen
Y52840520
Matemaattisten tieteiden laitos
Oulun yliopisto
Kevät 2023

Sisällys

Johdanto **2**

1 p-adiset luvut **4**
1.1 p-adinen itseisarvo 4
1.2 p-adinen valuaatio 7
1.3 Rationaaliluvun p-adinen esitys 9

2 Hilat **15**
2.1 p-adiset approksimaatiohilat 19
2.2 LLL-algoritmi 23

3 Selkäreppusalaukset **33**
3.1 Ensimmäinen p-adinen selkäreppusalaus 35
3.1.1 Esimerkki 40
3.1.2 Salauksen turvallisuus 43
3.2 Toinen p-adinen selkäreppusalaus 46
3.2.1 Esimerkki 52
3.2.2 Salauksen turvallisuus 57

Lähdeluettelo **61**

Johdanto

Tässä tutkielmassa tarkastellaan p-adisten lukujen käyttöä hilapohjaisissa salausmenetelmissä. Perinteiset käytössä olevat salausmenetelmät pohjautuvat vaikeisiin matemaattisiin ongelmiin, kuten kokonaisluvun tekijöihinjakoon ja diskreetin logaritmin ongelmaan. Kvanttitietokoneiden kehittyessä nämä ongelmat saadaan kuitenkin ratkaistua, jolloin salausmenetelmät menettävät turvallisuutensa. Tämän vuoksi uudenlaisten kvanttiturvallisten salausalgoritmien kehittäminen on erittäin tärkeää. Erityisesti hiloihin perustuvia salausmenetelmiä pidetään lupaavina kvanttiturvallisuuden kannalta, sillä toistaiseksi tiedossa ei ole kvanttialgoritmeja, jotka murtaisivat hilapohjaiset salaukset tavallisia tietokoneita nopeammin.

Tutkielman ensimmäisessä luvussa määritellään p-adinen itseisarvo ja p-adinen valuaatio, sekä todistetaan niiden tärkeimmät ominaisuudet. Erityisesti p-adisella itseisarvolla toteutuvaa vahvaa kolmioepäyhtälöä hyödynnetään seuraavissa luvuissa. Luvussa 1 määritellään lisäksi p-adisten lukujen muodostama kunta $\mathbb{Q}_p$ ja esitellään algoritmi rationaalilukujen muuttamiseksi p-adiseen muotoon. Algoritmia havainnollistetaan luvun lopussa esimerkillä. Lähteenä tässä luvussa käytetään G. Bachmanin teosta *Introduction to p-adic numbers and valuation theory* [1].

Luvun 2 alussa määritellään J. Hoffsteinin teoksen *An Introduction to Mathematical Cryptography* [2] pohjalta yleisiä lineaarialgebran käsitteitä ja konstruoidaan niiden avulla hilat. Tämän jälkeen laajennetaan hilan käsite p-adisiin lukuihin ja muodostetaan p-adiset approksimaatiohilat. Näiden hilojen konstruointia varten tarvitaan p-adisten kokonaislukujen jonoja, joiden generointiin näytetään luvussa kaksi erilaista tapaa. Luvun lopussa esitellään vielä lyhyesti LLL-algoritmi hilan lyhimmän vektorin löytämiseksi. Tässä luvussa käytetään päälähteinä S. Kamadan ja K. Naiton artikkeleita [4] ja [5].

Kolmannessa luvussa siirrytään käsittelemään salausmenetelmiä. Luvun alussa esitellään yleisellä tasolla selkäreppusalaukset käyttäen lähteenä J. Hoffsteinin teosta [2]. Tämän jälkeen tarkastellaan kahta selkäreppusalausta, jotka pohjautuvat luvussa 2 konstruoituihin p-adisiin approksimaatiohiloihin. Luvussa 3.1 esitellään ensimmäinen p-adinen selkäreppusalaus, joka eroaa tavallisten kokonaislukujen selkäreppusalauksesta siinä, että salaisena avaimena käytetään p-adista vähenevää jonoa superkasvavan jonon sijaan. Tämän eroavaisuuden vuoksi p-adinen selkäreppusalaus kestää esimerkiksi Shamirin hyökkäyksen, jolla tavalliset selkäreppusysteemit pystytään helposti murtamaan. Systeemin toimintaa havainnollistetaan esimerkillä, jossa avataan ja salataan lyhyt viesti. Lopuksi tarkastellaan vielä salauksen turvallisuutta erityisesti LLL-hyökkäystä vastaan. Luvun 3.1 päälähteitä ovat H. Inouen, S. Kamadan ja K. Naiton artikkeli [3], sekä S. Kamadan ym. artikkeli [4].

Luvussa 3.2 esitellään edellisen p-adisen selkäreppusalauksen toinen versio. Tässä selkäreppusalauksessa viestin vastaanottaja valitsee omat avaimensa hyvin samankaltaisesti, kuin edellisessä salauksessa. Eroavaisuutena edelliseen, viestin lähettäjä laskee itselleen yhden salaisen avaimen enemmän. Tämän avaimen vuoksi salattuun viestiin summataan yksi komponentti lisää, mikä kasvattaa systeemin turvallisuutta LLL-hyökkäystä kehittyneempiä algoritmeja vastaan. Tämän salauksen toinen merkittävä etu on se, että lisätyn salaisen avaimen avulla viestin lähettäjä laskee itselleen avaimen, joka toimii digitaalisena allekirjoituksena. Salattu viesti saadaan avattua ainoastaan jos sekä viesti, että lähetetty avain kuuluvat samalle henkilölle. Vastaanottaja pystyy näin ollen varmistamaan viestin lähettäjän. Myös tämän salausmenetelmän toimintaa havainnollistetaan esimerkillä. Luvun lopuksi tarkastellaan vielä systeemin turvallisuutta erilaisia hyökkäyksiä vastaan. Luvun 3.2 päälähteinä käytetään H. Inouen ym. artikkelia [3] ja S. Kamadan ja K. Naiton artikkelia [5].

Työssä käytetyt esimerkit, sekä Lemma 2.13 todistuksineen ovat tutkielman tekijän itse kehittämiä. Myös Seurauksen 1.6 todistus on keksitty itse. Lisäksi Luvussa 3.1 viestin avaamiseen liittyvät perustelut ovat tutkielman kirjoittajan omaa työtä.

1 p-adiset luvut

Tässä luvussa määritellään p-adinen itseisarvo laajentamalla tavallisen itseisarvon käsitettä. Tämän jälkeen esitellään p-adinen valuaatio ja sen tärkeimmät ominaisuudet. Lopuksi määritellään p-adisten lukujen joukko rationaalilukujen täydellistymänä ja tarkastellaan rationaalilukujen muuttamista p-adiseen muotoon.

1.1 p-adinen itseisarvo

Määritelmä 1.1. *Itseisarvokuvaukselle* $|\cdot| : \mathbb{Q} \to \mathbb{R}$ pätee

1. $|a| \geq 0$ ja $|a| = 0$ jos ja vain jos $a = 0$,
2. $|ab| = |a||b|$,
3. $|a + b| \leq |a| + |b|$,

kaikilla $a, b \in \mathbb{Q}$. Lisäksi, jos kuvaukselle $|\cdot|$ pätee

4. $|a + b| \leq \max(|a|, |b|)$,

kaikilla $a, b \in \mathbb{Q}$, niin kuvausta kutsutaan *epäarkhimediseksi itseisarvoksi.*

Määritelmä 1.2. Olkoon $c \in \mathbb{R}$ sellainen, että $0 < c < 1$ ja olkoon lisäksi p alkuluku. Tiedetään, että jokainen nollasta eroava rationaaliluku x voidaan esittää muodossa

$$x = p^{\alpha}\frac{a}{b},$$

missä $a, b, \alpha \in \mathbb{Z}$, $p \nmid a$ ja $p \nmid b$. Määritellään *p-adinen itseisarvo* siten, että

$$|x|_p = c^{\alpha} \text{ ja } |0|_p = 0.$$

Huomautus 1.3. Usein valitaan $c = p^{-1}$. Tällöin siis $|x|_p = p^{-\alpha}$, mistä seuraa, että $|p|_p = p^{-1}$.

Esimerkki 1.4. Olkoon $p = 5$. Nyt rationaaliluku $x = \frac{50}{3}$ voidaan esittää muodossa $x = 5^2 \cdot \frac{2}{3}$. Tällöin siis $\alpha = 2$. Jos nyt valitaan $c = p^{-1} = \frac{1}{5}$, niin

$$|x|_p = \left|\frac{50}{3}\right|_5 = \frac{1}{5^2} = \frac{1}{25}.$$

Lause 1.5. *Kuvaus $|\cdot|_p$ toteuttaa epäarkhimedisen itseisarvon ehdot rationaalilukujen kunnassa $\mathbb{Q}$. Kuvausta sanotaan kunnan $\mathbb{Q}$ p-adiseksi itseisarvoksi.*

Todistus. Määritelmästä 1.2 seuraa suoraan, että $|x|_p = 0$ jos ja vain jos $x = 0$. Lisäksi $|x|_p \geq 0$, sillä $0 < c < 1$ ja $\alpha \in \mathbb{Z}$. Näin ollen Määritelmän 1.1 kohta 1 toteutuu.

Olkoon nyt x kuten Määritelmässä 1.2 ja olkoon $y = p^\beta \frac{a'}{b'}$ sellainen, että $p \nmid a'$ ja $p \nmid b'$. Oletetaan lisäksi, että $x \neq 0$ ja $y \neq 0$. Tällöin

$$xy = p^\alpha \frac{a}{b} \cdot p^\beta \frac{a'}{b'} = p^{\alpha+\beta} \frac{aa'}{bb'}.$$

Nyt $p \nmid aa'$ ja $p \nmid bb'$, sillä alkuluku p ei ole tekijänä missään luvuista a, a', b ja b'. Määritelmän 1.2 nojalla voidaan kirjoittaa

$$|xy|_p = c^{\alpha+\beta} = c^\alpha \cdot c^\beta = |x|_p |y|_p.$$

Siis Määritelmän 1.1 kohta 2 toteutuu kun $x \neq 0$ ja $y \neq 0$. Olkoon nyt $x = 0$. Tällöin kohdan 1 nojalla

$$|xy|_p = |0 \cdot y|_p = |0|_p = 0$$

ja

$$|x|_p |y|_p = |0|_p |y|_p = 0 \cdot |y|_p = 0,$$

joten $|xy|_p = |x|_p |y|_p$, kun $x = 0$. Vastaavalla tavalla nähdään, että yhtälö pätee myös tapauksessa, jossa $y = 0$. Näin ollen ehto 2 toteutuu kaikilla $x \in \mathbb{Q}$.

Todistetaan seuraavaksi kohta 3. Nyt riittää todistaa, että kuvaukselle $|\cdot|_p$ pätee kohdan 4 epäyhtälö

$$|x + y|_p \leq \max(|x|_p, |y|_p),$$

sillä kohta 3 seuraa tästä. Tarkastellaan väitettä:

$$\text{Jos } |x|_p \leq 1, \text{ niin } |1 + x|_p \leq 1. \tag{1}$$

Tämä on yhtäpitävää epäyhtälön 4 kanssa, sillä jos epäyhtälöt 4 ja $|x|_p \leq 1$ toteutuvat, niin

$$|1 + x|_p \leq \max(|1|_p, |x|_p) = 1.$$

Vastaavasti väitteestä (1) seuraa epäyhtälö 4, sillä jos oletetaan, että $|x|_p \leq |y|_p$, niin $|x/y|_p \leq 1$ ja edelleen $|1+x/y|_p \leq 1$ väitteen (1) nojalla. Kertomalla tätä puolittain luvulla $|y|_p$, saadaan

$$|x+y|_p \leq |y|_p.$$

Koska edellä valittiin $|x|_p \leq |y|_p$, niin $|y|_p = \max(|x|_p, |y|_p)$ ja täten saadaan epäyhtälö 4. Siis Määritelmän 1.1 kohdan 3 toteamiseen riittää todistaa (1).

Nyt jos $x \neq 0$ ja $|x|_p \leq 1$, niin Määritelmässä 1.2 lukua x vastaavalle potenssille pätee $\alpha \geq 0$. Siis jos rationaalilukuun x sisältyy alkuluvun p potenssi, se on osoittajassa. Tällöin x voidaan kirjoittaa supistetussa muodossa $x = \frac{c}{d}$, missä $\text{syt}(c,d) = 1$ ja lisäksi $p \nmid d$. Näin ollen

$$1 + x = 1 + \frac{c}{d} = \frac{d+c}{d}.$$

Koska nyt luvun $1+x$ nimittäjä ei ole jaollinen alkuluvulla p, niin Määritelmässä 1.2 lukua $1+x$ vastaavalla potenssilla pätee $\alpha \geq 0$. Tästä seuraa, että $|1+x|_p = c^\alpha \leq 1$, koska $0 < c < 1$. Siis (1) toteutuu kun $x \neq 0$.

Jos taas $x = 0$, niin $|x|_p = 0 \leq 1$ ja $|1+x|_p = |1|_p = c^0 = 1$. Siis väite (1) on tosi. Näin ollen Määritelmän 1.1 kohta 3 toteutuu ja kuvaus $|\cdot|_p$ on epäarkhimedinen itseisarvo. □

Seuraus 1.6. *Jos $x, y \in \mathbb{Z}$, p on alkuluku ja $|x|_p \neq |y|_p$, niin*

$$|x+y|_p = \max(|x|_p, |y|_p).$$

Todistus. Olkoon nyt $|x|_p > |y|_p$, jolloin siis $\max(|x|_p, |y|_p) = |x|_p$. Edellisestä todistuksesta tiedetään, että $|x+y|_p \leq \max(|x|_p, |y|_p)$, jolloin oletuksen nojalla pätee $|x+y|_p \leq |x|_p$.

Nyt $|x|_p = |(x+y)-y|_p \leq \max(|x+y|_p, |y|_p) = |x+y|_p$, sillä muuten saataisiin $|x|_p \leq |y|_p$, mikä on ristiriita oletuksen kanssa. Yhdistämällä nämä epäyhtälöt saadaan $|x+y|_p = |x|_p = \max(|x|_p, |y|_p)$. Vastaavasti voidaan laskea tapauksessa, jossa $|y|_p > |x|_p$. Näin ollen väite on siis tosi. □

Määritelmä 1.7. Kuvaus $d : \mathbb{Q} \times \mathbb{Q} \to \mathbb{R}$ on *metriikka*, jos kaikilla $x, y, z \in \mathbb{Q}$ toteutuvat ehdot

1. $d(x,y) \geq 0$ ja $d(x,y) = 0$ jos ja vain jos $x = y$,
2. $d(x,y) = d(y,x)$,
3. $d(x,y) \leq d(x,z) + d(z,y)$.

Edellä kuvatut metriikan ehdot toteutuvat p-adisella itseisarvolla, kun käytetään merkintää $d(x, y) = |x - y|_p$. Näin ollen rationaalilukujen kunta $\mathbb{Q}$ varustettuna p-adisella itseisarvolla on *metrinen avaruus*. Koska p-adinen itseisarvo on epäarkhimedinen, voidaan sen määräämää metriikkaa kutsua myös *ultrametriikaksi*.

Kuten tavallinen itseisarvo, myös p-adinen itseisarvo voidaan ajatella etäisyytenä. Siis jos x ja y ovat rationaalilukuja, $|x - y|_p$ antaa niiden *p-adisen etäisyyden*. Tämä etäisyys on suuri silloin, kun $x-y$ on jaollinen vain alkuluvun p negatiivisella potenssilla, eli $\alpha < 0$ Määritelmässä 1.2. Mitä suurempi tämä negatiivinen potenssi itseisarvoltaan on, sitä kauempana luvut x ja y ovat toisistaan. Vastaavasti rationaalilukujen p-adinen etäisyys on pieni, kun niiden erotus on jaollinen korkealla alkuluvun p potenssilla, eli α on suuri ja positiivinen. Tutkielman seuraavissa luvuissa jonojen suppenemisella tarkoitetaan suppenemista p-adisen metriikan mielessä.

1.2 p-adinen valuaatio

Määritelmän 1.2 potenssille α voidaan ottaa käyttöön merkintä $v_p(x) = \alpha$. Kuvausta $v_p(x)$ kutsutaan rationaaliluvun x *p-adiseksi valuaatioksi*. Valuaatiolla tarkoitetaan siis itseisarvoltaan suurinta alkuluvun p potenssia, joka sisältyy rationaalilukuun x. Koska Määritelmä 1.2 on voimassa vain nollasta eroaville rationaaliluvuille x, määritellään lisäksi p-adinen valuaatio tapauksessa $x = 0$ siten, että $v_p(0) = \infty$. Näin ollen p-adisen valuaation saamat arvot kuuluvat joukkoon $\mathbb{Z} \cup \{\infty\}$.

Esimerkki 1.8. Olkoon $p = 5$. Esimerkissä 1.4 todettiin, että $x = \frac{50}{3}$ voidaan esittää muodossa $x = 5^2 \cdot \frac{2}{3}$. Tällöin siis itseisarvoltaan suurin alkuluvun p potenssi, joka esiintyy rationaaliluvussa x on 2, jolloin $v_5(\frac{50}{3}) = 2$.

Lause 1.9. *Valuaatiolle pätevät seuraavat ehdot:*

1. $v_p(x) = \infty$ *jos ja vain jos* $x = 0$,
2. $v_p(xy) = v_p(x) + v_p(y)$,
3. $v_p(x + y) \geq \min(v_p(x), v_p(y))$.

Todistus. Kohta 1 seuraa suoraan valuaation määritelmästä. Todistetaan nyt kohta 2. Olkoon $x = p^\alpha \frac{a}{b}$ ja $y = p^\beta \frac{a'}{b'}$ supistetuissa muodoissa siten, että $p \nmid a, b, a', b'$ ja $x \neq 0$ ja $y \neq 0$. Tällöin $|xy|_p = c^{\alpha+\beta}$, josta seuraa

$$v_p(xy) = \alpha + \beta = v_p(x) + v_p(y).$$

Väite siis toteutuu, kun $x \neq 0$ ja $y \neq 0$. Olkoon nyt $x = 0$. Tällöin

$$v_p(xy) = v_p(0 \cdot y) = v_p(0)$$

ja kohdan 1 nojalla $v_p(xy) = \infty$. Nyt

$$v_p(x) + v_p(y) = \infty + \beta = \infty = v_p(xy).$$

Vastaavasti voidaan laskea, jos $y = 0$. Näin ollen kohta 2 toteutuu kaikilla $x, y \in \mathbb{Q}$. Todistetaan seuraavaksi kohta 3. Olkoon $x \neq 0, y \neq 0$ ja $\alpha \geq \beta$, jolloin

$$\begin{aligned} x + y &= p^\alpha \frac{a}{b} + p^\beta \frac{a'}{b'} \\ &= p^\beta \left(p^{\alpha-\beta} \frac{a}{b} + \frac{a'}{b'} \right) \\ &= p^\beta \frac{ab' p^{\alpha-\beta} + ba'}{bb'}. \end{aligned}$$

Nyt $ab'p^{\alpha-\beta} + ba'$ on kokonaislukujen tulojen summana kokonaisluku. Tällöin jos siihen sisältyy jokin alkuluvun p potenssi, täytyy potenssin olla positiivinen. Siis $v_p(ab'p^{\alpha-\beta} + ba') \geq 0$. Valuaatiolle huomataan myös ominaisuus

$$v_p(\frac{1}{x}) = v_p(p^{-\alpha} \frac{b}{a}) = -\alpha = -v_p(x).$$

Tämän ja kohdan 2 nojalla saadaan

$$\begin{aligned} v_p(x + y) &= v_p(p^\beta \frac{ab' p^{\alpha-\beta} + ba'}{bb'}) \\ &= v_p(p^\beta) + v_p(ab' p^{\alpha-\beta} + ba') - v_p(bb'). \end{aligned}$$

Nyt $v_p(p^\beta) = \beta$ ja edellä todettiin, että $v_p(ab'p^{\alpha-\beta} + ba') \geq 0$. Lisäksi koska $p \nmid b$ ja $p \nmid b'$, niin $p \nmid bb'$ eli $v_p(bb') = 0$. Näin ollen saadaan

$$v_p(x + y) \geq \beta.$$

Koska alussa oletettiin, että $\alpha \geq \beta$, eli $\beta = \min(\alpha, \beta)$, niin $\beta = \min(v_p(x), v_p(y))$. Näin ollen saadaan siis $v_p(x+y) \geq \min(v_p(x), v_p(y))$, eli väite 3 toteutuu kun $x, y \neq 0$.

Olkoon nyt $x = 0$, jolloin kohdan 1 nojalla $v_p(x) = \infty$. Tällöin

$$v_p(x + y) = v_p(y) = \beta = \min(v_p(x), v_p(y))$$

Siis epäyhtälössä 3 toteutuu yhtäsuuruus, kun $x = 0$. Vastaavasti voidaan laskea, kun $y = 0$. Näin ollen kohta 3 toteutuu kaikilla $x, y \in \mathbb{Q}$. □

1.3 Rationaaliluvun p-adinen esitys

Määritelmä 1.10. Olkoon $|\cdot|$ itseisarvokuvaus kunnassa K ja $\{a_n\}$ jono kunnan K alkioita. Jono $\{a_n\}$ *suppenee* kohti kunnan K alkiota a, jos kaikille reaaliluvuille $\varepsilon > 0$ on olemassa kokonaisluku N siten, että

$$|a_n - a| < \varepsilon$$

kaikilla $n > N$. Tällöin merkitään $\lim_{n\to\infty} a_n = a$ ja alkiota a kutsutaan jonon $\{a_n\}$ *raja-arvoksi.*

Määritelmä 1.11. Olkoon $|\cdot|$ itseisarvokuvaus kunnassa K ja $\{a_n\}$ jono kunnan K alkioita. Jonoa $\{a_n\}$ kutsutaan *Cauchy-jonoksi* itseisarvokuvauksen $|\cdot|$ suhteen, jos kaikille reaaliluvuille $\varepsilon > 0$ on olemassa kokonaisluku N siten, että

$$|a_n - a_m| < \varepsilon$$

kaikilla $n, m > N$.

Määritelmä 1.12. Kunta K on *täydellinen* itseisarvokuvauksen $|\cdot|$ suhteen, jos kunnan K jokaisella Cauchy-jonolla on kuvauksen $|\cdot|$ suhteen raja-arvo kunnassa K. Toisin sanoen jokainen Cauchy-jono suppenee kohti jotakin kunnan K alkiota.

Jos kaikki reaaliluvut asetetaan lukusuoralle pisteinä, saadussa suorassa ei ole aukkoja, vaan se on yhtenäinen. Reaalilukujen kunta $\mathbb{R}$ on siis täydellinen. Jos taas kaikki rationaaliluvut asetetaan lukusuoralle pisteinä, huomataan suoralle jäävän aukkoja. Esimerkiksi irrationaaliluku $\sqrt{2}$ puuttuu rationaalilukujen muodostamalta lukusuoralta. Näin ollen rationaalilukujen kunta $\mathbb{Q}$ ei ole täydellinen. Seuraavan lauseen nojalla jokainen ei-täydellinen kunta voidaan kuitenkin täydellistää, eli aukot voidaan täyttää.

Lause 1.13. *Olkoon K kunta ja $|\cdot|$ itseisarvokuvaus kunnassa K. Tällöin on olemassa kuvauksen $|\cdot|'$ suhteen täydellinen kunta $\hat{K}$, jonka alkiot joko kuuluvat kuntaan K tai ovat mielivaltaisen lähellä jotain sen alkiota ja kuvaus $|\cdot|'$ vastaa kuvausta $|\cdot|$ kunnan K alkioilla. Kuntaa $\hat{K}$ kutsutaan kunnan K täydellistymäksi kuvauksen $|\cdot|$ suhteen.*

Todistus. Todistus on esitetty lähteessä [1]. □

Määritelmä 1.14. Olkoon p alkuluku, $|\cdot|_p$ sitä vastaava p-adinen itseisarvo ja $|p|_p = p^{-1}$. Rationaalilukujen kunnan $\mathbb{Q}$ täydellistymä p-adisen itseisarvon suhteen on *p-adisten lukujen kunta*, jota merkitään $\mathbb{Q}_p$. Lisäksi p-adisten kokonaislukujen joukoksi määritellään

$$\mathbb{Z}_p = \{z \in \mathbb{Q}_p : |z|_p \leq 1\}.$$

Huomautus 1.15. Kaikki kokonaisluvut $x \in \mathbb{Z}$ ovat p-adisia kokonaislukuja, sillä niihin ei voi sisältyä tekijänä alkulukua p negatiivisella potenssilla α. Täten kaikilla kokonaisluvuilla x toteutuu $|x|_p \leq 1$. Vastaava väite ei kuitenkaan päde toiseen suuntaan, eli kaikki p-adiset kokonaisluvut eivät välttämättä ole kokonaislukuja. Kuten Esimerkissä 1.4 havaittiin,

$$\left|\frac{50}{3}\right|_5 = \frac{1}{25} < 1,$$

joten $\frac{50}{3}$ on 5-adinen kokonaisluku. Selvästi $\frac{50}{3}$ ei kuitenkaan kuulu joukkoon $\mathbb{Z}$.

Rationaalilukujen kunta $\mathbb{Q}$ ei ole täydellinen p-adisen itseisarvon suhteen, mutta se voidaan täydellistää, jolloin saadaan p-adisten lukujen kunta $\mathbb{Q}_p$. Kunnan $\mathbb{Q}_p$ alkiot kuuluvat täydellistymän määritelmän nojalla joko kuntaan $\mathbb{Q}$ tai ovat mielivaltaisen lähellä jotain kunnan $\mathbb{Q}$ alkiota. Näin ollen ne täyttävät aiemmin mainitun lukusuoran kokonaan.

Lause 1.16. *Olkoon $|\cdot|$ itseisarvokuvaus ja $|K|$ kunnan K kuva. Jos kuvaus $|\cdot|$ on epäarkhimedinen kunnassa K, niin $|K| = |\hat{K}|$, missä $\hat{K}$ on kunnan K täydellistymä. Kunnan ja sen täydellistymän kuvat ovat siis epäarkhimedisen itseisarvokuvauksen suhteen samat.*

Todistus. Todistus on esitetty lähteessä [1]. □

Tarkastellaan seuraavaksi rationaaliluvun muuttamista p-adiseen muotoon. Olkoon $\alpha \in \mathbb{Q}_p$ sellainen, että $\alpha \neq 0$. Koska p-adisten lukujen kunta $\mathbb{Q}_p$ on rationaalilukujen kunnan $\mathbb{Q}$ täydellistymä, niin Lauseen 1.16 nojalla $|\mathbb{Q}_p|_p = |\mathbb{Q}|_p$. Koska nyt $|\mathbb{Q}|_p = \{|p|_p^n : n = 0, \pm 1, \pm 2, \dots\}$, niin $|\alpha|_p = |p|_p^n$ jollakin $n = 0, \pm 1, \pm 2, \dots$. Jakamalla tämä puolittain luvulla $|p|_p^n$ saadaan

$$\frac{|\alpha|_p}{|p|_p^n} = 1.$$

Määritelmän 1.2 nojalla $|p|_p = c$, joten $|p|_p^n = c^n$. Lisäksi $|p^n|_p = c^n$. Näin ollen potenssi voidaan siis siirtää p-adisen itseisarvon sisälle, eli

$$|p|_p^n = |p^n|_p.$$

Koska $|p^n|_p = c^n$ ja vastaavasti Määritelmän 1.2 nojalla $|\alpha|_p = c^m$ jollakin $m \in \mathbb{Z}$, niin

$$\frac{|\alpha|_p}{|p^n|_p} = \frac{c^m}{c^n} = c^{m-n} = \left|\frac{\alpha}{p^n}\right|_p.$$

Siis p-adinen itseisarvo voidaan ottaa rationaaliluvun osoittajasta ja nimittäjästä erikseen, tai koko rationaaliluvusta kerralla. Yhdistämällä nämä havainnot saadaan

$$\left|\frac{\alpha}{p^n}\right|_p = 1.$$

Jos nyt merkitään $\alpha/p^n = b_n$, niin $|b_n|_p = 1$.

Olkoon seuraavaksi $b_n = \frac{e_n}{d_n}$, missä $e_n, d_n \in \mathbb{Z}$ ja e_n ja d_n ovat jaottomia alkuluvulla p. Tällainen esitys on olemassa, sillä koska $|b_n|_p = 1$, lukuun b_n ei sisälly yhtään alkuluvun p potenssia, eli e_n ja d_n ovat jaottomia alkuluvulla p. Koska nyt $\text{syt}(d_n, p) = 1$, niin luvulle d_n on olemassa käänteisalkio modulo p. Täten on olemassa kokonaisluku x siten, että

$$d_n x \equiv 1 \pmod{p}.$$

Jos nyt asetetaan $e_n x \equiv a_n \pmod{p}$, niin $a_n \in \mathbb{Z}$ ja

$$a_n - b_n \equiv e_n x - \frac{e_n}{d_n} = \frac{e_n(d_n x - 1)}{d_n} \equiv 0 \pmod{p}.$$

Tällöin $p \mid a_n - b_n$, eli $a_n - b_n = pk$ jollakin $k \in \mathbb{Z}$. Jos $a_n - b_n = 0$, niin Määritelmän 1.2 nojalla $|a_n - b_n|_p = 0 < 1$. Jos taas $a_n - b_n \neq 0$, niin lukuun $a_n - b_n$ sisältyy vähintään yksi alkuluvun p potenssi ja Määritelmässä 1.2 täytyy näin olla $\alpha > 0$, jolloin pätee $|a_n - b_n|_p < 1$. Kertomalla tämä epäyhtälö puolittain p-adisella itseisarvolla $|p|_p^n$, saadaan

$$|a_n p^n - b_n p^n|_p < |p|_p^n.$$

Koska $\alpha/p^n = b_n$, voidaan kirjoittaa

$$\alpha = b_n p^n = a_n p^n + (b_n - a_n)p^n.$$

Merkitään tässä $(b_n - a_n)p^n = \gamma_1$, jolle edellä todetun epäyhtälön nojalla pätee $|\gamma_1|_p < |p|_p^n$. Nyt siis $|\gamma_1|_p = |p|_p^m$ jollakin $m < n$. Tämä on samankaltainen yhtälö kuin $|\alpha|_p = |p|_p^n$, josta alussa lähdettiin liikkeelle. Näin ollen edellä luvulle α suoritetut vaiheet voidaan toistaa seuraavaksi luvulle γ_1. Toistamalla edellä esitettyjä vaiheita k kertaa, eli luvuille $\alpha, \gamma_1, \gamma_2, ..., \gamma_{k-1}$, saadaan lopulta luvulle α seuraava esitys:

$$\alpha = a_n p^n + a_{n+1}p^{n+1} + ... + a_{n+k-1}p^{n+k-1} + \gamma_k,$$

missä kertoimet $a_i \in \mathbb{Z}$ ja niille pätee joko $|a_i|_p = 1$ tai $a_i = 0$. Tämän esityksen viimeinen termi γ_k lähestyy nollaa kun vaiheita toistetaan, sillä $|\gamma_k|_p \leq |p|_p^{n+k} \to 0$, kun $k \to \infty$. Näin ollen luvulle α saadaan seuraava esitys.

Lause 1.17. *Jokainen p-adinen luku α voidaan esittää p-kantaisessa muodossa*

$$\alpha = \sum_{n}^{\infty} a_j p^j,$$

missä $a_j \in \mathbb{Z}$ ja luvulla n pätee $|\alpha|_p = |p|_p^n$.

Määritelmä 1.18. Jos Lauseessa 1.17 pätee $0 \leq a_j \leq p-1$, niin esitystä kutsutaan luvun α *kanoniseksi esitykseksi*. Luku α voidaan tällöin kirjoittaa p-adisessa muodossa luettelemalla kertoimet a_j järjestyksessä pienimmästä indeksistä j suurimpaan. Käytetty alkuluku p merkitään näin saatuun esitykseen alaindeksiksi.

Huomautus 1.19. Lauseen 1.17 äärettömällä summalla tarkoitetaan jonon

$$\sum_{n}^{N} a_j p^j,$$

raja-arvoa p-adisessa metriikassa, kun $N \to \infty$. Tämän raja-arvon olemassaolo voidaan perustella seuraavan lauseen avulla.

Lause 1.20. *Olkoon K täydellinen kunta epäarkhimedisen itseisarvokuvauksen $|\cdot|$ suhteen ja $\{a_k\}$ jono kunnan K alkioita siten, että $\lim_{n\to\infty} a_n = 0$. Tällöin summa*

$$\sum_{n=1}^{\infty} a_n,$$

suppenee.

Todistus. Olkoon $s_n = a_1 + a_2 + \cdots + a_n$ ja $s_m = a_1 + a_2 + \cdots + a_m$ siten, että $m < n$. Tässä s_n on siis jonon $\{a_k\}$ alkioiden summa indeksiin n asti ja vastaavasti s_m on m:n ensimmäisen alkion summa. Tällöin epäarkhimedisuuden nojalla pätee

$$|s_n - s_m| = |a_{m+1} + a_{m+2} + \cdots + a_n| \leq \max_{m+1 \leq i \leq n} |a_i|.$$

Koska oletuksen nojalla $\lim_{n\to\infty} a_n = 0$, niin $\max_{m+1\leq i\leq n} |a_i| \to 0$, kun $n, m \to \infty$. Kunnan K täydellisyyden nojalla raja-arvo $\lim_{n\to\infty} s_n$ on siis olemassa ja täten summa suppenee. □

Koska p-adisten lukujen kunta $\mathbb{Q}_p$ on täydellinen epäarkhimedisen p-adisen itseisarvon suhteen ja jonon alkiot $a_n p^n$ ovat p-adisia lukuja, joilla pätee $|a_n p^n|_p = p^{-n}$ eli $\lim_{n\to\infty} a_n p^n = 0$, niin Lauseen 1.20 ehdot täyttyvät. Näin ollen summan raja-arvo on olemassa, eli Lauseen 1.17 ääretön summa suppenee.

Esimerkki 1.21. Olkoon $p = 5$. Esitetään luku $\alpha = \frac{1}{3}$ kunnassa $\mathbb{Q}_5$ käyttämällä edellä esitettyä tapaa. Nyt $b_0 = \alpha/p^0 = \frac{1}{3}$. Koska $|b_0|_5 = 1$, niin $n = 0$, sillä tällöin myös $|5|_5^n = 1$. Nyt siis $e_0 = 1$ ja $d_0 = 3$. Kongruenssiyhtälöstä saadaan

$$d_0 x \equiv 1 \pmod{p} \;\Leftrightarrow\; 3x \equiv 1 \pmod{5} \;\Leftrightarrow\; x \equiv 2 \pmod{5}.$$

Koska nyt $e_0 x = 1 \cdot 2 \equiv 2 \pmod 5$, saadaan esitykseen $a_0 = 2$. Lasketaan seuraavaksi a_1. Nyt

$$\gamma_1 = (b_0 - a_0) \cdot p^0 = (\frac{1}{3} - 2) \cdot 5^0 = -\frac{5}{3}$$

ja $|-\frac{5}{3}|_5 = |5|_5^1$, joten $n = 1$. Tästä nähdään, että $a_1 \neq 0$ ja

$$b_1 = \frac{\gamma_1}{p^1} = -\frac{5}{3}/5^1 = -\frac{1}{3}.$$

Nyt $e_1 = -1$ ja $d_1 = 3$. Kongruenssiyhtälön $3x \equiv 1 \pmod 5$ ratkaisuksi saatiin edellä $x = 2$ ja koska nyt $e_1 = -1$, niin

$$e_1 x = -1 \cdot 2 = -2 \equiv 3 \pmod{5}$$

ja esitykseen saadaan $a_1 = 3$. Jatkamalla samalla tavalla saadaan seuraavaksi

$$\gamma_2 = (b_1 - a_1) \cdot p^1 = (-\frac{1}{3} - 3) \cdot 5^1 = -\frac{50}{3}.$$

Koska $|-\frac{50}{3}|_5 = |5|_5^2$, niin $n = 2$. Siis $a_2 \neq 0$ ja

$$b_2 = \frac{\gamma_2}{p^2} = -\frac{50}{3}/5^2 = -\frac{2}{3}.$$

Nyt siis $e_2 = -2$ ja $d_2 = 3$. Kongruenssiyhtälön $3x \equiv 1 \pmod 5$ ratkaisu on edelleen $x = 2$ ja nyt $e_1 = -2$, jolloin

$$e_1 x = -2 \cdot 2 = -4 \equiv 1 \pmod{5}$$

ja täten $a_2 = 1$. Seuraavassa vaiheessa saadaan

$$\gamma_3 = (b_2 - a_2) \cdot p^2 = (-\frac{2}{3} - 1) \cdot 5^2 = -\frac{5}{3} \cdot 5^2.$$

Tällöin $|\gamma_3|_5 = |5|_5^3$. Siis $a_3 \neq 0$. Koska nyt

$$b_3 = \frac{\gamma_3}{5^3} = -\frac{1}{3} = b_1,$$

niin $a_3 = a_1 = 3$. Edelleen saadaan

$$\gamma_4 = (b_3 - a_3) \cdot p^3 = (-\frac{1}{3} - 3) \cdot 5^3 = -\frac{10}{3} \cdot 5^3.$$

Tällöin $|\gamma_4|_5 = |5|_5^4$, eli $a_4 \neq 0$. Nyt

$$b_4 = \frac{\gamma_4}{5^4} = -\frac{2}{3} = b_2,$$

joten $a_4 = a_2 = 1$.

Jatkamalla samalla tavalla nähdään, että $a_1 = a_3 = a_5 = \cdots = 3$ ja $a_2 = a_4 = a_6 = \cdots = 1$. Siis $\frac{1}{3} = 2,3131\ldots_5 = 2,\overline{31}_5$. Lisäksi koska $|\frac{1}{3}|_5 \leq 1$, niin $\frac{1}{3}$ on 5-adinen kokonaisluku, eli se kuuluu joukkoon $\mathbb{Z}_5$.

2 Hilat

Tämän luvun alussa esitellään tärkeitä lineaarialgebran määritelmiä ja muodostetaan niiden avulla hilat. Hiloilla tarkoitetaan vektorien kokonaislukukertoimisten lineaarikombinaatioiden joukkoa. Tämän jälkeen siirrytään käsittelemään p-adisia approksimaatiohiloja, joiden konstruoinnissa käytetään aiemmin todettuja p-adisten lukujen ominaisuuksia. Erityisen oleellinen tulos on Luvussa 1 todettu p-adisella itseisarvolla toteutuva epäyhtälö $|x+y|_p \leq \max(|x|_p, |y|_p)$. Luvun lopussa esitellään vielä lyhyesti LLL-algoritmi hilan lyhimmän vektorin löytämiseksi.

Määritelmä 2.1. *Vektoriavaruus* V on joukon $\mathbb{R}^m$ osajoukko, jolla pätee

$$x_1 v_1 + x_2 v_2 \in V$$

kaikilla $v_1, v_2 \in V$ ja $x_1, x_2 \in \mathbb{R}$.

Määritelmä 2.2. Olkoon $b_1, b_2, \ldots, b_n \in \mathbb{R}^m$. Vektoreiden *lineaarikombinaatio* on vektori

$$\beta = \sum_{i=1}^{n} x_i b_i,$$

missä $x_i \in \mathbb{R}$ kaikilla $i = 1, 2, \ldots, n$. Kaikkien lineaarikombinaatioiden kokoelmaa $\{x_1 b_1 + x_2 b_2 + \cdots + x_n b_n \mid x_i \in \mathbb{R}\}$ kutsutaan vektoreiden $b_1, b_2, \ldots, b_n$ *lineaariseksi verhoksi*. Sille käytetään merkintää $\operatorname{span}(b_1, b_2, \ldots, b_n)$.

Määritelmä 2.3. Vektorit $b_1, b_2, \ldots, b_n \in \mathbb{R}^m$ ovat *lineaarisesti riippumattomia*, jos ehdosta

$$\sum_{i=1}^{n} x_i b_i = 0,$$

seuraa, että $x_i = 0$ kaikilla $i = 1, 2, \ldots, n$. Muussa tapauksessa vektorit $b_1, b_2, \ldots, b_n$ ovat *lineaarisesti riippuvia*.

Esimerkki 2.4. Tarkastellaan joukon $\mathbb{R}^4$ vektoreiden $b_1 = (-2, 1, 3, 2)$, $b_2 = (4, 1, 1, 2)$ ja $b_3 = (1, 1, 3, -4)$ lineaarista riippuvuutta. Ratkaistaan kertoimet x_1, x_2 ja x_3 yhtälöstä

$$x_1(-2, 1, 3, 2) + x_2(4, 1, 1, 2) + x_3(1, 1, 3, -4) = 0.$$

Tämä voidaan kirjoittaa yhtälöryhmänä

$$\begin{cases} -2x_1 + 4x_2 + \ x_3 = 0 \\ \ \ x_1 + \ x_2 + \ x_3 = 0 \\ \ 3x_1 + \ x_2 + 3x_3 = 0 \\ \ 2x_1 + 2x_2 - 4x_3 = 0. \end{cases}$$

Kertomalla toinen yhtälö puolittain kahdella ja vähentämällä se alimmasta yhtälöstä, saadaan $-6x_3 = 0$, josta edelleen $x_3 = 0$. Kun tämä sijoitetaan ylimpään yhtälöön, saadaan $x_1 = 2x_2$. Sijoittamalla nämä toiseen yhtälöön, saadaan se muotoon $3x_2 = 0$, josta seuraa $x_2 = 0$. Koska $x_1 = 2x_2$, niin tällöin myös $x_1 = 0$.

Koska ehdosta $x_1b_1 + x_2b_2 + x_3b_3 = 0$ seuraa $x_1 = x_2 = x_3 = 0$, niin vektorit b_1, b_2 ja b_3 ovat lineaarisesti riippumattomia.

Määritelmä 2.5. Olkoon $b_1, b_2, \ldots, b_n \in \mathbb{R}^m$ lineaarisesti riippumattomia vektoreita. Vektoreiden $b_1, b_2, \ldots, b_n$ virittämä *hila* on joukko

$$L(b_1, b_2, \ldots, b_n) = \{\sum_{i=1}^{n} x_i b_i \mid x_i \in \mathbb{Z}\}.$$

Hila on siis vektoreiden $b_1, b_2, \ldots, b_n$ kaikkien kokonaislukukertoimisten lineaarikombinaatioiden joukko.

Hilan *kanta* on mikä tahansa lineaarisesti riippumattomien vektoreiden joukko, joka virittää hilan. Joukko $b_1, b_2, \ldots, b_n$ on siis tämän hilan eräs kanta. Hilan *aste* on kantavektoreiden lukumäärä, tässä tapauksessa siis n. Hilan *dimensio* on kantavektorin alkioiden lukumäärä eli m.

Esimerkki 2.6. Lineaarisesti riippumattomien vektoreiden $b_1 = (-2, 1, 3, 2)$, $b_2 = (4, 1, 1, 2)$ ja $b_3 = (1, 1, 3, -4)$ virittämä hila on joukko

$$L(b_1, b_2, b_3) = \{x_1(-2, 1, 3, 2) + x_2(4, 1, 1, 2) + x_3(1, 1, 3, -4) \mid x_1, x_2, x_3 \in \mathbb{Z}\}.$$

Vektorit b_1, b_2 ja b_3 muodostavat hilan erään kannan. Hilan aste on kantavektoreiden lukumäärä eli 3. Hilan dimensio on 4, koska kantavektorit kuuluvat joukkoon $\mathbb{R}^4$.

Esimerkki 2.7. Tarkistetaan kuuluuko vektori $\beta = (-4, 2, 4, 16)$ Esimerkin 2.6 hilaan. Jos vektori kuuluu hilaan, löytyy kokonaisluvut x_1, x_2 ja x_3 siten, että

$$x_1(-2, 1, 3, 2) + x_2(4, 1, 1, 2) + x_3(1, 1, 3, -4) = (-4, 2, 4, 16).$$

Tästä saadaan yhtälöryhmä

$$\begin{cases} -2x_1 + 4x_2 + \ x_3 = -4 \\ \ \ x_1 + \ x_2 + \ x_3 = 2 \\ \ 3x_1 + \ x_2 + 3x_3 = 4 \\ \ 2x_1 + 2x_2 - 4x_3 = 16. \end{cases}$$

Vähentämällä toinen yhtälö kolmannesta, saadaan $x_1 = 1 - x_3$ ja lisäämällä ylin yhtälö alimpaan, saadaan $x_3 = 2x_2 - 4$. Näiden avulla ensimmäisestä yhtälöstä voidaan ratkaista $x_2 = 1$. Tämän avulla saadaan

$$\begin{aligned} x_3 &= 2x_2 - 4 = 2 \cdot 1 - 4 = -2, \\ x_1 &= 1 - x_3 = 1 - (-2) = 3. \end{aligned}$$

Siis $(x_1, x_2, x_3) = (3, 1, -2)$. Koska kokonaisluvut löytyivät, vektori β on vektorien b_1, b_2 ja b_3 lineaarikombinaatio ja siten kuuluu niiden muodostamaan hilaan $L(b_1, b_2, b_3)$.

Määritelmä 2.8. Olkoon $a, b \in \mathbb{R}^m$ vektoreita, joiden koordinaattiesitykset ovat $a = (a_1, a_2, \ldots, a_m)$ ja $b = (b_1, b_2, \ldots, b_m)$. Tällöin niiden *pistetulo* määritellään

$$a \cdot b = a_1 b_1 + a_2 b_2 + \cdots + a_m b_m.$$

Määritelmä 2.9. Kanta $b_1, b_2, \ldots, b_n$ on *ortogonaalinen*, jos

$$b_i \cdot b_j = 0$$

kaikilla $i \neq j$. Kanta on *ortonormaali*, jos tämän lisäksi $\sqrt{b_i \cdot b_i} = 1$ kaikilla $i = 1, 2, \ldots, n$.

Esimerkki 2.10. Tarkastellaan Esimerkin 2.6 kantavektoreita $b_1 = (-2, 1, 3, 2)$, $b_2 = (4, 1, 1, 2)$ ja $b_3 = (1, 1, 3, -4)$. Koska

$$\begin{aligned} b_1 \cdot b_2 &= -2 \cdot 4 + 1 \cdot 1 + 3 \cdot 1 + 2 \cdot 2 = 0, \\ b_2 \cdot b_3 &= 4 \cdot 1 + 1 \cdot 1 + 1 \cdot 3 + 2 \cdot (-4) = 0, \\ b_1 \cdot b_3 &= -2 \cdot 1 + 1 \cdot 1 + 3 \cdot 3 + 2 \cdot (-4) = 0, \end{aligned}$$

niin kanta on ortogonaalinen. Kanta ei kuitenkaan ole ortonormaali, koska

$$b_1 \cdot b_1 = -2 \cdot (-2) + 1 \cdot 1 + 3 \cdot 3 + 2 \cdot 2 = 18$$

ja siten $\sqrt{b_1 \cdot b_1} = \sqrt{18} \neq 1$.

Määritelmässä 2.5 muodostettu hila voidaan myös määrätä matriisin avulla. Jos B on $m \times n$ -matriisi, jonka sarakkeina ovat kantavektorit $b_1, b_2, \ldots, b_n$, niin matriisin B määräämä hila on

$$L(B) = \{Bx \mid x \in \mathbb{Z}^n\}.$$

Hilan aste n saadaan tällöin matriisin sarakkeiden lukumääränä ja dimensio m rivien lukumääränä. Jos $m = n$, matriisi on neliömatriisi ja hilan sanotaan olevan *täyttä astetta*. Jatkossa tarkastellaan ainoastaan täyttä astetta olevia hiloja.

Määritelmä 2.11. Olkoon B $m \times n$ -matriisi, jonka sarakkeina ovat kantavektorit $b_1, b_2, \ldots, b_n$. Vektoreiden $b_1, b_2, \ldots, b_n$ virittämä *suuntaissärmiö* on

$$P(B) = \{Bx \mid x \in [0,1)^n\} = \{b_1x_1 + b_2x_2 + \cdots + b_nx_n \mid 0 \leq x_i < 1\}.$$

Määritelmä 2.12. Olkoon $L(B)$ astetta n oleva matriisin B määräämä hila. Tällöin hilan $L(B)$ *determinantti* $\det(L(B))$ saadaan suuntaissärmiön $P(B)$ n-ulotteisena tilavuutena. Jos hila $L(B)$ on täyttä astetta, niin

$$\det(L(B)) = |\det(B)|.$$

Lemma 2.13. *Hilan $L(B)$ determinantti ei riipu matriisin B valinnasta.*

Todistus. Olkoot $B = (b_1, b_2, \ldots, b_n)$ ja $B' = (b'_1, b'_2, \ldots, b'_n)$ toisistaan eroavia $n \times n$-matriiseja, joiden sarakkeet generoivat saman hilan, eli $L(B) = L(B')$. Tällöin jokainen matriisin B' kantavektori b'_i saadaan matriisin B kantavektoreiden b_i kokonaislukukertoimisena lineaarikombinaationa. Täten on olemassa kokonaislukualkioinen $n \times n$-matriisi U siten, että $B' = UB$.

Vastaava havainto pätee myös toiseen suuntaan, eli kantavektorit b_i voidaan esittää kantavektoreiden b'_i kokonaislukukertoimisina lineaarikombinaatioina. On siis olemassa $n \times n$-matriisi V siten, että $B = VB'$. Yhdistämällä nämä yhtälöt, saadaan $B = VUB$. Täten täytyy olla $VU = I$, missä I on $n \times n$-identiteettimatriisi. Determinantin laskusääntöjen nojalla tästä seuraa $\det(V)\det(U) = 1$.

Koska matriisien U ja V alkiot ovat kokonaislukuja, niin myös niiden determinantit ovat kokonaislukuja. Täten yhtälöstä $\det(V)\det(U) = 1$ seuraa $\det(U) = \det(V) = 1$ tai $\det(U) = \det(V) = -1$. Siis $|\det(U)| = 1$

Yhtälöstä $B' = UB$ seuraa determinantin laskusääntöjen nojalla yhtälö $\det(B') = \det(U)\det(B)$. Täten

$$|\det(B')| = |\det(U)\det(B)| = |\det(U)||\det(B)| = |\det(B)|.$$

Hilan determinantti ei siis riipu matriisin B valinnasta. □

2.1 p-adiset approksimaatiohilat

Määritellään ensin kaksiulotteinen p-adinen approksimaatiohila [11].

Määritelmä 2.14. Olkoon p alkuluku, m positiivinen kokonaisluku ja $\alpha \in \mathbb{Q}_p$.

i) Järjestetty rationaalilukupari (P, Q) on *astetta m oleva p-adinen approksimaatio luvulle* α, jos $|P - Q\alpha|_p = p^{-m}$.

ii) Joukkoa $\Gamma_m = \{(P, Q) \in \mathbb{Z}^2 \mid |P - Q\alpha|_p \leq p^{-m}\}$ kutsutaan *luvun* α *m-asteiseksi approksimaatiohilaksi.*

Edellä määritelty kaksiulotteinen p-adinen approksimaatiohila voidaan laajentaa korkeampiin ulottuvuuksiin käyttämällä samanaikaisen approksimaation ongelmaa, joka esitellään seuraavaksi. Olkoon nyt $n \geq 1$ kokonaisluku ja $\Xi = \{\xi_1, \xi_2, ..., \xi_n\}$ p-adisten kokonaislukujen jono, jossa on n alkiota.

Määritelmä 2.15. Olkoon $w_n(\Xi)$ sellaisten reaalilukujen w supremum, joilla epäyhtälöillä

$$0 < |a_{0,m} + a_{1,m}\xi_1 + \cdots + a_{n,m}\xi_n|_p \leq X_m^{-w-1},$$
$$\max_{0 \leq i \leq n} |a_{i,m}| \leq X_m$$

on olemassa kokonaislukuratkaisu $a_{0,m}, a_{1,m}, \ldots, a_{n,m}$ äärettömän monella reaaliluvulla X_m, jotka lähestyvät ääretöntä kun indeksi m kasvaa. Kokonaislukuratkaisun löytämisen ongelmaa kutsutaan p-adisten lukujen *samanaikaisen approksimaation ongelmaksi* (SAP, simultaneous approximation problem).

Jonon $\Xi = \{\xi_1, \xi_2, ..., \xi_n\}$ p-adiset kokonaislukualkiot ξ_i voidaan valita käyttämällä seuraavaa logistista kuvausta [9] tai tämän jälkeen esiteltävää lineaarikuvausta [7]. Molemmissa tapauksissa alkuarvona käytetään p-adista kokonaislukua ξ.

Määritelmä 2.16. Olkoon p alkuluku. Tällöin *p-adinen logistinen kuvaus* $L_p : \mathbb{Z}_p \to \mathbb{Z}_p$ määritellään

$$L_p(x) = \frac{x^p - x}{p}.$$

Huomautus 2.17. Edellä esitelty p-adinen logistinen kuvaus on hyvin määritelty. Lauseen 1.17 nojalla jokainen p-adinen luku α voidaan esittää muodossa

$$\alpha = \sum_{n}^{\infty} a_j p^j,$$

missä $a_j \in \mathbb{Z}$ ja luvulla n pätee $|\alpha|_p = |p|_p^n$. Jos α on p-adinen kokonaisluku, niin sen p-adisella itseisarvolla toteutuu $|\alpha|_p \leq 1$. Täten saadaan $|p|_p^n = p^{-n} \leq 1$, josta seuraa $n \geq 0$. Nyt

$$\begin{aligned}\alpha^p - \alpha &= \left(\sum_{j=0}^{\infty} a_j p^j\right)^p - \sum_{j=0}^{\infty} a_j p^j \\ &= (a_0 + a_1 p + a_2 p^2 + \dots)^p - (a_0 + a_1 p + a_2 p^2 + \dots).\end{aligned}$$

Kun lukua α kerrotaan itsellään p kertaa, saaduista termeistä ainoastaan a_0^p ei sisällä tekijänä lukua p. Näin ollen luku α^p on muotoa $a_0^p + f(p)$, missä $f(p)$ on alkuluvulla p jaollinen polynomi. Polynomi $f(p)$ saadaan siis yhdistämällä summaksi kaikki ne luvun α^p termit, joissa on kertoimena vähintään yksi p. Luku $\alpha^p - \alpha$ voidaan siis kirjoittaa muodossa

$$\begin{aligned}\alpha^p - \alpha &= a_0^p + f(p) - (a_0 + a_1 p + a_2 p^2 + \dots) \\ &= a_0^p - a_0 + f(p) - (a_1 p + a_2 p^2 + \dots),\end{aligned}$$

jossa loppuosa on jaollinen luvulla p. Fermat'n pienen lauseen nojalla kokonaisluvulla a_0 toteutuu kongruenssiyhtälö

$$a_0^p \equiv a_0 \pmod{p}.$$

Tällöin on olemassa kokonaisluku k siten, että $a_0^p - a_0 = kp$ ja $0 \leq k < p$. Näin ollen luku $\alpha^p - \alpha$ on jaollinen alkuluvulla p ja sillä pätee

$$\left|\frac{\alpha^p - \alpha}{p}\right|_p \leq 1.$$

Tarvittava p-adisten kokonaislukujen jono $\Xi = \{\xi_1, \xi_2, ..., \xi_n\}$ saadaan p-adisella logistisella kuvauksella alkuarvosta $\xi \in \mathbb{Z}_p$, jolle pätee $|\xi|_p = 1$ laskemalla

$$\begin{aligned}\xi_1 &= \xi, \\ \xi_{1+i} &= L_p^i(\xi),\end{aligned}$$

missä $i = 1, 2, \dots, n-1$.

Esimerkki 2.18. Olkoon $p = 3$ ja $n = 4$. Määritetään 3-adisella logistisella kuvauksella alkiot jonoon Ξ. Valitaan alkuarvoksi 3-adinen kokonaisluku $\xi = \frac{1}{4}$, jolloin pätee $|\xi|_3 = 1$. Tällöin

$$\begin{aligned}
\xi_1 &= \xi = \frac{1}{4}, \\
\xi_2 &= L_3(\xi) = \frac{(1/4)^3 - (1/4)}{3} = -\frac{5}{64}, \\
\xi_3 &= L_3^2(\xi) = \frac{(-5/64)^3 - (-5/64)}{3} = \frac{6785}{262144}, \\
\xi_4 &= L_3^3(\xi) = \frac{(6785/262144)^3 - (6785/262144)}{3} = -\frac{155316431289045}{18014398509481984}.
\end{aligned}$$

Kaikilla $i = 1, 2, 3, 4$ toteutuu $|\xi_i|_3 = 1$, sillä mikään luvuista ξ_i ei sisällä tekijänä alkulukua 3.

Toinen tapa valita p-adiset luvut ξ_i on käyttää lineaarikuvausta $f : \mathbb{Z}_p \to \mathbb{Z}/p^N\mathbb{Z}$, joka määritellään

$$f(x) = \omega x \pmod{p^N}.$$

Kuvauksessa $N \in \mathbb{N}$ ja $\omega \in \mathbb{Z}_p$ on sellainen, että $|\omega|_p = 1$. Tällöin p-adisten kokonaislukujen jono $\Xi = \{\xi_1, \xi_2, ..., \xi_n\}$ saadaan valitsemalla alkuarvo $\xi \in \mathbb{Z}_p$, jolle pätee $|\xi|_p = 1$ ja asettamalla kuvauksessa $\omega = \xi$. Jonon ensimmäiseksi alkioksi asetetaan $\xi_1 = \xi$ ja seuraavat alkiot saadaan laskemalla $\xi_i = f(\xi_{i-1})$ kun $i = 2, 3, \ldots, n$. Siis

$$\begin{aligned}
\xi_2 &= f(\xi_1) = \xi \cdot \xi_1 = \xi^2, \\
\xi_3 &= f(\xi_2) = \xi \cdot \xi_2 = \xi^3, \\
&\vdots \\
\xi_n &= f(\xi_{n-1}) = \xi \cdot \xi_{n-1} = \xi^n.
\end{aligned}$$

Tästä nähdään, että jonon $\Xi = \{\xi_1, \xi_2, ..., \xi_n\}$ alkiot saadaan laskemalla potensseja

$$\xi_i = \xi^i, \ i = 1, 2, \ldots, n.$$

Esimerkki 2.19. Olkoon $p = 7$ ja $n = 4$. Määritetään 3-adiset kokonaisluvut jonoon Ξ. Valitaan alkuarvoksi $\xi = \frac{2}{5}$, joka on sellainen 3-adinen koko-

naisluku, että $|\xi|_7 = 1$. Nyt voidaan laskea

$$\begin{aligned}
\xi_1 &= \xi = \frac{2}{5}, \\
\xi_2 &= \xi^2 = \left(\frac{2}{5}\right)^2 = \frac{4}{25}, \\
\xi_3 &= \xi^3 = \left(\frac{2}{5}\right)^3 = \frac{8}{125}, \\
\xi_4 &= \xi^4 = \left(\frac{2}{5}\right)^4 = \frac{16}{625}.
\end{aligned}$$

Kaikki saadut luvut ξ_i ovat 7-adisia kokonaislukuja, joille pätee $|\xi_i|_7 = 1$, sillä luvuissa ei ole tekijänä alkulukua 7.

Määritelmä 2.20. Olkoon p alkuluku ja m positiivinen kokonaisluku. Vaihtamalla vähenevä jono $\{p^{-m}\}$ Määritelmän 2.15 ongelmassa jonon $\{X_m^{-w-1}\}$ tilalle, voidaan määritellä *p-adinen approksimaatiohila* Γ_m siten, että

$$\Gamma_m = \{(a_0, a_1, ..., a_n) \in \mathbb{Z}^{n+1} \mid |a_0 + a_1\xi_1 + ... + a_n\xi_n|_p \leq p^{-m}\}.$$

Määritetään seuraavaksi hilalle Γ_m kanta ja matriisiesitys. Lauseen 1.17 tapaisesti p-adiselle kokonaisluvulle ξ_i voidaan määrittää p-adinen kanoninen esitys

$$\xi_i = \sum_{k=0}^{\infty} x_{i,k} p^k, \tag{2}$$

missä $0 \leq x_{i,k} \leq p-1$. Lopettamalla tässä summan laskeminen potenssiin $m-1$, saadaan p-adisen luvun ξ_i kertalukua m oleva approksimaatio

$$\xi_{i,m} = \sum_{k=0}^{m-1} x_{i,k} p^k. \tag{3}$$

Approksimaatio $\xi_{i,m}$ on p-adisessa metriikassa hyvin lähellä lukua ξ_i, sillä summan loppuosa lähestyy p-adisen itseisarvon määritelmän nojalla nollaa kun k kasvaa kohti ääretöntä. Lukujen p-adiselle etäisyydelle pätee epäyhtälö $|\xi_{i,m} - \xi_i|_p \leq p^{-m}$, sillä

$$\begin{aligned}
\xi_{i,m} - \xi_i &= \sum_{k=0}^{m-1} x_{i,k} p^k - \sum_{k=0}^{\infty} x_{i,k} p^k \\
&= -\sum_{k=m}^{\infty} x_{i,k} p^k,
\end{aligned}$$

jonka p-adiselle itseisarvolle pätee

$$|-\sum_{k=m}^{\infty} x_{i,k}p^k|_p \leq p^{-m}.$$

Hilalle Γ_m voidaan nyt määrittää kanta $\{b_{0,m}, b_{1,m}, ..., b_{n,m}\} \subset \mathbb{Z}^{n+1}$, missä

$$\begin{aligned}
b_{0,m} &= (p^m, 0, \ldots, 0)^\top, \\
b_{1,m} &= (\xi_{1,m}, -1, 0, ..., 0)^\top, \\
b_{2,m} &= (\xi_{2,m}, 0, -1, 0, \ldots, 0)^\top, \\
&\vdots \\
b_{n,m} &= (\xi_{n,m}, 0, \ldots, 0, -1)^\top.
\end{aligned}$$

Tässä merkinnällä $(\cdot)^\top$ tarkoitetaan vektorin transpoosia. Näin määritellyt vektorit ovat kantavektoreita, sillä ne ovat lineaarisesti riippumattomia ja virittävät Määritelmän 2.20 hilan Γ_m. Kantavektoreille pätee $b_{i,m} \in \Gamma_m$ jokaisella $i = 0, 1, \ldots, n$ edellä todetun epäyhtälön $|\xi_{i,m} - \xi_i|_p \leq p^{-m}$ nojalla.

Määritetään nyt matriisi B_m siten, että hilan Γ_m kantavektorit ovat sen sarakkeita. Siis $B_m = (b_{0,m}b_{1,m} \ldots b_{n,m})$, mikä voidaan myös kirjoittaa muodossa

$$B_m = \begin{pmatrix}
p^m & \xi_{1,m} & \xi_{2,m} & \ldots & \xi_{n,m} \\
0 & -1 & 0 & \ldots & 0 \\
0 & 0 & -1 & \ldots & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & \ldots & -1
\end{pmatrix}.$$

Hilan Γ_m determinantti saadaan Määritelmän 2.12 avulla, kun tiedetään, että matriisi B_m on täyttä astetta. Siis

$$\det(\Gamma_m) = |\det(B_m)| = p^m.$$

2.2 LLL-algoritmi

Hilan Γ_m lyhin vektori euklidisen normin $||b|| = \sqrt{b \cdot b}$ mielessä voidaan löytää A. Lenstran, H. Lenstran ja L. Lovászin kehittämän LLL-algoritmin avulla. Algoritmissa lähdetään liikkeelle jostain hilan kannasta ja muokataan se

uudeksi kannaksi, jonka vektorit ovat mahdollisimman lyhyitä ja ortogonaalisia keskenään. Uudessa kannassa vektorit ovat lisäksi pituusjärjestyksessä, lyhin ensimmäisenä. Algoritmin ensimmäisessä vaiheessa tapahtuu redusointi, eli vektoria lyhennetään lisäämällä tai vähentämällä siitä toisia kannan vektoreita. Toisessa vaiheessa redusoitu vektori vaihdetaan toiseen kannan vektoriin, joka on pidempi. Ennen varsinaisen LLL-algoritmin käyttöä hilan kanta muokataan ortogonaaliseksi Gram-Schmidt-algoritmin avulla [2].

Määritelmä 2.21. Olkoon $\{b_1, b_2, \ldots, b_n\} \subset \mathbb{Z}^{n+1}$ hilan Γ_m kanta. *Gram-Schmidt-ortogonalisoitu kanta* $\{b_1^*, b_2^*, \ldots, b_n^*\}$ saadaan asettamalla ensin $b_1^* = b_1$ ja laskemalla sitten kaikille $1 \leq i < k \leq n$

$$\mu_{k,i} = \frac{b_k \cdot b_i^*}{b_i^* \cdot b_i^*}.$$

Seuraavat ortogonaalisen kannan vektorit saadaan laskemalla

$$b_k^* = b_k - \sum_{i=1}^{k-1} \mu_{k,i} b_i^*.$$

Huomautus 2.22. Gram-Schmid-algoritmilla saadut ortogonaaliset vektorit $\{b_1^*, b_2^*, \ldots, b_n^*\}$ virittävät saman vektoriavaruuden kuin vektorit $\{b_1, b_2, \ldots, b_n\}$, mutta eivät muodosta hilalle Γ_m kantaa. Tämä johtuu siitä, että edellä kuvatussa algoritmissa lineaarikombinaatioiden kertoimet $\mu_{k,i}$ eivät välttämättä ole kokonaislukuja, mikä on vaatimus hilan määritelmässä. Vektorit $\{b_1^*, b_2^*, \ldots, b_n^*\}$ ovat vektoriavaruuden kanta, sillä vektoriavaruuden määritelmässä kertoimien ei tarvitse olla kokonaislukuja.

Määritelmä 2.23. Olkoon $\{b_1, b_2, \ldots, b_n\}$ hilan eräs kanta ja $\{b_1^*, b_2^*, \ldots, b_n^*\}$ siitä Määritelmän 2.21 tavalla saatu Gram-Schmidt ortogonalisoitu kanta. Olkoon lisäksi $\delta : \frac{1}{4} < \delta < 1$ kiinnitetty. Tällöin sanotaan, että kanta $\{b_1, b_2, \ldots, b_n\}$ on *δ-LLL-redusoitu kanta*, jos se toteuttaa seuraavat kaksi ehtoa:

1. $|\mu_{k,i}| = \left| \frac{b_k \cdot b_i^*}{b_i^* \cdot b_i^*} \right| \leq \frac{1}{2}, \ \forall i < k.$

2. Kaikille peräkkäisten vektoreiden pareille b_i, b_{i+1} pätee epäyhtälö

   $$\delta(\pi_i(b_i) \cdot \pi_i(b_i)) \leq \pi_i(b_{i+1}) \cdot \pi_i(b_{i+1}).$$

Ehdon 2 projektiot π_i avaruudelta $\mathbb{R}^n$ lineaariselle verholle $\text{span}\{b_i^*, b_{i+1}^*, \ldots, b_n^*\}$ määritellään

$$\pi_i(x) = \sum_{j=1}^{n} \frac{x \cdot b_j^*}{b_j^* \cdot b_j^*} b_j^*.$$

LLL-algoritmin ensimmäistä ehtoa kutsutaan usein *suuruusehdoksi* ja toista ehtoa *Lovászin ehdoksi*.

Huomautus 2.24. Koska Gram-Schmidt-ortogonalisoitu vektori voidaan kirjoittaa projektion avulla $b_i^* = \pi_i(b_i)$, Lovászin ehto voidaan yhtäpitävästi esittää muodossa

$$(\delta - \mu_{i+1,i}^2)(b_i^* \cdot b_i^*) \leq (b_{i+1}^* \cdot b_{i+1}^*).$$

LLL-algoritmi aloitetaan asettamalla $b_1^* = b_1$ ja $k = 2$. Ensimmäisessä vaiheessa tarkastellaan suuruusehdon toteutumista annetun kannan vektorilla b_k. Jos suuruusehto toteutuu, voidaan siirtyä tarkistamaan Lovászin ehto. Jos myös se toteutuu, asetetaan $k = k + 1$ ja toistetaan samat tarkastelut seuraavalla kantavektorilla b_{k+1}.

Jos suuruusehto ei toteudu joillakin luvuilla k ja i, suoritetaan kantavektorin b_k redusointi laskemalla

$$b_k = b_k - \lfloor \mu_{k,i} \rceil \cdot b_i,$$

missä merkintä $\lfloor \mu_{k,i} \rceil$ tarkoittaa rationaaliluvun $\mu_{k,i}$ pyöristämistä lähimpään kokonaislukuun. Uusi kantavektori saadaan siis vähentämällä tai lisäämällä siihen edeltävä kantavektori jollain kokonaisluvulla kerrottuna. Rationaaliluku täytyy pyöristää kokonaisluvuksi, että uusi vektori b_k kuuluu hilaan. Tämä seuraa siitä, että hilan määritelmässä kantavektoreiden lineaarikombinaatioiden kertoimien tulee olla kokonaislukuja. Näin lasketulla uudella kantavektorilla b_k kertoimeksi saadaan

$$\begin{aligned}\mu_{k,i}^* &= \frac{(b_k - \lfloor \mu_{k,i} \rceil \cdot b_i) \cdot b_i^*}{b_i^* \cdot b_i^*} = \frac{b_k \cdot b_i^* - \lfloor \mu_{k,i} \rceil \cdot b_i \cdot b_i^*}{b_i^* \cdot b_i^*} \\ &= \frac{b_k \cdot b_i^*}{b_i^* \cdot b_i^*} - \lfloor \mu_{k,i} \rceil \cdot \frac{b_i \cdot b_i^*}{b_i^* \cdot b_i^*} = \mu_{k,i} - \lfloor \mu_{k,i} \rceil.\end{aligned}$$

Tästä seuraa $|\mu_{k,i} - \lfloor \mu_{k,i} \rceil| \leq \frac{1}{2}$. Siis $|\mu_{k,i}^*| \leq \frac{1}{2}$, eli suuruusehto toteutuu kantavektorin redusoinnin jälkeen.

Jos Lovászin ehto ei toteudu joillekin peräkkäiselle kantavektoreille b_k ja b_{k+1}, vektoreiden paikat vaihdetaan ja algoritmi aloitetaan alusta. Edellä kuvattuja vaiheita toistetaan, kunnes molemmat ehdot saadaan toteutumaan kaikilla kantavektoreilla. Havainnollistetaan LLL-algoritmia seuraavaksi esimerkillä.

Esimerkki 2.25. Lasketaan matriisille

$$B_m = \begin{pmatrix} 0 & 1 & 2 \\ -1 & 0 & 1 \\ 2 & -2 & 2 \end{pmatrix}$$

δ-LLL-redusoitu kanta, kun valitaan $\delta = \frac{3}{4}$. Matriisin kantavektorit ovat $b_1 = (0, -1, 2)$, $b_2 = (1, 0, -2)$ ja $b_3 = (2, 1, 2)$. Asetetaan ensimmäiseksi vektoriksi $b_1^* = b_1 = (0, -1, 2)$ ja lasketaan kerroin

$$\mu_{2,1} = \frac{b_2 \cdot b_1^*}{b_1^* \cdot b_1^*} = \frac{(1, 0, -2) \cdot (0, -1, 2)}{(0, -1, 2) \cdot (0, -1, 2)} = -\frac{4}{5}.$$

Koska $|\mu_{2,1}| > \frac{1}{2}$, LLL-algoritmin suuruusehto ei toteudu. Vektori b_2 redusoidaan laskemalla

$$\begin{aligned} b_2 &= b_2 - \lfloor \mu_{2,1} \rceil \cdot b_1 = (1, 0, -2) - \left\lfloor -\frac{4}{5} \right\rceil \cdot (0, -1, 2) \\ &= (1, 0, -2) + (0, -1, 2) = (1, -1, 0). \end{aligned}$$

Näin saatu uusi vektori b_2 on aiempaa lyhyempi ja uudeksi kertoimeksi saadaan

$$\mu_{2,1} = \frac{b_2 \cdot b_1^*}{b_1^* \cdot b_1^*} = \frac{(1, -1, 0) \cdot (0, -1, 2)}{(0, -1, 2) \cdot (0, -1, 2)} = \frac{1}{5}.$$

Nyt $|\mu_{2,1}| < \frac{1}{2}$, joten suuruusehto toteutuu. Seuraavaksi vektoriksi saadaan

$$b_2^* = b_2 - \mu_{2,1} \cdot b_1^* = (1, -1, 0) - \frac{1}{5} \cdot (0, -1, 2) = \frac{1}{5}(5, -4, -2).$$

Tarkistetaan toteutuuko Lovászin ehto, valitulla arvolla $\delta = \frac{3}{4}$. Koska

$$\begin{aligned} \delta - \mu_{2,1}^2 &= \frac{3}{4} - \left(\frac{1}{5}\right)^2 = \frac{71}{100}, \\ b_1^* \cdot b_1^* &= (0, -1, 2) \cdot (0, -1, 2) = 5, \\ b_2^* \cdot b_2^* &= \frac{1}{5}(5, -4, -2) \cdot \frac{1}{5}(5, -4, -2) = \frac{9}{5}, \end{aligned}$$

niin saadaan

$$(\delta - \mu_{2,1}^2)(b_1^* \cdot b_1^*) = \frac{71}{100} \cdot 5 = \frac{71}{20} = 3,55 > 1,8 = \frac{9}{5} = b_2^* \cdot b_2^*.$$

Ehto ei siis toteudu, joten vaihdetaan vektoreiden b_1 ja b_2 paikat. Uudet kantavektorit ovat täten $b_1 = (1, -1, 0)$, $b_2 = (0, -1, 2)$ ja $b_3 = (2, 1, 2)$.

Aloitetaan algoritmi alusta asettamalla $b_1^* = b_1 = (1, -1, 0)$. Ensimmäiseksi kertoimeksi saadaan

$$\mu_{2,1} = \frac{b_2 \cdot b_1^*}{b_1^* \cdot b_1^*} = \frac{(0, -1, 2) \cdot (1, -1, 0)}{(1, -1, 0) \cdot (1, -1, 0)} = \frac{1}{2}$$

ja LLL-algoritmin suuruusehto toteutuu. Seuraava ortogonaalinen vektori saadaan laskemalla

$$b_2^* = b_2 - \mu_{2,1} \cdot b_1^* = (0, -1, 2) - \frac{1}{2} \cdot (1, -1, 0) = \frac{1}{2}(-1, -1, 4).$$

Koska nyt

$$\begin{aligned} \delta - \mu_{2,1}^2 &= \frac{3}{4} - \left(\frac{1}{2}\right)^2 = \frac{1}{2}, \\ b_1^* \cdot b_1^* &= (1, -1, 0) \cdot (1, -1, 0) = 2, \\ b_2^* \cdot b_2^* &= \frac{1}{2}(-1, -1, 4) \cdot \frac{1}{2}(-1, -1, 4) = \frac{9}{2}, \end{aligned}$$

niin saadaan

$$(\delta - \mu_{2,1}^2)(b_1^* \cdot b_1^*) = \frac{1}{2} \cdot 2 = 1 < 4,5 = \frac{9}{2} = b_2^* \cdot b_2^*$$

eli Lovászin ehto toteutuu. Näin ollen voidaan siirtyä eteenpäin ja laskea seuraava kerroin. Nyt saadaan

$$\mu_{3,2} = \frac{b_3 \cdot b_2^*}{b_2^* \cdot b_2^*} = \frac{(2, 1, 2) \cdot \frac{1}{2}(-1, -1, 4)}{\frac{1}{2}(-1, -1, 4) \cdot \frac{1}{2}(-1, -1, 4)} = \frac{5}{9}.$$

Suuruusehto ei toteudu, joten päivitetään vektori b_3 laskemalla

$$\begin{aligned} b_3 = b_3 - \lfloor \mu_{3,2} \rceil \cdot b_2 &= (2, 1, 2) - \left\lfloor \frac{5}{9} \right\rceil \cdot (0, -1, 2) \\ &= (2, 1, 2) - (0, -1, 2) = (2, 2, 0). \end{aligned}$$

Uudeksi kertoimeksi saadaan

$$\mu_{3,2} = \frac{b_3 \cdot b_2^*}{b_2^* \cdot b_2^*} = \frac{(2, 2, 0) \cdot \frac{1}{2}(-1, -1, 4)}{\frac{1}{2}(-1, -1, 4) \cdot \frac{1}{2}(-1, -1, 4)} = -\frac{4}{9},$$

jolloin algoritmin suuruusehto toteutuu. Voidaan siirtyä eteenpäin ja laskea seuraava kerroin

$$\mu_{3,1} = \frac{b_3 \cdot b_1^*}{b_1^* \cdot b_1^*} = \frac{(2,2,0) \cdot (1,-1,0)}{(1,-1,0) \cdot (1,-1,0)} = 0.$$

Suuruusehto toteutuu myös tällä kertoimella, joten voidaan laskea viimeinen ortogonaalinen vektori

$$\begin{aligned} b_3^* &= b_3 - \mu_{3,1} \cdot b_1^* - \mu_{3,2} \cdot b_2^* = (2,2,0) - 0 \cdot (1,-1,0) + \frac{4}{9} \cdot \frac{1}{2}(-1,-1,4) \\ &= \frac{1}{9}(16,16,8). \end{aligned}$$

Nyt myös Lovászin ehto toteutuu, sillä

$$\begin{aligned} \delta - \mu_{3,2}^2 &= \frac{3}{4} - \left(-\frac{4}{9}\right)^2 = \frac{179}{324}, \\ b_2^* \cdot b_2^* &= \frac{1}{2}(-1,-1,4) \cdot \frac{1}{2}(-1,-1,4) = \frac{9}{2}, \\ b_3^* \cdot b_3^* &= \frac{1}{9}(16,16,8) \cdot \frac{1}{9}(16,16,8) = \frac{64}{9}, \end{aligned}$$

mistä seuraa

$$(\delta - \mu_{3,2}^2)(b_2^* \cdot b_2^*) = \frac{179}{324} \cdot \frac{9}{2} = \frac{179}{72} = 2,4861\cdots < 7,1111\cdots = \frac{64}{9} = b_3^* \cdot b_3^*.$$

Koska kaikki ehdot toteutuvat, saatu kanta $b_1 = (1,-1,0)$, $b_2 = (0,-1,2)$ ja $b_3 = (2,2,0)$ on $\frac{3}{4}$-LLL-redusoitu. Matriisiksi saadaan siis

$$B = \begin{pmatrix} 1 & 0 & 2 \\ -1 & -1 & 2 \\ 0 & 2 & 0 \end{pmatrix}.$$

Hilan lyhin kantavektori on vektori b_1, jonka pituus on

$$\sqrt{b_1 \cdot b_1} = \sqrt{1 \cdot 1 + (-1) \cdot (-1) + 0 \cdot 0} = \sqrt{2}.$$

Huomautus 2.26. Kuten edeltävästä esimerkistä nähdään, pienilläkin matriisin dimensioilla joudutaan toistamaan algoritmin vaiheita useita kertoja, joten laskeminen käsin on melko hidasta. Tämän vuoksi luvun 3 esimerkeissä LLL-redusoidun matriisin laskemiseen käytetään avoimen lähdekoodin ohjelmaa Sagea ja komentoa `LLL()`. Sagen LLL-algoritmi suorittaa samat vaiheet kuin edellä ja on melko nopea suuremmillakin dimensioilla. Ohjelmaa käyttäessä on huomattava, että redusoidut kantavektorit saadaan luettua tulosteen vaakariveinä, ei sarakkeina.

Arvioidaan seuraavaksi hilan lyhimmän vektorin pituutta normin l_∞ mielessä. Vektorille $x \in \mathbb{R}^n$ normi l_∞ määritellään $||x||_\infty = \sup_n |x_n|$. Merkitään Määritelmän 2.20 hilan Γ_m lyhimmän vektorin pituutta $\lambda_1^{(\infty)}(\Gamma_m)$.

Lause 2.27. *Olkoon $n \geq 1$ ja $\Xi = \{\xi_1, \xi_2, \ldots, \xi_n\}$ p-adisten kokonaislukujen jono, jossa on n alkiota ja jonka alkiot ovat irrationaalisia ja lineaarisesti riippumattomia kunnan $\mathbb{Q}$ suhteen. Tällöin jokaiselle positiiviselle kokonaisluvuille m on olemassa kokonaislukuratkaisu $(a_{0,m}, a_{1,m}, \ldots, a_{n,m}) \in \mathbb{Z}^{n+1}$, joka toteuttaa epäyhtälöt*

$$0 < |a_{0,m} + a_{1,m}\xi_1 + \cdots + a_{n,m}\xi_n|_p \leq p^{-m},$$
$$\max_{0 \leq i \leq n} |a_{i,m}| \leq p^{\frac{m}{n+1}}.$$

Lisäksi tällöin

$$\lambda_1^{(\infty)}(\Gamma_m) \leq \det(\Gamma_m)^{\frac{1}{n+1}}$$

ja Määritelmän 2.15 supremumille saadaan arvio $w_n(\Xi) \geq n$.

Todistus. Käytetään todistuksessa hyödyksi kyyhkyslakkaperiaatetta. Jokaiselle positiiviselle kokonaisluvulle m voidaan muodostaa kyyhkyslakat

$$H_k = \{z \in \mathbb{Z}_p \mid z \equiv \sum_{j=0}^{m-1} h_{k,j}p^j \pmod{p^m}\},$$

kun $0 \leq h_{k,j} \leq p-1, j = 0, 1, \ldots m-1$ ja $k = 1, 2, \ldots, p^m$. Tässä summat ovat siis p-kantaisia esityksiä luvuille $0, 1, \ldots, p^m - 1$. Lukujen k määräämien joukkojen H_k yhdisteenä saadaan p-adisten kokonaislukujen joukko kokonaisuudessaan, eli

$$\mathbb{Z}_p = \bigcup_{k=1}^{p^m} H_k.$$

Tämä seuraa siitä, että Lauseen 1.17 nojalla jokaisella p-adisella kokonaisluvulla z on yksikäsitteinen potenssiesitys. Ottamalla tästä esityksestä modulo p^m, saadaan

$$z = \sum_{j=0}^{\infty} h_{k,j}p^j \equiv \sum_{j=0}^{m-1} h_{k,j}p^j \pmod{p^m},$$

missä $0 \leq h_{k,j} \leq p-1$. Tästä nähdään, että jokainen p-adinen kokonaisluku z kuuluu johonkin joukkoon H_k ja täten joukkojen yhdisteenä saadaan kaikki p-adiset kokonaisluvut. Lisäksi, koska edeltävä esitys on yksikäsitteinen, mikään

luku ei kuulu kahteen eri joukkoon. Määritetyt joukot H_k ovat siis erillisiä, eli

$$H_k \cap H_{k'} = \emptyset$$

aina kun $k \neq k'$. Koska kyyhkyslakat muodostettiin siten, että tarkasteltiin kongruenssia kokonaislukujen $0, 1, \ldots, p^m - 1$ kanssa, toisistaan erillisiä kyyhkyslakkoja saadaan yhteensä p^m kappaletta.

Tarkastellaan nyt nollasta eroavia p-adisia kokonaislukuja, jotka ovat muotoa

$$b_0 + b_1\xi_1 + \ldots b_n\xi_n,$$

missä kaikilla $i = 0, 1, \ldots, n$ kertoimet $b_i \in \{0, 1, \ldots, l\}$, kun l on luvun $p^{m/n+1}$ kokonaisosa. Jokaisessa tätä muotoa olevassa p-adisessa kokonaisluvussa on $n+1$ kappaletta kertoimia b_i ja niistä jokaisella on $l+1$ eri vaihtoehtoa. Näin ollen tätä muotoa olevien p-adisten kokonaislukujen lukumäärä on $(l+1)^{n+1}$. Koska tällöin pätee

$$(l+1)^{n+1} > (p^{\frac{m}{n+1}})^{n+1} = p^m,$$

niin p-adisia kokonaislukuja on enemmän kuin aiemmin määriteltyjä kyyhkyslakkoja. Näin ollen on olemassa kyyhkyslakka H_k, joka sisältää vähintään kaksi erisuurta p-adista kokonaislukua. Olkoon nämä luvut

$$z := b_0 + b_1\xi_1 + \cdots + b_n\xi_n,$$
$$z' := b'_0 + b'_1\xi_1 + \cdots + b'_n\xi_n.$$

Koska z ja z' kuuluvat samaan kyyhkyslakkaan, ne ovat kongruentteja saman luvun kanssa modulo p^m. Tästä seuraa

$$z - z' \equiv 0 \pmod{p^m},$$

mikä tarkoittaa sitä, että erotus $z - z'$ on jaollinen luvulla p^m. Luvussa $z - z'$ alkuluvun p korkein potenssi on siis vähintään m, mistä p-adisen itseisarvon määritelmän nojalla seuraa

$$|z - z'|_p \leq p^{-m}.$$

Jos nyt asetetaan $a_i = b_i - b'_i$ kaikilla $i = 0, 1, \ldots, n$, niin edeltävä epäyhtälö saadaan muotoon

$$|a_0 + a_1\xi_1 + \cdots + a_n\xi_n|_p \leq p^{-m}.$$

Koska p-adiset luvut z ja z' ovat oletuksen nojalla erisuuret, jollakin indeksillä $i = 0, 1, \ldots, n$ täytyy päteä $b_i \neq b_i'$, eli $a_i \neq 0$. Tästä seuraa

$$a_0 + a_1\xi_1 + \cdots + a_n\xi_n \neq 0,$$

sillä jonon $\{\xi_1, \xi_2, \ldots, \xi_n\}$ alkiot ovat oletuksen nojalla lineaarisesti riippumattomia kunnan $\mathbb{Q}$ suhteen. Näin ollen p-adisen itseisarvon ominaisuuksien nojalla pätee

$$|a_0 + a_1\xi_1 + \cdots + a_n\xi_n|_p > 0.$$

Yhdistämällä nämä epäyhtälöt saadaan

$$0 < |a_0 + a_1\xi_1 + \cdots + a_n\xi_n|_p \leq p^{-m}.$$

Koska $b_i, b_i' \in \{0, 1, \ldots, l\}$, kaikilla $i = 0, 1, \ldots, n$, niin saadaan

$$\max_{0\leq i\leq n} |a_i| = \max_{0\leq i\leq n} |b_i - b_i'| \leq l \leq p^{\frac{m}{n+1}}.$$

Olkoon nyt hilan Γ_m lyhimmän vektorin pituus l_∞-normin mielessä $\lambda_1^{(\infty)}(\Gamma_m)$. Koska aiemmin todettiin, että $\det(\Gamma_m) = p^m$, niin l_∞-normin määritelmän ja edeltävän epäyhtälön nojalla hilan Γ_m lyhimmälle vektorille saadan arvio

$$\lambda_1^{(\infty)}(\Gamma_m) \leq p^{\frac{m}{n+1}} = \det(\Gamma_m)^{\frac{1}{n+1}}.$$

Arvioidaan seuraavaksi, millä luvuilla w Määritelmän 2.15 epäyhtälöille

$$\begin{aligned} 0 < |a_{0,m} + a_{1,m}\xi_1 + \cdots + a_{n,m}\xi_n|_p &\leq X_m^{-w-1}, \\ \max_{0\leq i\leq n} |a_{i,m}| &\leq X_m \end{aligned}$$

löytyy ratkaisu $(a_{0,m}, a_{1,m}, \ldots, a_{n,m}) \in \mathbb{Z}^{n+1}$. Koska edellä todettiin, että epäyhtälöille

$$\begin{aligned} 0 < |a_{0,m} + a_{1,m}\xi_1 + \cdots + a_{n,m}\xi_n|_p &\leq p^{-m}, \\ \max_{0\leq i\leq n} |a_{i,m}| &\leq p^{\frac{m}{n+1}}. \end{aligned}$$

löytyy ratkaisu $(a_{0,m}, a_{1,m}, \ldots, a_{n,m}) \in \mathbb{Z}^{n+1}$, asetetaan nyt

$$X_m = p^{\frac{m}{n+1}}.$$

Tällöin Määritelmän 2.15 alempi epäyhtälö toteutuu ja saadaan

$$X_m^{-w-1} = \left(p^{\frac{m}{n+1}}\right)^{-w-1} = \left(p^{\frac{-m}{n+1}}\right)^{w+1} = \left(p^{-m}\right)^{\frac{n+1}{w+1}}.$$

Koska tiedetään, että

$$0 < |a_{0,m} + a_{1,m}\xi_1 + \cdots + a_{n,m}\xi_n|_p \leq p^{-m},$$

niin Määritelmän 2.15 ylempi epäyhtälö toteutuu, kun

$$p^{-m} \leq \left(p^{-m}\right)^{\frac{n+1}{w+1}}.$$

Tästä seuraa

$$\frac{n+1}{w+1} \leq 1,$$

josta kertomalla puolittain positiivisella luvulla $w+1$ saadaan $w \geq n$. Siis Määritelmän 2.15 epäyhtälöille löytyy ratkaisu kun $w_n(\Xi) \geq n$. □

3 Selkäreppusalaukset

Tässä luvussa käsitellään tilannetta, jossa on annettu jono positiivisia kokonaislukuja $(a_1, a_2, \ldots, a_n)$ ja jokin kokonaisluku S. Tarkoituksena on löytää jonon alkiot, joiden summana saadaan S. Tämä osajoukko ei välttämättä ole yksikäsitteinen, mutta voidaan olettaa, että ainakin yksi ratkaisu löytyy. Tätä ongelmaa kutsutaan *selkäreppuongelmaksi* ja se on NP-täydellinen. Ongelman NP-täydellisyydellä tarkoitetaan sitä, että löydetty ratkaisu voidaan varmistaa oikeaksi polynomisessa ajassa ja toisaalta ongelma on vähintään yhtä vaikea ratkaista, kuin muutkin NP-luokkaan kuuluvat ongelmat. Selkäreppuongelmaa voidaan havainnollistaa ajattelemalla lukua S selkärepun tilavuutena ja jonoa listana esineitä, joiden tilavuudet ovat $a_1, a_2, \ldots, a_n$. Tarkoitus on siis täyttää selkäreppu tasan täyteen listan esineillä. Selkäreppuongelma voidaan muotoilla seuraavasti.

Määritelmä 3.1. Olkoon $(a_1, a_2, \ldots, a_n)$ julkinen jono positiivisia kokonaislukuja ja $x = (x_1, x_2, \ldots, x_n) \subset \{0, 1\}^n$ salainen vektori. Summa

$$S = \sum_{i=1}^{n} a_i x_i$$

määrää yhdessä jonon $(a_1, a_2, \ldots, a_n)$ kanssa *selkäreppuongelman*.

Edellä kuvattu selkäreppuongelma ratkeaa, jos vastaanottaja löytää alkuperäisen vektorin x tai toisen binäärisen vektorin, jota käyttämällä saadaan sama summa S. Koska vektori x on binäärinen, sen löytäminen vastaa sopivan osajoukon ratkaisemista.

Esimerkki 3.2. Olkoon $S = 27$ ja annettu jono $(2, 6, 7, 10, 13, 15)$. Tarkoituksena on löytää vektori $x = (x_1, x_2, x_3, x_4, x_5, x_6) \subset \{0, 1\}^6$ siten, että

$$27 = 2x_1 + 6x_2 + 7x_3 + 10x_4 + 13x_5 + 15x_6.$$

Kokeilemalla nähdään, että sopiva vektori on $x = (1, 0, 0, 1, 0, 1)$. Osajoukoksi saadaan siis $(2, 10, 15)$.

Siirrytään seuraavaksi tarkastelemaan salausmenetelmiä. Salausmenetelmät mahdollistavat luottamuksellisen tiedon siirtämisen henkilöiden välillä, vaikka viestintää salakuunnteltaisiin. Ideana salausmenetelmissä on muuttaa viesti ennen lähetystä sellaiseen muotoon, että mahdolliset salakuuntelijat eivät saa siitä selvää. Käytännössä tällöin viestin lähettäjä salaa selkokielisen viestin x ennen sen lähettämistä salakirjoitukseksi C. Viestin vastaanottaja

puolestaan avaa salakirjoituksen C takaisin selkokieliseksi viestiksi x. Salaaminen ja avaaminen suoritetaan käyttämällä merkkijonoja, joita kutsutaan avaimiksi.

Salausmenetelmät voidaan jakaa kahteen luokkaan. Symmetrisen avaimen salausmenetelmissä samaa avainta käytetään sekä viestin salaamiseen, että avaamiseen. Tällöin avain täytyy jollakin keinolla onnistua jakamaan kaikille menetelmän käyttäjille, mutta samalla se täytyy pitää salassa ulkopuolisilta. Tämä ei välttämättä käytännössä ole kovin helppoa. Asymmetrisen avaimen eli julkisen avaimen salausmenetelmissä salaamiseen ja avaamiseen käytetään eri avaimia. Menetelmissä jokaisella käyttäjällä on kaksi avainta, joista toinen julkaistaan ja toinen pidetään salaisena. Julkisen avaimen salausmenetelmissä viestin lähettäjä käyttää selkokielisen viestin x salaamiseen vastaanottajan julkista avainta. Viestin tarkoitettu vastaanottaja saa avattua salakirjoituksen omaa salaista avaintaan käyttämällä.

Sellaisia julkisen avaimen kryptosysteemejä, jotka perustuvat edellä kuvattuun ongelmaan kutsutaan *selkäreppusalauksiksi*. Näissä systeemeissä Määritelmän 3.1 vektori x on selkokielinen viesti, jono $(a_1, a_2, \ldots, a_n)$ on viestin vastaanottajan julkinen avain ja summa S on salattu viesti. Jos n valitaan suureksi, on yleensä hyvin vaikeaa löytää sopiva vektori x ja ratkaista selkäreppuongelma. Kuitenkin, jos jonosta $(a_1, a_2, \ldots, a_n)$ on olemassa jotain lisätietoa, ratkaiseminen helpottuu huomattavasti. Tällaista laskemista helpottavaa lisätietoa kutsutaan usein salaoveksi. Käytännössä salaoven avulla löydetään jokin oikotie, jonka avulla vaikea lasku muuttuu helpoksi. Täten vain viestin tarkoitettu vastaanottaja, jolla on tieto oman avaimensa $(a_1, a_2, \ldots, a_n)$ salaovesta, saa helposti ratkaistua viestin x summasta S.

Merkle ja Hellman esittivät ensimmäisen selkäreppuongelmaan perustuvan kryptosysteemin vuonna 1978 [6]. Systeemi pohjautuu havaintoon, että edellä kuvattu selkäreppuongelma on helppo ratkaista suurillakin luvuilla n, jos annettu jono $(a_1, a_2, \ldots, a_n)$ on superkasvava. Superkasvavalla jonolla tarkoitetaan positiivisten kokonaislukujen jonoa, jonka alkioilla pätee $a_{i+1} \geq 2a_i$ kaikilla $1 \leq i \leq n-1$. Menetelmän idea on valita salaiseksi avaimeksi superkasvava lukujono ja muuttaa se lineaarioperaatioita ja kongruenssia käyttäen jonoksi, joka ei enää ole superkasvava. Näin saatu jono on menetelmässä käyttäjän julkinen avain, jonka muodostama selkäreppuongelma on vaikea ratkaista. Menetelmän salaovi on tieto siitä, miten julkisen avaimen määräämä selkäreppuongelma voidaan muuttaa superkasvavaksi ja siten helposti ratkeavaksi. Superkasvavaa jonoa käyttävä selkäreppusalaus on kuitenkin hyvin helppo murtaa. Jo vuonna 1984 Shamir onnistui murtamaan järjestelmän [8]. Systeemi voidaan murtaa myös Luvussa 2 esitellyllä LLL-algoritmilla. Näin ollen kyseistä selkäreppusalausta ei pidetä nykyisin turvallisena.

3.1 Ensimmäinen p-adinen selkäreppusalaus

Tässä luvussa tarkastellaan edellä esitetyn selkäreppusalauksen paranneltua p-adista versiota. Toisin kuin Merklen ja Hellmanin selkäreppusalauksessa, *p-adisessa selkärepussa* käytetään salaisena avaimena vähenevää p-adista jonoa. Salaovi on Seurauksessa 1.6 todettu p-adisen itseisarvon ominaisuus

$$|x + y|_p = \max(|x|_p, |y|_p),$$

kun $|x|_p \neq |y|_p$. Tässä Luvussa esiteltävässä selkäreppusalauksessa salattavat viestit x kuuluvat joukkoon $\{0, 1, 2, \ldots, K\}^n$, missä $K \leq p - 1$. Viestien pituus on siis n. Vastaavanlainen systeemi voidaan myös rakentaa binäärisille viesteille, joiden pituus on n. Luvut n ja K ovat tiedossa kaikilla systeemiä käyttävillä. Lisäksi Määritelmässä 1.2 asetetaan $c = p^{-1}$, jolloin $|x|_p = p^{-v_p(x)}$. Käsitellään tässä luvussa tilannetta, jossa Alice haluaa lähettää Bobille viestin.

Avainten luominen

Bob valitsee aluksi salaisen alkuluvun p ja p-adisen kokonaisluvun ξ siten, että $|\xi|_p = 1$. Seuraavaksi hän käyttää lukuun ξ p-adista logistista kuvausta $L_p(x) = (x^p - x)/p$ ja laskee

$$\begin{aligned} \xi_1 &= \xi, \\ \xi_2 &= L_p^1(\xi), \\ &\vdots \\ \xi_{1+i} &= L_p^i(\xi), \end{aligned}$$

missä $i = 1, 2, \ldots, n-1$. Käyttämällä p-adisen valuaation $v_p(x)$ määritelmää $|x|_p = p^{-v_p(x)}$, Bob laskee

$$\begin{aligned} \eta_1 &= \xi_1, \\ \eta_2 &= p^{v_p(\eta_1)+1}\xi_2, \\ &\vdots \\ \eta_i &= p^{v_p(\eta_{i-1})+1}\xi_i, \end{aligned}$$

missä $i = 2, 3, \ldots, n$. Näin saadut luvut muodostavat p-adisen kokonaislukujonon $\{\eta_1, \eta_2, \ldots, \eta_n\} \subset \mathbb{Z}_p$, jolla pätee $|\eta_1|_p > |\eta_2|_p > \cdots > |\eta_n|_p$. Tämä voidaan osoittaa lukujen p-adisten valuaatioiden avulla. Koska ξ valittiin siten, että $|\xi|_p = 1$, niin kaikilla $i = 1, 2, \ldots, n$ pätee $|\xi_i|_p = 1$. Luvut ξ_i eivät

näin ollen sisällä tekijänä alkulukua p, eivätkä siten vaikuta lukujen η_i valuaatioihin. Lukujen η_i p-adiset valuaatiot nähdään täten suoraan edeltävästä laskusta alkuluvun p potensseina. Valuaatiot ovat siis

$$\begin{aligned} v_p(\eta_1) &= 0, \\ v_p(\eta_2) &= v_p(\eta_1) + 1 = 1, \\ &\vdots \\ v_p(\eta_n) &= v_p(\eta_{n-1}) + 1 = n - 1. \end{aligned}$$

Tästä nähdään, että valuaatioille pätee

$$v_p(\eta_1) < v_p(\eta_2) < \cdots < v_p(\eta_n),$$

josta seuraa edellä todettu ominaisuus

$$|\eta_1|_p > |\eta_2|_p > \cdots > |\eta_n|_p.$$

Seuraavaksi Bob valitsee positiivisen kokonaisluvun m, jolla pätee $|\eta_n|_p > p^{-m}$. Tällainen luku on edellisten epäyhtälöiden nojalla olemassa. Kuten edellä lasketuista valuaatioista nähdään, luvuksi m riittäisi teoriassa valita viestin pituus n, mutta käytännössä m valitaan paljon suuremmaksi. Lukua m kutsutaan approksimaatioasteeksi, ja se on yksi Bobin salaisista avaimista. Seuraavaksi Bob määrittää luvuille η_i astetta m olevat approksimaatiot $\eta_{i,m}$ kaavan (3) mukaisesti laskemalla summat

$$\eta_{i,m} = \sum_{k=0}^{m-1} x_{i,k} p^k.$$

Summassa tarvittavat kertoimet $x_{i,k}$ Bob saa laskettua Esimerkin 1.21 tavalla, kun laskeminen lopetetaan potenssiin $m - 1$.

Koska kaikilla $i = 1, 2, \ldots, n$ pätee $|\eta_i|_p > p^{-m}$, niin lukuihin η_i sisältyvä alkuluvun p potenssi on enintään $m - 1$. Yhtälön (2) mukaisessa p-adisen luvun summaesityksessä tätä korkeampien alkuluvun p potenssien kertoimet $x_{i,k}$ ovat siis nollia, joten ne voidaan jättää pois summasta. Tällöin saadaan

$$|\eta_i|_p = |\sum_{k=0}^{\infty} x_{i,k} p^k|_p = |\sum_{k=0}^{m-1} x_{i,k} p^k + \sum_{k=m}^{\infty} x_{i,k} p^k|_p = |\sum_{k=0}^{m-1} x_{i,k} p^k|_p = |\eta_{i,m}|_p.$$

Siis $|\eta_i|_p = |\eta_{i,m}|_p$, kun $i = 1, 2, \ldots, n$. Näin ollen myös approksimaatioille pätee

$$|\eta_{1,m}|_p > |\eta_{2,m}|_p > \cdots > |\eta_{n,m}|_p.$$

Bob asettaa $\eta := (\eta_{1,m}, \eta_{2,m}, \ldots, \eta_{n,m}) \in \mathbb{Z}^n$, mikä on salauksessa käytettävä vähenevä p-adinen jono ja yksi salaisista avaimista.

Seuraavaksi Bob määrittää loput salauksessa tarvittavat avaimet valitsemalla ensin riittävän suuren alkuluvun q, jolla pätee $q > p^2 p^m$. Lukua q käytetään laskuissa modulona. Lisäksi hän valitsee suuren satunnaisen kokonaisluvun r siten, että $\text{syt}(p, r) = 1$ ja $rp^m > q$. Luvun valinnassa voidaan käyttää esimerkiksi jotain satunnaislukugeneraattoria. Näiden lisäksi laskuissa tarvitaan kokonaisluvun r käänteisalkio s, jonka Bob saa ratkaisemalla kongruenssiyhtälön

$$sr \equiv 1 \pmod{q}.$$

Systeemissä Bobin salainen avain on siis (p, m, η, q, r, s).

Bob määrittää vielä itselleen julkisen avaimen $\beta = (\beta_1, \beta_2, \ldots, \beta_n) \in \mathbb{Z}^n$ laskemalla

$$\beta_i \equiv r\eta_{i,m} \pmod{q}.$$

Salaus

Alice haluaa lähettää Bobille selkokielisen viestin $x = (x_1, x_2, \ldots, x_n) \in \{0, 1, 2, \ldots, K\}^n$, missä $K \leq p - 1$. Salaamiseen Alice käyttää Bobin julkista avainta β. Salakirjoitus $C \in \mathbb{Z}$ saadaan laskemalla

$$C := x \cdot \beta = \sum_{i=1}^{n} x_i \beta_i.$$

Avaus

Bob vastaanottaa salatun viestin C. Käyttämällä salaista avainta s hän laskee

$$C' := C \cdot s \pmod{q}.$$

Salatun viestin C voi avata vain Bob, koska salauksessa käytettiin hänen julkista avaintaan β. Tällöin edellä laskettiin tosiasiassa

$$C \cdot s = \sum_{i=1}^{n} x_i \beta_i s \equiv \sum_{i=1}^{n} x_i r \eta_{i,m} s \equiv \sum_{i=1}^{n} x_i \eta_{i,m} \pmod{q},$$

josta kertoimet x_i ratkeavat helposti, jos luvut $\eta_{i,m}$ ovat tiedossa. Koska viestin tarkoitettu vastaanottaja Bob tietää luvut $\eta_{i,m}$, hän saa viestin selville seuraavia vaiheita seuraamalla.

Vaihe 1

Jos on olemassa $j_1 : 1 \leq j_1 \leq K$ siten, että $|C' - j\eta_{1,m}|_p = |\eta_{1,m}|_p$ pätee kaikilla $j : 0 \leq j < j_1$, mutta ei päde kun $j = j_1$, niin $x_1 = j_1$. Muussa tapauksessa $x_1 = 0$.

Vaihe 2

Jos on olemassa $j_2 : 1 \leq j_2 \leq K$ siten, että $|C' - x_1\eta_{1,m} - j\eta_{2,m}|_p = |\eta_{2,m}|_p$ pätee kaikilla $j : 0 \leq j < j_2$, mutta yhtälö ei päde kun $j = j_2$, niin $x_2 = j_2$. Muussa tapauksessa $x_2 = 0$.

$\vdots$

Vaihe n

Jos on olemassa $j_n : 1 \leq j_n \leq K$ siten, että $|C' - (x_1\eta_{1,m} + x_2\eta_{2,m} + \cdots + x_{n-1}\eta_{n-1,m}) - j\eta_{n,m}|_p = |\eta_{n,m}|_p$ pätee kaikilla $j : 0 \leq j < j_n$, mutta yhtälö ei päde kun $j = j_n$, niin $x_n = j_n$. Muussa tapauksessa $x_n = 0$.

Viestin avaamisen ensimmäisessä vaiheessa verrataan siis salaisen avaimen η ensimmäisen alkion p-adista itseisarvoa $|\eta_{1,m}|_p$ salatun viestin C' p-adiseen itseisarvoon, josta vähennetään luvun $\eta_{1,m}$ monikertoja. Viestin C' ja luvun $\eta_{1,m}$ p-adiset itseisarvot ovat yhtäsuuret silloin, kun salattu viesti C' sisältää komponenttia $\eta_{1,m}$ jollain positiivisella kertoimella. Kun viestistä on saatu vähennettyä komponentti $\eta_{1,m}$ kokonaan pois, yhtäsuuruus ei enää päde.

Näin ollen, jos yhtäsuuruus ei päde enää, kun salatusta viestistä on vähennetty luku $\eta_{1,m}$ j_1-kertaa, niin tiedetään, että salatussa viestissä C' luvun $\eta_{1,m}$ kertoimen täytyy olla j_1. Koska salattu viesti on muotoa

$$C' \equiv \sum_{i=1}^{n} x_i\eta_{i,m} \pmod{q}, \tag{4}$$

niin tästä seuraa, että viestin alkio $x_1 = j_1$.

Jos taas ei löydy sellaista lukua j_1, että yhtäsuuruus pätee kaikilla sitä pienemmillä positiivisilla kokonaisluvuilla, mutta sillä ei, niin salattu viesti ei sisällä ollenkaan komponenttia $\eta_{1,m}$. Tällöin sen kertoimen täytyy siis olla edellä esitetyssä summassa nolla, joten $x_1 = 0$.

Seuraavassa vaiheessa salatusta viestistä C' vähennetään aluksi edellä ratkaistu summan termi $x_1\eta_{1,m}$. Tämän jälkeen siitä vähennetään salaisen avaimen toisen alkion $\eta_{2,m}$ monikertoja, ja verrataan tätä p-adista itseisarvoa

lukuun $|\eta_{2,m}|_p$. Samalla tavalla kuin ensimmäisessä vaiheessa, yhtäsuuruutta tarkastelemalla saadaan ratkaistua x_2. Jos viestin pituus on n, vaiheita toistetaan n kertaa.

Perustellaan vaihe 1 vielä hieman täsmällisemmin käyttämällä hyödyksi tietoa $|\eta_{1,m}|_p > |\eta_{2,m}|_p > \cdots > |\eta_{n,m}|_p$ ja Seurausta 1.6, jonka mukaan p-adisella itseisarvolla toteutuu $|x+y|_p = \max(|x|_p, |y|_p)$, kun $|x|_p \neq |y|_p$. Yhtälön (4) nojalla voidaan kirjoittaa

$$\begin{aligned} |C' - j\eta_{1,m}|_p &= |x_1\eta_{1,m} + x_2\eta_{2,m} + \cdots + x_n\eta_{n,m} - j\eta_{1,m}|_p \\ &= |(x_1 - j)\eta_{1,m} + x_2\eta_{2,m} + \cdots + x_n\eta_{n,m}|_p. \end{aligned}$$

Oletetaan nyt, että yhtälö $|C' - j\eta_{1,m}|_p = |\eta_{1,m}|_p$ toteutuu, kun $0 \leq j < j_1$, mutta ei toteudu arvolla j_1. Tällöin siis

$$|(x_1 - j)\eta_{1,m} + x_2\eta_{2,m} + \cdots + x_n\eta_{n,m}|_p = |\eta_{1,m}|_p,$$

kun $0 \leq j < j_1$. Tästä seuraa $x_1 - j \neq 0$, eli $x_1 \neq j$, sillä jos olisi $x_1 = j$, niin yhtälö saataisiin muotoon

$$|x_2\eta_{2,m} + \cdots + x_n\eta_{n,m}|_p = |\eta_{1,m}|_p.$$

Kuitenkin p-adisen itseisarvon ominaisuuksien ja epäyhtälöiden $|\eta_{1,m}|_p > |\eta_{2,m}|_p > \cdots > |\eta_{n,m}|_p$ nojalla pätee

$$|x_2\eta_{2,m} + \cdots + x_n\eta_{n,m}|_p \leq |\eta_{2,m}|_p.$$

Jos siis olisi $x_1 = j$, niin saataisiin $|\eta_{1,m}|_p \leq |\eta_{2,m}|_p$ mikä on ristiriita oletuksen $|\eta_{1,m}|_p > |\eta_{2,m}|_p$ kanssa. Näin ollen $x_1 \neq j$, kaikilla $0 \leq j < j_1$.

Osoitetaan seuraavaksi, että tällöin täytyy olla $x_1 = j_1$. Koska oletetaan, että yhtälö ei toteudu, kun $j = j_1$, niin

$$|(x_1 - j_1)\eta_{1,m} + x_2\eta_{2,m} + \cdots + x_n\eta_{n,m}|_p \neq |\eta_{1,m}|_p.$$

Tästä seuraa $x_1 - j_1 = 0$, eli $x_1 = j_1$. Nimittäin, jos olisi $x_1 - j_1 \neq 0$, niin $|x_1 - j_1|_p = 1$, sillä $0 \leq x_1 \leq p-1$ ja $1 \leq j_1 \leq p-1$ ja tällöin saataisiin

$$\begin{aligned} |(x_1 - j)\eta_{1,m} + x_2\eta_{2,m} + \cdots + x_n\eta_{n,m}|_p &= |(x_1 - j)\eta_{1,m}|_p \\ &= |x_1 - j|_p|\eta_{1,m}|_p = |\eta_{1,m}|_p, \end{aligned}$$

mikä on ristiriita oletuksen kanssa. Siis jos yhtälö toteutuu kaikilla luvuilla j, joilla pätee $0 \leq j < j_1$, mutta ei luvulla j_1, niin täytyy olla $x_1 = j_1$.

Oletetaan seuraavaksi, että ei löydy sellaista lukua j_1, että $1 \leq j_1 \leq K$ ja yhtäsuuruus $|C' - j\eta_{1,m}|_p = |\eta_{1,m}|_p$ toteutuisi kaikilla $j \in \{0, 1, \ldots, j_1 - 1\}$. Tällöin erityisesti yhtälö ei toteudu, kun $j = 0$. Näin ollen

$$|C'|_p \neq |\eta_{1,m}|_p.$$

Yhtälön (4) nojalla tästä saadaan

$$|x_1\eta_{1,m} + x_2\eta_{2,m} + \cdots + x_n\eta_{n,m}|_p \neq |\eta_{1,m}|_p.$$

Tällöin täytyy olla $x_1 = 0$, sillä jos olisi $x_1 \neq 0$, niin $|x_1|_p = 1$, mistä seuraa

$$|x_1\eta_{1,m} + x_2\eta_{2,m} + \cdots + x_n\eta_{n,m}|_p = |x_1\eta_{1,m}|_p = |x_1|_p|\eta_{1,m}|_p = |\eta_{1,m}|_p,$$

mikä on ristiriita oletuksen kanssa. Siis, jos sellaista lukua j_1 ei löydy, että yhtälö toteutuisi kaikilla sitä pienemmillä luvuilla j, niin täytyy olla $x_1 = 0$. Vastaava päättely voidaan suorittaa avaamisen jokaiselle vaiheelle.

3.1.1 Esimerkki

Tässä luvussa käytetään edellä esiteltyä p-adista selkäreppusalausta viestin salaamiseen ja avaamiseen. Systeemissä käytettävä alkuluku p, sekä salattavan viestin pituus n valitaan tässä esimerkissä pieniksi algoritmin selkeyttämisen ja laskujen helpottamisen vuoksi. Laskuissa käytetään avoimen lähdekoodin ohjelmaa Sagea.

Avainten luominen

Bob valitsee systeemiin salaiseksi alkuluvuksi $p = 5$ ja salattavien viestien pituudeksi $n = 3$. Viestin alkioiden ylärajaksi hän valitsee $K = p - 1 = 4$. Kaikki salattavat viestit x kuuluvat siis joukkoon $\{0, 1, 2, 3, 4\}^3$, joka on julkista tietoa. Seuraavaksi Bob määrittää itselleen jonon $\{\eta_1, \eta_2, \eta_3\}$ valitsemalla ensin 5-adisen kokonaisluvun $\xi = \frac{1}{3}$, jolla pätee

$$\left|\frac{1}{3}\right|_5 = 1.$$

Bob käyttää tähän 5-adista logistista kuvausta $L_5(x) = (x^5 - x)/5$ ja laskee

$$\begin{aligned}
\xi_1 &= \xi = \frac{1}{3}, \\
\xi_2 &= L_5(\xi) = \frac{(1/3)^5 - (1/3)}{5} = -\frac{16}{243}, \\
\xi_3 &= L_5^2(\xi) = \frac{(-16/243)^5 - (-16/243)}{5} = \frac{11157500368}{847288609443}.
\end{aligned}$$

Jonon $\{\eta_1, \eta_2, \eta_3\}$ ensimmäiseksi alkioksi Bob asettaa

$$\eta_1 = \xi_1 = \frac{1}{3}.$$

Luvun η_1 5-adinen valuaatio $v_5(\eta_1) = 0$, koska

$$|\eta_1|_5 = \left|\frac{1}{3}\right|_5 = 1 = 5^0.$$

Tämän avulla Bob saa laskettua jonon toiseksi alkioksi

$$\eta_2 = p^{v_5(\eta_1)+1}\xi_2 = 5^{0+1} \cdot \left(-\frac{16}{243}\right) = -\frac{80}{243},$$

jonka 5-adinen itseisarvo on

$$|\eta_2|_5 = \left|-\frac{80}{243}\right|_5 = \left|-5 \cdot \frac{16}{243}\right|_5 = 5^{-1}.$$

Näin ollen valuaatioksi saadaan $v_5(\eta_2) = 1$. Bob käyttää tätä ja laskee jonoon viimeisen alkion

$$\eta_3 = p^{v_5(\eta_2)+1}\xi_3 = 5^{1+1} \cdot \frac{11157500368}{847288609443} = \frac{278937509200}{847288609443}.$$

Koska nyt

$$|\eta_3|_5 = \left|\frac{278937509200}{847288609443}\right|_5 = \left|5^2 \cdot \frac{11157500368}{847288609443}\right|_5 = 5^{-2},$$

niin Bob valitsee salaiseksi approksimaatioasteeksi $m = 4$. Tällöin pätee $|\eta_3|_5 > 5^{-m}$.

Seuraavaksi Bob määrittää luvuille η_1, η_2 ja η_3 4-asteiset approksimaatiot $\eta_{1,4}, \eta_{2,4}$ ja $\eta_{3,4}$. Yhtälössä (3) summaus lopetetaan siis kun $k = 3$, eli

$$\eta_{i,4} = \sum_{k=0}^{3} x_{i,k}5^k.$$

Summan kertoimet $x_{i,k}$ Bob saa selvitettyä Luvussa 1.3 esitetyllä tavalla. Koska Esimerkistä 1.21 tiedetään, että $\frac{1}{3} = 2,3131..._5$, niin $\{x_{1,0}, x_{1,1}, x_{1,2}, x_{1,3}\} = \{2, 3, 1, 3\}$. Sijoittamalla nämä edelliseen summaan, saadaan

$$\eta_{1,4} = 2 + 3 \cdot 5 + 5^2 + 3 \cdot 5^3 = 417.$$

Suorittamalla vastaavat laskut luvuille η_2 ja η_3, Bob saa approksimaatiot

$$\eta_{2,4} = 3 \cdot 5 + 2 \cdot 5^2 + 5^3 = 190,$$
$$\eta_{3,4} = 5^2 = 25.$$

Bob merkitsee nyt $\eta = \{\eta_{1,4}, \eta_{2,4}, \eta_{3,4}\} = \{417, 190, 25\}$. Saatu jono on vähenevä, ja sillä toteutuu

$$|\eta_{1,4}|_5 > |\eta_{2,4}|_5 > |\eta_{3,4}|_5.$$

Seuraavaksi Bob valitsee alkuluvun q siten, että $q > p^2 p^m$. Koska $p^2 p^m = 5^2 \cdot 5^4 = 15625$, hän valitsee $q = 15629$. Lisäksi Bob tarvitsee satunnaisen kokonaisluvun r, jolla pätee $rp^m > q$ ja $\text{syt}(p, r) = 1$. Satunnaislukugeneraattoria käyttäen hän valitsee $r = 62$. Tämä toteuttaa annetut ehdot, sillä $\text{syt}(5, 62) = 1$ ja $rp^m = 62 \cdot 5^4 = 38750 > 15629 = q$. Bob laskee vielä luvulle r käänteisalkion s ratkaisemalla kongruenssiyhtälön

$$s \cdot 62 \equiv 1 \pmod{15629}.$$

Tästä saadaan ratkaistua $s = 9327$. Bob saa täten salaiseksi avaimekseen $(p, m, \eta, q, r, s) = (5, 4, \{417, 190, 25\}, 15629, 62, 9327)$.

Lopuksi Bob määrittää vielä itselleen julkisen avaimen $\beta = (\beta_1, \beta_2, \beta_3) \in \mathbb{Z}^3$ laskemalla

$$\begin{aligned}
\beta_1 &= r \cdot \eta_{1,4} = 62 \cdot 417 = 25854 \equiv 10225 && \pmod{15629}, \\
\beta_2 &= r \cdot \eta_{2,4} = 62 \cdot 190 = 11780 && \pmod{15629}, \\
\beta_3 &= r \cdot \eta_{3,4} = 62 \cdot 25 = 1550 && \pmod{15629}.
\end{aligned}$$

Näin ollen Bobin julkinen avain on $\beta = (10225, 11780, 1550)$.

Viestin salaus

Alice haluaa nyt lähettää Bobille viestin $x = (1, 3, 0)$. Alice saa salakirjoituksen $C \in \mathbb{Z}$ käyttämällä Bobin julkista avainta β ja laskemalla

$$C = x \cdot \beta = \sum_{i=1}^{3} x_i \beta_i = 1 \cdot 10225 + 3 \cdot 11780 + 0 \cdot 1550 = 45565.$$

Nyt Alice voi lähettää salatun viestin $C = 45565$ Bobille.

Viestin avaus

Bob vastaanottaa salatun viestin $C = 45565$. Salaista avaintaan $s = 9327$ käyttämällä hän laskee ensin

$$C' = Cs = 45565 \cdot 9327 = 137050938 \equiv 987 \pmod{15629}.$$

Bob avaa vastaanottamansa viestin käyttämällä salaista vähenevää jonoa $\{\eta_{1,4}, \eta_{2,4}, \eta_{3,4}\} = \{417, 190, 25\}$. Koska alussa valittiin viestin alkioiden ylärajaksi $K = p - 1 = 4$, niin seuraavissa laskuissa $j = 0, 1, 2, 3, 4$.

Bob avaa ensin viestin ensimmäisen alkion x_1 laskemalla 5-adisia itseisarvoja $|C' - j\eta_{1,4}|_5$, kun $j = 0, 1, 2, 3, 4$ ja vertaamalla näitä lukuun $|\eta_{1,4}|_5$. Nyt $|\eta_{1,4}|_5 = |417|_5 = 1$, jolloin

$$|C' - 0 \cdot \eta_{1,4}|_5 = |987|_5 = 1 = |\eta_{1,4}|_5,$$
$$|C' - 1 \cdot \eta_{1,4}|_5 = |987 - 417|_5 = |570|_5 = 5^{-1} \neq |\eta_{1,4}|_5.$$

Laskeminen voidaan lopettaa tähän, koska saatiin erisuuruus. Koska yhtälö $|C' - j\eta_{1,4}|_5 = |\eta_{1,4}|_5$ toteutuu, kun $j = 0$, mutta ei toteudu, kun $j = 1$, niin $x_1 = 1$.

Seuraavaksi Bob avaa viestin toisen alkion x_2. Nyt $|\eta_{2,4}|_5 = |190|_5 = 5^{-1}$. Hän laskee 5-adisia itseisarvoja $|C' - x_1\eta_{1,4} - j\eta_{2,4}|_5$, kun $j = 0, 1, 2, 3, 4$ ja vertaa näitä lukuun $|\eta_{2,4}|_5$, jolloin

$$|C' - x_1\eta_{1,4} - 0 \cdot \eta_{2,4}|_5 = |987 - 417|_5 = |570|_5 = 5^{-1} = |\eta_{2,4}|_5,$$
$$|C' - x_1\eta_{1,4} - 1 \cdot \eta_{2,4}|_5 = |987 - 417 - 190|_5 = |380|_5 = 5^{-1} = |\eta_{2,4}|_5,$$
$$|C' - x_1\eta_{1,4} - 2 \cdot \eta_{2,4}|_5 = |987 - 417 - 2 \cdot 190|_5 = |190|_5 = 5^{-1} = |\eta_{2,4}|_5,$$
$$|C' - x_1\eta_{1,4} - 3 \cdot \eta_{2,4}|_5 = |987 - 417 - 3 \cdot 190|_5 = |0|_5 = 0 \neq |\eta_{2,4}|_5.$$

Koska nyt yhtälö $|C' - x_1\eta_{1,4} - j\eta_{2,4}|_5 = |\eta_{2,4}|_5$ toteutuu, kun $j = 0, 1, 2$, mutta ei toteudu, kun $j = 3$, niin $x_2 = 3$.

Bob avaa lopuksi viestin viimeisen alkion laskemalla 5-adisia itseisarvoja $|C' - (x_1\eta_{1,4} + x_2\eta_{2,4}) - j\eta_{3,4}|_5$, kun $j = 0, 1, 2, 3, 4$. Nyt $|\eta_{3,4}|_5 = |25|_5 = 5^{-2}$ ja Bob laskee

$$|C' - (x_1\eta_{1,4} + x_2\eta_{2,4}) - 0 \cdot \eta_{3,4}|_5 = |987 - (417 + 3 \cdot 190)|_5 = |0|_5 = 0 \neq |\eta_{3,4}|_5.$$

Koska yhtälö ei toteudu, kun $j = 0$, seuraa suoraan, että $x_3 = 0$.

Bob onnistuu näin selvittämään selkokielisen viestin $x = (x_1, x_2, x_3) = (1, 3, 0)$. Tämä vastaa Alicen lähettämää viestiä.

3.1.2 Salauksen turvallisuus

Koska p-adisessa selkäreppusalauksessa käytetään p-adista vähenevää lukujonoa η superkasvavan jonon sijaan, systeemi on turvallinen Shamir-hyökkäystä vastaan. Merklen ja Hellmanin selkäreppusysteemi voidaan murtaa helposti myös Luvussa 2.2 esitettyä LLL-algoritmia käyttämällä. Tarkastellaan nyt tarkemmin LLL-hyökkäystä ja sen onnistumista p-adiseen selkäreppusalaukseen.

Koska edellä kuvatussa salausmenetelmässä salattu viesti on muotoa

$$C = \sum_{i=1}^{n} x_i \beta_i,$$

ja alkiot $\beta_1, \beta_2, \ldots, \beta_n$ ovat julkisia, LLL-hyökkäys voidaan muodostaa, jos viesti C paljastuu. Selkäreppuongelman ratkaisemiseksi tulee löytää kongruenssiyhtälölle

$$x_1\beta_1 + x_2\beta_2 + \cdots + x_n\beta_n \equiv 0 \pmod{C}$$

ratkaisu $(x_1, x_2, \ldots, x_n) \in \mathbb{Z}^n$. Tällöin hyökkääjä muodostaa hilan konstruoinnissa käytettyä matriisia B_m vastaavan matriisin

$$C_m = \begin{pmatrix} -C & \beta_1 & \beta_2 & \ldots & \beta_n \\ 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \end{pmatrix}$$

ja saa LLL-algoritmilla redusoidun matriisin. Jos selkokielinen teksti x löytyy redusoidusta matriisista, hyökkäys onnistuu. Perustellaan tämä seuraavaksi.

Oletetaan, että selkäreppuongelmaan on ratkaisu $x = (x_1, x_2, \ldots, x_n) \in \mathbb{Z}^n$ ja asetetaan $y = (1, x_1, x_2, \ldots, x_n) \in \mathbb{Z}^{n+1}$. Tällöin matriisin C_m generoimaan hilaan täytyy kuulua vektori $C_m y$, joka on muotoa

$$C_m y = (-C + x_1\beta_1 + x_2\beta_2 + \cdots + x_n\beta_n, x_1, \ldots, x_n) = (0, x_1, x_2, \ldots, x_n).$$

Vastaava yhtälö voidaan myös kirjoittaa käyttämällä matriisien lohkomuotoja, jolloin saadaan

$$C_m y = \begin{pmatrix} -C_{1\times 1} & \beta_{1\times n} \\ 0_{n\times 1} & I_{n\times n} \end{pmatrix} \cdot \begin{pmatrix} 1_{1\times 1} \\ x_{n\times 1} \end{pmatrix} = \begin{pmatrix} 0_{1\times 1} \\ x_{n\times 1} \end{pmatrix}.$$

Käyttämällä LLL-algoritmia matriisiin C_m saadaan hilalle redusoidut kantavektorit. Näiden joukosta voidaan etsiä sopivaa muotoa oleva kantavektori, eli vektori jonka ensimmäinen koordinaatti on 0 ja loput kuuluvat salausmenetelmässä käytettävien viestialkioiden joukkoon. Tätä muotoa olevan vektorin euklidinen pituus on lyhyt hilan muihin vektoreihin verrattuna, joten

se hyökkäyksen onnistuessa se on yksi redusoidun matriisin sarakevektoreista [10].

Testaamalla hyökkäystä eri alkuluvuilla p ja hilan dimensioilla n satunnaisesti vaihteleviin viesteihin x ja laskemalla onnistumisprosentteja, on havaittu että p-adinen selkäreppu on turvallinen, kun hilan dimensio on vähintään 60. Vähenevän jonon η määrittämisen vuoksi systeemissä täytyy olettaa, että $m \geq n$, sillä tällöin epäyhtälö $|\eta_n|_p > p^{-m}$ toteutuu. Näin ollen myös approksimaatioasteen m tulee olla yli 60.

Esimerkki 3.3. Yritetään ratkaista Esimerkin 3.1.1 selkokielinen viesti x LLL-hyökkäyksellä. Nyt viestin pituus, eli luku $n = 3$, sekä salattu viesti $C = 45565$ ovat tiedossa. Muodostetaan viestin tarkoitetun vastaanottajan eli Bobin julkisen avaimen $\beta = (10225, 11780, 1550)$ avulla matriisi

$$C_m = \begin{pmatrix} -45565 & 10225 & 11780 & 1550 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Valitsemalla $\delta = 0,99$ ja käyttämällä LLL-algoritmia Sagessa, matriisi saadaan muotoon

$$C = \begin{pmatrix} 0 & -5 & -5 & -20 \\ 1 & 1 & 0 & -67 \\ 3 & -1 & 1 & 24 \\ 0 & 1 & -37 & -5 \end{pmatrix}.$$

Koska tiedetään, että viestin alkiot kuuluvat joukkoon $\{0, 1, 2, 3, 4\}^3$, selvästi matriisin kantavektorit c_2, c_3 ja c_4 eivät voi olla salattuja viestejä. Jäljelle jää siis vektori $c_1 = (0, 1, 3, 0)$. Kun ensimmäinen koordinaatti jätetään pois, saadaan salattu viesti $x = (1, 3, 0)$. Hyökkäys onnistuu helposti, sillä hilan dimensio on vain 4.

3.2 Toinen p-adinen selkäreppusalaus

Tässä luvussa esitellään edellisen p-adisen selkärepun toinen versio. Kuten edellisessä salausmenetelmässä, viestin vastaanottaja Bob valitsee itselleen salaisen alkuluvun p ja approksimaatioasteen m. Tässä systeemissä myös viestin lähettäjä Alice valitsee oman alkuluvun p_0, sekä approksimaatioasteen m_0. Systeemi eroaa edellisestä siinä, että viestin salaaminen ja avaaminen tapahtuvat näitä eri alkulukuja käyttämällä.

Bob laskee itselleen julkisen avaimen β samalla tavalla kuin Luvussa 3.1. Viestin lähettäjä Alice käyttää tätä avainta oman salaisen avaimensa luomiseen. Salaisen avaimen, sekä lukujen p_0 ja m_0 avulla Alice laskee vielä avaimen ρ, joka tarvitaan viestin avaamiseen. Tässä salausmenetelmässä viestin lähettäjällä on siis yksi avain enemmän edelliseen menetelmään verrattuna.

Alice salaa viestin muuten samalla tavalla kuin edellisessä salauksessa, mutta viestiin summataan vielä toinen komponentti lisätyn salaisen avaimen takia. Salaamisen jälkeen Alice lähettää Bobille viestin ja sen avaamiseen tarvittavat avaimet, viimeistä lukuunottamatta. Tässä menetelmässä viestin vastaanottajan täytyy ensin varmistaa lähettäjälle, että tämän valitsemat luvut p_0 ja m_0 ovat riittävän suuret vastaanottajan valitsemiin salaisiin avaimiin nähden. Jos näin on, Bob hyväksyy viestin ja Alice lähettää viimeisen tarvittavan avaimen ρ.

Viestin vastaanottaja Bob aloittaa salatun viestin avaamisen käyttämällä siihen avainta ρ. Tämän jälkeen viestin avaaminen tapahtuu samoja vaiheita toistamalla, kuin Luvussa 3.1. Koska tässä salausmenetelmässä Alice lähettää ensin salatun viestin ja vasta sen jälkeen avaimen ρ, Bob pystyy varmistamaan lähettäjän olleen juuri Alice. Jos viesti ja avain ρ eivät ole samalta lähettäjältä, Bob ei saa viestiä avattua. Samoin käy, jos Alice muuttaa avainta ρ viestin lähettämisen jälkeen. Bob ei saa viestiä avattua myöskään silloin, jos joku ulkopuolinen henkilö onnistuu muuttamaan salattua viestiä tai avainta ρ niiden lähettämisen jälkeen. Avainta ρ voi siis ajatella digitaalisena allekirjoituksena, joka varmistaa vastaanottajalle viestin lähettäjän henkilöllisyyden.

Tässä systeemissä käytetään Luvussa 2 esitettyä lineaarikuvausta salaisen vähenevän jonon η laskemiseen. Jonon voi laskea myös kuten edellisessä menetelmässä, eli p-adista logistista kuvausta käyttämällä. Vastaavasti muissakin kohdissa, joissa tässä salauksessa käytetään lineaarikuvausta, voitaisiin yhtä hyvin käyttää p-adista logistista kuvausta.

Kuten edellisessä salausmenetelmässä, myös tässä salattava viesti x kuuluu joukkoon $\{0, 1, 2, \ldots, K\}^n$, missä $K \leq p - 1$. Tämä joukko on tiedossa kaikilla menetelmää käyttävillä. Vastaava salausmenetelmä voitaisiin rakentaa myös ainoastaan binäärisille viesteille.

Viestin vastaanottajan avainten luominen

Bob valitsee ensin p-adisen kokonaisluvun ξ, jolla toteutuu $|\xi|_p = 1$ ja laskee

$$\eta_i = p^{i-1}\xi^i,$$

kun $i = 1, 2, \ldots, n$. Käyttämällä p-adisen itseisarvon ominaisuuksia, saadaan

$$|\eta_i|_p = |p^{i-1}\xi^i|_p = |p^{i-1}|_p|\xi|_p^i = |p^{i-1}|_p = p^{1-i}.$$

Tästä nähdään, että indeksin i kasvaessa p-adinen itseisarvo pienenee. Siis Bobin laskemalla p-adisella jonolla $\{\eta_1, \eta_2, \ldots, \eta_n\} \subset \mathbb{Z}_p$, toteutuu $|\eta_1|_p > |\eta_2|_p > \cdots > |\eta_n|_p$.

Epäyhtälöiden nojalla löytyy riittävän suuri positiivinen kokonaisluku m, jolla toteutuu $|\eta_n|_p > p^{-m}$. Bob laskee m-asteiset approksimaatiot luvuille η_i yhtälön (3) mukaisesti laskemalla summat

$$\eta_{i,m} = \sum_{k=0}^{m-1} x_{i,k}p^k,$$

kun $i = 1, 2, \ldots, n$. Kertoimet $x_{i,k}$ Bob saa laskettua Esimerkin 1.21 tavalla. Hän asettaa saadut approksimaatiot jonoksi $\eta := (\eta_{1,m}, \eta_{1,m}, \ldots, \eta_{n,m}) \in \mathbb{Z}^n$. Koska $|\eta_i|_p = |\eta_{i,m}|_p$ kaikilla $i = 1, 2, \ldots, n$, niin myös approksimaatioiden p-adisilla itseisarvoilla toteutuu $|\eta_{1,m}|_p > |\eta_{2,m}|_p > \cdots > |\eta_{n,m}|_p$.

Seuraavaksi Bob valitsee alkuluvun q siten, että $q > np^m$. Tätä lukua hän käyttää laskuissa modulona. Bob valitsee myös satunnaisen kokonaisluvun r siten, että $\text{syt}(p, r) = 1$ ja $rp^m > q$. Lopuksi Bob ratkaisee vielä luvun r käänteisalkion s kongruenssiyhtälöstä

$$sr \equiv 1 \pmod{q}.$$

Bobin salainen avain on (p, m, η, q, r, s).

Bob määrittää vielä oman julkisen avaimensa $\beta = (\beta_1, \beta_2, \ldots, \beta_n) \in \mathbb{Z}^n$ laskemalla

$$\beta_i \equiv r\eta_{i,m} \pmod{q}.$$

Viestin lähettäjän avainten luominen

Alice valitsee itselleen alkuluvun p_0 sekä approksimaatioasteen m_0 ja käyttää Bobin julkista avainta β oman salaisen avaimensa laskemiseen. Alice valitsee satunnaisesti joukosta $\{1, 2, \ldots, n\}$ luvun k_0 ja jonosta $\beta = (\beta_1, \beta_2, \ldots, \beta_n)$ sitä vastaavan alkion β_{k_0}. Alice asettaa $\xi_1 = \beta_{k_0}$ ja laskee

$$\xi_{i+1} = \xi^i,$$

kun $i = 1, 2, \ldots, n-1$. Näin laskemalla hän saa jonon $\xi = (\xi_1, \xi_2, \ldots, \xi_n) \in \mathbb{Z}_{p_0}^n$. Alice saa näille luvuille m_0-approksimaatiot laskemalla summat

$$\xi_{i,m_0} = \sum_{k=0}^{m_0-1} b_k p_0^k,$$

kun $i = 1, 2, \ldots, n$. Summassa olevat kertoimet b_k Alice saa kuten Esimerkissä 1.21. Approksimaatiot muodostavat jonon $\xi^{(m_0)} = (\xi_{1,m_0}, \xi_{2,m_0}, \ldots, \xi_{n,m_0})$, jonka avulla hän muodostaa matriisin

$$B_m = \begin{pmatrix} p_0^{m_0} & \xi_{1,m_0} & \xi_{2,m_0} & \ldots & \xi_{n,m_0} \\ 0 & -1 & 0 & \ldots & 0 \\ 0 & 0 & -1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & -1 \end{pmatrix}.$$

Käyttämällä tähän matriisiin LLL-algoritmia, Alice saa δ-LLL redusoidun matriisin B, josta salainen avain $a = (a_0, a_1, \ldots, a_n) \in \mathbb{Z}^{n+1}$ saadaan SAP:n ratkaisuna. Kun asetetaan $\xi_0 = \xi_{0,m_0} = 1$, saatu ratkaisu toteuttaa epäyhtälöt

$$\left| \sum_{i=0}^{n} a_i \xi_i \right|_{p_0} \leq p_0^{-m_0},$$
$$\max_{0 \leq i \leq n} |a_i| \leq p_0^{\frac{m_0}{n+1}} := K_0.$$

Koska $|\xi_i|_{p_0} = |\xi_{i,m_0}|_{p_0}$, kun $i = 0, 1, \ldots, n$, niin tällöin toteutuu myös

$$\left| \sum_{i=0}^{n} a_i \xi_{i,m_0} \right|_{p_0} \leq p_0^{-m_0}. \tag{5}$$

Seuraavaksi Alice määrittää itselleen salaisen avaimen $\sigma = (\sigma_0, \sigma_1, \ldots, \sigma_n)$ ja viestin avauksessa käytettävän avaimen $\rho = (\rho_0, \rho_1, \ldots, \rho_n)$. Näiden avainten laskemiseen Alice käyttää edellä ratkaisemaansa salaista avainta $a = (a_0, a_1, \ldots, a_n)$ ja valitsee satunnaiset kokonaisluvut σ_i ja ρ_i siten, että

$$a_i = \sigma_i + \rho_i,$$

missä $|\sigma_i|, |\rho_i| \leq K_0$ kaikilla $i = 0, 1, \ldots, n$. Alicen lähettämän viestin avaamiseen tarvittava avain on siis (p_0, m_0, k_0, ρ).

Salaus

Alice salaa selkokielisen viestin $x = (x_1, x_2, \ldots, x_n) \in \{0, 1, 2, \ldots, K\}^n$, missä $K \leq p - 1$ käyttämällä omaa salaista avaintaan σ ja jonoa $\xi^{(m_0)}$, sekä vastaanottajan julkista avainta β. Alice saa salakirjoituksen $C \in \mathbb{Z}$ laskemalla

$$C = \sum_{i=0}^{n} \sigma_i \xi_{i,m_0} + \sum_{i=1}^{n} x_i \beta_i.$$

Vaihe 1

Alice lähettää Bobille salatun viestin ja kolme ensimmäistä avaamiseen tarvittavaa avainta, eli (C, p_0, m_0, k_0). Bob tarkistaa, toteutuuko tällöin epäyhtälö $q < p_0^{m_0}$. Jos epäyhtälö toteutuu, Bob lähettää Alicelle luvun 0.

Jos epäyhtälö ei toteudu, Bob laskee $d = \min\{d' \in \mathbb{Z}_{>0} \mid q < p_0^{m_0+d'}\}$ ja lähettää Alicelle luvun d.

Vaihe 2

Jos Alice vastaanottaa luvun 0, hän lähettää Bobille viimeisen avaamiseen tarvittavan avaimen, eli jonon ρ.

Jos Alice vastaanottaa luvun $d \neq 0$, hän valitsee kaksi pientä positiivista kokonaislukua c_0 ja d_0 siten, että

$$p_0^{m_0+d} < (p_0 + c_0)^{m_0+d_0}$$

ja p_0+c_0 on alkuluku. Alice asettaa $p_1 = p_0+c_0$ ja $m_1 = m_0+d_0$ ja muodostaa itselleen uudet avaimet käyttämällä alkulukua p_1 ja approksimaatioastetta m_1. Alice laskee uuden salatun viestin C_1 ja lähettää Bobille (C_1, p_1, m_1, k_1).

Vaihe 3

Koska Alice valitsi uudet luvut siten, että $p_0^{m_0+d} < p_1^{m_1}$ ja Bob valitsi luvun d siten, että $q < p_0^{m_0+d}$, niin tällöin $q < p_1^{m_1}$ ja Alice vastaanottaa Bobilta luvun 0. Hän lähettää Bobille viimeisen avaamiseen tarvittavan avaimen, eli uuden jonon ρ'.

Avaus

Käsitellään tässä tilannetta, jossa viestin salaamisen vaihe 1 onnistuu, eikä Alicen tarvitse muodostaa avaimiaan uudelleen.

Käyttämällä Alicen lähettämiä avaimia (p_0, m_0, k_0, ρ), Bob laskee luvut ξ_{i,m_0} asettamalla ensin $\xi_1 = \beta_{k_0}$ ja laskemalla sitten

$$\xi_{i+1} = \xi^i$$

kaikilla $i = 1, 2, \ldots, n-1$. Näille luvuille hän saa m_0-asteiset approksimaatiot laskemalla summat

$$\xi_{i,m_0} = \sum_{k=0}^{m_0-1} b_k p_0^k,$$

kun $i = 1, 2, \ldots, n$. Summan kertoimet b_k Bob saa Esimerkin 1.21 tavalla. Näin laskemalla Bob saa saman jonon $\xi^{(m_0)}$, minkä Alice laski aiemmin. Seuraavaksi Bob käyttää avainta ρ ja laskee

$$C' := C + \sum_{i=0}^{n} \rho_i \xi_{i,m_0}.$$

Laskemalla näin, hän saa tosiasiassa

$$\begin{aligned} C + \sum_{i=0}^{n} \rho_i \xi_{i,m_0} &= \sum_{i=0}^{n} \sigma_i \xi_{i,m_0} + \sum_{i=1}^{n} x_i \beta_i + \sum_{i=0}^{n} \rho_i \xi_{i,m_0} \\ &= \sum_{i=0}^{n} (\sigma_i + \rho_i) \xi_{i,m_0} + \sum_{i=1}^{n} x_i \beta_i \\ &= \sum_{i=0}^{n} a_i \xi_{i,m_0} + \sum_{i=1}^{n} x_i \beta_i. \end{aligned}$$

Koska luvut a_i valittiin siten, että summalle

$$\sum_{i=0}^{n} a_i \xi_{i,m_0}$$

pätee epäyhtälö (5), niin summan p_0-adinen itseisarvo on enintään $p_0^{-m_0}$. Summa sisältää siis tekijänä vähintään alkuluvun p_0 potenssin m_0. Tällöin se voidaan kirjoittaa muodossa

$$\sum_{i=0}^{n} a_i \xi_{i,m_0} = p_0^{m_0} \cdot z,$$

missä $z \in \mathbb{Z}/\{0\}$. Tästä seuraa

$$\sum_{i=0}^{n} a_i \xi_{i,m_0} = p_0^{m_0} \cdot z \equiv 0 \pmod{p_0^{m_0}}.$$

Ottamalla luvusta C' modulon $p_0^{m_0}$ Bob saa täten

$$C' = \sum_{i=0}^{n} a_i \xi_{i,m_0} + \sum_{i=1}^{n} x_i \beta_i \equiv \sum_{i=1}^{n} x_i \beta_i := C'' \pmod{p_0^{m_0}}.$$

Bob käyttää seuraavaksi salaista avainta s ja laskee

$$C''' := sC'' \equiv \sum_{i=1}^{n} x_i \eta_{i,m} \pmod{q}.$$

Tämä pätee, koska

$$sC'' = \sum_{i=1}^{n} s x_i \beta_i = \sum_{i=1}^{n} s x_i r \eta_{i,m} \equiv \sum_{i=1}^{n} x_i \eta_{i,m} \pmod{q},$$

kun epäyhtälö $q < p_0^{m_0}$ toteutuu. Salatun viestin avaaminen tapahtuu samoja vaiheita toistamalla kuin Luvun 3.1 systeemissä.

Vaihe 1

Jos on olemassa $j_1 : 1 \leq j_1 \leq K$ siten, että $|C''' - j\eta_{1,m}|_p = |\eta_{1,m}|_p$ pätee kaikilla $j : 0 \leq j < j_1$, mutta ei päde kun $j = j_1$, niin $x_1 = j_1$. Muussa tapauksessa $x_1 = 0$.

Vaihe 2

Jos on olemassa $j_2 : 1 \leq j_2 \leq K$ siten, että $|C''' - x_1\eta_{1,m} - j\eta_{2,m}|_p = |\eta_{2,m}|_p$ pätee kaikilla $j : 0 \leq j < j_2$, mutta yhtälö ei päde kun $j = j_2$, niin $x_2 = j_2$. Muussa tapauksessa $x_2 = 0$.

$\vdots$

Vaihe n

Jos on olemassa $j_n : 1 \leq j_n \leq K$ siten, että $|C''' - (x_1\eta_{1,m} + x_2\eta_{2,m} + \cdots + x_{n-1}\eta_{n-1,m}) - j\eta_{n,m}|_p = |\eta_{n,m}|_p$ pätee kaikilla $j : 0 \leq j < j_n$, mutta yhtälö ei päde kun $j = j_n$, niin $x_n = j_n$. Muussa tapauksessa $x_n = 0$.

3.2.1 Esimerkki

Salataan ja avataan viesti edellä esitettyä salausmenetelmää käyttämällä. Laskuissa käytetään avoimen lähdekoodin ohjelmaa Sagea.

Viestin vastaanottajan avainten luominen

Bob valitsee omaksi alkuluvukseen $p = 5$ ja salattavien viestien pituudeksi $n = 4$. Viestin alkioiden ylärajaksi hän valitsee $K = 3$. Tässä esimerkissä salattava viesti x kuuluu siis joukkoon $\{0, 1, 2, 3\}^4$, joka on tiedossa kaikilla systeemiä käyttävillä.

Bob valitsee 5-adisen kokonaisluvun $\xi = \frac{1}{4}$, jolla toteutuu $|\xi|_5 = 1$. Käyttämällä tätä, hän laskee

$$\begin{aligned}
\eta_1 &= \xi = \frac{1}{4}, \\
\eta_2 &= p \cdot \xi^2 = 5 \cdot \left(\frac{1}{4}\right)^2 = \frac{5}{16}, \\
\eta_3 &= p^2 \cdot \xi^3 = 5^2 \cdot \left(\frac{1}{4}\right)^3 = \frac{25}{64}, \\
\eta_4 &= p^3 \cdot \xi^4 = 5^3 \cdot \left(\frac{1}{4}\right)^4 = \frac{125}{256}.
\end{aligned}$$

Koska

$$|\eta_4|_5 = \left|\frac{125}{256}\right|_5 = \left|5^3 \cdot \frac{1}{256}\right|_5 = 5^{-3},$$

niin Bob valitsee approksimaatioasteeksi $m = 4$. Tällöin toteutuu $|\eta_4| > 5^{-m}$. Bob laskee luvuille η_1, η_2, η_3 ja η_4 4-asteiset approksimaatiot laskemalla summat

$$\eta_{i,4} = \sum_{k=0}^{3} x_{i,k} 5^k,$$

kun $i = 1, 2, 3, 4$. Näin laskemalla hän saa

$$\begin{aligned}
\eta_{1,4} &= 4 + 3 \cdot 5 + 3 \cdot 5^2 + 3 \cdot 5^3 = 469, \\
\eta_{2,4} &= 5 + 2 \cdot 5^2 + 3 \cdot 5^3 = 430, \\
\eta_{3,4} &= 4 \cdot 5^2 + 5^3 = 225, \\
\eta_{4,4} &= 5^3 = 125
\end{aligned}$$

ja asettaa $\eta = \{\eta_{1,4}, \eta_{2,4}, \eta_{3,4}, \eta_{4,4}\} = \{469, 430, 225, 125\}$. Kuten approksimaatioiden potenssiesityksistä nähdään, niiden 5-adisilla itseisarvoilla toteutuu

$$|\eta_{1,4}|_5 > |\eta_{2,4}|_5 > |\eta_{3,4}|_5 > |\eta_{3,4}|_5.$$

Seuraavaksi Bob laskee $np^m = 4{\cdot}5^4 = 2500$ ja valitsee alkuluvun $q = 2549$. Tällöin ehto $q > np^m$ toteutuu. Bob tarvitsee lisäksi satunnaisen kokonaisluvun r siten, että $\text{syt}(p, r) = 1$ ja $rp^m > q$. Hän valitsee $r = 19$, jolloin $\text{syt}(5, 19) = 1$ ja $rp^m = 19 \cdot 5^4 = 11875 > q$. Bob ratkaisee vielä luvulle r käänteisalkion s kongruenssiyhtälöstä

$$s \cdot 19 \equiv 1 \pmod{2549}.$$

Kongruenssiyhtälön ratkaisuna Bob saa $s = 805$. Hänen salainen avaimensa on näin ollen $(p, m, \eta, q, r, s) = (5, 4, \{469, 430, 225, 125\}, 2549, 19, 805)$.

Bob saa itselleen julkisen avaimen $\beta = (\beta_1, \beta_2, \beta_3, \beta_4) \in \mathbb{Z}^4$ laskemalla

$$\begin{aligned}
\beta_1 &= r\eta_{1,4} = 19 \cdot 469 = 8911 \equiv 1264 && \pmod{2549},\\
\beta_2 &= r\eta_{2,4} = 19 \cdot 430 = 8170 \equiv 523 && \pmod{2549},\\
\beta_3 &= r\eta_{3,4} = 19 \cdot 225 = 4275 \equiv 1726 && \pmod{2549},\\
\beta_4 &= r\eta_{4,4} = 19 \cdot 125 = 2375 && \pmod{2549}.
\end{aligned}$$

Siis Bobin julkinen avain on $\beta = (1264, 523, 1726, 2375)$.

Viestin lähettäjän avainten luominen

Alice valitsee omaksi alkuluvukseen $p_0 = 3$ ja approksimaatioasteeksi $m_0 = 8$. Hän valitsee Bobin julkisesta avaimesta $\beta = (1264, 523, 1726, 2375)$ satunnaisesti komponentin $\beta_2 = 523$, jolloin $k_0 = 2$. Käyttämällä lukuun β_2 lineaarista kuvausta Alice saa

$$\begin{aligned}
\xi_1 &= \beta_2 = 523,\\
\xi_2 &= \beta_2^2 = 523^2 = 273529,\\
\xi_3 &= \beta_2^3 = 523^3 = 143055667,\\
\xi_4 &= \beta_2^4 = 523^4 = 74818113841.
\end{aligned}$$

Alice laskee näille luvuille 8-asteiset approksimaatiot

$$\begin{aligned}
\xi_{1,8} &= 1 + 3^2 + 3^3 + 2 \cdot 3^5 = 523,\\
\xi_{2,8} &= 1 + 2 \cdot 3^2 + 2 \cdot 3^3 + 3^4 + 2 \cdot 3^7 = 4528,\\
\xi_{3,8} &= 1 + 3^3 + 3^4 + 3^5 + 2 \cdot 3^6 + 2 \cdot 3^7 = 6184,\\
\xi_{4,8} &= 1 + 3^2 + 2 \cdot 3^3 + 3^4 + 3^5 + 2 \cdot 3^6 + 2 \cdot 3^7 = 6220
\end{aligned}$$

ja saa approksimaatiojonon $\xi^{(8)} = (523, 4528, 6184, 6220)$. Hän laskee seuraavaksi

$$p_0^{m_0} = 3^8 = 6561$$

ja muodostaa approksimaatioita ja tätä lukua käyttämällä matriisin

$$B_8 = \begin{pmatrix} 6561 & 523 & 4528 & 6184 & 6220 \\ 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & -1 \end{pmatrix}.$$

Tämän matriisin pystyvektorit ovat hilan Γ_8 kanta. Alice valitsee $\delta = 0,99$ ja käyttää kantavektoreihin LLL-algoritmia Sagessa. Hän saa näin matriisin

$$B = \begin{pmatrix} 2 & 0 & -2 & 1 & -8 \\ 1 & 2 & -3 & 5 & 7 \\ 1 & 1 & -4 & -5 & 2 \\ -4 & 1 & 0 & 0 & -2 \\ 0 & -4 & 0 & -1 & 1 \end{pmatrix}$$

ja selvittää siitä SAP:n ratkaisun $a = (a_0, a_1, a_2, a_3, a_4)$. Ratkaisun täytyy toteuttaa ehdot

$$|a_0\xi_{0,8} + a_1\xi_{1,8} + \cdots + a_4\xi_{4,8}|_3 \leq 3^{-8} \text{ ja } |a_i| \leq K_0,$$

missä $K_0 = p_0^{m_0/n+1} = 3^{8/5} \approx 5,799\ldots$ ja $\xi_{0,8} = 1$. Alice valitsee $a = (2, 1, 1, -4, 0)$, jolloin $|a_i| \leq K_0$ kaikilla $i = 0, 1, 2, 3, 4$. Tällöin

$$\begin{aligned} \left|\sum_{i=0}^{4} a_i\xi_{i,8}\right|_3 &= |2 \cdot 1 + 1 \cdot 523 + 1 \cdot 4528 - 4 \cdot 6184 + 0 \cdot 6220|_3 \\ &= |-19683|_3 = |-3^9|_3 = 3^{-9} < 3^{-8}. \end{aligned}$$

Näin ollen ehdot toteutuvat ja vektori a on SAP:n ratkaisu.

Alice valitsee seuraavaksi avaimen σ alkiot satunnaisesti väliltä $[-5, 5]$. Hän valitsee $\sigma = (4, 0, 2, 1, -3)$ ja määrittää viestin avaamisessa tarvittavan avaimen ρ alkiot laskemalla $\rho_i = a_i - \sigma_i$ kun $i = 0, 1, 2, 3, 4$. Näin Alice saa $\rho = (-2, 1, -1, -5, 3)$, missä alkiot kuuluvat välille $[-5, 5]$.

Alicen lähettämän viestin avaamiseen tarvitan täten avaimet $(p_0, m_0, k_0, \rho) = (3, 8, 2, (-2, 1, -1, -5, 3))$.

Viestin salaus

Alice haluaa lähettää Bobille viestin $x = (2, 3, 0, 1)$. Alice käyttää Bobin julkista avainta $\beta = (1264, 523, 1726, 2375)$ ja salaa viestin laskemalla

$$\begin{aligned} C =& \sum_{i=0}^{4} \sigma_i \xi_{i,8} + \sum_{i=1}^{4} x_i \beta_i \\ =& 4 \cdot 1 + 0 \cdot 523 + 2 \cdot 4528 + 1 \cdot 6184 - 3 \cdot 6220 \\ & + 2 \cdot 1264 + 3 \cdot 523 + 0 \cdot 1726 + 1 \cdot 2375 \\ =& 3056. \end{aligned}$$

Alice lähettää Bobille $(C, p_0, m_0, k_0) = (3056, 3, 8, 2)$ ja Bob tarkistaa toteutuuko epäyhtälö $p_0^{m_0} > q$ näillä luvuilla. Koska

$$p_0^{m_0} = 3^8 = 6561,$$

ja $q = 2549$, epäyhtälö toteutuu ja Bob lähettää Alicelle viestin 0.

Alice vastaanottaa viestin 0 ja lähettää Bobille viimeisen viestin avaamiseen tarvittavan avaimen $\rho = (-2, 1, -1, -5, 3)$.

Viestin avaus

Nyt Bobilla on tiedossa kaikki viestin C avaamiseen tarvittavat avaimet. Koska $k_0 = 2$, hän aloittaa approksimaatiojonon $\xi^{(8)}$ laskemisen alkuarvosta $\beta_2 = 523$. Bob käyttää tähän lukuun lineaarikuvausta $\xi_i = \xi^i$ ja laskee

$$\begin{aligned} \xi_1 &= \beta_2 = 523, \\ \xi_2 &= \beta_2^2 = 523^2 = 273529, \\ \xi_3 &= \beta_2^3 = 523^3 = 143055667, \\ \xi_4 &= \beta_2^4 = 523^4 = 74818113841. \end{aligned}$$

Bob laskee näille luvuille 8-asteiset approksimaatiot

$$\begin{aligned}
\xi_{1,8} &= 1 + 3^2 + 3^3 + 2 \cdot 3^5 = 523, \\
\xi_{2,8} &= 1 + 2 \cdot 3^2 + 2 \cdot 3^3 + 3^4 + 2 \cdot 3^7 = 4528, \\
\xi_{3,8} &= 1 + 3^3 + 3^4 + 3^5 + 2 \cdot 3^6 + 2 \cdot 3^7 = 6184, \\
\xi_{4,8} &= 1 + 3^2 + 2 \cdot 3^3 + 3^4 + 3^5 + 2 \cdot 3^6 + 2 \cdot 3^7 = 6220
\end{aligned}$$

ja saa jonon $\xi^{(8)} = (523, 4528, 6184, 6220)$. Tämä on sama jono, jota Alice käytti viestin salaamiseen. Bob laskee tätä jonoa käyttämällä

$$\begin{aligned}
C' &:= C + \sum_{i=0}^{4} \rho_i \xi_{i,m_0} \\
&= 3056 - 2 \cdot 1 + 1 \cdot 523 - 1 \cdot 4528 - 5 \cdot 6184 + 3 \cdot 6220 \\
&= -13211
\end{aligned}$$

Koska

$$C' = -13211 \equiv 6472 \pmod{6561},$$

niin Bob saa $C'' = 6472$. Salaista avaintaan s käyttämällä hän laskee

$$C''' \equiv C''s = 6472 \cdot 805 = 5209960 \equiv 2353 \pmod{2549}.$$

Bob käyttää viestin avaamiseen salaista vähenevää jonoa $\{\eta_{1,8}, \eta_{2,8}, \eta_{3,8}, \eta_{4,8}\} = \{469, 430, 225, 125\}$. Koska alussa valittiin viestin alkioiden ylärajaksi $K = 3$, niin seuraavissa laskuissa $j = 0, 1, 2, 3$.

Bob avaa viestin ensimmäisen alkion x_1 laskemalla 5-adisia itseisarvoja $|C''' - j\eta_{1,8}|_5$, kun $j = 0, 1, 2, 3$ ja vertaamalla näitä lukuun $|\eta_{1,8}|_5$. Nyt $|\eta_{1,8}|_5 = |469|_5 = 1$, jolloin

$$\begin{aligned}
|C''' - 0 \cdot \eta_{1,8}|_5 &= |2353|_5 = 1 = |\eta_{1,8}|_5, \\
|C''' - 1 \cdot \eta_{1,8}|_5 &= |2353 - 469|_5 = |1884|_5 = 1 = |\eta_{1,8}|_5, \\
|C''' - 2 \cdot \eta_{1,8}|_5 &= |2353 - 2 \cdot 469|_5 = |1415|_5 = 5^{-1} \neq |\eta_{1,8}|_5.
\end{aligned}$$

Laskeminen lopetetaan tähän, koska saatiin erisuuruus. Koska yhtälö $|C''' - j\eta_{1,8}|_5 = |\eta_{1,8}|_5$ toteutuu kun $j = 0$ tai 1, mutta ei toteudu, kun $j = 2$, niin $x_1 = 2$.

Seuraavaksi Bob avaa viestin toisen alkion x_2. Nyt $|\eta_{2,8}|_5 = |430|_5 = 5^{-1}$. Hän laskee 5-adisia itseisarvoja $|C''' - x_1\eta_{1,8} - j\eta_{2,8}|_5$, kun $j = 0, 1, 2, 3$ ja vertaa näitä lukuun $|\eta_{2,8}|_5$, jolloin

$$\begin{aligned}
|C''' - x_1\eta_{1,4} - 0 \cdot \eta_{2,4}|_5 &= |2353 - 2 \cdot 469|_5 = |1415|_5 = 5^{-1} = |\eta_{2,8}|_5, \\
|C''' - x_1\eta_{1,4} - 1 \cdot \eta_{2,4}|_5 &= |2353 - 2 \cdot 469 - 430|_5 = |985|_5 = 5^{-1} = |\eta_{2,8}|_5, \\
|C''' - x_1\eta_{1,4} - 2 \cdot \eta_{2,4}|_5 &= |2353 - 2 \cdot 469 - 2 \cdot 430|_5 = |555|_5 = 5^{-1} = |\eta_{2,8}|_5, \\
|C''' - x_1\eta_{1,4} - 3 \cdot \eta_{2,4}|_5 &= |2353 - 2 \cdot 469 - 3 \cdot 430|_5 = |125|_5 = 5^{-3} \neq |\eta_{2,8}|_5.
\end{aligned}$$

Koska nyt yhtälö $|C''' - x_1\eta_{1,4} - j\eta_{2,4}|_5 = |\eta_{2,8}|_5$ toteutuu, kun $j = 0, 1, 2$, mutta ei toteudu kun $j = 3$, niin $x_2 = 3$.

Bob avaa viestin kolmannen alkion laskemalla 5-adisia itseisarvoja $|C''' - (x_1\eta_{1,8} + x_2\eta_{2,8}) - j\eta_{3,8}|_5$, kun $j = 0, 1, 2, 3$. Nyt $|\eta_{3,8}|_5 = |225|_5 = 5^{-2}$ ja hän laskee

$$\begin{aligned} |C''' - (x_1\eta_{1,8} + x_2\eta_{2,8}) - 0 \cdot \eta_{3,8}|_5 &= |2353 - (2 \cdot 469 + 3 \cdot 430)|_5 \\ &= |125|_5 = 5^{-3} \neq |\eta_{3,4}|_5. \end{aligned}$$

Koska yhtälö ei toteudu, kun $j = 0$, niin B saa $x_3 = 0$.

Bob avaa lopuksi viestin viimeisen alkion x_4 laskemalla 5-adisia itseisarvoja $|C''' - (x_1\eta_{1,8} + x_2\eta_{2,8} + x_3\eta_{3,8}) - j\eta_{4,8}|_5$, kun $j = 0, 1, 2, 3$. Nyt $|\eta_{4,8}|_5 = |125|_5 = 5^{-3}$ ja Bob laskee

$$\begin{aligned} |C''' - (x_1\eta_{1,8} + x_2\eta_{2,8} + x_3\eta_{3,8}) - 0 \cdot \eta_{4,8}|_5 &= |2353 - (2 \cdot 469 + 3 \cdot 430)|_5 \\ &= |125|_5 = 5^{-3} = |\eta_{4,8}|_5, \\ |C''' - (x_1\eta_{1,8} + x_2\eta_{2,8} + x_3\eta_{3,8}) - 1 \cdot \eta_{4,8}|_5 &= |2353 - (2 \cdot 469 + 3 \cdot 430) - 125|_5 \\ &= |0|_5 = 0 \neq |\eta_{4,8}|_5. \end{aligned}$$

Koska yhtälö toteutuu, kun $j = 0$, mutta ei toteudu, kun $j = 1$, niin Bob saa $x_4 = 1$. Avattu viesti on siis $x = (2, 3, 0, 1)$, mikä vastaa Alicen lähettämää viestiä.

3.2.2 Salauksen turvallisuus

Kuten luvussa 3.1.2 todettiin, ensimmäisenä esitelty p-adinen selkäreppusalaus on turvallinen LLL-hyökkäyksiä vastaan riittävän suurilla hilan dimensioilla. On kuitenkin myös olemassa LLL-hyökkäystä kehittyneempiä algoritmeja, joita vastaan tämä systeemi ei välttämättä ole turvallinen korkeallakaan dimensiolla. Luvun 3.2 salausmenetelmään lisätty avain ρ tuo lisää turvallisuutta sekä LLL-hyökkäyksiä, että sitä kehittyneempiä algoritmeja vastaan. Esitellään tässä kaksi LLL-hyökkäystä, joilla tämän salausmenetelmän voi yrittää murtaa.

Tarkastellaan ensin tilannetta, jossa jollekin salakuuntelijalle paljastuu lähetetty vektori (C, p_0, m_0, k_0). Hyökkääjä pystyy tällöin laskemaan hilalle kannan $\xi^{(m_0)} = (\xi_{1,m_0}, \xi_{2,m_0}, \ldots, \xi_{n,m_0})$ käyttämällä Bobin julkisen avaimen β alkiota β_{k_0} ja lineaarikuvausta $\xi_i = \xi^i$.

Jos hyökkääjä tietää lisäksi lähetetyn selkokielisen viestin x, hän voi laskea

$$D := C - \sum_{i=1}^{n} x_i\beta_i = \sum_{i=0}^{n} \sigma_i\xi_{i,m_0}$$

ja yrittää löytää ratkaisun $(\sigma_0, \sigma_1, \ldots, \sigma_n)$ selkäreppuongelmaan

$$\sigma_1\xi_{1,m_0} + \sigma_1\xi_{2,m_0} + \cdots + \sigma_n\xi_{n,m_0} \equiv 0 \pmod{D}.$$

Käyttämällä LLL-algoritmia matriisiin

$$B_D = \begin{pmatrix} -D & \xi_{1,m_0} & \xi_{2,m_0} & \ldots & \xi_{n,m_0} \\ 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \end{pmatrix},$$

hyökkääjä saa redusoidun matriisin, josta avain σ löytyy, jos hyökkäys onnistuu.

Toinen mahdollisuus on se, että hyökkääjälle paljastuu viestivektorin lisäksi lähettäjän salainen avain ρ. Tällöin hän voi laskea

$$C' = C + \sum_{i=0}^{n} \rho_i\xi_{i,m_0}.$$

Laskemalla tälle luvulle kongruenssin modulo $p_0^{m_0}$, hyökkääjä saa selville

$$C'' = \sum_{i=1}^{n} x_i\beta_i,$$

mikä vastaa luvun 3.1.2 tilannetta. Näin ollen hyökkääjä voi käyttää LLL-algoritmia matriisiin

$$B_C = \begin{pmatrix} -C & \beta_1 & \beta_2 & \ldots & \beta_n \\ 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \end{pmatrix},$$

josta viesti x löytyy, jos hyökkäys onnistuu. Ratkaistuaan viestin x, hyökkääjä saa selvitettyä myös salaisen avaimen σ suorittamalla edeltävän hyökkäyksen, eli käyttämällä LLL-algoritmia matriisiin B_D. Jos hyökkääjä saa onnistuneesti avaimen σ selvitettyä, hän saa myös salaisen avaimen a laskettua, sillä $a_i = \sigma_i + \rho_i$ kaikilla $i = 0, 1, 2, \ldots, n$.

Kuten aiemman salauksen tapauksessa, nämäkin LLL-hyökkäykset vaikeutuvat hilan dimension kasvaessa. Salausmenetelmän turvallisuuden kannalta on siis olennaista valita riittävän suuri dimensio. Myös tälle salausmenetelmälle turvallisuuden rajana pidetään hilan dimensiota 60. Koska hilan dimension kasvattaminen pidentää myös salaisten avainten pituutta, ne voidaan laskujen helpottamiseksi konstruoida sopivan pienissä ositetuissa hiloissa.

On huomattava, että edelliseen salaukseen verrattuna tässä esitetyt LLL-hyökkäykset vaativat pienilläkin dimensioilla onnistuakseen tiedon joko lähetetystä viestistä x tai salaisesta avaimesta ρ. Pelkkä viestin (C, p_0, m_0, k_0) paljastuminen ei tässä menetelmässä riitä onnistuneeseen LLL-hyökkäyksen, toisin kuin edellisen salauksen tapauksessa.

Oletetaan nyt, että salattu viesti x ja avain ρ pysyvät salassa, mutta vektori (C, p_0, m_0, k_0) paljastuu. Koska tiedetään, että tällöin täytyy päteä $q < p_0^{m_0}$, niin hyökkääjä voi yrittää viestin C ensimmäiseen komponenttiin brute-force -hyökkäystä ja näin pyrkiä selvittämään avaimen ρ. Tällöin hyökkääjä laskee ensin $K = p_0^{m_0/n+1}$ ja asettaa kokonaisluvut $d_0, d_1, \ldots, d_n$ siten, että $|d_i| \leq K$ kaikilla $i = 0, 1, \ldots, n$. Tämän jälkeen hän laskee

$$\begin{aligned} C_0 &= C + \sum_{i=0}^{n} d_i \xi_{i,m_0}, \\ C_1 &\equiv C_0 \pmod{p_0^{m_0}}. \end{aligned}$$

Käytännössä ylempi yhtälö on tällöin muotoa

$$\begin{aligned} C_0 = C + \sum_{i=0}^{n} d_i \xi_{i,m_0} &= \sum_{i=0}^{n} \sigma_i \xi_{i,m_0} + \sum_{i=1}^{n} x_i \beta_i + \sum_{i=0}^{n} d_i \xi_{i,m_0} \\ &= \sum_{i=0}^{n} (\sigma_i + d_i) \xi_{i,m_0} + \sum_{i=1}^{n} x_i \beta_i. \end{aligned}$$

Hyökkääjä arvioi seuraavaksi erotusta $C_2 := C_0 - C_1$. Jos $C_2 \sim p_0^{m_0}$, niin hyökkäys onnistuu. Tämä seuraa siitä, että jos hyökkääjä onnistui valitsemaan luvut d_i siten, että $d_i = a_i - \sigma_i$, niin

$$C_0 = \sum_{i=0}^{n} (\sigma_i + d_i) \xi_{i,m_0} + \sum_{i=1}^{n} x_i \beta_i \equiv \sum_{i=1}^{n} x_i \beta_i \pmod{p_0^{m_0}}$$

epäyhtälön (5) nojalla. Tällöin erotus $C_2 := C_0 - C_1$ on

$$C_2 = C_0 - C_1 = \sum_{i=0}^{n} (\sigma_i + d_i) \xi_{i,m_0} + \sum_{i=1}^{n} x_i \beta_i - \sum_{i=1}^{n} x_i \beta_i = \sum_{i=0}^{n} (\sigma_i + d_i) \xi_{i,m_0},$$

josta seuraa $C_2 \sim p_0^{m_0}$. Hyökkäystä voi kuitenkin joutua toistamaan jopa K^n kertaa ennen onnistumista, joten se ei ole erityisen tehokas lukujen K ja n kasvaessa.

Lähdeluettelo

[1] G. Bachman: *Introduction to p-adic numbers and valuation theory.* Academic Press Inc., New York, 1964.

[2] J. Hoffstein, J. Pipher, J. H. Silverman: *An Introduction to Mathematical Cryptography.* Springer, New York, 2014.

[3] H. Inoue, S. Kamada, K. Naito: *Simultaneous Approximation Problems of p-Adic Numbers and p-Adic Knapsack Cryptosystems - Alice in p-Adic Numberland.* p-Adic Numbers, Ultrametric Analysis and Applications, 2016, Vol. 8, No. 4, pp. 312–324.

[4] S. Kamada, K. Naito: *Shortest vector problems of p-adic random lattices and their application to a p-adic knapsack type cryptosystem.* Journal of Nonlinear and Convex Analysis, 2018, Vol. 19, No. 9, pp.1587-1597.

[5] S. Kamada, K. Naito: *Simultaneous approximation problems and knapsack cryptosystems with commitment schemes in p-adic numberlands.* Journal of Nonlinear and Convex Analysis, 2018, Vol. 19, No. 9, pp.1599-1608.

[6] R. Merkle, M. Hellman, *Hiding information and signature in trapdoor knapsacks*, IEEE Transactions on Information Theory, 1978, Vol. 24, no. 5, pp. 525-530.

[7] J. Pettigrew, J. A. G. Roberts, F. Vivaldi, *Complexity of regular invertible p-adic motions*, Chaos: An Interdisciplinary Journal of Nonlinear Science, 2001, Vol. 11, pp. 849–857.

[8] A. Shamir *A polynomial-time algorithm for breaking the basic Merkle - Hellman cryptosystem*, IEEE Transactions on Information Theory, 1984, Vol. 30, no. 5, pp. 699-704.

[9] N. P. Smart, C. F. Woodcock, *p-adic chaos and random number generation*, Experimental Mathematics, 1998, Vol.7, No. 4, pp. 333–342.

[10] M. Stamp, R. M. Low, *Applied Cryptanalysis: Breaking Ciphers in the Real World.* Wiley, New Jersey, 2007.

[11] B. M. M. De Weger: *Approximation Lattices of p-adic Numbers.* Journal of Number Theory, 1986, Vol.24 , pp.70-88.