JYVÄSKYLÄN YLIOPISTO
MATEMATIIKAN JA TILASTO-
TIETEEN LAITOS

Pro gradu-tutkielma

Lineaariset Diofantoksen yhtälöryhmät

Miro Seppänen

15. helmikuuta 2024

Tekijä
Miro Seppänen

Otsikko
Lineaariset Diofantoksen
yhtälöryhmät (engl. Diophantine system of linear equations)

Tutkinto-ohjelma
Matematiikan aineenopettajan maisteriohjelma

Päivämäärä	**Sivumäärä**
15. helmikuuta 2024	45

Tiivistelmä

Tämä pro gradu -tutkielma käsittelee lineaarisia Diofantoksen yhtälöryhmiä. Tällä tarkoitetaan, että ratkaistavana on samanaikaisesti useampia lineaarisia kokonaislukukertoimisia yhtälöitä, joille etsitään kokonaislukuratkaisua. Diofantoksen yhtälöt ovat yleisesti laajempi kokonaisuus, josta lineaariset Diofantoksen yhtälöryhmät ovat erikoistapaus. Kokonaislukukertoimiset yhtälöt ovat saaneet nimekseen Diofantoksen yhtälöt kreikkalaisen matemaatikon Diofantos Aleksandrialaisen mukaan.

Pro gradu -tutkielman lähtökohtina toimivat lukion matematiikasta tutut lineaarinen yhtälöryhmä sekä Diofantoksen yhtälö. Lukion oppikirjoissa nämä kaksi aihetta esitetään erillään ja ovat toisistaan selvästi eroavia aiheita. Tässä tutkielmassa yhdistetään nämä kaksi aihetta yhdeksi kokonaisuudeksi lineaarisiksi Diofantoksen yhtälöryhmiksi. Lineaarisille Diofantoksen yhtälöryhmille esitetään tutkielmassa tuloksia, joita vertaillaan lineaarisen yhtälöryhmien sekä Diofantoksen yhtälöiden vastaaviin tuloksiin.

Lineaarisen yhtälöryhmän ja lineaaristen Diofantoksen yhtälöryhmien välillä esitetään niiden samankaltaisuus ratkaisujoukon kohdalla. Ratkaisujoukot pitävät sisällään yhtälöryhmän yksittäisratkaisun sekä yhtälöryhmän homogeenisen osan ratkaisun. Lineaarisen yhtälöryhmän kohdalla ratkaisujoukon homogeenista osaa kutsutaan lineaariavaruudeksi ja lineaaristen Diofantoksen yhtälöryhmien kohdalla hilaksi.

Lineaaristen Diofantoksen yhtälöryhmien ja Diofantoksen yhtälöiden kohdalla samankaltaisuutta löydetään ratkaisumenetelmistä. Molemmissa ratkaisumenetelmissä Eukleideen algoritmi on merkittävässä osassa. Diofantoksen yhtälöiden tapauksessa Eukleideen algoritmia suoritetaan pääsääntöisesti algebrallisesti, kun taas lineaaristen Diofantoksen yhtälöryhmien tapauksessa Eukleideen algoritmi on piilotettuna matriisikertolaskuun. Tutkielmassa

kuitenkin osoitetaan, että itse asiassa algoritmit hyödyntävät Eukleideen algoritmia samalla tavalla.

Lineaaristen Diofantoksen yhtälöryhmien ratkaisemista varten pro gradu -tutkielmassa tärkeimpinä sisältöinä toimivat Smithin normaalimuoto ja Siegelin lemma. Smithin normaalimuodon avulla lineaarinen Diofantoksen yhtälöryhmä voidaan muuttaa ekvivalenttiin muotoon yksinkertaisemman lineaarisen Diofantoksen yhtälöryhmän kanssa, josta sen ratkaiseminen on yksinkertaisempaa. Siegelin lemma taas antaa arviota lineaarisen Diofantoksen yhtälöryhmän homogeeniselle osalle. Lemman avulla homogeenisen osan ratkaisun koolle pystytään antamaan arvio.

Tutkielman lopuksi lineaarisia Diofantoksen yhtälöryhmiä tutkitaan opetuksen näkökulmasta. Diofantoksen yhtälöiden ratkaisumenetelmiä sekä esitystapoja lukion oppikirjoissa vertaillaan tämän tutkielman ratkaisumenetelmiin ja esitystapoihin. Vertailussa pyritään löytämään yhtäläisyyksiä sekä eroavaisuuksia. Lisäksi aivan tutkielman viimeisenä asiana pohditaan, miten Diofantoksen yhtälöiden opettamista voitaisiin kehittää kouluissa. Pohdinnoissa mietitään muun muassa, miten koulussa Diofantoksen yhtälöiden avulla voitaisiin luoda syvempää ymmärrystä lineaarisiin yhtälöryhmiin.

Sisällys

Johdanto

Tämä pro gradu -tutkielma käsittelee lineaarisia Diofantoksen yhtälöryhmiä. Lineaariset Diofantoksen yhtälöryhmät ovat erikoistapaus Diofantoksen yhtälöistä ja niille etsitään kokonaislukuratkaisuja. Diofantoksen yhtälöt on nimetty kreikkalaisen matemaatikon Diofantos Aleksandrialaisen mukaan, joka eli 250 jKr. Yksinkertaisin muoto Diofantoksen yhtälöistä on lineaarinen kahden tuntemattoman muuttujan Diofantoksen yhtälö, joka on muotoa

$$ax + by = c,$$

missä $a, b, c \in \mathbb{Z}$. Diofantoksen kirjoittama Arithmetica-kirja on toiminut myöhemmin lähtökohtana monille lukuteoreetikoille [11].

Pro gradu -tutkielman lähtökohtina ovat lukiosta tutut lineaarinen yhtälöryhmä sekä Diofantoksen yhtälö. Lukion oppikirjoissa nämä kaksi asiaa esitetään hyvin pitkälti toisistaan poikkeavina ja toisistaan erillään. Tämän tutkielman tarkoituksena on yhdistää nämä kaksi aihetta yhdeksi kokonaisuudeksi, lineaarisiksi Diofantoksen yhtälöryhmiksi. Lineaarisiin Diofantoksen yhtälöryhmiin liittyviä tuloksia vertaillaan lineaarista yhtälöryhmää sekä Diofantoksen yhtälöä koskeviin tuloksiin.

Lineaarisen yhtälöryhmän ja lineaaristen Diofantoksen yhtälöryhmien välillä esitetään niiden samankaltaisuus ratkaisujoukon osalta. Lineaarisen yhtälöryhmän kohdalla ratkaisujoukon homogeeninen osa on lineaariavaruus ja lineaaristen Diofantoksen yhtälöryhmien kohdalla hila. Lineaariavaruuden ja hilan rakenne koitetaan osoittaa yhtäläiseksi. Lineaaristen Diofantoksen yhtälöryhmien ja Diofantoksen yhtälöiden osalta samankaltaisuutta löydetään ratkaisumenetelmistä. Tutkielmassa osoitetaan, että lukiokirjoissa esiintyvä ratkaisumenetelmä on Smithin normaalimuotoon perustuvan ratkaisumenetelmän erikoistapaus.

Lineaaristen Diofantoksen yhtälöryhmien ratkaisemisen tueksi pro gradu -tutkielmassa tärkeimpinä sisältöinä toimivat Smithin normaalimuoto ja Siegelin lemma. Smithin normaalimuodon avulla lineaarinen Diofantoksen yhtälöryhmä voidaan muuttaa ekvivalenttiin muotoon yksinkertaisemman lineaarisen Diofantoksen yhtälöryhmän kanssa, josta sen ratkaiseminen on helpompaa. Siegelin lemma taas antaa lineaarisia Diofantoksen yhtälöryhmien homogeenista osaa vastaavalle yhtälöryhmälle arvion ratkaisun koosta.

Tutkielman lopuksi lineaarisia Diofantoksen yhtälöryhmiä käsitellään opetuksen näkökulmasta. Ratkaisumenetelmiä ja esitystapoja vertaillaan tämän tutkielman ja lukion oppikirjojen välillä. Tutkielman viimeisessä kappaleessa pohditaan, miten Diofantoksen yhtälöiden opettamista voitaisiin kehittää. Pohdinnoissa mietitään muun muassa, miten koulussa Diofantoksen yhtälöiden avulla voitaisiin luoda syvempää ymmärrystä lineaarisiin yhtälöryhmiin.

1 Esitietoja

Tämän tutkielman pohjatietoina oletetaan Jyväskylän yliopiston Lineaarinen algebra ja geometria 1 sekä Lukuteoria 1 -kursseja vastaavat tiedot [4] [12]. Esitiedoista esitellään hieman lineaarialgebraa, kokonaislukumatriisit sekä hila. Lineaarialgebran kohdalla esitietoja esitellään sen verran, että myöhemmin lineaaristen yhtälöryhmien ja lineaaristen Diofantoksen yhtälöryhmien vertaileminen mahdollistuu. Lineaaristen Diofantoksen yhtälöryhmien tulokset pyritään myöhemmin tutkielmassa esittämään lineaarisia yhtälöryhmiä vastaavina. Tähän liittyen esitietojen loppuosassa määritellään hilan käsite, jotta lineaarisille Diofantoksen yhtälöryhmien ratkaisujoukoille saadaan lineaarisia yhtälöryhmiä vastaavat tulokset. Lineaarisiin Diofantoksen yhtälöryhmiin liittyvien tulosten esittämiseen ja johtamiseen tarvitaan kokonaislukumatriisien ominaisuuksia, joita esitellään kokonaislukumatriisien kappaleessa.

1.1 Lineaarinen yhtälöryhmä

Kappaleen tarkoituksena on esittää lineaarisesta yhtälöryhmästä sen määritelmä ja näyttää yhtälöryhmän ratkaisujoukko avaruudessa $\mathbb{R}^n$. Varsinkin yhtälöryhmän ratkaisujoukkoa tullaan myöhemmin vertaamaan lineaaristen Diofantoksen yhtälöryhmän vastaaviin tuloksiin avaruudessa $\mathbb{Z}^n$. Esitetään seuraavaksi lineaarisen yhtälöryhmän määritelmä.

Määritelmä 1.1. Lineaarinen yhtälöryhmä avaruudessa $\mathbb{R}^n$ on m:n yhtälön ja n:n muuttuja lineaarinen yhtälöryhmä, missä m ja n ovat luonnollisia lukuja. Se voidaan esittää muodossa

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n & = b_1 \\ & \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n & = b_m. \end{cases}$$

Ylläoleva yhtälöryhmä voidaan esittää myös matriisiyhtälönä muodossa $A\overline{x} = \overline{b}$, missä $m \times n$-matriisia A kutsutaan yhtälöryhmän kerroinmatriisiksi. Vektoria $\overline{x}$, joka toteuttaa yhtälön $A\overline{x} = \overline{b}$ kutsutaan yhtälöryhmän ratkaisuksi.

Määritelmä 1.2. Joukkoa

$$\{\overline{x} \in \mathbb{R}^n \mid A\overline{x} = \overline{b}\}$$

kutsutaan yhtälöryhmän $A\overline{x} = \overline{b}$ ratkaisujoukoksi.

Nyt on saatu esitettyä lineaarisen yhtälöryhmän määritelmä ja sen ratkaisujoukko. Muistutetaan seuraavaksi, mitä ekvivalenssi tarkoittaa avaruudessa $\mathbb{R}^n$.

Ekvivalenssinuoli $\Leftrightarrow$ tarkoittaa kahden yhtälön välillä, että yhtälöt ovat yhtäpitäviä kaikilla $\overline{x} \in \mathbb{R}^n$. Esimerkiksi yhtälöiden $A\overline{x} = \overline{b} \Leftrightarrow \overline{x} = A^{-1}\overline{b}$ välillä ekvivalenssinuoli tarkoittaa, että kaikilla $\overline{x} \in \mathbb{R}^n$ pätee, että $A\overline{x} = \overline{b}$ jos ja vain jos $\overline{x} = A^{-1}\overline{b}$.

Lineaarisen yhtälöryhmän erikoistapausta, jossa luvut $b_1 = \cdots = b_m = 0$ kutsutaan lineaariseksi homogeeniseksi yhtälöryhmäksi [1]. Homogeeniseen yhtälöryhmään törmätään tutkielmassa myöhemmin muuan muassa Siegelin lemman 5.8 kohdalla.

Pyritään seuraavaksi selvittämään yhtälöryhmän $A\overline{x} = \overline{b}$ ratkaisujoukon rakenne. Voidaan osoittaa, että on olemassa sellainen $m \times m$ -matriisi H, että matriisi HA on niin kutsutussa redusoidussa porrasmuodossa [4] ja yhtälöryhmä $HA\overline{x} = H\overline{b}$ on ekvivalentti yhtälöryhmän $A\overline{x} = \overline{b}$ kanssa. Matriisi H voidaan löytää Gauss-Jordanin menetelmällä. Redusoidussa porrasmuodossa oleva matriisi $HA = R$ voi olla esimerkiksi muotoa

$$\begin{bmatrix} 1 & 0 & \cdots & 0 \\ & \ddots & & \\ & & \ddots & \\ 0 & \cdots & 0 & 1 \end{bmatrix},$$

joka on ekvivalentti alkuperäisen kerroinmatriisin kanssa. Redusoidusta porrasmuodosta lineaarisen yhtälöryhmän ratkaisut on helppo nähdä. Voidaan osoittaa, että yhtälöryhmän $A\overline{x} = \overline{b}$ ratkaisujoukon rakenteelle on kolme vaihtoehtoa:

- Ei ratkaisua eli tyhjä joukko $\emptyset$
- Yksi ratkaisu $\overline{x} = \{(x_1, \ldots, x_n)\}$
- Äärettömän monta ratkaisua, jotka voidaan esittää seuraavassa muodossa $\overline{x} = \{\overline{p} + a_1\overline{v}_1 + \cdots + a_k\overline{v}_k \,|\, a_1, \ldots, a_k \in \mathbb{R}\}$, missä $\overline{p}$ on yhtälöryhmän yksittäisratkaisu ja $1 \leq k$. Yhtälöryhmän homogeeninen ratkaisu taas on $\{a_1\overline{v}_1 + \cdots + a_k\overline{v}_k \,|\, a_1, \ldots, a_k \in \mathbb{R}\}$ [1].

Tarkastellaan tarkemmin lineaarisen homogeenisen yhtälöryhmän ratkaisujoukkoa. Ratkaisujoukkoa $\{a_1\overline{v}_1 + \cdots + a_k\overline{v}_k \,|\, a_1, \ldots, a_k \in \mathbb{R}\}$ kutsutaan lineaariavaruudeksi avaruudessa $\mathbb{R}^n$. Kyseisen lineaariavaruuden kantana toimivat lineaarisesti riippumattomat vektorit $\overline{v}_1, \ldots, \overline{v}_k$.

Tutkielman kannalta tärkeimmät tulokset lineaarisista yhtälöryhmistä on nyt saatu esitettyä. Lineaarisen yhtälöryhmän ratkaisujoukkoa vertaillaan

myöhemmin lineaarisen Diofantoksen yhtälöryhmän ratkaisujoukkoon. Esitetään vielä kappaleen lopuksi esimerkki lineaaristen yhtälöryhmien ratkaisemisesta. Kyseinen esimerkki tullaan ratkaisemaan myöhemmin tutkielmassa myös Smithin normaalimuodon avulla.

Esimerkki 1.3. Ratkaise lineaarinen yhtälöryhmä

$$\begin{cases} 3x_1 + 2x_2 + x_3 & = 12 \\ -4x_1 + 2x_2 + 3x_3 & = -15. \end{cases}$$

Yhtälöryhmää vastaava matriisiyhtälö on

$$\begin{bmatrix} 3 & 2 & 1 \\ -4 & 2 & 3 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 12 \\ -15 \end{bmatrix}.$$

Gauss-Jordan menetelmällä matriisiyhtälö voidaan ratkaista redusoituun porrasmuotoon

$$\left[\begin{array}{ccc|c} 1 & 0 & -4/30 & 114/30 \\ 0 & 1 & 7/10 & 3/10 \end{array}\right].$$

Redusoidusta porrasmuodosta yhtälöryhmän ratkaisuksi saadaan

$$\begin{cases} x_1 = \dfrac{4}{30}x_3 + \dfrac{114}{30} \\ \\ x_2 = \dfrac{-7}{10}x_3 + \dfrac{3}{10} \\ \\ x_3 \in \mathbb{R}. \end{cases}$$

Lineaarisen yhtälöryhmän yksittäisratkaisu on

$$\overline{p} = \begin{pmatrix} \dfrac{114}{30} & \dfrac{3}{10} & 0 \end{pmatrix}^T.$$

Merkitsemällä

$$x_3 = t \quad \text{ja} \quad \overline{v}_1 = \begin{pmatrix} \dfrac{4}{30} & \dfrac{-7}{10} & 1 \end{pmatrix}^T$$

voidaan yhtälöryhmän kaikki ratkaisut esittää muodossa $\{\overline{p} + t\overline{v}_1 \,|\, t \in \mathbb{R}\}$.

1.2 Kokonaislukumatriisit

Seuraavina esitietoina ovat *kokonaislukumatriisit*. Kappaleessa esitellään kokonaislukumatriisien ominaisuuksia. Kyseisiä ominaisuuksia tullaan hyödyntämään lineaarisiin Diofantoksen yhtälöryhmiin liittyvissä lauseissa ja todistuksissa kuten Smithin normaalimuodossa ja lauseessa 4.1. Kappaleessa määritellään muun muassa kokonaislukumatriisi, osamatriisi ja kokonaismatriisien tulo. Lisäksi kappaleessa tutustutaan kokonaislukumatriisien osajoukkoon $GL_n(\mathbb{Z})$ ja esitetään kyseiseen joukkoon liittyen käytännöllinen lemma. Kappaleen lopuksi esitellään vielä alkeismatriisit, joita tullaan hyödyntämään Smithin normaalimuodossa 2.2. Aloitetaan nyt kokonaislukumatriisin määritelmällä.

Määritelmä 1.4. Olkoon $a_{11}, a_{12}, \ldots, a_{mn}$ kokonaislukuja ja m sekä n luonnollisia lukuja. Tällöin $m \times n$-matriisia

$$A = \begin{pmatrix} a_{11} & \ldots & a_{1n} \\ a_{21} & \ldots & a_{2n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \ldots & a_{mn} \end{pmatrix}$$

kutsutaan kokonaislukumatriisiksi. Merkitään $m \times n$ -kokonaislukumatriisien joukkoa $M_{m\times n}(\mathbb{Z})$.

Hyödyntämällä kokonaislukumatriisin määritelmää voidaan seuraavaksi määritellä kokonaislukumatriisin osamatriisi sekä kokonaislukumatriisien tulomatriisi.

Määritelmä 1.5. Olkoon $m \times n$-matriisi A kuten määritelmässä 1.4. Tällöin matriisin A *osamatriisiksi* kutsutaan matriisia, mikä saadaan poistamalla matriisista A ensimmäinen rivi ja sarake. $(m-1) \times (n-1)$ -kokoista osamatriisia merkitään (c_{kl}), missä $k = m-1$ ja $l = n-1$. Osamatriisin (c_{kl}) paikalla $(1,1)$ on alkuperäisen matriisin A alkio a_{22}.

Määritelmä 1.6. Olkoon $m \times n$-matriisi A kuten määritelmässä 1.4 ja olkoon $n \times s$-matriisi

$$B = \begin{pmatrix} b_{11} & \ldots & b_{1s} \\ b_{21} & \ldots & b_{2s} \\ \vdots & \ddots & \vdots \\ b_{n1} & \ldots & b_{ns} \end{pmatrix},$$

missä $b_{ij} \in \mathbb{Z}$. Tällöin matriisien A ja B tulo on $m \times s$ -kokonaislukumatriisi

$$AB = C = \begin{pmatrix} c_{11} & \dots & c_{1s} \\ c_{21} & \dots & c_{2s} \\ \vdots & \ddots & \vdots \\ c_{m1} & \dots & c_{ms} \end{pmatrix}, \quad c_{rt} = \sum_{k=1}^{n} a_{rk} b_{kt},$$

missä $r = 1, \dots, m; t = 1, \dots, s$ ja $c_{rt} \in \mathbb{Z}$.

Nyt on saatu esitettyä osamatriisiin ja tulomatriisiin liittyvät määritelmät. Esitetään seuraavaksi kokonaislukumatriisien determinanttiin liittyvä lemma. Lemman tulos on suoraviivainen seuraus determinantin määritelmästä.

Lemma 1.7. *Olkoon A $n \times n$ -kokonaislukumatriisi. Tällöin matriisin A determinantti on kokonaisluku.*

Tarkastellaan seuraavaksi kokonaislukumatriisien erikoistapausta. Neliömatriisia, jonka determinantti on ± 1 kutsutaan *unimodulaarimatriisiksi*. Erityisesti jos neliömatriisin determinantti on 1, niin sitä kutsutaan *positiiviseksi unimodulaarimatriisiksi*. Unimodulaarimatriiseja tullaan tarvitsemaan myöhemmin tutkielmassa käsiteltäessä Smithin normaalimuotoa. Seuraavassa määritelmässä esitetään unimodulaarimatriisien joukolle merkintä.

Määritelmä 1.8. Kokonaislukualkioisten $k \times k$-kokoisten unimodulaaristen matriisien joukkoa merkitään $GL_k(\mathbb{Z})$.

Unimodulaaristen matriisien joukolle voidaan todistaa, että unimodulaarimatriisien käänteismatriisit ovat myös unimodulaarimatriiseja. Tämän osoittamiseksi tarvitaan neliömatriiseihin liittyvää Cramerin sääntöä [4], joka esitellään seuraavaksi.

Lemma 1.9 (Cramerin sääntö)**.** *Olkoon A kääntyvä $n \times n$-neliömatriisi ja $\overline{b} \in \mathbb{Z}^n$. Jos $A\overline{x} = \overline{b}$, niin*

$$x_i = \frac{\det B_i}{\det A}, \quad i = 1, \dots, n,$$

missä B_i on se osamatriisi, joka saadaan korvaamalla matriisin A i:s sarake vektorilla $\overline{b}$.

Cramerin sääntö on saatu nyt esitettyä. Käytetään sitä apuna seuraavan lemman todistuksessa. Lemmassa osoitetaan, että unimodulaaristen matriisien käänteismatriisit ovat myös unimodulaarimatriiseja.

Lemma 1.10. *Jos matriisi $S \in GL_k(\mathbb{Z})$, niin myös käänteismatriisi $S^{-1} \in GL_k(\mathbb{Z})$.*

Todistus. Olkoon $S \in GL_k(\mathbb{Z})$. Koska matriisi S on kääntyvä, niin tällöin on olemassa matriisi $X \in M_{k\times k}(\mathbb{Z})$, jolla $SX = I$. Tiedetään, että käänteismatriisi on yksikäsitteinen, jolloin $X = S^{-1}$. Osoitetaan nyt, että matriisi $X \in GL_k(\mathbb{Z})$.

Merkitään matriisin X sarakkeita $\overline{x}_1, \ldots, \overline{x}_k$. Tällöin matriisin SX sarakkeita voidaan merkitä $S\overline{x}_1, \ldots, S\overline{x}_k$ ja lisäksi identiteettimatriisin I sarakkeita merkitään $\overline{e}_1, \ldots, \overline{e}_k$. Tällöin matriisiyhtälössä $SX = I$ on k kappaletta vektoriyhtälöitä. Vektoriyhtälöitä merkitään $S\overline{x}_1 = \overline{e}_1, \ldots, S\overline{x}_k = \overline{e}_k$.

Tarkastellaan tässä yhtälöä

$$S\overline{x}_j = \overline{e}_j, \quad \text{missä} \quad 1 \leq j \leq k.$$

Pyritään osoittamaan, että x_j:n koordinaatit ovat kokonaislukuja indeksistä j riippumatta. Cramerin säännön 1.9 nojalla $\overline{x}_j$:n i:s koordinaatti on kokonaisluku, sillä kun matriisissa S korvataan i:s sarake vektorilla $\overline{e}_j$, niin näin muodostettu matriisi S_i on kokonaislukumatriisi. Tiedetään, että jokaisen kokonaislukumatriisin determinantti on kokonaisluku, jolloin saadaan, että jokainen vektoreista $\overline{x}_1, \ldots, \overline{x}_k$ on kokonaislukuvektori. Näin ollen $X \in GL_k(\mathbb{Z})$ ja, koska $X = S^{-1}$, niin voidaan päätellä, että $S^{-1} \in GL_k(\mathbb{Z})$. □

Lemma 1.11. *Olkoon matriisi $R \in GL_n(\mathbb{Z})$. Tällöin joukoille $\mathbb{Z}^n$, $R\mathbb{Z}^n$ ja $\mathbb{Z}^n R$ pätee, että*

$$R\mathbb{Z}^n = \mathbb{Z}^n = \mathbb{Z}^n R.$$

Vastaavasti joukoille $R^{-1}\mathbb{Z}^n$, $\mathbb{Z}^n$ ja $\mathbb{Z}^n R^{-1}$ pätee, että

$$R^{-1}\mathbb{Z}^n = \mathbb{Z}^n = \mathbb{Z}^n R^{-1}.$$

Todistus. Todistetaan ensin lemman ensimmäinen väite. Koska matriisi $R \in GL_n(\mathbb{Z})$, niin matriisin R alkiot ovat kokonaislukuja. Tiedetään, että kokonaislukujen kerto- ja yhteenlasku tuottaa kokonaisluvun. Näin ollen $R\mathbb{Z}^n \subset \mathbb{Z}^n$ ja $\mathbb{Z}^n R \subset \mathbb{Z}^n$.

Osoitetaan vielä, että $\mathbb{Z}^n \subset R\mathbb{Z}^n$ ja $\mathbb{Z}^n \subset \mathbb{Z}^n R$. Olkoon $\overline{y} \in \mathbb{Z}^n$. Tiedetään lemman 1.10 nojalla $R^{-1} \in GL_n(\mathbb{Z})$ ja lisäksi valitsemalla $\overline{x}_1 = R^{-1}\overline{y}$ ja $\overline{x}_2 = \overline{y}R^{-1}$ voidaan päätellä, että $\overline{x}_1$ ja $\overline{x}_2 \in \mathbb{Z}^n$. Näin ollen selvästi $\overline{y} = R\overline{x}_1$ ja $\overline{y} = \overline{x}_2 R$, josta voidaan päätellä, että $\mathbb{Z}^n \subset R\mathbb{Z}^n$ ja $\mathbb{Z}^n \subset \mathbb{Z}^n R$. Siispä $R\mathbb{Z}^n = \mathbb{Z}^n = \mathbb{Z}^n R$.

Lemman 1.10 nojalla tiedetään, että $R^{-1} \in GL_n(\mathbb{Z})$. Tällöin lemman toisen väitteen todistus menee vastavasti kuin ensimmäisen väitteen. Näin ollen $R^{-1}\mathbb{Z}^n = \mathbb{Z}^n = \mathbb{Z}^n R^{-1}$. □

Nyt on saatu esitettyä unimodulaaristen matriisien joukko sekä niiden käänteismatriiseihin liittyvä lemma. Jotta kokonaislukumatriiseilla pystytään suorittamaan vastaavia rivi- ja sarakeoperaatioita kuin reaalilukumatriiseilla, niin esitellään alkeismatriisit. Alkeismatriiseja tullaan hyödyntämään tutkielmassa myöhemmin Smithin normaalimuodon yhteydessä. Alkeismatriisit suorittavat annettuun kokonaislukumatriisiin vastaavia rivioperaatioita Smithin normaalimuotoon muokattaessa kuin reaalilukumatriisit Gauss-Jordan ratkaisumenetelmässä.

Lemma 1.12. *Olkoon*

$$T_{ij}(b) = \begin{pmatrix} 1 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & 1 & & & & & & \vdots \\ \vdots & & \ddots & & & & & \vdots \\ \vdots & & & 1 & b & & & \vdots \\ \vdots & & & 0 & 1 & & & \vdots \\ \vdots & & & & & \ddots & & \vdots \\ \vdots & & & & & & 1 & 0 \\ 0 & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & 1 \end{pmatrix}, \quad D_i(u) = \begin{pmatrix} 1 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & 1 & & & & & & \vdots \\ \vdots & & \ddots & & & & & \vdots \\ \vdots & & & u & 0 & & & \vdots \\ \vdots & & & 0 & 1 & & & \vdots \\ \vdots & & & & & \ddots & & \vdots \\ \vdots & & & & & & 1 & 0 \\ 0 & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & 1 \end{pmatrix} \text{ ja}$$

$$P_{ij} = \begin{pmatrix} 1 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & 1 & & & & & & \vdots \\ \vdots & & \ddots & & & & & \vdots \\ \vdots & & & 0 & 1 & & & \vdots \\ \vdots & & & 1 & 0 & & & \vdots \\ \vdots & & & & & \ddots & & \vdots \\ \vdots & & & & & & 1 & 0 \\ 0 & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & 1 \end{pmatrix}$$

alkeismatriiseja, missä $b \in \mathbb{Z}$ ja $u \in \mathbb{Z}$. Matriisi $T_{ij}(b)$ saadaan identiteettimatriisista kertomalla j:s rivi vakiolla b ja lisäämällä se riviin i. Matriisi $D_i(u)$ saadaan identiteettimatriisista kertomalla riviä i vakiolla u ja matriisi P_{ij} tulee identiteettimatriisista vaihtamalla rivien i ja j paikkoja. Jokainen alkeismatriiseista on selvästi kääntyvä, sillä niiden determinantit ovat nollasta poikkeavia.

Alkeismatriisit on näin ollen saatu esitettyä. Esitellään kahdessa seuraavassa lemmassa alkeismatriiseihin liittyviä ominaisuuksia. Kyseisiä ominaisuuksia tullaan tarvitsemaan varsinkin käsiteltäessä Smithin normaalimuotoa myöhemmin tutkielmassa.

Lemma 1.13. *Alkeismatriisit $T_{ij}(b)$ ja P_{ij} kuuluvat unimodulaaristen matriisien joukkoon $GL_k(\mathbb{Z})$. Lisäksi alkeismatriisi $D_i(u) \in GL_k(\mathbb{Z})$, kun $u = \pm 1$.*

Todistus. Huomataan ensin, että jokaisen alkeismatriisin kaikki alkiot t_{ij}, d_{ij} ja $p_{ij} \in \mathbb{Z}$. Riittää siis todistaa, että alkeismatriisien determinantti on ± 1. Alkeismatriisi $D_i(u)$ on identtinen matriisi, jonka jokin rivi tai sarake on kerrottu vakiolla u. Tällöin alkeismatriisin determinantti on identiteettimatriisin determinantti kerrottuna vakiolla u. Koska $u = \pm 1$, niin $\det D_i(u) = \pm 1$ ja näin ollen $D_i(u) \in GL_k(\mathbb{Z})$.

Alkeismatriisit $T_{ij}(b)$ ja P_{ij} on saatu identiteettimatriisista lisäämällä johonkin riviin toinen rivi kerrottuna vakiolla b tai vaihtamalla kaksi riviä keskenään. Näin ollen alkeismatriisien determinantti on sama kuin identiteettimatriisin determinantti. Siispä $\det T_{ij}(b) = 1$ ja $\det P_{ij} = 1$ ja tällöin $T_{ij}(b), P_{ij} \in GL_k(\mathbb{Z})$. □

Seuraavan lemman todistus on suoraviivainen ja se jätetään lukijalle harjoitustehtäväksi.

Lemma 1.14. *Alkeismatriiseilla matriisin $A \in M_{n\times m}(\mathbb{Z})$ kertominen muuttaa matriisia A seuraavasti:*

i. Vasemmalta matriisin A kertominen $m \times m$-matriisilla $T_{ij}(b)$ lisää matriisin A riviin i rivin j kerrottuna kokonaisluvulla b. Oikealta matriisin A kertominen $n \times n$-matriisilla $T_{ij}(b)$ lisää matriisin A sarakkeeseen j sarakkeen i kerrottuna kokonaisluvulla b.

ii. Vasemmalta matriisin A kertominen $m \times m$-matriisilla $D_i(u)$ kertoo matriisin A rivin i kokonaisluvulla u. Oikealta matriisin A kertominen $n \times n$-matriisilla $D_i(u)$ kertoo matriisin A sarakkeen i kokonaisluvulla u.

iii. Vasemmalta matriisin A kertominen $m \times m$-matriisilla P_{ij} vaihtaa matriisin A rivien i ja j paikat. Oikealta matriisin A kertominen $n \times n$-matriisilla P_{ij} vaihtaa matriisin A sarakkeiden i ja j paikat.

Alkeismatriiseihin liittyvät kaksi lemmaa on saatu nyt esitettyä. Näin ollen kokonaislukumatriiseihin liittyvistä määritelmistä ja lemmoista on saatu käytyä läpi kaikki, joita myöhemmin tullaan käyttämään tässä tutkielmassa. Seuraavassa kappaleessa esitetään vielä viimeiset tutkielman kannalta tärkeät esitiedot, jotka liittyvät hilan käsitteeseen.

1.3 Hila

Esitetään viimeisenä esitietona hilan käsite. Kappaleessa 1.1 mainittiin, että lineaarisen yhtälöryhmän ratkaisujoukon homogeeninen osa on lineaariavaruus $\{a_1\overline{v}_1 + \cdots + a_k\overline{v}_k \,|\, a_1, \ldots, a_k \in \mathbb{R}\}$. Annetaan seuraavaksi hilan määritelmä. Määritelmästä voidaan havaita sen ero lineaariavaruuteen $\{a_1\overline{v}_1 + \cdots + a_k\overline{v}_k \,|\, a_1, \ldots, a_k \in \mathbb{R}\}$.

Määritelmä 1.15. Hila $H \subset \mathbb{R}^n$ on joukko

$$H = \{a_1\overline{w}_1 + \cdots + a_k\overline{w}_k \mid a_1, \ldots, a_k \in \mathbb{Z}\},$$

missä vektorit $\overline{w}_1, \ldots, \overline{w}_k \in \mathbb{R}^n$ ovat lineaarisesti riippumattomat [5].

Vektoreita $\overline{w}_1, \ldots, \overline{w}_k \in \mathbb{R}^n$ kutsutaan hilan kannaksi. Huomataan hilan määritelmästä 1.15, että hila eroaa lineaariavaruudesta siten, että lineaarisesti riippumattomien vektoreiden $\overline{w}_1, \ldots, \overline{w}_k$ kertoimet $a_1, \ldots, a_k$ kuuluvat kokonaislukuihin eivätkä reaalilukuihin. Esitetään seuraavaksi hilaan liityviä ominaisuuksia lemman muodossa. Lemma on muodostettu luentomonisteen [6] pohjalta.

Lemma 1.16. *Olkoon $H \subset \mathbb{R}^n$ hila. Tällöin se on additiivinen ryhmä.*

Todistus. Todistetaan, että määritelmän 1.15 mukainen joukko H on ryhmän $\mathbb{R}$ aliryhmä. Olkoon

$$x = a_1\overline{w}_1 + \cdots + a_k\overline{w}_k \in H \text{ ja } y = b_1\overline{w}_1 + \cdots + b_k\overline{w}_k \in H.$$

Tällöin

$$x+y = a_1\overline{w}_1+\cdots+a_k\overline{w}_k+b_1\overline{w}_1+\cdots+b_k\overline{w}_k = (a_1+b_1)\overline{w}_1+\cdots+(a_k+b_k)\overline{w}_k.$$

Koska kertoimet $a_1, \ldots, a_k \in \mathbb{Z}$ ja $b_1, \ldots, b_k \in \mathbb{Z}$, niin $a_1 + b_1, \ldots, a_k + b_k \in \mathbb{Z}$. Näin ollen $x + y \in H$. Lisäksi tiedosta $a_1, \ldots, a_k \in \mathbb{Z}$ saadaan, että $-a_1, \ldots, -a_k \in \mathbb{Z}$. Näin ollen $-x \in H$. Siispä joukko H on ryhmän $\mathbb{R}$ aliryhmä ja tällöin se on additiivinen ryhmä. □

Esimerkki 1.17. Osoitetaan esimerkissä, että vaikka jokainen hila on additiivinen ryhmä, niin jokainen additiivinen ryhmä ei ole hila. Esimerkiksi joukko $H = \mathbb{Z} + \pi\mathbb{Z}$ on ryhmä mutta kuitenkin voidaan osoittaa, että se ei ole hila.

Tehdään antiteesi ja oletetaan, että H on hila joukossa $\mathbb{R}$. Avaruudessa $\mathbb{R}$ voi olla korkeintaan yksi lineaarisesti riippumaton alkio, niin tällöin on olemassa alkio $x \in \mathbb{R}$, jolla $\mathbb{Z} + \pi\mathbb{Z} = x\mathbb{Z}$. Erityisesti tällöin on olemassa kokonaisluku a, jolla $ax = \pi$. Samoin on olemassa kokonaisluku b, jolla $bx = 1$. Tällöin

$$x = \frac{1}{b} \quad \text{ja} \quad \frac{a}{b} = \pi.$$

Tämä on ristiriita ja näin ollen H ei ole hila.

Hilaa tullaan esittelemään myöhemmin tutkielmassa vielä lineaaristen Diofantoksen yhtälöryhmien kohdalla. Tällöin kyseessä on hilan erikoistapaus, missä lineaarisesti riippumattomat kantavektorit $\overline{w}_1, \ldots, \overline{w}_k \in \mathbb{Z}^n$. Kaikki esitiedot on saatu käytyä nyt läpi. Seuraavassa kappaleessa päästään käsiksi Smithin normaalimuotoon, jota hyödynnetään lineaaristen Diofantoksen yhtälöryhmien ratkaisemisessa.

2 Smithin normaalimuoto

Tämän kappaleen tarkoituksena on todistaa Smithin normaalimuoto. Käytetään tässä kappaleessa merkintää L_i, kun lemman 1.12 alkeismatriisilla kerrotaan vasemmalta puolelta ja R_i, kun alkeismatriisilla kerrotaan oikealta puolelta. Järjestysluku $i = 1, \ldots, n$ kertoo, missä järjestyksessä matriiseilla kertominen suoritetaan. Sopivien matriisien L_i ja R_i valinnassa käytetään apuna Eukleideen algoritmia, joka esitellään seuraavaksi lemmana. Eukleideen algoritmin avulla jakoyhtälöä hyödyntäen alkuperäisen matriisin rivi- ja sarakealkioita on mahdollista muuttaa lopulta nollaksi. Myöhemmin tutkielmassa myös osoitetaan, että lukion oppikirjoissa esiintyvä Eukleideen algoritmi on erikoistapaus Smithin normaalimuodon ratkaisumenetelmästä.

Lemma 2.1 (Eukleideen algoritmi)**.** *Olkoon $a, b \in \mathbb{Z}$, $b \neq 0$ ja s_i sekä r_i kokonaislukuja jokaisella $i = 0, \ldots, n$. Tällöin jakoyhtälön nojalla*

$$a = s_0 b + r_0, \ \textit{missä}\ 0 < r_0 < |b|.$$

Toistamalla jakoyhtälöä saadaan

$$\begin{aligned} b &= s_1 r_0 + r_1, \ \textit{missä}\ 0 < r_1 < r_0 \\ r_0 &= s_2 r_1 + r_2, \ \textit{missä}\ 0 < r_2 < r_1 \\ &\vdots \\ r_{n-2} &= s_{n-1} r_{n-1} + r_n, \ \textit{missä}\ 0 < r_n < r_{n-1} \\ r_{n-1} &= s_n r_n + 0. \end{aligned}$$

Tällöin viimeinen jakojäännös $r_n = syt(a, b)$.

Esitetään seuraavaksi Smithin normaalimuotoon liittyvä lause 2.2. Hyödynnetään todistuksessa apuna Jacobsonin todistusta Smithin normaalimuodolle Eukleideen alueessa [2] kappaleessa 3. Esitetään vielä yksi notaatio Smithin normaalimuodon lauseeseen liittyen. Olkoot n ja m luonnollisia lukuja ja $k = \min(n, m)$. Tällöin notaatiolla $D = \operatorname{diag}(d_1, \ldots, d_s, 0, \ldots, 0)$ viitataan $m \times n$-matriisiin D, jonka vasemmassa yläkulmassa on diagonaalinen $k \times k$-alimatriisi, jonka diagonaalilla ovat alkiot $d_1, \ldots, d_s$ ja muut matriisin alkiot ovat nollia.

Lause 2.2 (Smithin normaalimuoto)**.** *Olkoon $A \in M_{m \times n}(\mathbb{Z})$. Tällöin on olemassa $L \in GL_m(\mathbb{Z})$ ja $R \in GL_n(\mathbb{Z})$, joille pätee*

$$LAR = D = \operatorname{diag}(d_1, d_2, \ldots, d_s, 0, \ldots, 0),$$

missä luvut $d_i > 0$ ovat kokonaislukuja jokaisella $i = 1, \ldots, s$ ja $d_i | d_{i+1}$, $i = 1, \ldots, s-1$. Tällöin D on $m \times n$-matriisi.

Todistus. Jos matriisi A on nollamatriisi, niin väitteessä ei ole mitään todistettavaa. Oletetaan siis, että $A \neq 0$. Olkoon a_{ij} matriisin A itseisarvoltaan pienin nollasta eroava kokonaislukualkio. Siirretään a_{ij} rivi- ja sarakeoperaatioiden avulla matriisissa A paikalle $(1,1)$.

Olkoon $k > 1$ ja merkitään paikan $(1,k)$ alkiota a_{1k} Eukleideen algoritmin nojalla $a_{1k} = a_{11}b_k + b_{1k}$, missä $|b_{1k}| < |a_{11}|$. Kertomalla matriisia A oikealta sopivalla matriisilla R_i saadaan vähennettyä sarakkeesta k ensimmäinen sarake kerrottuna luvulla b_k. Tällöin matriisissa A paikalle $(1,k)$ tulee alkio b_{1k}. Toistetaan oikealta sopivalla matriisilla kertomista, jolloin saadaan ensimmäiselle riville alkiot $b_{12}, \ldots, b_{1n}$. Jos jokin alkio $b_{1k} \neq 0$, missä $k = 1, \ldots n$, niin vaihdetaan itseisarvoltaan pienimmän nollasta eroavan b_{1k} alkion sarake ja ensimmäinen sarake keskenään kertomalla oikealta sopivalla matriisilla R_i. Tällöin matriisin A paikalle $(1,1)$ tulee alkio b_{1k}. Toistetaan Eukleideen algoritmin prosessia ensimmäiselle riville, jolloin matriisissa A paikalla $(1,1)$ alkion itseisarvo pienenee jokaisella prosessin toistolla. Näin ollen Eukleideen algoritmin prosessia voidaan jatkaa niin pitkään kunnes $b_{12} = \cdots = b_{1n} = 0$.

Vastaavasti merkitään $a_{k1} = a_{11}b_k + b_{k1}$, missä $|b_{k1}| < |a_{k1}|$. Kertomalla matriisia A vasemmalta sopivalla matriisilla L_i saadaan vähennettyä riviltä k ensimmäinen rivi kerrottuna luvulla b_k. Tällöin matriisissa A paikalle $(k,1)$ tulee alkio b_{k1}. Toistetaan vasemmalta sopivalla matriisilla kertomista Eukleideen algoritmin vaatimasti vastaavasti kuin sarakkeiden kohdalla oikealta sopivalla matriisilla kertomista. Tällöin jos jokin $b_{k1} \neq 0$, niin vaihdetaan itseisarvoltaan pienimmän alkion b_{k1} rivi ja ensimmäinen rivi keskenään kertomalla vasemmalta sopivalla matriisilla L_i vastaavasti kuin sarakkeiden kohdalla.

On mahdollista, että kun ensimmäisen sarakkeen alkiot $b_{21} = \cdots = b_{m1} = 0$, niin vasemmalta matriisilla L_i kertominen on muuttanut ensimmäistä riviä. Tämän vuoksi jos jokin $b_{1k} \neq 0$, missä $k = 2, \ldots, n$, jatketaan Eukleideen algoritmin prosessia uudestaan ensimmäiselle riville. Kun ensimmäisellä rivillä saadaan taas alkiot muotoon $b_{12} = \cdots = b_{1n} = 0$, niin on mahdollista, että oikealta matriisilla R_i kertominen on muuttanut ensimmäisen sarakkeen alkioita b_{k1}. Koska Eukleideen algoritmin avulla matriisin A paikan $(1,1)$ alkion itseisarvo pienenee jokaisella prosessin kerralla, Eukleideen algoritmia vuorottelemalla ensimmäinen sarake ja rivi tulee lopulta muotoon $b_{12} = \cdots = b_{1n} = 0$ ja $b_{21} = \cdots = b_{m1} = 0$. Tällöin saadaan matriisin A kanssa yhtäpitävä matriisi B, joka on muotoa

$$\begin{pmatrix} b_{11} & 0 & \ldots & 0 \\ 0 & c_{22} & \ldots & c_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ 0 & c_{m2} & \ldots & c_{mn} \end{pmatrix}. \tag{2.1}$$

Matriisi (2.1) voidaan myös muuttaa muotoon, jossa $b_{11} \mid c_{kl}$ jokaisella $k, l \in \mathbb{N}$. Jos $b_{11} \nmid c_{kl}$, niin vasemmalta kertomalla sopivalla matriisilla L_i voidaan lisätä rivi k ensimmäiseen riviin. Tällöin ensimmäiseksi riviksi tulee $(b_{11}, c_{k2}, \ldots, c_{kl}, \ldots, c_{kn})$. Toistamalla Eukleideen algoritmia kertoen vasemmalta ja oikealta sopivilla matriiseilla L_i ja R_i voidaan matriisia B muuttaa niin että $b_{11} \mid c_{kl}$ kaikilla $k, l \in \mathbb{N}$, sillä paikan $(1,1)$ alkion itseisarvo pienenee jokaisessa Eukleideen algoritmin vaiheessa. Lopulta saadaan matriisin (2.1) kanssa yhtäpitävä matriisi, jossa $b_{11} \neq 0$ ja $b_{11} \mid c_{kl}$ kaikilla $k, l \in \mathbb{N}$. Eukleideen algoritmin avulla tehty prosessi alkuperäiselle matriisille A voidaan toistaa osamatriisille (c_{kl}), jolloin saadaan yhtäpitävä matriisi

$$\begin{pmatrix} b_{11} & 0 & \ldots & \ldots & 0 \\ 0 & c_{22} & 0 & \ldots & 0 \\ 0 & 0 & d_{33} & \ldots & d_{3n} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & d_{m3} & \ldots & d_{mn} \end{pmatrix}, \tag{2.2}$$

missä $c_{22} \mid d_{pq}$ kaikilla $p, q \in \mathbb{N}$. Koska $b_{11} \mid c_{22}$ ja $c_{22} \mid d_{pq}$ niin pätee myös, että $b_{11} \mid d_{pq}$. Jatkamalla Eukleideen algoritmin hyödyntämistä vastaavalla tavalla osamatriisin d_{pq} kanssa kuin alkuperäisen matriisin A tai osamatriisin (c_{kl}) kanssa saadaan lopulta matriisin A kanssa yhtäpitävä matriisi $\operatorname{diag}(d_1, d_2, \ldots, d_s, 0, \ldots, 0)$, missä $d_1 = b_{11}, d_2 = c_{22}, \ldots$ ja $d_i \mid d_j$ kaikilla $i \leq j$.

Merkitään vasemmalta kerrottujen matriisien L_i tulomatriisia L ja oikealta kerrottujen matriisien R_i tulomatriisia R. Koska matriisit L_i ja $R_i \in GL_n(\mathbb{Z})$, niin tällöin myös matriisit $L, R \in GL_n(\mathbb{Z})$. Näin ollen on saatu todistettua, että on olemassa matriisit L ja $R \in GL_n(\mathbb{Z})$, joille pätee, että $LAR = D = \operatorname{diag}(d_1, d_2, \ldots, d_s, 0, \ldots, 0)$. □

Smithin normaalimuoto on saatu esitettyä ja siihen liittyvä lause 2.2 todistettua. Kappaleessa 4 lineaaristen Diofantoksen yhtälöryhmien kohdalla kyseinen lause on keskeisessä osassa. Smithin normaalimuodon avulla lineaaristen Diofantoksen yhtälöryhmien ratkaiseminen helpottuu huomattavasti. Lisäksi myöhemmin kappaleessa 6.1 tullaan näyttämään Smithin normaalimuodon ja Eukleideen algoritmin samankaltaisuus, jotta nähdään Diofantoksen yhtälöiden ja lineaaristen Diofantoksen yhtälöryhmien yhteneväisyys ratkaisumenetelmässä.

3 Lineaariset Diofantoksen yhtälöt

Tämän kappaleen tarkoituksena on käydä yksityiskohtaisesti läpi lineaarisen Diofantoksen yhtälöiden ratkaiseminen ja ratkaisujoukko ennen kappalee-

seen 4 siirtymistä. Lineaariset Diofantoksen yhtälöt esitetään lukiossa valtakunnallissa syventävissä moduuleissa. Lineaarisesta Diofantoksen yhtälöstä esimerkkinä toimii yhtälö

$$3x + 6y = 9,$$

jolle kokeilemalla voidaan löytää ratkaisu $x = 1$ ja $y = 1$. Käydään tässä kappaleessa täsmällisesti läpi, miten lukuteorian kirjallisuudessa lineaariset Diofantoksen yhtälöt esitetään ja ratkaistaan. Esitys seurailee lähteen [13] kappaleen 2.2 esitystä. Kappaleen lopuksi määritetään Diofantoksen yhtälön ratkaisujoukon rakenne.

Lineaarisella Diofantoksen yhtälöllä tarkoitetaan muotoa

$$ax + by = c$$

olevaa yhtälöä, jossa muuttujien x ja y kertoimet a ja b sekä luku c ovat kokonaislukuja. Yhtälölle haetaan ainoastaan kokonaislukuratkaisuja. Diofantoksen yhtälölle voidaan löytää ratkaisu kokeilemalla tai käyttämällä hyödyksi Eukleideen algoritmia 2.1. Seuraavassa lauseessa osoitetaan milloin Diofantoksen yhtälölle löytyy ratkaisu.

Lause 3.1. *Olkoot a, b ja c nollasta eroavia kokonaislukuja. Tällöin lineaarisella Diofantoksen yhtälöllä $ax + by = c$ on ratkaisu jos ja vain jos $d \mid c$, missä $d = syt(a, b)$.*

Todistus. Oletetaan ensin, että lineaarisella Diofantoksen yhtälöllä $ax+by = c$ on ratkaisu x_0, y_0. Koska $d = \text{syt}(a, b)$, niin on olemassa suhteelliset alkuluvut r ja s, joille pätee, että $a = dr$ ja $b = ds$. Tällöin

$$c = ax_0 + by_0 = drx_0 + dsy_0 = d(rx_0 + sy_0).$$

Näin ollen $d \mid c$.

Oletetaan seuraavaksi, että $d \mid c$, jolloin $c = dt$. Lisäksi tiedetään Bezoutin identiteetin nojalla, että on olemassa luvut x_0 ja y_0, joille pätee $d = ax_0+by_0$. Tällöin

$$c = dt = (ax_0 + by_0)t = a(tx_0) + b(ty_0),$$

missä tx_0 ja ty_0 on Diofantoksen yhtälön ratkaisu. Siispä lineaarisella Diofantoksen yhtälöllä on ratkaisu jos ja vain jos $d \mid c$. □

Edellä nähtiin, että lineaarisella Diofantoksen yhtälöllä on ratkaisu jos ja vain jos $\text{syt}(a, b) \mid c$. Oletetaan tämän kappaleen ajan, että $\text{syt}(a, b) \mid c$.

Osoitetaan seuraavaksi, miten Eukleideen algoritmin avulla lineaariselle Diofantoksen yhtälölle voidaan löytää sen eräs ratkaisu. Algoritmissa jakoyhtälön nojalla merkitään

$$a = s_0 b + r_0, \qquad \text{missä } 0 < r_0 < b$$

kuten lemmassa 2.1. Jakoyhtälö voidaan toistaa nyt luvuille b ja r_0, jolloin saadaan

$$b = s_1 r_0 + r_1, \qquad \text{missä } 0 < r_1 < r_0.$$

Vastaavasti jakoyhtälöä toistamalla päästään lopulta tilanteeseen, jossa jakojäännöstä ei synny eli lemman 2.1 nojalla tilanteeseen

$$\begin{aligned} r_{n-2} &= s_{n-1} r_{n-1} + r_n \\ r_{n-1} &= s_n r_n + 0. \end{aligned}$$

Tällöin viimeinen jakojäännös r_n on Eukleideen algoritmin ratkaisu kokonaislukujen a ja b suurimmaksi yhteiseksi tekijäksi $\text{syt}(a, b)$. Merkitään, että $r_n = c = \text{syt}(a, b)$.

Määritellään nyt rekursiivisesti lukujonot (x_i) ja (y_i) asettamalla $x_0 = 1$, $x_1 = 0$, $y_0 = 0$ ja $y_1 = 1$. Muut lukujonojen alkiot saadaan rekursiivisesti ehdosta $x_{i+1} = x_{i-1} - x_i s_i$ ja $y_{i+1} = y_{i-1} - y_i s_i$, missä alaindeksi i kertoo kuinka monta vaihetta jakoyhtälössä on lukujen a ja b suurimman yhteisen tekijän selvittämiseksi.

Lemma 3.2. *Lukujonoille (x_i) ja (y_i) pätee, että*

$$r_i = a x_i + b y_i \quad \textit{kaikilla} \quad i,$$

kun tiedetään, että jakojäännöksille pätee $r_{i+1} = r_{i-1} - r_i s_i$. Erityisesti siis pätee, että

$$a x_n + b y_n = r_n = \textit{syt}(a, b).$$

Todistus. Todistetaan lemman ensimmäinen väite induktion avulla. Kun $i = 0$ tai $i = 1$ väite pätee, sillä Eukleideen algoritmin ensimmäiset jakojäännökset ovat $r_0 = a$ ja $r_1 = b$. Osoitetaan induktiolla, että väite pätee myös, kun $i > 1$. Oletetaan, että väite on tosi, kun $i \leq k$. Tällöin

$$\begin{aligned} r_{k+1} = r_{k-1} - r_k s_k &= (a x_{k-1} + b y_{k-1}) - (a x_k + b y_k) s_k \\ &= a(x_{k-1} - x_k s_k) + b(y_{k-1} - y_k s_k) = a x_{k+1} + b y_{k+1}. \end{aligned}$$

Näin ollen

$$r_i = a x_i + b y_i \quad \text{kaikilla} \quad i.$$

Lemman toinen väite seuraa edellisestä, kun tiedetään, että $r_n = c$. Siispä $a x_n + b y_n = r_n = \text{syt}(a, b)$. □

Näin ollen käänteisellä Eukleideen algoritmilla saadaan, että x_n ja y_n on Diofantoksen yhtälön $ax + by = c$ yksittäisratkaisu. Merkitään yksittäisratkaisua vielä tutumassa muodossa $x_n = \tilde{x}_0$ ja $y_n = \tilde{y}_0$. Näin on saatu näytettyä, miten Eukleideen algoritmin avulla saadaan lineaariselle Diofantoksen yhtälölle löydettyä yksittäisratkaisu.

Huomautus 3.3. Huomautuksen tarkoituksena on osoittaa, että halutut kertoimet x_n ja y_n voidaan selvittää tehokkaasti matriisikertolaskulla. Merkitään matriisia

$$A_i = \begin{pmatrix} x_{i-1} & x_i \\ y_{i-1} & y_i \end{pmatrix}.$$

Lukujen x_i ja y_i rekursiivisen määritelmän nojalla pätee, että

$$A_i \cdot \begin{pmatrix} 0 & 1 \\ 1 & -s_i \end{pmatrix} = \begin{pmatrix} x_i & x_{i-1} - x_i s_i \\ y_i & y_{i-1} - y_i s_i \end{pmatrix} = \begin{pmatrix} x_i & x_{i+1} \\ y_i & y_{i+1} \end{pmatrix} = A_{i+1}.$$

Merkitään

$$S_i = \begin{pmatrix} 0 & 1 \\ 1 & -s_i \end{pmatrix} \quad \text{ja} \quad A_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Tällöin

$$A_{n+1} = A_1 S_1 \dots S_{n-1} \begin{pmatrix} 0 & 1 \\ 1 & -s_n \end{pmatrix} = \begin{pmatrix} x_n & x_{n+1} \\ y_n & y_{n+1} \end{pmatrix}.$$

Edellä esitettiin huomautuksen muodossa tehokkaampi tapa selvittää yksittäisratkaisu lineaariselle Diofantoksen yhtälölle $ax+by = \text{syt}(a,b)$. Matriisista A_{n+1} nähdään lineaarisen Diofantoksen yhtälön ratkaisu x_n ja y_n. Seuraavassa huomautuksessa saadaan lisätietoa huomautuksessa 3.3 esiintyvästä matriisista.

Huomautus 3.4. Matriisi

$$S_i = \begin{pmatrix} 0 & 1 \\ 1 & -s_i \end{pmatrix}$$

on alkeismatriisien

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{ja} \quad \begin{pmatrix} 1 & -s_i \\ 0 & 1 \end{pmatrix}$$

tulomatriisi. Tätä tulosta tullaan hyödyntämään tutkielmassa myöhemmin ratkaisutapoja vertailtaessa.

Jos alkuperäisessä Diofantoksen yhtälössä $r_n = \text{syt}(a,b) \neq c$, niin tästä saadaan yhtälön ratkaisu kertomalla $\tilde{x}_0$ ja $\tilde{y}_0$ vakiolla k. Tällöin päädytään lopulta tilanteeseen

$$ak\tilde{x}_0 + bk\tilde{y}_0 = c,$$

josta Diofantoksen yhtälön yksittäisratkaisu $k\tilde{x}_0$, $k\tilde{y}_0$ voidaan nähdä.

Esitetään ja todistetaan vielä tämän kappaleen lopuksi Diofantoksen yhtälöiden ratkaisuihin liittyvä lause, mikä määrittelee ratkaisujoukon rakenteen. Käytetään lauseen todistuksessa apuna Burtonin Elementary Number Theory -kirjaa [11].

Lause 3.5. *Olkoot a, b ja c nollasta eroavia kokonaislukuja. Jos x_0, y_0 on Diofantoksen yhtälön yksittäisratkaisu, niin kaikki ratkaisut ovat muotoa*

$$x = x_0 + \frac{nb}{d} \quad ja \quad y = y_0 - \frac{na}{d},$$

missä n on mikä tahansa kokonaisluku ja $d = syt(a, b)$.

Todistus. Olkoon x_0, y_0 Diofantoksen yhtälön yksittäisratkaisu. Jos $\tilde{x}$, $\tilde{y}$ on toinen ratkaisu, niin

$$ax_0 + by_0 = c = a\tilde{x} + b\tilde{y},$$

mikä on yhtäpitävää sen kanssa, että

$$a(\tilde{x} - x_0) = b(y_0 - \tilde{y}).$$

Koska $d = \text{syt}(a, b)$, niin luvut a ja b voidaan esittää muodossa $a = dr$ ja $b = ds$, missä r, s ovat suhteellisia alkulukuja. Tällöin sijoittamalla $a = dr$ ja $b = ds$ sekä jakamalla puolittain luvulla d yhtälö

$$a(\tilde{x} - x_0) = b(y_0 - \tilde{y})$$

voidaan muuttaa muotoon

$$r(\tilde{x} - x_0) = s(y_0 - \tilde{y}). \tag{3.1}$$

Näin ollen tiedetään, että $r \mid s(y_0 - \tilde{y})$ ja koska $\text{syt}(r, s) = 1$, niin saadaan että $r \mid (y_0 - \tilde{y})$. Tällöin pätee, että

$$y_0 - \tilde{y} = rn, \quad \text{missä} \quad n \in \mathbb{Z}.$$

Sijoittamalla yhtälöön 3.1 $y_0 - \tilde{y} = rn$ ja jakamalla puolittain luvulla r saadaan, että

$$\tilde{x} - x_0 = sn.$$

Täten, koska $a = dr$ ja $b = ds$, niin

$$\tilde{x} = x_0 + sn = x_0 + \frac{nb}{d} \quad \text{ja} \quad \tilde{y} = y_0 - rn = y_0 - \frac{na}{d}.$$

Osoitetaan vielä, että kyseiset lausekkeet toteuttavat Diofantoksen yhtälön riippumatta kokonaisluvun n valinnasta.

$$\begin{aligned} a\tilde{x} + b\tilde{y} &= a(x_0 + \frac{nb}{d}) + b(y_0 - \frac{na}{d}) \\ &= ax_0 + \frac{nab}{d} + by_0 - \frac{nab}{d} \\ &= ax_0 + by_0 = c \end{aligned}$$

Näin ollen Diofantoksen yhtälöllä on olemassa äärettömän monta ratkaisua. Lisäksi kaikki ratkaisut ovat muotoa

$$\tilde{x} = x_0 + \frac{nb}{d} \quad \text{ja} \quad \tilde{y} = y_0 - \frac{na}{d}.$$

□

Nyt on todistettu Diofantoksen yhtälöiden ratkaisujoukon rakenteeseen liittyvä lause 3.5. Käytiin myös läpi täsmällisesti milloin lineaarisella Diofantoksen yhtälölle löytyy ratkaisu. Lisäksi löydettiin tehokas tapa löytää lineaarisen Diofantoksen yhtälön ratkaisu hyödyntäen matriisikertolaskua. Seuraavassa kappaleessa tätä menetelmää sovelletaan lineaarisen Diofantoksen yhtälöryhmän tapaukseen. Kappaleessa lineaaristen Diofantoksen yhtälöryhmien ratkaisemiseksi tullaan myös hyödyntämään aiemmin tutkielmassa esitettyä Smithin normaalimuotoa.

4 Lineaariset Diofantoksen yhtälöryhmät

Lineaarisella Diofantoksen yhtälöryhmällä tarkoitetaan yhtälöryhmää

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n & = b_1 \\ & \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n & = b_m, \end{cases}$$

missä sekä muuttujien x_i kertoimet a_{ij}, että luvut b_i ovat kokonaislukuja. Diofantoksen yhtälöryhmälle etsitään ainoastaan kokonaislukuratkaisuja. Lineaarisesta Diofantoksen yhtälöryhmästä esimerkkinä toimii yhtälöryhmä

$$\begin{cases} 3x + 4y & = 11 \\ 5x + 8y & = 21 \\ 3x + 7y & = 17. \end{cases}$$

Lineaaristen yhtälöryhmien kohdalla tiedetään, että ratkaisuja voi olla yksi, äärettömän monta tai ei ollenkaan kuten kappaleessa 1.1 kerrottiin. Lineaaristen Diofantoksen yhtälöryhmien kohdalla heräävät samat kysymykset. Mistä tiedetään milloin lineaarisella Diofantoksen yhtälöryhmällä on ratkaisu? Ja jos sillä on ratkaisu, miten on mahdollista löytää sen koko ratkaisujoukko? Tässä kappaleessa lähdetään selvittämään näihin kahteen kysymykseen vastausta.

Lineaarisiin Diofantoksen yhtälöryhmiin liittyvien kysymysten ratkaisemisen tueksi esitellään lause, jossa lineaariselle Diofantoksen yhtälöryhmälle esitetään neljä yhtäpitävä väitettä. Lauseen 4.1 tarkoituksena on antaa ehtoja, sille, milloin lineaarisella Diofantoksen yhtälöryhmällä on ratkaisu. Lauseen todistuksessa käytetään hyödyksi edellisen kappaleen Smithin normaalimuotoa. Kappaleen lopussa vertaillaan myös, miten lineaaristen Diofantoksen yhtälöryhmien ratkaisujoukko vertautuu lineaaristen yhtälöryhmien ratkaisujoukkoon. Aloitetaan kuitenkin ensin määrittelemällä, mitä tarkoitetaan ekvivalenssinuolella $\Leftrightarrow$ tässä kappaleessa, sillä se poikkeaa hieman ekvivalenssinuolen merkityksestä aiemmin tässä tutkielmassa.

Ekvivalenssinuoli $\Leftrightarrow$ tarkoittaa tässä kappaleessa, että kaksi yhtälöä ovat yhtäpitävät jokaisella $\overline{x} \in \mathbb{Z}^n$. Esimerkiksi matriisiyhtälöiden $A\overline{x} = \overline{b} \Leftrightarrow \overline{x} = A^{-1}\overline{b}$ kohdalla ekvivalenssinuoli tarkoittaa, että kaikilla $\overline{x} \in \mathbb{Z}^n$ pätee, että $A\overline{x} = \overline{b}$ jos ja vain jos $\overline{x} = A^{-1}\overline{b}$. Lisäksi tässä kappaleessa jos $\overline{y}$ on vaakavektori, niin merkinnällä $R\overline{y}$ tarkoitetaan $R\overline{y}^T$.

Nyt voidaan esittää lineaarisiin Diofantoksen yhtälöryhmiin liittyvä ensimmäinen lause. Todistetaan lause 4.1 käyttäen apuna Lazebnikin artikkelia [3].

Lause 4.1. *Olkoon A, L, R, D kuten lauseessa 2.2, $\overline{b} \in \mathbb{Z}^n$ ja $\overline{c} = L\overline{b}$. Tällöin seuraavat neljä väitettä ovat yhtäpitäviä:*
(1) Lineaarisella yhtälöryhmällä $A\overline{x} = \overline{b}$ on kokonaislukuratkaisu
(2) Lineaarisella yhtälöryhmällä $D\overline{y} = \overline{c}$ on kokonaislukuratkaisu
(3) Jokaiselle rationaalivektorille $\overline{u}$, jolle $\overline{u}A$ on kokonaislukuvektori pätee, että $\overline{u}\overline{b}$ on kokonaisluku
(4) Jokaiselle rationaalivektorille $\overline{v}$, jolle $\overline{v}D$ on kokonaislukuvektori pätee, että $\overline{v}\overline{c}$ on kokonaisluku.

Todistus. Todistetaan ensin, että väitteet (1) ja (2) ovat yhtäpitäviä keskenään. Aloitetaan olettamalla, että on olemassa vektori $\overline{x} \in \mathbb{Z}$, jolla $A\overline{x} = \overline{b}$. Koska $D = LAR$, niin saadaan yhtälön $A\overline{x} = \overline{b}$ kanssa ekvivalentti muoto $(L^{-1}DR^{-1})\overline{x} = \overline{b}$. Kertomalla puolittain vasemmalta yhtälöä $(L^{-1}DR^{-1})\overline{x} = \overline{b}$ matriisilla L sekä merkitsemällä $\overline{c} = L\overline{b}$ saadaan yhtälö muotoon $D(R^{-1}\overline{x}) = \overline{c}$. Merkitsemällä $\overline{y} = R^{-1}\overline{x}$ yhtälö $D(R^{-1}\overline{x}) = \overline{c}$ on ekvivalentti yhtälön $D\overline{y} = \overline{c}$ kanssa. Koska $R \in GL_n(\mathbb{Z})$, niin lemman 1.10 nojalla $R^{-1} \in GL_n(\mathbb{Z})$. Tällöin, koska $\overline{x} \in \mathbb{Z}^n$, niin $\overline{y} = R^{-1}\overline{x} \in \mathbb{Z}^n$ lemman 1.6 nojalla. Näin ollen (1) $\Rightarrow$ (2). Suunta (2) $\Rightarrow$ (1) osoitetaan vastaavasti. Siispä väitteet (1) ja (2) ovat yhtäpitäviä keskenään.

Todistetaan seuraavaksi, että väitteet (3) ja (4) ovat yhtäpitäviä keskenään. Oletetaan aluksi, että jokaiselle rationaalivektorille $\overline{u}$, jolle $\overline{u}A$ on kokonaislukuvektori pätee, että $\overline{u}\overline{b}$ on kokonaisluku. Oletetaan lisäksi, että $\overline{v}D \in \mathbb{Z}^n$, kun $\overline{v}$ on rationaalivektori. Todistetaan, että tällöin $\overline{v}\overline{c} \in \mathbb{Z}$.

Koska $D = LAR$, niin ehdosta $\overline{v}D$ seuraa, että $\overline{v}(LAR) \in \mathbb{Z}^n$ ja edelleen $(\overline{v}L)AR \in \mathbb{Z}^n$. Kertomalla puolittain oikealta matriisilla R^{-1} väite $(\overline{v}L)AR \in \mathbb{Z}^n$ voidaan muuttaa ekvivalenttiin muotoon $(\overline{v}L)A \in \mathbb{Z}^n R^{-1}$. Lemman 1.11 nojalla seuraa siis, että $(\overline{v}L)A \in \mathbb{Z}^n$. Merkitsemällä $\overline{v}L = \overline{u}$ yhtälö $(\overline{v}L)A \in \mathbb{Z}^n$ on ekvivalentti väitteen $\overline{u}A \in \mathbb{Z}^n$ kanssa. Nyt koska $L \in GL_n(\mathbb{Z})$ ja $\overline{v} \in \mathbb{Q}^n$, niin $\overline{u} \in \mathbb{Q}^m$ ja tällöin väitteen (3) nojalla $\overline{u}\overline{b} \in \mathbb{Z}$. Huomataan, että tiedoista $\overline{u} = \overline{v}L$ ja $\overline{c} = L\overline{b}$ saadaan, että $\overline{v}\,\overline{c} = (\overline{v}L)(L^{-1}\overline{c}) = \overline{u}\overline{b} \in \mathbb{Z}$. Näin ollen (3) $\Rightarrow$ (4). Vastakkainen suunta (4) $\Rightarrow$ (3) tulee vastaavasti aloittamalla oletuksesta $\overline{u}A \in \mathbb{Z}^n$. Siispä väitteet (3) ja (4) ovat keskenään yhtäpitäviä.

Vielä viimeisenä todistetaan, että väitteet (2) ja (4) ovat yhtäpitäviä. Oletetaan ensin, että on olemassa vektori $y \in \mathbb{Z}^n$, jolla $D\overline{y} = \overline{c}$. Todistetaan, että tällöin jokaiselle rationaalivektorille $\overline{v}$, jolle $\overline{v}D$ on kokonaislukuvektori pätee, että $\overline{v}\overline{c} \in \mathbb{Z}$. Oletetaan nyt, että $\overline{v}$ on ratinaalivektori, jolla $\overline{v}D \in \mathbb{Z}^n$. Jokaiselle $\overline{v} \in \mathbb{Q}^m$ pätee, että $\overline{v}(D\overline{y}) = \overline{v}\overline{c}$, kun yhtälöä $D\overline{y} = \overline{c}$ molempia puolia kerrotaan vasemmalta. Koska $\overline{y} \in \mathbb{Z}^n$ ja jos $\overline{v}D \in \mathbb{Z}^n$ niin määritelmän 1.6 nojalla $\overline{v}D\overline{y} \in \mathbb{Z}$. Tällöin siis $\overline{v}\overline{c} \in \mathbb{Z}$. Näin ollen (2) $\Rightarrow$ (4). Osoitetaan seuraavaksi vastakkainen suunta (4) $\Rightarrow$ (2). Oletetaan, että (4) on voimassa ja $\overline{c}$ on ehdon (4) mukainen. Osoitetaan, että tällöin $\overline{c} = (c_1, \ldots, c_s, 0, \ldots, 0)$. Tehdään antiteesi, että on olemassa sellainen $\overline{c}$, että sen j:s koordinaatti $c_j \neq 0$, $j > s$. Olkoon lisäksi $\overline{v} = (0, \ldots, 0, 1/(2c_j), 0, \ldots, 0)$, missä $1/(2c_j)$ on j:s koordinaatti. Koska $\overline{v}D = \overline{0} \in \mathbb{Z}^n$, niin väitteen (4) nojalla $\overline{v}\overline{c} \in \mathbb{Z}$. Toisaalta suoraan laskemalla havaitaan, että $\overline{v}\overline{c} = 1/2$, joka on ristiriita. Siispä $c_j = 0$ kaikille $j > s$. Olkoon seuraavaksi, että $\overline{v_i} = (0, , \ldots, 0, 1/d_i, 0, \ldots, 0)$, missä $i = 1, \ldots, s$. Nyt koska jokaisella indeksillä i $\overline{v_i}D \in \mathbb{Z}^n$, niin väitteen (4) nojalla $\overline{v_i c} \in \mathbb{Z}$. Näin ollen $c_i/d_i \in \mathbb{Z}$. Tällöin löytyy kokonaislukuvektori $\overline{y} = (y_1, \ldots, y_s, 0, \ldots, 0)$, missä $y_i = c_i/d_i \in \mathbb{Z}$, joka on yhtälön $D\overline{y} = \overline{c}$ ratkaisu. Näin ollen (4) $\Rightarrow$ (2) ja olemme osoittaneet väitteet (2) ja (4) yhtäpitäviksi.

Väitteiden (1) $\Leftrightarrow$ (3), (1) $\Leftrightarrow$ (4) ja (2) $\Leftrightarrow$ (3) yhtäpitävyys seuraa ylläolevista kolmesta yhtäpitävyydestä. Näin ollen kaikki väitteet ovat keskenään yhtäpitäviä. □

Nyt on saatu todistettua lause 4.1. Esitetään seuraavassa lauseessa, mikä yhteys ratkaisujoukoilla $\{\overline{x} \in \mathbb{Z}^n \mid A\overline{x} = \overline{b}\}$ ja $\{\overline{y} \in \mathbb{Z}^n \mid D\overline{y} = \overline{c}\}$ on.

Lause 4.2. *Merkitään ratkaisujoukkoa* $\{\overline{x} \in \mathbb{Z}^n \mid A\overline{x} = \overline{b}\} = \tilde{A}$ *ja ratkaisujoukkoa* $\{\overline{y} \in \mathbb{Z}^n \mid D\overline{y} = \overline{c}\} = \tilde{D}$. *Tällöin pätee, että*

$$R\tilde{D} = \tilde{A}.$$

Todistus. Todistuksessa riittää osoittaa, että jokainen joukon $R\tilde{D}$ alkio kuuluu joukkoon $\tilde{A}$ sekä, että jokainen joukon $\tilde{A}$ alkio kuuluu joukkoon $R\tilde{D}$.

Osoitetaan ensin, että jokainen joukon $R\tilde{D}$ alkio kuuluu joukkoon $\tilde{A}$. Olkoon $\overline{y}$, jolle pätee $D\overline{y} = c = L\overline{b}$. Tällöin Smithin normaalimuodon nojalla saadaan, että $D\overline{y} = L\overline{b}$ on ekvivalenttia yhtälön $LAR\overline{y} = L\overline{b}$. Nyt kertomalla yhtälöä puolittain vasemalta matriisilla L^{-1} saadaan

$$AR\overline{y} = \overline{b}.$$

Siispä $R\overline{y} \in \tilde{A}$ ja todistuksen toinen suunta on saatu osoitettua.

Osoitetaan seuraavaksi, että jokainen joukon $\tilde{A}$ alkio kuuluu joukkoon $R\tilde{D}$. Olkoon $\overline{x} \in \tilde{A}$. Nyt riittää osoittaa, että $\overline{x} = R\overline{y}$ jollain $\overline{y}$, jolla $D\overline{y} = \overline{c} = L\overline{b}$. Matriisilla R kertominen antaa bijektion joukosta $\mathbb{Z}^n$ joukkoon $\mathbb{Z}^n$, niin on olemassa jokin $\overline{y} \in \mathbb{Z}^n$, jolla $R\overline{y} = \overline{x}$. Tällöin sijoittamalla $\overline{x} = R\overline{y}$ sekä kertomalla yhtälöä vasemmalta matriisilla L yhtälö $A\overline{x} = \overline{b}$ on ekvivalentti yhtälön $LAR\overline{y} = L\overline{b}$ kanssa. Nyt Smithin normaalimuodon nojalla yhtälö saadaan ekvivalenttiin muotoon yhtälön

$$D\overline{y} = \overline{c}$$

kanssa. Siispä $\overline{x} \in R\tilde{D}$. Ja näin ollen $R\tilde{D} = \tilde{A}$. □

Nyt on saatu esitettyä ratkaisujoukkojen $\{\overline{x} \in \mathbb{Z}^n \mid A\overline{x} = \overline{b}\}$ ja $\{\overline{y} \in \mathbb{Z}^n \mid D\overline{y} = \overline{c}\}$ välinen yhteys. Määritetään seuraavaksi lineaarisen Diofantoksen yhtälöryhmän $A\overline{x} = \overline{b}$ ratkaisujoukko. Ratkaisujoukon selvittämiseksi esitetään ensin lause 4.3, jossa määritellään yhtälöryhmän $D\overline{y} = \overline{c}$ ratkaisujoukko.

Lause 4.3. *Yhtälöryhmällä $D\overline{y} = \overline{c}$ on ratkaisu jos ja vain jos*

$$c_{s+1} = \cdots = c_n = 0 \quad ja \quad d_i | c_i, \quad i = 1, \ldots, s.$$

Lisäksi jos Diofantoksen yhtälöryhmällä on ratkaisu sen ratkaisujoukko on muotoa

$$\{(y_1, \ldots, y_s, t_1, \ldots, t_{n-s}) \mid t_1, \ldots, t_{n-s} \in \mathbb{Z}\}.$$

Todistus. Lause on suoraviivainen seuraus lauseen 4.1 todistuksesta. □

Nyt voidaan määrittää alkuperäisen lineaarisen Diofantoksen yhtälöryhmän $A\overline{x} = \overline{b}$ ratkaisujoukko. Lauseen 4.2 nojalla lineaarisen Diofantoksen yhtälöryhmän muodosta $D\overline{y} = \overline{c}$ saadaan alkuperäisen Diofantoksen yhtälöryhmän $A\overline{x} = \overline{b}$ ratkaisut yhtälön $\overline{x} = R\overline{y}$ avulla. Tässä matriisi $R \in GL_n(\mathbb{Z})$ esittää Smithin normaalimuodon oikelta suoritettavia matriisikertolaskuja. Esitetään vielä alkuperäisen lineaaristen Diofantosten yhtälöryhmien $A\overline{x} = \overline{b}$ ratkaisuvaihtoehdot vastaavasti kuin lineaaristen yhtälöryhmien ratkaisuvaihtoehdot kappaleessa 1.1. Ratkaisujoukossa vektorilla $\overline{e}_i$ tarkoitetaan vektoria. jossa koordinaatin i paikalla on luku 1 ja muut koordinaatit ovat 0. Lineaarisen Diofantoksen yhtälöryhmän ratkaisuvaihtoehdot ovat

- tyhjä joukko $\emptyset$
- yksittäinen ratkaisu $\overline{x} = R\overline{y} = R(y_1, \ldots, y_n)^T$
- äärettömän monta ratkaisua, jotka voidaan esittää muodossa

$$\{R(y_1, \ldots, y_s, 0 \ldots, 0)^T + t_1 R\overline{e}_{s+1} \\ + \cdots + t_{n-s} R\overline{e}_n \,|\, t_1, \ldots, t_{n-s} \in \mathbb{Z}\}.$$

Lineaarisen Diofantoksen yhtälöryhmän ratkaisujoukko jakaantuu yksittäisratkaisuun sekä yhtälöryhmän homogeenisen osan ratkaisuun. Yhtälöryhmän yksittäisratkaisu on $R(y_1, \ldots, y_s, 0, \ldots, 0)$. Tällöin lineaarisen Diofantoksen yhtälöryhmän homogeenisen osan ratkaisu on muotoa $t_1 R\overline{e}_{s+1} + \cdots + t_{n-s} R\overline{e}_n$. Lineaariseen homogeeniseen Diofantoksen yhtälöryhmään tutustutaan tarkemmin kappaleessa 5, jossa käsitellään Siegelin lemmaa [1].

Vertaillaan seuraavaksi hieman lineaarisen yhtälöryhmän ja lineaarisen Diofantoksen yhtälöryhmän ratkaisujoukkojen homogeenisiä osia. Lineaarisen yhtälöryhmän kohdalla ratkaisujoukon homogeeninen osa on aliavaruus avaruudessa $\mathbb{R}^n$. Vastaavasti lineaarisen Diofantoksen yhtälöryhmän kohdalla homogeenisen osan ratkaisujoukko

$$\{t_1 R\overline{e}_{s+1} + \cdots + t_{n-s} R\overline{e}_n \,|\, t_1, \ldots, t_{n-s} \in \mathbb{Z}\}$$

on hila. Kuten kappaleessa 1.3 kerrottiin, niin lineaarisen Diofantoksen yhtälöryhmän ratkaisujoukon kohdalla kyseessä on hilan erikoistapaus, sillä vektorit $R\overline{e}_{s+1}, \ldots, R\overline{e}_n \in \mathbb{Z}^n$. Hilan generoivat vektorit $R\overline{e}_{s+1}, \ldots, R\overline{e}_n \in \mathbb{Z}^n$ ovat lineaarisesti riippumattomia, koska vektorit $\overline{e}_i$ ovat lineaarisesti riippumattomia ja $R \in GL_n(\mathbb{Z})$, jolloin vektoreita $R\overline{e}_{s+1}, \ldots, R\overline{e}_n \in \mathbb{Z}^n$ ei voida esittää toistensa lineaarikombinaatioina. Nämä lineaarisesti riippumattomat vektorit toimivat hilan kantavektoreina.

Lineaarisen Diofantoksen yhtälöryhmien ratkaisujoukkoa on saatu verrattua lineaarisen yhtälöryhmien ratkaisujoukkoon. Voidaan havaita, että ne ovat hyvin samankaltaiset. Esitetään seuraavaksi esimerkki lineaarisen Diofantoksen yhtälöryhmän ratkaisemista. Esimerkissa käytetään hyödyksi Smithin normaalimuotoa 2.2 sekä lausetta 4.1 Diofantoksen yhtälöryhmän ratkaisemiseksi.

Esimerkki 4.4. Ratkaise lineaarinen Diofantoksen yhtälöryhmä $A\overline{x} = \overline{b}$, missä

$$A = \begin{pmatrix} 3 & 2 & 1 \\ -4 & 2 & 3 \end{pmatrix}, \quad \overline{x} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \text{ ja } \overline{b} = \begin{pmatrix} 12 \\ -15 \end{pmatrix}.$$

Ratkaisu. Matriisi A voidaan muuttaa muotoon $D = LAR$ hyödyntäen modulaarimatriiseja, jotka toteuttavat matriisille A rivi- ja sarakeoperaatiot säilyttäen kuitenkin kokonaislukualkiot. Rivien välisiä operaatioita suoritetaan 2×2-kokoisilla matriiseilla L_i ja sarakeoperaatioita suoritetaan 3×3-kokoisilla matriiseilla R_i. Matriisien alaindeksi kertoo järjestyksen, jossa matriisitulo toteutetaan.

$$R_1 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \quad R_2 = \begin{pmatrix} 1 & -2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad R_3 = \begin{pmatrix} 1 & 0 & -3 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

$$L_4 = \begin{pmatrix} 1 & 0 \\ -3 & 1 \end{pmatrix}, \quad R_5 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & -2 \\ 0 & -1 & 1 \end{pmatrix}, \quad R_6 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 5 \\ 0 & 0 & 1 \end{pmatrix}.$$

Jokainen matriisi L_i ja R_i ovat modulaarimatriiseja, sillä niiden determinantti on 1 tai -1, joten R_1, R_2, R_3, L_4, R_5 ja $R_6 \in GL_n(\mathbb{Z})$. Olkoon $L = L_4$ ja $R = R_1R_2R_3R_5R_6$. Tällöin matriisi D voidaan esittää muodossa

$$D = LAR = \begin{pmatrix} 1 & 0 \\ -3 & 1 \end{pmatrix} \begin{pmatrix} 3 & 2 & 1 \\ -4 & 2 & 3 \end{pmatrix} \begin{pmatrix} 0 & -1 & -4 \\ 0 & 3 & 13 \\ 1 & -3 & -14 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \text{ ja}$$

$$\overline{c} = L\overline{b} = \begin{pmatrix} 1 & 0 \\ -3 & 1 \end{pmatrix} \begin{pmatrix} 12 \\ -15 \end{pmatrix} = \begin{pmatrix} 12 \\ -51 \end{pmatrix}.$$

Nyt ratkaisemalla $\overline{y}$ yhtälöstä $D\overline{y} = \overline{c}$ ja sijoittamalla $\overline{x} = R\overline{y}$ saadaan lopulta

$$\overline{x} = \begin{pmatrix} 0 & -1 & -4 \\ 0 & 3 & 13 \\ 1 & -3 & -14 \end{pmatrix} \begin{pmatrix} 12 \\ -51 \\ t_1 \end{pmatrix} = \begin{pmatrix} 51 - 4t_1 \\ -153 + 13t_1 \\ 165 - 14t_1 \end{pmatrix}, \quad t_1 \in \mathbb{Z}.$$

Ratkaisujoukko $\overline{x}$ voidaan halutessaan esittää myös muodossa

$$\overline{x} = \begin{pmatrix} 51 \\ -153 \\ 165 \end{pmatrix} + t_1 \begin{pmatrix} -4 \\ 13 \\ -14 \end{pmatrix},$$

missä $\left(\begin{smallmatrix} 51 \\ -153 \\ 165 \end{smallmatrix}\right)$ on yhtälöryhmän yksittäisratkaisu. □

Näin on saatu esitettyä esimerkki lineaarisen Diofantoksen yhtälöryhmän ratkaisemisesta. Myöhemmin tutkielmassa kappaleessa 6 käydään läpi muutama esimerkki lisää. Seuraavaksi vuorossa on kappale 5, jossa kerrotaan Siegelin lemmasta. Siegelin lemma käsittelee erikoistapausta lineaarisesta Diofantoksen yhtälöryhmästä.

5 Siegelin lemma

Tämän kappaleen tarkoituksena on esitellä Siegelin lemma 5.8. Kyseinen lemma todistuksineen esitetään kappaleen lopuksi. Siegelin lemmaan johdatellaan ensin hieman lemman 5.7 avulla, joka mukailee Siegelin lemman tulosta. Kappaleen aluksi esitetään kuitenkin muutama lemma ja määritelmä, joita tarvitaan myöhemmin tässä kappaleessa. Aloitetaan esittelemällä kyyhkyslakkaperiaate [7].

Lemma 5.1 (Kyyhkyslakkaperiaate)**.** *Olkoon A ja B äärellisiä epätyhjiä joukkoja, joille pätee, että $|A| > |B|$. Olkoon $f : A \to B$ kuvaus. Tällöin joukossa A on olemassa alkiot x ja y, siten että $x \neq y$, joille pätee, että $f(x) = f(y)$.*

Näin on saatu esitettyä kyyhkyslakkaperiaate, jota tullaan hyödyntämään myöhemmin tässä kappaleessa Siegelin lemman todistuksessa. Seuraavaksi määritelmissä esitetään joukko R_B sekä matriisia A vastaava kuvaus. Kyseisiä määritelmiä hyödynnetään tulevissa lemmoissa.

Määritelmä 5.2. Olkoon matriisi

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1N} \\ \vdots & \ddots & \vdots \\ a_{M1} & \cdots & a_{MN} \end{pmatrix},$$

missä $a_{ij} \in \mathbb{Z}$. Tällöin määritellään, että $|A| := \max\limits_{1 \leq i \leq M, 1 \leq j \leq N} |a_{ij}|$.

Seuraavassa määritelmässä esitetään merkintä $[-B, B]$, missä B on positiivinen kokonaisluku. Kyseisellä merkinnällä tarkoitetaan kokonaislukuväliä luvusta $-B$ lukuun B.

Määritelmä 5.3. Olkoon matriisi A kuten määritelmässä 5.2 sekä merkitään joukkoa $R_B = [-B, B] \times \cdots \times [-B, B] \subset \mathbb{Z}^N$. Tällöin merkitään

$$AR_B := \{A\overline{r} \,|\, \overline{r} \in R_B\}.$$

Nyt on saatu määriteltyä, mitä tarkoittavat merkinnät $|A|$ sekä AR_B. Kyseisiä määritelmiä tullaan käyttämään lemmoissa, jotka esitellään seuravaaksi. Määritetään seuraavaksi joukon R_B koko, jonka jälkeen esitetään lemma 5.5, joka kertoo millainen joukko AR_B on.

Lemma 5.4. *Olkoon $R_B = [-B, B] \times \cdots \times [-B, B] \subset \mathbb{Z}^N$ joukko, missä B on positiivinen kokonaisluku. Tällöin*

$$|R_B| = (2B + 1)^N.$$

Todistus. Joukon koolla $|R_B|$ tarkoitetaan joukon alkioiden lukumäärää. Koska välillä $[-B, B]$ on $2B+1$ alkiota, niin tuloperiaatteen nojalla joukossa R_B on $(2B+1)^N$ alkiota. □

Lemma 5.5. *Olkoon matriisi $A \in M_{M\times N}(\mathbb{Z})$ ja joukko R_B kuten lemmassa 5.4. Tällöin pätee, että*

$$AR_B \subset [-N|A|B, N|A|B] \times \cdots \times [-N|A|B, N|A|B] \subset \mathbb{Z}^M.$$

Lisäksi pätee, että

$$|AR_B| \leq (2N|A|B+1)^M.$$

Todistus. Olkoon matriisi A ja joukko R_B kuten määritelmässä 5.3. Osoitetaan ensin, että

$$AR_B \subset [-N|A|B, N|A|B] \times \cdots \times [-N|A|B, N|A|B].$$

Määritelmän 5.3 nojalla tiedetään, että $a_{ij} \in \mathbb{Z}$ kaikilla i, j. Lisäksi jos $\overline{r} = (r_1, \ldots, r_N) \in R_B$, niin $a_{i1}r_1 + \cdots + a_{iN}r_N \in \mathbb{Z}$ kaikilla $1 \leq i \leq m$. Tällöin siis $A\overline{r} \in \mathbb{Z}^M$. Tutkitaan seuraavaksi vektorin $A\overline{r}$ ensimmäisen koordinaatin $a_{11}r_1 + \cdots + a_{1N}r_N$ kokoa. Kolmioepäyhtälön nojalla

$$|a_{11}r_1 + \cdots + a_{1N}r_N| \leq |a_{11}r_1| + \cdots + |a_{1N}r_N|.$$

Nyt ottamalla tulosta itseisarvot erikseen sekä arvioimalla, että $|r_1|, \ldots, |r_N| \leq |B|$ ja $|a_{11}|, \ldots, |a_{1N}| \leq |A|$ saadaan

$$|a_{11}r_1| + \cdots + |a_{1N}r_N| \leq |a_{11}||r_1| + \cdots + |a_{1N}||r_N| \leq |A||B| + \cdots + |A||B|.$$

Muodostamalla summasta kertolasku saadaan luvun $a_{11}r_1 + \cdots + a_{1N}r_N$ koolle lopullinen arvio

$$|a_{11}r_1 + \cdots + a_{1N}r_N| \leq N|A||B|.$$

Nyt, koska $|a_{11}r_1 + \cdots + a_{1N}r_N| \leq N|A||B|$, niin täytyy olla, että

$$a_{11}r_1 + \cdots + a_{1N}r_N \subset [-N|A|B, N|A|B].$$

Vastaavasti muille koordinaateille saadaan samanlainen arvio, jolloin ollaan saatu osoitettua, että

$$AR_B \subset [-N|A|B, N|A|B] \times \cdots \times [-N|A|B, N|A|B].$$

Näytetään vielä, että $[-N|A|B, N|A|B] \times \cdots \times [-N|A|B, N|A|B] \subset \mathbb{Z}^M$. Tiedetään, että $N, |A|$ ja $B \in \mathbb{Z}$, jolloin myös $N|A|B \in \mathbb{Z}$. Lisäksi koordinaatteja on M kappaletta, jolloin

$$AR_B \subset [-N|A|B, N|A|B] \times \cdots \times [-N|A|B, N|A|B] \subset \mathbb{Z}^M.$$

Arvio $|AR_B| \leq (2N|A|B+1)^M$ seuraa lemman 5.4 tuloksesta. □

Nyt on saatu todistettua lemmat 5.4 ja 5.5. Esitetään vielä yksi lemma, jota tullaan hyödyntämään Siegelin lemmaa mukailevan lemman 5.7 todistuksessa. Seuraavassa lemmassa tulevat esiintymään merkinnät N, M, B ja $|A|$. Kyseisessä lemmassa esiintyvät luvut N ja M, B ja $|A|$ ovat kaikki luonnollisia lukuja.

Lemma 5.6. *Olkoon $N > M$. Tällöin pätee, että*

$$(2N|A|B+1)^M < (2B+1)^N,$$

kunhan B on kokonaisluku, joka toteuttaa ehdon

$$B \geq (2N|A|)^{\frac{M}{N-M}}.$$

Todistus. Tiedetään, että $N > 1$, M, B ja $|A| \geq 1$, jolloin saadaan, että

$$(2N|A|B+1)^M < (2N|A|B+2N|A|B)^M = (4N|A|B)^M.$$

Lisäksi tiedetään, että $(2B)^N < (2B+1)^N$. Näin ollen väitteen

$$(2N|A|B+1)^M < (2B+1)^N,$$

todistamiseksi riittää osoittaa, että

$$(4N|A|B)^M < (2B)^N, \quad \text{kun} \quad B \geq (2N|A|)^{\frac{M}{N-M}}.$$

Lähdetään etsimään kokonaislukua B, jolla epäyhtälö $(4N|A|B)^M < (2B)^N$ toteutuu. Ottamalla kantaluvun B potenssi molemmilta puolilta potenssilaskusääntöjen mukaisesti erikseen saadaan

$$B^M(4N|A|)^M < B^N 2^N.$$

Epäyhtälö voidaan jakaa puolittain luvuilla B^M ja 2^N, jolloin se voidaan muokata muotoon

$$\frac{(4N|A|)^M}{2^N} < B^{N-M}.$$

Tarkastellaan nyt ylläolevan epäyhtälön vasenta puolta. Oletuksen nojalla $N > M$ ja, koska $N, M \in \mathbb{N}$, niin $\frac{1}{2^N} < \frac{1}{2^M}$. Tällöin

$$\frac{(4N|A|)^M}{2^N} < \frac{(4N|A|)^M}{2^M} = (2N|A|)^M.$$

Nyt siis riittää etsiä sellainen B, jolla

$$(2N|A|)^M \leq B^{N-M}.$$

Ottamalla tästä juuren puolittain saadaan ekvivalentti epäyhtälö

$$(2N|A|)^{\frac{M}{N-M}} \leq B.$$

Siispä on saatu osoitettua, että

$$(2N|A|B+1)^M < (2B+1)^N, \quad \text{kun} \quad B \geq (2N|A|)^{\frac{M}{N-M}}.$$

□

Näin ollen on saatu esitettyä lemmat, joita tullaan tarvitsemaan lauseen 5.7 todistamista varten. Lause 5.7 käsittelee erikoistapausta lineaarisesta Diofantoksen yhtälöryhmästä, sillä kyseessä on pelkästään yhtälöryhmän homogeeninen osa. Lause on mukaileva versio Siegelin lemmasta. Mukailevan version ajatuksena on selittää alkuperäisen Siegelin lemman todistuksen idea hieman yksinkertaisemmin. Myöhemmin esitetään alkuperäinen Siegelin lemma 5.8 todistuksineen. Kahdessa seuraavassa lauseessa käytetään notaatiota $\lfloor x \rfloor$ viittaamaan lattiafunktioon ja $\lceil x \rceil$ viittaamaan kattofunktioon.

Lause 5.7. *Olkoot $N > M$ positiivisia kokonaislukuja ja olkoon*

$$\begin{aligned} a_{11}T_1 + \cdots + a_{1N}T_N &= 0 \\ &\vdots \\ a_{M1}T_1 + \cdots + a_{MN}T_N &= 0 \end{aligned}$$

lineaarinen Diofantoksen yhtälöryhmä, jonka jokin kokonaislukukerroin on nollasta poikkeava. Tällöin yhtälöryhmällä on olemassa ratkaisu $(T_1, \ldots, T_N)$, missä ainakin jokin kokonaisluvuista $T_1, \ldots, T_N$ on nollasta poikkeava ja

$$\max_{1 \leq i \leq N} |T_i| \leq 2 \cdot \left\lceil (2N|A|)^{\frac{M}{N-M}} \right\rceil.$$

Todistus. Olkoon $\bar{t} = (T_1, T_2, \ldots, T_N) \in \mathbb{Z}^N$, siten, että $\bar{t} \neq \bar{0}$ ja $\bar{t} \in R_B$, missä $B = \left\lceil (2N|A|)^{\frac{M}{N-M}} \right\rceil$. Ja olkoon joukko R_B on kuten lemmassa 5.4 määriteltiin. Tällöin $|R_B| = (2B+1)^N$.

Määritetään kuvaus $f_A : R_B \to AR_B$, missä $f_A(\overline{t}) = A\overline{t}$. Merkitään lemmassa 5.5 esiintyvää joukkoa $[-N|A|B, N|A|B] \times \cdots \times [-N|A|B, N|A|B] = S_B$. Tällöin lemman 5.5 nojalla $AR_B \subset S_B$ ja tiedetään, että joukon S_B koko on $|S_B| = (2N|A|B + 1)^M$. Lemmasta 5.6 seuraa, että kun

$$B = \left\lceil (2N|A|)^{\frac{M}{N-M}} \right\rceil, \quad \text{niin } |S_B| < |R_B|.$$

Tällöin myös $|AR_B| < |R_B|$. Lemman 5.1 nojalla tästä seuraa, että on olemassa vektorit $\overline{t_1}$ ja $\overline{t_2} \in R_B$ siten, että $\overline{t_1} \neq \overline{t_2}$ joille pätee $A\overline{t_1} = A\overline{t_2}$. Vähentämällä molemmilta puolilta $A\overline{t_2}$ ja ottamalla matriisi A yhteiseksi tekijäksi yhtälö muutetaan muotoon $A(\overline{t_1} - \overline{t_2}) = \overline{0}$. Koska $\overline{t_1} \neq \overline{t_2}$, niin merkitsemällä $\overline{t} = \overline{t_1} - \overline{t_2}$ saadaan yhtälöryhmälle $A\overline{t} = \overline{0}$ ratkaisu, joka on nollasta poikkeava. Lisäksi, koska $|\overline{t_1}| \leq B$ ja $|\overline{t_2}| \leq B$, niin kolmioepäyhtälön nojalla saadaan, että

$$|\overline{t}| \leq 2B \quad \text{eli} \quad |\overline{t}| \leq 2 \cdot \left\lceil (2N|A|)^{\frac{M}{N-M}} \right\rceil.$$

□

Näin ollen on saatu todistettua, että lemmalla 5.7 on yhtälöryhmän toteuttava ratkaisu $(T_1, T_2, \ldots, T_N)$. Lisäksi ratkaisu toteuttaa epäyhtälön

$$\max_{1 \leq i \leq N} |T_i| \leq 2 \cdot \left\lceil (2N|A|)^{\frac{M}{N-M}} \right\rceil.$$

Kyseisen lauseen arviota voidaan kuitenkin vielä tarkentaa. Siegelin lemma esittää samalle yhtälöryhmälle tarkemman tuloksen. Vaikka lemman johtopäätös näyttää hieman monimutkaiselta, niin se kertoo kuitenkin jotain yksinkertaista. Lineaarisessa yhtälöryhmässä, jossa muuttujia on enemmän kuin yhtälöitä, niin tiedetään, että yhtälöryhmällä on ei-triviaali ratkaisu. Lisäksi ratkaisusta tiedetään, että on olemassa kokonaislukuratkaisu, jossa ainakin osa muuttujista on nollasta poikkeavia. Lemman viimeinen osa taas kertoo, että voidaan löytää ratkaisu, joka ei ole kooltaan liian suuri. Tarkemmin ottaen on mahdollista löytää ratkaisu, jonka kokoa rajoittaa yhtälöiden lukumäärä M, muuttujien lukumäärä N sekä kertoimien a_{ij} koko. Lemman todellinen sisältö onkin se, että ratkaisu on olemassa siten, että sen koordinaattien koko on rajoitettu. Esitetään seuraavaksi Siegelin lemma ja todistetaan se.

Lause 5.8 (Siegelin lemma)**.** *Olkoot $N > M$ positiivisia kokonaislukuja ja olkoon*

$$\begin{aligned} a_{11}T_1 + \cdots + a_{1N}T_N &= 0 \\ &\vdots \\ a_{M1}T_1 + \cdots + a_{MN}T_N &= 0 \end{aligned}$$

lineaarinen yhtälöryhmä, jonka jokin kokonaislukukerroin on nollasta poikkeava. Tällöin yhtälöryhmälle on olemassa ratkaisu $(T_1, \ldots, T_N)$, missä ainakin jokin kokonaisluvuista $T_1, \ldots, T_N$ on nollasta poikkeava. Lisäksi ratkaisu toteuttaa seuraavan ehdon

$$\max_{1\le i\le N}|T_i| \le \left(N \max_{1\le i\le M, 1\le j\le N}|a_{ij}|\right)^{\frac{M}{N-M}}.$$

Todistus. Aloitetaan todistus yksinkertaistamalla Siegelin lemman väitettä. Jokaiselle vektorille $\bar{t} = (T_1, \ldots, T_N) \in \mathbb{R}^N$ merkitään, että

$$|\bar{t}| = \max_{1\le i\le N}|T_i|.$$

Vastaavasti merkitään

$$|A| = \max_{1\le i\le M, 1\le j\le N}|a_{ij}|.$$

Tällöin Siegelin lemma yksinkertaistuu muotoon, että yhtälöryhmällä $A\bar{t} = \overline{0}$ on ratkaisu $\bar{t} \in \mathbb{Z}^n$, $\bar{t} \neq 0$, joka toteuttaa ehdon

$$|\bar{t}| \le (N|A|)^{\frac{M}{N-M}}.$$

Jokaiselle reaaliluvulle a määritellään

$$a^+ := \max(a, 0) \quad \text{ja} \quad a^- := \max(-a, 0).$$

Tällöin pätee, että $a = a^+ - a^-$ ja $|a| = a^+ + a^-$. Määritellään seuraavaksi lineaariset yhtälöt $L_j(\bar{t}) = \sum_{i=1}^N a_{ji}T_i$ ja asetetaan

$$L_j^+ = \sum_{i=1}^N a_{ji}^+, \quad L_j^- = \sum_{i=1}^N a_{ji}^-, \quad \text{jolloin} \quad L_j = L_j^+ + L_j^- = \sum_{i=1}^N |a_{ji}|.$$

Lisäksi määritellään vielä tulojoukko

$$R_B^+ := [0, B] \times \cdots \times [0, B] \subset \mathbb{Z}^N.$$

Oletetaan, että $\bar{t} = (T_1, \ldots, T_N) \in \mathbb{R}_B^+$, jolloin $0 \leq T_i \leq B$. Tällöin, koska

$$-L_j^- B \leq \sum_{i=1}^{N} T_i a_{ji}^- \leq L_j(\bar{t}) = \sum_{i=1}^{N} T_i a_{ji} \leq \sum_{i=1}^{N} T_i a_{ji}^+ \leq L_j^+ B,$$

niin voidaan päätellä, että j:s koordinaatti $L_j(\bar{t})$ vektorista $A\bar{t}$ sijaitsee välillä

$$-L_j^- B \leq L_j(\bar{t}) \leq L_j^+ B.$$

Voidaan päätellä, että $f_A(R_B^+) \subset \prod_{j=1}^{M}[-L_j^- B, L_j^+ B]$. Olkoon B positiivinen kokonaisluku. Tällöin kokonaislukuvektorien määrä rajatussa alueessa $\prod_{j=1}^{M}[-L_j^- B, L_j^+ B]$ on

$$\prod_{j=1}^{M}(L_j^- B + L_J^+ B + 1) = \prod_{j=1}^{M}(L_j B + 1).$$

Toisaalta joukon R_B^+ koko on tuloperiaatteen nojalla $(B+1)^N$ Jos nyt B valitaan siten, että

$$(B+1)^N > \prod_{j=1}^{M}(L_j B + 1), \qquad (*)$$

niin kyyhkyslakkaperiaatteen nojalla joukossa R_B^+ on olemassa erilliset kokonaislukuvektorit $\bar{t}_1$ ja $\bar{t}_2$, $\bar{t}_1 \neq \bar{t}_2$, joilla $f_A(\bar{t}_1) = f_A(\bar{t}_2)$. Tällöin erotusvektori $\bar{t} = \bar{t}_1 - \bar{t}_2$ on lineaarisen yhtälöryhmän $A\bar{t} = \bar{0}$ kokonaislukuratkaisu siten, että $|\bar{t}| \leq B$.

Jotta Siegelin lemma saadaan todistettua, niin enää riittää varmistaa, että

$$B := \left\lfloor \left(N \max_{i,j} |a_{ij}| \right)^{\frac{M}{N-M}} \right\rfloor$$

toteuttaa ehdon (*). Kyseiselle luvun B arvolle pätee, että

$$B + 1 > (N \max |a_{ij}|)^{\frac{M}{N-M}},$$

ja täten

$$(B+1)^N = (B+1)^M (B+1)^{N-M} > (B+1)^M (N \max |a_{ij}|)^M.$$

Havaitaan, että

$$L_j \leq N \max_{i,j} |a_{ij}| \quad \text{ja } 1 \leq N \max_{i,j} |a_{ij}|,$$

jolloin

$$\prod_{j=1}^{M}(L_jB+1) \leq \left((B+1)N\max_{i,j}|a_{ij}|\right)^M < (B+1)^N.$$

□

Nyt on saatu käytyä läpi myös varsinainen Siegelin lemma. Täten lineaarisiin Diofantoksen yhtälöihin liittyvät päätulokset tämän tutkielman osalta on käyty läpi. Seuraavassa esimerkissä näytetään, miten lauseiden 5.7 ja 5.8 arviot ratkaisun koordinaattien koosta eroavat.

Esimerkki 5.9. Olkoon lineaarinen Diofantoksen yhtälöpari muotoa

$$\begin{cases} 6x+2y+14z=0 \\ x+3y+9z=0 \end{cases}.$$

Tällöin $|A|=14$, $M=2$ ja $N=3$. Lauseen 5.7 nojalla yhtälöparin ratkaisun koordinaattien koko on

$$\begin{aligned} \max_{1\leq i\leq N}|T_i| &\leq 2\cdot\lceil(2N|A|)^{\frac{M}{N-M}}\rceil \\ &= 2\cdot\lceil(2\cdot 3\cdot 14)^{\frac{2}{3-2}}\rceil \\ &= 2\cdot\lceil(6\cdot 14)^2\rceil = 2\cdot(6\cdot 14)^2. \end{aligned}$$

Vastaavasti lauseen 5.8 nojalla yhtälöparin ratkaisun koordinaattien koko on

$$\max_{1\leq i\leq N}|T_i| \leq (N|A|)^{\frac{M}{N-M}} = (3\cdot 14)^{\frac{2}{3-2}} = (3\cdot 14)^2.$$

Näin on esitetty havainnollistava esimerkki, miten lauseiden 5.7 ja 5.8 tulokset ratkaisun koordinaattien koosta eroavat. Seuraavassa kappaleessa Diofantoksen yhtälöihin tutustutaan enemmän opetuksen ja koulun näkökulmasta.

6 Diofantoksen yhtälöt kouluopetuksessa

Tämän kappaleen tarkoituksena on tutustua Diofantoksen yhtälöihin syvällisemmin. Lukiokirjojen tapaa esittää lineaariset Diofantoksen yhtälöt vertaillaan lineaarisiin Diofantoksen yhtälöryhmiin. Näistä koitetaan löytää yhteisiä

esitystapoja sekä eroavaisuuksia. Kappaleen lopuksi on tarkoitus pohtia, miten Diofantoksen yhtälöitä voisi hyödyntää peruskoulu- ja lukio-opetuksessa paremmin. Lisäksi pohditaan, miten Diofantoksen yhtälöitä voisi käyttää apuna ymmärtämään lineaarisia yhtälöryhmiä helpommin ja syvällisemmin.

Esitetään seuraavaksi kuitenkin esimerkit Diofantoksen yhtälöistä lukion oppikirjojen ratkaisumenetelmällä sekä Smithin normaalimuodon avulla, kun kokonaislukukertoimet a ja b sekä kokonaisluku c ovat kiinnitettyjä. Pidetään esimerkit yksinkertaisina, jotta ratkaisumenetelmien vaiheita olisi mahdollisimman helppo seurata.

Esimerkki 6.1. Ratkaistaan lukion oppikirjoissa esitettävällä menetelmällä Diofantoksen yhtälö $16x + 12y = 4$. Lähdetään etsimään Eukleideen algoritmin avulla lukujen 16 ja 12 suurinta yhteistä tekijää. Eukleideen algoritmin nojalla saadaan

$$\begin{aligned} 16 &= 1 \cdot 12 + 4 \\ 12 &= 3 \cdot 4. \end{aligned}$$

Näin ollen lukujen 16 ja 12 suurin yhteinen tekijä on 4. Peruuttamalla Eukleideen algoritmia saadaan

$$4 = 16 - 1 \cdot 12.$$

Näin ollen Diofantoksen yhtälön $16x + 12y = 4$ yksittäisratkaisu on $x_0 = 1$ ja $y_0 = -1$. Tällöin lauseen 3.5 nojalla Diofantoksen yhtälön kaikki ratkaisut ovat muotoa

$$x = 1 + \frac{12n}{4} = 1 + 3n \quad \text{ja} \quad y = -1 - \frac{16n}{4} = -1 - 4n.$$

Esimerkki 6.2. Merkitään Diofantoksen yhtälöä $16x + 12y = 4$ vastaavia matriiseja seuraavasti

$$A = \begin{pmatrix} 16 & 12 \end{pmatrix}, \quad \overline{x} = \begin{pmatrix} x \\ y \end{pmatrix} \quad \text{ja} \quad \overline{b} = \begin{pmatrix} 4 \end{pmatrix}.$$

Kerrotaan matriisia A oikealta matriisilla

$$R_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

jotta matriisin A paikalle a_{11} saadaan sen itseisarvoltaan pienin alkio. Tällöin

$$AR_1 = \begin{pmatrix} 12 & 16 \end{pmatrix}.$$

Nyt Eukleideen algoritmia hyödyntämällä kerrotaan matriisia AR_1 oikealta matriisilla

$$R_2 = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}, \quad \text{jolloin saadaan} \quad AR_1R_2 = \begin{pmatrix} 12 & 4 \end{pmatrix}.$$

Matriisissa AR_1R_2 alkioiden paikkojen vaihtamiseksi kerrotaan matriisilla

$$R_3 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \text{jolloin} \quad AR_1R_2R_3 = \begin{pmatrix} 4 & 12 \end{pmatrix}.$$

Taas Eukleideen algoritmia hyödyntäen valitaan matriisiksi

$$R_4 = \begin{pmatrix} 1 & -3 \\ 0 & 1 \end{pmatrix}.$$

Tällöin matriisia $AR_1R_2R_3$ oikealta kertomalla saadaan diagonaalimatriisi

$$D = AR_1R_2R_3R_4 = \begin{pmatrix} 4 & 0 \end{pmatrix}.$$

Vasemmalta matriisia A ei tässä tapauksessa kerrota, joten $L = \begin{pmatrix} 1 \end{pmatrix}$. Merkitään oikealta matriisia A kertovien matriisien R_i tulomatriisia

$$R = R_1R_2R_3R_4 = \begin{pmatrix} 1 & 3 \\ -1 & -4 \end{pmatrix}.$$

Nyt lausekkeen $\overline{c} = L\overline{b}$ nojalla saadaan, että

$$\overline{c} = \begin{pmatrix} 4 \end{pmatrix}.$$

Seuraavaksi lausekkeen $D\overline{y} = \overline{c}$ avulla diagonaalimatriisia D hyödyntäen saadaan ratkaistua, että

$$\overline{y} = \begin{pmatrix} 1 \\ n \end{pmatrix}, \quad n \in \mathbb{Z}.$$

Ja lopulta Diofantoksen yhtälön kaikki ratkaisut voidaan selvittää yhtälön $\overline{x} = R\overline{y}$ avulla, jolloin

$$\overline{x} = R\overline{y} = \begin{pmatrix} 1 & 3 \\ -1 & -4 \end{pmatrix} \begin{pmatrix} 1 \\ n \end{pmatrix} = \begin{pmatrix} 1 + 3n \\ -1 - 4n \end{pmatrix},$$

missä yhtälön $16x + 12y = 4$ yksittäinen ratkaisu on $\begin{pmatrix} 1 \\ -1 \end{pmatrix}$.

Esimerkkien 6.1 ja 6.2 ratkaisumenetelmät eivät vaikuta suoranaisesti samanlaisilta. Niillä saadaan kuitenkin sekä yksittäisratkaisuksi, että yleiseksi ratkaisuksi samat ratkaisut. Seuraavassa kappaleessa osoitetaan, että nämä kaksi ratkaisumenetelmää ovat yhtäläiset.

6.1 Diofantoksen yhtälön ratkaisumenetelmien vertailu

Kappaleessa 3 käytiin täsmällisesti läpi, miten Diofantoksen yhtälöitä ratkaistaan. Tässä kappaleessa tarkoituksena on osoittaa, että koulussa opetettava lineaarisen Diofantoksen yhtälön ratkaisumenetelmä toimii vastaavasti kuin Smithin normaalimuotoon perustuva yleinen menetelmä, kun yhtälö on muotoa

$$ax + by = c.$$

Aloitetaan esittämällä lineaarisen Diofantoksen yhtälön ratkaiseminen lukion oppikirjoissa kuten esimerkiksi Juuri 11-kirjassa esiintyvällä menetelmällä [8]. Tarkastellaan erikoistapausta, missä Eukleideen algoritmissa on vain kaksi askelta ja kiinnitetään yksinkertaisuuden vuoksi $\text{syt}(a, b) = r_0 = c$. Oletetaan, että $|a| > b$. Nyt Eukleideen algoritmia voidaan lähteä suorittamaan ja jakoyhtälön nojalla merkitään

$$a = s_0 b + r_0, \qquad \text{missä } 0 < r_0 < b$$

kuten lemmassa 2.1. Jakoyhtälö voidaan toistaa nyt luvuille b ja r_0, jolloin saadaan

$$b = s_1 r_0.$$

Eukleideen algoritmi on saatu nyt suoritettua loppuun, joten lähdetään suorittamaan algoritmia käänteisesti yksittäisratkaisun x_0 ja y_0 ratkaisemiseksi. Käänteisellä Eukleideen algoritmilla saadaan, että

$$r_0 = a - s_0 b.$$

Näin ollen yksittäisratkaisu Diofantoksen yhtälölle $ax + by = c$ on

$$x_0 = 1 \quad \text{ja} \quad y_0 = -s_0.$$

Tällöin lukion oppikirjojen tavalla saadaan, että kaikki ratkaisut ovat muotoa

$$x = x_0 + \frac{nb}{\text{syt}(a, b)} = 1 + \frac{nb}{r_0} \quad \text{ja} \quad y = y_0 - \frac{na}{\text{syt}(a, b)} = -s_0 - \frac{na}{r_0}.$$

Nyt on saatu esitettyä Diofantoksen yhtälön $ax + by = c$ ratkaisu lukion oppikirjoissa käytetyllä tavalla. Tämä ratkaisumenetelmä ei suoranaisesti vaikuta samalta kuin Smithin normaalimuodon avulla lineaarisen Diofantoksen yhtälön ratkaiseminen. Kuitenkin kappaleessa 3 osoitettiin, että käänteisen Eukleideen algoritmin suorittaminen voidaan tehdä matriisikertolaskulla. Seuraavaksi osoitetaan, että kappaleen 3 ja Smithin normaalimuodon ratkaisutavat ovat yhtäläiset ja, että erityisesti ne johtavat samaan yksittäisratkaisuun.

Kappaleessa 3 osoitettiin, että Diofantoksen yhtälön ratkaisu voidaan esittää muodossa $A_{n+1}\begin{pmatrix}1\\0\end{pmatrix}$, missä matriisi A_{i+1} määriteltiin rekursiivisesti säännöillä

$$A_{i+1} = A_i S_i, \quad S_i = \begin{pmatrix}0 & 1\\1 & -s_i\end{pmatrix} \quad \text{ja} \quad A_1 = \begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}.$$

Matriisissa S_i kertoimet $-s_i$ ovat kertoimia Eukleideen algoritmista. Tällöin matriisi A_{n+1} on tulomatriisi

$$A_{n+1} = A_1 S_1 \cdots S_n.$$

Olkoot Diofantoksen yhtälö $ax + by = c$ kuten edellä. Lisäksi Eukleideen algoritmi luvuilla a ja b suoritetaan kuten aikaisemmin esitettiin. Tällöin kappaleessa 3 esiintyvät matriisit ovat

$$A_1 = \begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}, \quad S_1 = \begin{pmatrix}0 & 1\\1 & -s_0\end{pmatrix} \quad \text{ja} \quad S_2 = \begin{pmatrix}0 & 1\\1 & -s_1\end{pmatrix}.$$

Tällöin ratkaisu voidaan esittää matriisikertolaskuna

$$A_3\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}x_3\\y_3\end{pmatrix}. \tag{6.1}$$

Tämä alkaa jo näyttämään huomattavasti samanlaiselta kuin Smithin normaalimuotoon perustuvassa ratkaisumenetelmässä. Esitetään seuraavaksi saman Diofantoksen yhtälön $ax + by = c$ ratkaisu Smithin normaalimuodon avulla.

Lineaarista Diofantoksen yhtälöä $ax + by = c$ vastaavat matriisit ovat

$$A = \begin{pmatrix}a & b\end{pmatrix}, \quad x = \begin{pmatrix}x\\y\end{pmatrix} \quad \text{ja} \quad b = \begin{pmatrix}c\end{pmatrix}.$$

Seuraamalla lauseen 2.2 todistusta huomataan, että matriisin A Smithin normaalimuoto on matriisi $D = \begin{pmatrix}c & 0\end{pmatrix}$, missä $\text{syt}(a, b) = c$. Tällöin päädytään ratkaisemaan yhtälöryhmää

$$\begin{pmatrix}c & 0\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix} = c,$$

mistä yksittäisratkaisuksi saadaan vektori $\begin{pmatrix}1\\0\end{pmatrix}$. Lauseen 4.1 mukaan yhtälön $A\overline{x} = \overline{c}$ yksittäisratkaisu on tällöin $R\begin{pmatrix}1\\0\end{pmatrix}$, missä matriisi R toteuttaa ehdon

$AR = \begin{pmatrix} \text{syt}(a,b) & 0 \end{pmatrix}$. Jotta voidaan osoittaa, että kappaleiden 3 ja 4 ratkaisumenetelmät ovat samat tässä erikoistapauksessa, niin riittää osoittaa, että $R = A_3$.

Käydään seuraavaksi läpi Diofantoksen yhtälön ratkaiseminen Smithin normaalimuodon avulla ja osoitetaan, että $R = A_3$. Oletetaan, että $|a| > b$ ja alun oletuksen nojalla $\text{syt}(a,b) = r_0 = c$. Nyt, koska $|a| > b$, niin matriisia A halutaan kertoa matriisilla, joka vaihtaa sen alkioiden paikkoja. Kertomalla oikealta matriisia A matriisilla

$$R_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{saadaan} \quad AR_1 = \begin{pmatrix} b & a \end{pmatrix}.$$

Nyt jakoyhtälön $a = s_0 b + r_0$ nojalla kertomalla oikealta matriisilla

$$R_2 = \begin{pmatrix} 1 & -s_0 \\ 0 & 1 \end{pmatrix}, \quad \text{saadaan} \quad AR_1R_2 = \begin{pmatrix} b & r_0 \end{pmatrix}.$$

Merkitään matriisia $R_1R_2 = R_{12}$. Tiedetään, että $r_0 < |b|$, joten halutaan taas kertoa matriisilla, joka vaihtaa alkioiden paikkoja keskenään. Näin ollen kertomalla seuraavaksi oikealta matriisilla

$$R_3 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \text{saadaan} \quad AR_{12}R_3 = \begin{pmatrix} r_0 & b \end{pmatrix}.$$

Jakoyhtälön nojalla $b = s_1 r_0$, joten kertomalla oikealta matriisilla

$$R_4 = \begin{pmatrix} 1 & -s_1 \\ 0 & 1 \end{pmatrix} \quad \text{taas} \quad AR_{12}R_3R_4 = \begin{pmatrix} r_0 & 0 \end{pmatrix}.$$

Merkitään matriisia $R_3R_4 = R_{34}$. Nyt matriisi A on saatu muutettua diagonaalimuotoon, missä diagonaalimatriisi $D = AR_{12}R_{34}$. Merkitään matriisia A oikealta kertovien matriisien R_i tulomatriisia $R = R_{12}R_{34}$. Tulomatriisi

$$R = R_{12}R_{34} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & -s_0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & -s_1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & s_1 \\ -s_0 & -s_0 s_1 - 1 \end{pmatrix}.$$

Nyt havaitaan, että $R_{12} = S_1$ sekä $R_{34} = S_2$. Tällöin saadaan, että $A_3 = R$, koska jokainen matriisitulon tulontekijä on samankaltainen. Suorittamalla Smithin normaalimuoto loppuun saadaan Diofantoksen yhtälön $ax + by = c$ ratkaisuksi

$$x = 1 + \frac{nb}{r_0} \quad \text{ja} \quad y = -s_0 - \frac{na}{r_0}.$$

Näin on saatu esitettyä Diofantoksen yhtälön ratkaiseminen vapailla kokonaisluvuilla a ja b Smithin normaalimuodon avulla. Voidaan havaita, että

aina pätee, että $S_i = R_{i(i+1)}$. Tästä seuraa, että kappaleen 3 matriisi A_{n+1} ja kappaleen 4 matriisi R ovat aina yhtäsuuret. Tällöin kappaleessa 3 löydetty erikoisratkaisu $A_{n+1}\begin{pmatrix}1\\0\end{pmatrix}$ on yhtäsuuri kuin kappaleen 4 erikoisratkaisu $R\begin{pmatrix}1\\0\end{pmatrix}$. Edellä tämä todistettiin tapauksessa tapauksessa, missä Eukleideen algoritmissa oli vain kaksi askelta. On ilmeistä, että tulos on voimassa myös yleisesti mutta tässä tutkielmassa sitä ei todisteta yleisellä tasolla. Näin ollen ollaan saatu osoitettua, että koulukirjojen ratkaisumenetelmä lineaariselle Diofantoksen yhtälölle, joka on muotoa $ax + by = c$ on vastaavanlainen kuin Smithin normaalimuotoon perustuvassa ratkaisumenetelmässä.

Vertaillaan ratkaisumenetelmän lisäksi lukion oppikirjan [8] ja tämän tutkielman tapaa esittää lineaarisen Diofantoksen yhtälön ratkaisujoukko. Näiden kahden tavan välillä löytyy yhtäläisyyttä ratkaisujoukon esittämisessä. Lukion oppikirjassa ratkaisujoukko esitetään muodossa

$$x = x_0 + \frac{nb}{\text{syt}(a,b)} \quad \text{ja} \quad y = y_0 - \frac{na}{\text{syt}(a,b)}, \quad n \in \mathbb{Z}.$$

Kyseisessä ratkaisun esitystavassa on ensin esitetty yhtälön yksittäisratkaisu x_0 ja y_0 ja ratkaisujoukon loppuosa on Diofantoksen yhtälön homogeeninen osa. Vastaavasti tässä tutkielmassa ratkaisujoukossa on ensin esitetty yhtälön yksittäisratkaisu ja yksittäisratkaisuun on lisätty yhtälön homogeenisen osan ratkaisu. Tästä esimerkkinä toimii esimerkin 6.2 ratkaisujoukko, joka oli muotoa

$$\overline{x} = \begin{pmatrix}1+3n\\-1-4n\end{pmatrix},$$

missä $\left(\begin{smallmatrix}1\\-1\end{smallmatrix}\right)$ on yhtälön $16x + 12y = 4$ yksittäisratkaisu.

Ratkaisujoukkoon liittyen löytyy myös lukion oppikirjan [8] ja tämän tutkielman esitystavoissa eroavaisuus. Lukion oppikirjassa Diofantoksen yhtälöiden ratkaisujoukko esitetään koordinaatti kerrallaan muodossa

$$x = x_0 + \frac{nb}{\text{syt}(a,b)} \quad \text{ja} \quad y = y_0 - \frac{na}{\text{syt}(a,b)}, \quad n \in \mathbb{Z}.$$

Tämän tutkielman kohdalla Diofantoksen yhtälön ratkaisujoukko esitetään hieman erilaisessa muodossa. Ratkaisujoukko esitetään tämän tutkielman kohdalla vektorimuodossa

$$\overline{x} = R\overline{y} = R\begin{pmatrix}y_1\\t\end{pmatrix}, \text{ missä } t \in \mathbb{Z}.$$

Näiden kahden esitystavan välillä löytyy siis eroavaisuus. Lukion oppikirjassa [8] painotetaan enemmän ratkaisun esittämistä koordinaatti kerrallaan,

jolloin x-koordinaatti ja y-koordinaatti on esitettynä erikseen. Taas tässä tutkielmassa ratkaisujoukossa on näkyvissä jokaisen koordinaatin ratkaisut, kun ratkaisujoukko esitetään vektorimuodossa. Ratkaisujoukkojen esitystavan erilaisuuteen ja niiden vaikutusta oppimiseen pohditaan tarkemmin kappaleessa 6.2.

6.2 Miten Diofantoksen yhtälöitä voisi hyödyntää opetuksessa?

Tässä kappaleessa pohditaan, miten ja missä tapauksissa lineaarisia Diofantoksen yhtälöitä voitaisiin hyödyntää lukion matematiikan opetuksessa. Rajoitun tässä kappaleessa vain lukion matematiikkaan, sillä Diofantoksen yhtälöt esitetään oppilaille vasta lukion oppikirjoissa. Kappaleessa esitettävät väitteet opetuksen vaihtoehtoisista toteutustavoista ovat omia mielipiteitäni, jotka ovat muodostuneet tätä tutkielmaa tehdessä. Kaikki toteutusehdotukset eivät välttämättä toimisi täysin sellaisenaan mutta tarkoituksena on myös herättää tutkielman lukevia muita matematiikan opettajia pysähtymään ja pohtimaan matematiikan sisällön opettamistaan.

Lukion opetussuunnitelman perusteiden 2019 [9] mukaan Eukleideen algoritmi kuuluu pitkän matematiikan valinnaiseksi luokiteltavaan Algoritmit ja lukuteoria -moduuliin. Diofantoksen yhtälöt mainitaan lukion oppikirjoissa, kuten kirjassa Juuri 11 Eukleideen algoritmiin liittyvässä kappaleessa. Diofantoksen yhtälöt toimivat lukion oppikirjoissa hyvinä soveltavina esimerkkeinä Eukleideen algoritmin hyödyntämisestä. Lyhyen matematiikan kohdalla Diofantoksen yhtälöitä tai Eukleideen algoritmia ei mainita pakollisten eikä valinnaisten moduulien keskeisissä sisällöissä.

Lukion pitkän matematiikan oppikirjoissa Diofantoksen yhtälöllä tarkoitetaan tilannetta, jossa kyseessä on kokonaislukukertoiminen kahden muuttujan yhtälö

$$ax + by = c,$$

missä a, b ja $c \in \mathbb{Z}$. Ramirezin artikkelin [10] mukaan juuri Diofantoksen yhtälön tapaisissa tilanteissa oppilailla on koettu olevan ongelmia. Oppilailla on ollut vaikeuksia artikkelin mukaan ymmärtää, että yhtälöllä voisi olla yksittäinen ratkaisu tai toisaalta, että sillä voi olla äärettömän monta ratkaisua.

Mielestäni Ramirezin artikkelin ongelmaan voisi olla apua siitä, miten oppilaita opettaisiin esittämään vastaukset Diofantoksen yhtälöihin. Kappaleessa 6.1 kerrotaan, että lukion oppikirjoissa ratkaisujoukko esitetään muodossa

$$x = x_0 + \frac{nb}{\text{syt}(a,b)} \quad \text{ja} \quad y = y_0 - \frac{na}{\text{syt}(a,b)}, \quad n \in \mathbb{Z}.$$

Itse koen, että kyseinen ratkaisujoukon esitysmuoto saattaa tuoda oppilaille mielikuvaa, missä muuttujien x ja y arvot eivät riipu toisistaan mitenkään. Kuitenkin todellisuudessa x ja y ovat lukupari, joka toteuttaa Diofantoksen yhtälön $ax + by = c$. Tässä tutkielmassa ratkaisujoukko esitetään vektorimuodossa

$$\overline{x} = R\overline{y} = R\begin{pmatrix} y_1 \\ t \end{pmatrix}, \text{ missä } t \in \mathbb{Z}.$$

Lukion oppikirjoihin en usko myöskään vektorimuodon olevan paras tapa esittää Diofantoksen yhtälöiden ratkaisua. Kokisin itse yhdeksi hyväksi vaihtoehdoksi esittää ratkaisujoukko esimerkiksi muodossa

$$(x, y) = \left(x_0 + \frac{nb}{\text{syt}(a, b)}, y_0 - \frac{na}{\text{syt}(a, b)}\right),$$

jolloin ratkaisujoukosta esiintyisi, että muuttujat x ja y ovat lukupari. Ratkaisujoukon esitysmuoto olisi tämän lisäksi mielestäni lukiolaisille ymmärrettävässä muodossa, kun se vastaisi heille jo tuttua esitystapaa lukion oppikirjoista.

Kuten aiemmin jo mainitsin, niin lyhyen matematiikan keskeisissä sisällöissä ei Eukleideen algoritmia tai Diofantoksen yhtälöitä ole mainittuna minkään moduulin kohdalla. Yksi mahdollinen paikka, jossa Diofantoksen yhtälöt voitaisiin ainakin pintapuolisesti esitellä sijoittuisi kaikille pakolliseen matematiikan MAY1 -moduuliin. Kyseisen moduulin keskeisissä sisällöissä on mainittuna ensimmäisen asteen yhtälö sekä yhtälöpari. Diofantoksen yhtälöiden ratkaisemiseen käytettävä Eukleideen algoritmi ei oikein sopisi kyseisen moduulin sisältöihin. Koen kuitenkin, että Diofantoksen yhtälöitä voisi esittää kyseisessä moduulissa kokeilemismenetelmän avulla havainnollistamaan, miten esimerkiksi muuttuja x on riippuvainen ensimmäisen asteen yhtälön ratkaisusta y [9].

Lukion matematiikan opetussuunnitelman muuttaminen ei välttämättä ole yksinkertaisin tehtävä. Näin ollen yksi näkökulma, jota pohdin myös on, että miten Diofantoksen yhtälöistä saataisiin oppilaille mahdollisimman paljon matemaattista hyötyä nykyisessä moduulissaan. Ainakin Juuri 11 -lukiokirjassa Diofantoksen yhtälöt esiteltiin, jotta Eukleideen algoritmia päästään soveltamaan erilaisissa tilanteissa. Diofantoksen yhtälöitä esittäessä opettaja voisi hyödyntää sitä myös esimerkiksi ensimmäisen asteen yhtälöiden, yhtälöparien tai yhtälöihin liittyvien käsitteiden kertaamisessa. Ensimmäisen asteen yhtälöiden tai yhtälöparien kertaaminen Diofantoksen yhtälöitä hyödyntäen toisi mielestäni oppilaille mahdollisuuden kerrata yhtälöiden algebrallista ratkaisemista. Lisäksi kokonaislukukertoimisten yhtälöiden ratkaiseminen voisi tuoda oppilaille syvempää ymmärtämistä yhtälöiden ratkaisemiseen, kun muuttujien kertoimet olisivat hallittavammassa muodossa.

Esitetään lopuksi vielä kaksi esimerkkiä, miten Diofantoksen yhtälöitä voi hyödyntää kertaamaan, onko yhtälöryhmällä ratkaisua. Esimerkkien tarkoituksena on antaa vain pari mahdollista tapaa, miten lineaarisia Diofantoksen yhtälöitä voisi hyödyntää opetuksessa.

Esimerkki 6.3. Tutkitaan löytyykö yhtälöparille

$$\begin{cases} 8x + 4y = 6 \\ 4x + 2y = 3 \end{cases}$$

reaalilukuratkaisua. Entä löytyykö sille kokonaislukuratkaisua?

Huomataan, että jos yhtälöparille olisi ratkaisu, niin täytyisi päteä, että

$$6 = 8x + 4y = 2(4x + 2y) = 2 \cdot 3 = 6.$$

Tämä on tosi ja koska yhtälölle $4x + 2y = 3$ on olemassa äärettömän monta ratkaisua, niin yhtälöparilla on olemassa äärettömän monta reaalilukuratkaisua. Kokeilemalla huomataan, että yhtälöparille löytyy ratkaisu $x = 0$ ja $y = \frac{3}{2}$. Tällöin sen kaikki ratkaisut ovat kappaleen 1.1 nojalla muotoa

$$\left(0, \frac{3}{2}\right) + t(-1, 2), \quad \text{missä} \quad t \in \mathbb{R}.$$

Ratkaisujoukon rakenteesta ei voida helposti päätellä, onko yhtälöparilla kokonaislukuratkaisua. Eukleideen algoritmin nojalla alemman yhtälön muuttujien kertoimien 4 ja 2 $\text{syt}(4, 2) = 2$. Koska $2 \nmid 3$, niin lauseen 3.1 nojalla yhtälöllä $4x + 2y = 3$ ei ole olemassa kokonaislukuratkaisua. Siispä yhtälöparilla ei ole olemassa kokonaislukuratkaisua.

Esimerkki 6.4. Tutkitaan löytyykö lineaariselle yhtälöparille

$$\begin{cases} 3x + y = 2 \\ x + y = 1 \end{cases}$$

kokonaislukuratkaisua.

Huomataan kokeilemalla, että ylemmälle yhtälölle löytyy kokonaislukuratkaisu $x = 1$ ja $y = -1$ ja alemmalle yhtälölle kokonaislukuratkaisu $x = 1$ ja $y = 0$. Ongelmana on, että löytyykö kokonaislukuratkaisua, joka toimii yhtälöparin molemmille yhtälöille.

Ratkaistaan alempi yhtälöistä muotoon $y = 1 - x$ ja sijoitetaan ylempään yhtälöön muuttujan y paikalle.

$$3x + y = 3x + (1 - x) = 3x + 1 - x = 2x + 1 = 2.$$

Yhtälöstä $2x + 1 = 2$ puolittain vähentämällä luvun -1 ja jakamalla puolittain luvulla 2 saadaan lopulta, että $x = \frac{1}{2}$. Sijoittamalla $x = \frac{1}{2}$ yhtälöön $y = 1 - x$ saadaan $y = \frac{1}{2}$. Näin ollen yhtälöparille löytyy yksikäsitteinen rationaalilukuratkaisu $x = \frac{1}{2}$ ja $y = \frac{1}{2}$. Koska ratkaisu ei ole kokonaisratkaisu, niin yhtälöparille ei löydy kokonaislukuratkaisua.

Viitteet

[1] Jim Hefferon: *Linear Algebra*. Ortogonal Publishing L3C, 2017.

[2] Nathan Jacobson: *Basic Algebra I*. toinen painos, Dover Publications, 2009.

[3] Felix Lazebnik: *On Systems of Linear Diophantine Equations*. Mathematics Magazine, 1996.

[4] Tuomo Äkkinen: *Lineaarinen algebra ja geometria 1*. Luentomoniste, Matematiikan ja tilastotieteen laitos, Jyväskylän yliopisto, 2019. https://tim.jyu.fi/files/202738/Linkku1uusi.pdf, viitattu 2.12.2023.

[5] Alexander Schrijver: *Theory of Linear and Integer Programming*. John Wiley and Sons, 1998.

[6] Lenny Fukshansky: *Geometric Number Theory*. Lecture notes. https://www1.cmc.edu/pages/faculty/lenny/classes/spring_2019/m195/GNT_lecture-notes.pdf, viitattu 2.12.2023.

[7] Ralph P. Grimaldi: *Discrete and Combinatorial Mathematics*. Viides painos, Pearson Education, 1999.

[8] M. Hähkiöniemi, S. Juhala, P. Juutinen, A. Laitinen, E. Luoma-aho, T: Raittila ja T. Tikka: *Juuri 11, Algoritmit ja lukuteoria*. 1. painos, Otava kirjapaino, 2021.

[9] Opetushallitus: *Lukion opetussuunnitelman perusteet 2019*. https://www.oph.fi/sites/default/files/documents/lukion_opetussuunnitelman_perusteet_2019.pdf, viitattu 10.1.2024.

[10] Ariel A. Ramirez: *A cognitive approach to solving systems of linear equations*. PhD thesis. Illinois State University, 2009.

[11] David M. Burton *Elementary Number Theory*. 7 painos, McGraw-Hill, 2011.

[12] Esko Heinonen: *Lukuteoria 1*. Luentomoniste, Matematiikan ja tilastotieteen laitos, Jyväskylän yliopisto, 2020. https://koppa.jyu.fi/kurssit/jy-CUR-5688/Luennot/luentomoniste20.pdf, viitattu 18.1.2024

[13] Kenneth H. Rosen: *Elementary Number theory and Its Applications*. Addison-Wesley publishing company, 1986.