Tampereen yliopisto

Mona Hirsimäki

LINEAARISET KONGRUENSSIRYHMÄT

Informaatioteknologian ja viestinnän tiedekunta
Kandidaattitutkielma
Joulukuu 2020

Tiivistelmä

Mona Hirsimäki: Lineaariset kongruenssiryhmät
Kandidaattitutkielma
Tampereen yliopisto
Matematiikan ja tilastotieteen tutkinto-ohjelma
Joulukuu 2020

Tämän tutkielman tarkoituksena on esitellä lineaaristen kongruenssiryhmien ratkaisumenetelmiä, kun muuttujien ja kongruenssien lukumäärät vaihtelevat. Kongruenssien modulien arvoilla on myös vaikutusta ratkaisutapaan. Tutkielma nojaa kirjallisuuteen ja päälähdeteoksena käytetään Rosenin kirjaa Elementary Number Theory and its Applications.

Tutkielma kuuluu pääasiassa matematiikassa lukuteorian osa-alueeseen. Keskeisiä tutkielman käsitteitä ovat muun muassa jaollisuus, kongruenssi ja suurin yhteinen tekijä. Lukijalta oletetaankin osaamista lukuteorian alkeista, vaikka joitakin tärkeimpiä perusasioita esitetään tutkielman alussa. Tutkielma kuuluu myös matematiikassa lineaarialgebran osa-alueeseen, koska kongruenssiryhmä muodostuu kongruenssiyhtälöistä, ja siksi lineaarisen yhtälöryhmän käsitteen ymmärtäminen on tärkeää. Lukijan oletetaan myös hallitsevan matriisilaskennan perusteet.

Tutkielmassa esitetään ensin yhden muuttujan ja kahden kongruenssin muodostaman lineaarisen kongruenssiryhmän ratkaisumenetelmä. Kongruenssien modulien ei tarvitse olla sama positiivinen kokonaisluku. Tulokseksi saadaan, että jos kongruenssiryhmä on ratkeava, niin ratkaisu on yksikäsitteinen modulo $\mathrm{pyj}(m, n)$, missä m ja n ovat kongruenssien modulit.

Toiseksi esitetään kahden muuttujan ja kahden kongruenssin muodostaman lineaarisen kongruenssiryhmän kaksi eri ratkaisumenetelmää. Tässä kongruenssiryhmässä kongruenssien modulien on oltava sama positiivinen kokonaisluku. Ensin esitetään yksinkertainen eliminointimenetelmä, jossa tarkoituksena on eliminoida toinen kongruenssiryhmän muuttujista. Ratkaistun muuttujan arvo sijoitetaan toiseen alkuperäiseen kongruenssiryhmän kongruenssiyhtälöön, jolloin saadaan myös toisen muuttujan arvo. Toisen ratkaisumenetelmän avulla

saadaan selvitettyä sekä lineaarisen kongruenssiryhmän ratkeavuus että ratkaisun muoto, jos se on olemassa. Jos ratkaisu on olemassa, se on yksikäsitteinen modulo m.

Viimeisessä luvussa esitellään, miten matriiseja voidaan esittää kongruenssimuodossa ja miten matriisimerkintöjä käyttäen voidaan ratkaista suuriakin lineaarisia kongruenssiryhmiä. Määritelmien ja lauseiden perusteella saadaan johdettua tulos, että kongruenssi $\mathbf{X} \equiv \mathbf{A}^{-1}\mathbf{B} \pmod{m}$ antaa ratkaisumenetelmän ratkaista lineaarinen kongruenssiryhmä.

Avainsanat: kongruenssi, lineaarinen kongruenssiryhmä, matriisien kongruenssi, lukuteoria

Sisältö

1 Johdanto

Tässä tutkielmassa tarkastellaan lineaarisia kongruenssiryhmiä ja niiden ratkaisumenetelmiä, kun muuttujien ja kongruenssien lukumäärät vaihtelevat. Erityisesti luvussa 4 esitetään, miten matriiseja voidaan käyttää suurtenkin lineaaristen kongruenssiryhmien ratkaisemiseen.

Luvussa 2 käydään läpi joitakin tutkielman ymmärtämisen kannalta tärkeimpiä lukuteorian perusasioita, jotka lukijan kuitenkin oletetaan tuntevan. Lukuteorian perusasioiden tuntemisen lisäksi lukijalta edellytetään matriisilaskennan perusteiden hallitsemista sekä lineaarisen yhtälöryhmän määritelmän ymmärtämistä.

Luvun 3 pykälässä 3.1 todistetaan lause 3.1, joka kertoo, milloin yhden muuttujan ja kahden kongruenssin muodostama lineaarinen kongruenssiryhmä on ratkeava, kun kongruenssien modulit m ja n voivat olla eri positiiviset kokonaisluvut. Lause kertoo myös ratkaisun muodon.

Luvun 3 pykälässä 3.2 käsitellään, milloin kahden muuttujan ja kahden kongruenssin muodostama lineaarinen kongruenssiryhmä on ratkeava sekä millainen ratkaisun muoto on, kun kongruenssien modulit ovat sama positiivinen kokonaisluku. Esitetään kaksi eri ratkaisumenetelmää, joista ensimmäinen on esimerkin 3.3 kautta esitettävä eliminointimenetelmä. Toinen menetelmä esitetään todistamalla lause 3.2, joka antaa matriisiavusteisen tavan ratkaista lineaarinen kongruenssiryhmä.

Luvussa 4 käsitellään matriisien esittämistä kongruenssimuodossa, sekä sitä, miten lineaarisia kongruenssiryhmiä voidaan ratkaista käyttäen matriisimerkintöjä. Keskeinen tulos, joka saadaan, on kongruenssi $\mathbf{X} \equiv \mathbf{A}^{-1}\mathbf{B} \pmod{m}$, jonka avulla lineaarinen kongruenssiryhmä pystytään ratkaisemaan.

Tutkielmassa esitetään myös havainnollistavia esimerkkejä todistettujen lauseiden käytöstä. Tutkielman päälähdeteoksena käytetään Rosenin kirjaa Elementary Number Theory and its Applications. Muut käytettävät lähdeteokset ovat Koshyn kirja Elementary Number Theory with Applications sekä Antonin ja Rorresin kirja Elementary Linear Algebra: Applications version.

2 Valmistelevia tarkasteluja

Luvussa 2 esitetään muutamia tutkielman keskeisiä pääaiheen käsittelyssä tarvittavia apuneuvoja.

2.1 Tarvittavien käsitteiden määritelmiä

Esitetään tässä pykälässä seuraavat neljä tärkeää määritelmää: jaollisuuden, suurimman yhteisen tekijän, pienimmän yhteisen jaettavan ja suhteellisten alkulukujen määritelmän.

Määritelmä 2.1. [3, s. 36–37] Olkoot a, $b \in \mathbb{Z}$. Luku b on *jaollinen* luvulla a, jos on olemassa sellainen $c \in \mathbb{Z}$, että $b = ac$. Voidaan myös sanoa, että luku a on luvun b tekijä tai että luku b on luvun a monikerta.

Luvun b jaollisuutta luvulla a merkitään $a \mid b$. Jos luku b ei ole jaollinen luvulla a, merkitään $a \nmid b$.

Määritelmä 2.2. [2, s. 155] Olkoot a, $b \in \mathbb{Z}$ ja olkoon ainakin toinen luvuista nollasta eroava. Lukujen a ja b *suurin yhteinen tekijä* on suurin positiivinen kokonaisluku, joka jakaa sekä luvun a että luvun b. Suurinta yhteistä tekijää merkitään $\text{syt}(a, b)$.

Määritelmä 2.3. [2, s. 184] Olkoot a, $b \in \mathbb{Z}_+$. Lukujen a ja b pienin yhteinen monikerta eli *pienin yhteinen jaettava* on pienin positiivinen kokonaisluku, joka on jaollinen sekä luvulla a että luvulla b. Merkitään pienintä yhteistä jaettavaa $\text{pyj}(a, b)$.

Määritelmä 2.4. [2, s. 156] Olkoot a ja $b \in \mathbb{Z}_+$. Luvut a ja b ovat *suhteellisia alkulukuja*, jos $\text{syt}(a, b) = 1$.

2.2 Kongruenssista ja lineaarisesta kongruenssista

Määritelmä 2.5. [3, s. 145] Olkoot a, $b \in \mathbb{Z}$ ja olkoon $m \in \mathbb{Z}_+$. Luku a on *kongruentti luvun b kanssa modulo m*, jos $m \mid (a - b)$.

Jos luku a on kongruentti luvun b kanssa, niin merkitään $a \equiv b \pmod{m}$. Jos luku a ei ole kongruentti luvun b kanssa, eli $m \nmid (a - b)$, niin merkitään

$a \not\equiv b \pmod{m}$. Tällöin voidaan myös sanoa, että luku a on epäkongruentti luvun b kanssa modulo m.

Lause 2.1. *Olkoot $a, b \in \mathbb{Z}$ ja olkoon $m \in \mathbb{Z}_+$. Silloin $a \equiv b \pmod{m}$, jos ja vain jos on olemassa sellainen $k \in \mathbb{Z}$, että $a = b + km$.*

Todistus. Ks. [3, s. 146]. □

Lause 2.2. *Olkoot a, b, $c \in \mathbb{Z}$ ja olkoon $m \in \mathbb{Z}_+$. Silloin kongruensseilla modulo m on seuraavat ominaisuudet:*

(i) $a \equiv a \pmod{m}$ *(refleksiivisyys),*

(ii) *jos* $a \equiv b \pmod{m}$, *niin* $b \equiv a \pmod{m}$ *(symmetrisyys),*

(iii) *jos* $a \equiv b \pmod{m}$ *ja* $b \equiv c \pmod{m}$, *niin* $a \equiv c \pmod{m}$ *(transitiivisuus).*

Todistus. Ks. [3, s. 146–147]. □

Lause 2.3. *Olkoot a, b, $c \in \mathbb{Z}$ ja olkoon $m \in \mathbb{Z}_+$. Jos $a \equiv b \pmod{m}$, niin*

(i) $a + c \equiv b + c \pmod{m}$,

(ii) $a - c \equiv b - c \pmod{m}$,

(iii) $ac \equiv bc \pmod{m}$.

Todistus. Ks. [3, s. 148]. □

Määritelmä 2.6. [3, s. 159] Olkoot $a, x \in \mathbb{Z}$ ja olkoon $m \in \mathbb{Z}_+$. Jos $\text{syt}(a, m) = 1$, niin kongruenssin $ax \equiv 1 \pmod{m}$ ratkaisua x kutsutaan luvun a *käänteisluvuksi* modulo m.

Lause 2.4. *Olkoot a, $b \in \mathbb{Z}$, olkoot d, $m \in \mathbb{Z}_+$ ja $\text{syt}(a, m) = d$. Jos $d \nmid b$, niin kongruenssiyhtälöllä $ax \equiv b \pmod{m}$ ei ole ratkaisuja. Jos $d \mid b$, niin kongruenssiyhtälöllä $ax \equiv b \pmod{m}$ on täsmälleen d epäkongruenttia ratkaisua modulo m.*

Todistus. Ks. [3, s. 158]. □

Seuraus 2.1. *Olkoot a, $b \in \mathbb{Z}$ ja olkoon $m \in \mathbb{Z}_+$. Jos luvut a ja m ovat suhteellisia alkulukuja, niin lineaarisella kongruenssilla $ax \equiv b \pmod{m}$ on yksikäsitteinen ratkaisu modulo m.*

Todistus. Ks. [3, s. 158]. □

3 Lineaarisista kongruenssiryhmistä

3.1 Yhden muuttujan ja kahden kongruenssin muodostama lineaarinen kongruenssiryhmä

Todistetaan tässä pykälässä seuraava lause 3.1, joka antaa yksinkertaisen tavan selvittää, onko yhden muuttujan ja kahden kongruenssin muodostama lineaarinen kongruenssiryhmä ratkeava. Lisäksi lause kertoo ratkaisun muodon, jos ratkaisu on olemassa.

Lause 3.1. *Olkoot a, $b \in \mathbb{Z}$ ja olkoot m, $n \in \mathbb{Z}_+$. Silloin yhden muuttujan ja kahden kongruenssin muodostama lineaarinen kongruenssiryhmä*

$$\begin{aligned} x &\equiv a \pmod{m} \\ x &\equiv b \pmod{n} \end{aligned}$$

on ratkeava, jos ja vain jos $\mathrm{syt}(m,n) \mid (a-b)$. *Jos kongruenssiryhmä on ratkeava, niin ratkaisu on yksikäsitteinen modulo* $\mathrm{pyj}(m,n)$.

Todistus (vrt. [2, s. 303–304]). Todistus koostuu kahdesta osasta. Todistetaan ensin, että lineaarinen kongruenssiryhmä on ratkeava, jos ja vain jos $\mathrm{syt}(m,n) \mid (a-b)$.

Oletetaan, että x_0 on lineaarisen kongruenssiryhmän eräs ratkaisu. Silloin $x_0 \equiv a \pmod{m}$ ja $x_0 \equiv b \pmod{n}$. Lauseen 2.1 perusteella saadaan, että $x_0 = a + km$, kun $k \in \mathbb{Z}$. Kun muuttujan x_0 paikalle sijoitetaan $a + km$, saadaan $a + km \equiv b \pmod{n}$, joka voidaan kirjoittaa muodossa $km \equiv b - a \pmod{n}$. Lauseen 2.4 perusteella kongruenssilla $km \equiv b - a \pmod{n}$ on siis olemassa ratkaisu k, jos ja vain jos $\mathrm{syt}(m,n) \mid (b-a)$, joka voidaan kirjoittaa muodossa $\mathrm{syt}(m,n) \mid (a-b)$. Täten yhtäpitävästi, $\mathrm{syt}(m,n) \mid (a-b)$, jos ja vain jos lineaarinen kongruenssiryhmä on ratkeava.

Todistetaan sitten, että kun ratkaisu on olemassa, niin ratkaisu on yksikäsitteinen modulo $\mathrm{pyj}(m,n)$. Oletetaan, että $\mathrm{syt}(m,n) \mid (a-b)$ ja että x_0 on eräs lineaarisen kongruenssiryhmän ratkaisu. Olkoon lisäksi x_1 mielivaltainen lineaarisen kongruenssiryhmän ratkaisu. Osoitetaan siis, että $x_1 \equiv x_0 \pmod{\mathrm{pyj}(m,n)}$.

Koska x_0 ja x_1 ovat lineaarisen kongruenssiryhmän ratkaisuja, niin kongruenssit $x_1 \equiv a \pmod{m}$, $x_1 \equiv b \pmod{n}$, $x_0 \equiv a \pmod{m}$ ja $x_0 \equiv b \pmod{n}$ ovat voimassa. Kongruenssien symmetrisyyden ja transitiivisuuden perusteella saadaan, että $x_1 \equiv x_0 \pmod{m}$ ja $x_1 \equiv x_0 \pmod{n}$, joten $m \mid (x_1 - x_0)$ ja $n \mid (x_1 - x_0)$. Tällöin $\text{pyj}(m,n) \mid (x_0 - x_1)$ eli $x_1 \equiv x_0 \pmod{\text{pyj}(m,n)}$. Täten jokainen ratkaisu x_1 on kongruentti luvun x_0 kanssa mod $\text{pyj}(m,n)$, mikä tarkoittaa, että ratkaisu on yksikäsitteinen modulo $\text{pyj}(m,n)$. Lause on siis todistettu. □

Esitetään kaksi esimerkkiä lauseen 3.1 käytöstä.

Esimerkki 3.1. Tutkitaan, ovatko seuraavat lineaariset kongruenssiryhmät ratkeavia.

$$\text{a)} \quad \begin{aligned} x &\equiv 3 \pmod{5} \\ x &\equiv 8 \pmod{10} \end{aligned} \qquad\qquad \text{b)} \quad \begin{aligned} x &\equiv 4 \pmod{6} \\ x &\equiv 1 \pmod{4} \end{aligned}$$

Ratkaisu.

a) Koska $\text{syt}(5,10) = 5$ ja $5 \mid (3-8)$, niin lineaarinen kongruenssiryhmä on ratkeava.

b) Koska $\text{syt}(6,4) = 2$, mutta $2 \nmid (4-1)$, niin lineaarinen kongruenssiryhmä ei ole ratkeava.

Esimerkki 3.2. Ratkaistaan lineaarinen kongruenssiryhmä

$$x \equiv 3 \pmod{5} \tag{3.1}$$

$$x \equiv 8 \pmod{10}. \tag{3.2}$$

Edellisen esimerkin 3.1 perusteella tiedetään, että lineaarisella kongruenssiryhmällä on yksikäsitteinen ratkaisu modulo $\text{pyj}(5,10)$, eli modulo 10.

Koska $x \equiv 3 \pmod{5}$, saadaan, että $x = 3 + 5k$, kun $k \in \mathbb{Z}$. Sijoitetaan $3 + 5k$ kongruenssiin (3.2) muuttujan x paikalle:

$$\begin{aligned} 3 + 5k &\equiv 8 \pmod{10} \\ 5k &\equiv 5 \pmod{10}. \end{aligned}$$

Jaetaan kongruenssin molemmat puolet luvulla 5, jolloin saadaan

$$k \equiv 1 \pmod{2}.$$

Siis, koska $k = 1 + 2t$, kun $t \in \mathbb{Z}$, niin $x = 3 + 5(1 + 2t) = 3 + 5 + 10t = 8 + 10t$. Täten $x = 8$ on yksikäsitteinen ratkaisu modulo $\text{pyj}(5,10) = 10$.

3.2 Kahden muuttujan ja kahden kongruenssin muodostama lineaarinen kongruenssiryhmä

Seuraavaksi esitetetään määritelmä kahden muuttujan ja kahden kongruenssin muodostamasta lineaarisesta kongruenssiryhmästä. Huomionarvoista on, että nyt kongruensseilla on sama moduli m, toisin kuin lauseessa 3.1 kongruenssien modulit m ja n voivat olla eri lukuja.

Määritelmä 3.1. [2, s. 308] Olkoot a, b, c, d, e, $f \in \mathbb{Z}$ ja olkoon $m \in \mathbb{Z}_+$. Silloin 2×2 *lineaarinen kongruenssiryhmä* on muotoa

$$\begin{aligned} ax + by &\equiv e \pmod{m} \\ cx + dy &\equiv f \pmod{m}. \end{aligned}$$

Lineaarisen kongruenssiryhmän ratkaisu on pari

$$\begin{aligned} x &\equiv x_0 \pmod{m} \\ y &\equiv y_0 \pmod{m}, \end{aligned}$$

joka toteuttaa molemmat 2×2 lineaarisen kongruenssiryhmän kongruenssit.

Esitetään sitten kaksi eri menetelmää, joilla voidaan ratkaista 2×2 lineaarisia kongruenssiryhmiä. Ensimmäinen menetelmä on eliminointimenetelmä, jossa eliminoidaan toinen kongruenssiryhmän muuttujista. Esitetään eliminointimenetelmä esimerkin 3.3 avulla. Toinen menetelmä esitetään todistamalla lause 3.2, joka kertoo matriisiavusteisen tavan ratkaista 2×2 lineaarinen kongruenssiryhmä.

Esimerkki 3.3. Ratkaistaan eliminointimenetelmää käyttäen lineaarinen kongruenssiryhmä

$$6x + 2y \equiv 2 \pmod{5} \tag{3.3}$$

$$2x + y \equiv 3 \pmod{5}. \tag{3.4}$$

Kerrotaan kongruenssin (3.4) molemmat puolet luvulla 2, jotta voidaan eliminoida muuttuja y:

$$4x + 2y \equiv 6 \pmod{5}.$$

Vähennetään kongruenssista (3.3) edellä saatu kongruenssi, jolloin saadaan

$$\begin{aligned} 2x &\equiv -4 \pmod{5} \\ x &\equiv 3 \pmod{5}. \end{aligned}$$

Muuttujan y arvo saadaan, kun korvataan kongruenssin (3.3) muuttuja x luvulla 3:

$$\begin{aligned} 6 \cdot 3 + 2y &\equiv 2 \pmod 5 \\ 2y &\equiv -16 \pmod 5 \\ y &\equiv 2 \pmod 5. \end{aligned}$$

Täten ratkaisu on pari $x \equiv 3 \pmod 5$, $y \equiv 2 \pmod 5$. Toisin sanoen, jokainen pari (x, y), joka toteuttaa kongruenssit $x \equiv 3 \pmod 5$ ja $y \equiv 2 \pmod 5$, on lineaarisen kongruenssiryhmän ratkaisu. Yleinen lineaarisen kongruenssiryhmän ratkaisu on täten muotoa $x = 3 + 5k$, $y = 2 + 5k$, kun $k \in \mathbb{Z}$.

Lause 3.2. *Olkoot a, b, c, d, e, $f \in \mathbb{Z}$, olkoon $m \in \mathbb{Z}_+$ ja* $\operatorname{syt}(\Delta, m) = 1$, *missä $\Delta = ad - bc$. Silloin lineaarisella kongruenssiryhmällä*

$$\begin{aligned} ax + by &\equiv e \pmod m \\ cx + dy &\equiv f \pmod m \end{aligned}$$

on yksikäsitteinen ratkaisu modulo m, mikä on muotoa

$$\begin{aligned} x_0 &\equiv \Delta^{-1}(de - bf) \pmod m \\ y_0 &\equiv \Delta^{-1}(af - ce) \pmod m, \end{aligned}$$

missä Δ^{-1} on luvun Δ käänteisluku modulo m.

Todistus (vrt. [3, s. 179–180]), (vrt. [2, s. 309–311]). Oletetaan, että lineaarisella kongruenssiryhmällä on ratkaisu $x \equiv x_0 \pmod m$ ja $y \equiv y_0 \pmod m$:

$$ax_0 + by_0 \equiv e \pmod m \tag{3.5}$$

$$cx_0 + dy_0 \equiv f \pmod m. \tag{3.6}$$

Kerrotaan kongruenssin (3.5) molemmat puolet luvulla d ja kongruenssin (3.6) molemmat puolet luvulla b, jotta saadaan eliminoitua muuttuja y_0:

$$adx_0 + bdy_0 \equiv de \pmod m \tag{3.7}$$

$$bcx_0 + bdy_0 \equiv bf \pmod m. \tag{3.8}$$

Vähentämällä kongruenssista (3.7) kongruenssi (3.8) saadaan

$$(ad - bc)x_0 \equiv (de - bf) \pmod m,$$

ja koska $\Delta = ad - bc$, niin saadaan

$$\Delta x_0 \equiv (de - bf) \pmod{m}.$$

Kun vielä kerrotaan kongruenssin molemmat puolet luvulla Δ^{-1}, saadaan

$$x_0 \equiv \Delta^{-1}(de - bf) \pmod{m},$$

koska $\Delta\Delta^{-1} \equiv 1 \pmod{m}$.

Samalla tavalla eliminoidaan muuttuja x_0, eli kerrotaan kongruenssin (3.5) molemmat puolet luvulla c ja kongruenssin (3.6) molemmat puolet luvulla a:

$$acx_0 + bcy_0 \equiv ce \pmod{m} \tag{3.9}$$

$$acx_0 + ady_0 \equiv af \pmod{m}. \tag{3.10}$$

Vähentämällä kongruenssista (3.10) kongruenssi (3.9) saadaan

$$(ad - bc)y_0 \equiv (af - ce) \pmod{m},$$

eli

$$\Delta y_0 \equiv (af - ce) \pmod{m}.$$

Kun vielä kerrotaan kongruenssin molemmat puolet luvulla Δ^{-1}, saadaan

$$y_0 \equiv \Delta^{-1}(af - ce) \pmod{m}.$$

Lisäksi seurauksen 2.1 nojalla tiedetään, että koska $\text{syt}(\Delta, m) = 1$, niin muuttujilla x_0 ja y_0 on yksikäsitteiset arvot modulo m. Koska oletuksen mukaan $\text{syt}(\Delta, m) = 1$, on täten osoitettu, että pari (x_0, y_0) on lineaarisen kongruenssiryhmän yksikäsitteinen ratkaisu, joka on muodoltaan $x_0 \equiv \Delta^{-1}(de - bf) \pmod{m}$ ja $y_0 \equiv \Delta^{-1}(af - ce) \pmod{m}$.

Seuraavaksi todistetaan, että yllä oleva pari (x_0, y_0) todella on lineaarisen kongruenssiryhmän ratkaisu. Siis, jos $x_0 \equiv \Delta^{-1}(de - bf) \pmod{m}$ ja $y_0 \equiv \Delta^{-1}(af - ce) \pmod{m}$, niin

$$\begin{aligned}
ax_0 + by_0 &\equiv a\Delta^{-1}(de - bf) + b\Delta^{-1}(af - ce) \\
&\equiv \Delta^{-1}(ade - abf) + \Delta^{-1}(abf - bce) \\
&\equiv \Delta^{-1}(ade - abf + abf - bce) \\
&\equiv \Delta^{-1}(ad - bc)e \\
&\equiv \Delta^{-1}\Delta e \\
&\equiv e \pmod{m}
\end{aligned}$$

ja

$$\begin{aligned} cx_0 + dy_0 &\equiv c\Delta^{-1}(de - bf) + d\Delta^{-1}(af - ce) \\ &\equiv \Delta^{-1}(cde - bcf) + \Delta^{-1}(adf - cde) \\ &\equiv \Delta^{-1}(cde - bcf + adf - cde) \\ &\equiv \Delta^{-1}(ad - bc)f \\ &\equiv \Delta^{-1}\Delta f \\ &\equiv f \pmod{m}. \end{aligned}$$

Täten $x \equiv x_0 \pmod{m}$, $y \equiv y_0 \pmod{m}$ on todella lineaarisen kongruenssiryhmän yksikäsitteinen ratkaisu. □

Esitetään lauseen 3.2 käytöstä esimerkki.

Esimerkki 3.4. Osoitetaan ensin, että lineaarisella kongruenssiryhmällä

$$\begin{aligned} 3x + 9y &\equiv 6 \pmod{13} \\ 9x + 3y &\equiv 7 \pmod{13} \end{aligned}$$

on yksikäsitteinen ratkaisu modulo 13.

Lauseen 3.2 perusteella riittää siis tarkistaa, että $\text{syt}(\Delta, 13) = 1$. Koska $\Delta \equiv ad - bc \equiv 3 \cdot 3 - 9 \cdot 9 \equiv -72 \equiv 6 \pmod{13}$, niin $\text{syt}(6, 13) = 1$. Täten lineaarisella kongruenssiryhmällä on yksikäsitteinen ratkaisu modulo 13.

Ratkaistaan sitten, mikä kyseinen yksikäsitteinen ratkaisu modulo 13 on. Määritelmän 2.6 nojalla saadaan, että luku 11 on luvun 6 käänteisluku modulo 13, eli $\Delta^{-1} \equiv 11 \pmod{13}$, koska $\Delta\Delta^{-1} \equiv 1 \pmod{13}$. Tällöin saadaan, että

$$\begin{aligned} x_0 &\equiv \Delta^{-1}(de - bf) \equiv 11(3 \cdot 6 - 9 \cdot 7) \equiv -495 \equiv 12 \pmod{13} \\ y_0 &\equiv \Delta^{-1}(af - ce) \equiv 11(3 \cdot 7 - 9 \cdot 6) \equiv -363 \equiv 1 \pmod{13}. \end{aligned}$$

Siis $x \equiv 12 \pmod{13}$ ja $y \equiv 1 \pmod{13}$ on lineaarisen kongruenssiryhmän yksikäsitteinen ratkaisu.

Ratkaisun paikkansapitävyys voidaan vielä tarkistaa sijoittamalla saadut ratkaisut muuttujille x ja y alkuperäiseen lineaariseen kongruenssiryhmään. Tällöin saadaan

$$\begin{aligned} 3x + 9y &\equiv 3 \cdot 12 + 9 \cdot 1 \equiv 45 \equiv 6 \pmod{13} \\ 9x + 3y &\equiv 9 \cdot 12 + 3 \cdot 1 \equiv 111 \equiv 7 \pmod{13}. \end{aligned}$$

Koska pari $(12, 1)$ toteuttaa lineaarisen kongruenssiryhmän, niin se on todella lineaarisen kongruenssiryhmän yksikäsitteinen ratkaisu.

4 Lineaaristen kongruenssiryhmien matriisiesitys

Kun muuttujien ja kongruenssien lukumäärä kasvaa suureksi, on hyödyllistä käyttää lineaarialgebraa ja erityisesti matriiseja apuna ratkaisun löytämiseksi. Tässä luvussa siis käsitellään sitä, miten matriisien avulla voidaan ratkaista lineaarisia kongruenssiryhmiä. Luvun lopussa esitetään havainnollistava esimerkki kolmen muuttujan ja kolmen kongruenssin muodostaman lineaarisen kongruenssiryhmän ratkaisemisesta.

Huomautus. Matriisien alkioiden oletetaan olevan kokonaislukuja.

Määritelmä 4.1. [3, s. 180–181] Olkoot $\mathbf{A}$ ja $\mathbf{B}$ $n \times k$ -matriiseja, joiden alkioita merkitään a_{ij} ja b_{ij}. Matriisi $\mathbf{A}$ on *kongruentti matriisin* $\mathbf{B}$ *kanssa modulo* m, jos $a_{ij} \equiv b_{ij} \pmod{m}$ kaikilla pareilla (i, j), kun $1 \leq i \leq n$ ja $1 \leq j \leq k$. Tällöin merkitään $\mathbf{A} \equiv \mathbf{B} \pmod{m}$.

Esitetään yksinkertainen esimerkki.

Esimerkki 4.1. Helposti nähdään, että

$$\begin{bmatrix} 8 & 5 \\ 3 & 10 \end{bmatrix} \equiv \begin{bmatrix} 1 & -2 \\ 3 & 3 \end{bmatrix} \pmod{7}.$$

Siis esimerkiksi kun $i, j = 1$, niin $8 \equiv 1 \pmod{7}$, koska $7 \mid (8 - 1)$.

Lause 4.1. *Olkoot* $\boldsymbol{A}$ *ja* $\boldsymbol{B}$ $n \times k$ *-matriiseja,* $\boldsymbol{C}$ $k \times p$ *-matriisi,* $\boldsymbol{D}$ $p \times n$ *-matriisi ja* $\boldsymbol{A} \equiv \boldsymbol{B} \pmod{m}$. *Silloin* $\boldsymbol{AC} \equiv \boldsymbol{BC} \pmod{m}$ *ja* $\boldsymbol{DA} \equiv \boldsymbol{DB} \pmod{m}$.

Todistus (vrt. [3, s. 181]). Todistetaan ensin tapaus $\mathbf{AC} \equiv \mathbf{BC} \pmod{m}$. Merkitään matriisien $\mathbf{A}$ ja $\mathbf{B}$ alkioita a_{ij} ja b_{ij}, kun $1 \leq i \leq n$ ja $1 \leq j \leq k$, ja vastaavasti merkitään matriisin $\mathbf{C}$ alkiota c_{ij}, kun $1 \leq i \leq k$ ja $1 \leq j \leq p$. Silloin matriisien $\mathbf{AC}$ ja $\mathbf{BC}$ alkiot ovat $\sum_{t=1}^{k} a_{it}b_{tj}$ ja $\sum_{t=1}^{k} b_{it}c_{tj}$, kun $1 \leq i \leq n$ ja $1 \leq j \leq p$. Koska $\mathbf{A} \equiv \mathbf{B} \pmod{m}$, niin määritelmän 4.1 perusteella $a_{it} \equiv b_{it} \pmod{m}$ kaikilla pareilla (i, t). Lauseen 2.3 kohtien (i) ja (iii) nojalla $\sum_{t=1}^{k} a_{it}c_{tj} \equiv \sum_{t=1}^{k} b_{it}c_{tj} \pmod{m}$, joten $\mathbf{AC} \equiv \mathbf{BC} \pmod{m}$.

Todistetaan sitten vastaavasti, että $\mathbf{DA} \equiv \mathbf{DB} \pmod{m}$. Merkitään edelleen matriisien $\mathbf{A}$ ja $\mathbf{B}$ alkioita a_{ij} ja b_{ij}, kun $1 \leq i \leq n$ ja $1 \leq j \leq k$, ja merkitään matriisin $\mathbf{D}$ alkiota d_{ij}, kun $1 \leq i \leq p$ ja $1 \leq j \leq n$. Silloin matriisien $\mathbf{DA}$ ja $\mathbf{DB}$ alkiot ovat $\sum_{t=1}^{n} d_{it}a_{tj}$ ja $\sum_{t=1}^{n} d_{it}b_{tj}$, kun $1 \leq i \leq p$ ja $1 \leq j \leq k$. Koska $\mathbf{A} \equiv \mathbf{B} \pmod{m}$, niin määritelmän 4.1 perusteella $a_{it} \equiv b_{it} \pmod{m}$ kaikilla pareilla (i, t). Lauseen 2.3 kohtien (i) ja (iii) nojalla $\sum_{t=1}^{n} d_{it}a_{tj} \equiv \sum_{t=1}^{n} d_{it}b_{tj} \pmod{m}$, joten $\mathbf{DA} \equiv \mathbf{DB} \pmod{m}$. Lause on siis todistettu. □

Huomautus. Edellisen lauseen tapauksen $\mathbf{DA} \equiv \mathbf{DB} \pmod{m}$ todistus on sivuutettu lähdekirjassa, joten tekijä on laatinut sen itse.

Tarkastellaan seuraavaksi lineaarista kongruenssiryhmää

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &\equiv b_1 \pmod{m} \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &\equiv b_2 \pmod{m} \\ &\vdots \\ a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nn}x_n &\equiv b_n \pmod{m}. \end{aligned}$$

Käyttämällä matriisimerkintöjä kongruenssiryhmä voidaan esittää matriisien kongruenssina eli $\mathbf{AX} \equiv \mathbf{B} \pmod{m}$, missä

$$\mathbf{A} = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix}, \quad \mathbf{X} = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} \quad \text{ja} \quad \mathbf{B} = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix}.$$

Tarkoituksena on ratkaista kongruensseja, jotka ovat muodoltaan $\mathbf{AX} \equiv \mathbf{B} \pmod{m}$. Ratkaisumenetelmä perustuu sellaisen matriisin $\mathbf{A}^{-1}$ löytämiseen, että $\mathbf{A}^{-1}\mathbf{A} \equiv \mathbf{I} \pmod{m}$, missä $\mathbf{I}$ on identiteettimatriisi.

Määritelmä 4.2. [3, s. 182] Olkoot matriisit $\mathbf{A}$ ja $\mathbf{A}^{-1}$ $n \times n$ -matriiseja. Jos $\mathbf{A}^{-1}\mathbf{A} \equiv \mathbf{A}\mathbf{A}^{-1} \equiv \mathbf{I} \pmod{m}$, niin matriisia $\mathbf{A}^{-1}$ kutsutaan matriisin $\mathbf{A}$ *käänteismatriisiksi* modulo m.

Jos matriisi $\mathbf{A}^{-1}$ on matriisin $\mathbf{A}$ käänteismatriisi ja $\mathbf{B} \equiv \mathbf{A}^{-1} \pmod{m}$, niin tällöin myös matriisi $\mathbf{B}$ on matriisin $\mathbf{A}$ käänteismatriisi. Tulos seuraa lauseesta 4.1, koska $\mathbf{BA} \equiv \mathbf{A}^{-1}\mathbf{A} \equiv \mathbf{I} \pmod{m}$ ja $\mathbf{AB} \equiv \mathbf{A}\mathbf{A}^{-1} \equiv \mathbf{I} \pmod{m}$.

Jos matriisit $\mathbf{B}_1$ ja $\mathbf{B}_2$ ovat matriisin $\mathbf{A}$ käänteismatriiseja, niin $\mathbf{B}_1 \equiv \mathbf{B}_2 \pmod{m}$. Lauseen 4.1 ja kongruenssin $\mathbf{B}_1\mathbf{A} \equiv \mathbf{B}_2\mathbf{A} \equiv \mathbf{I} \pmod{m}$ perusteella

saadaan, että $\mathbf{B}_1\mathbf{A}\mathbf{B}_1 \equiv \mathbf{B}_2\mathbf{A}\mathbf{B}_1 \equiv \mathbf{I} \pmod{m}$. Koska $\mathbf{A}\mathbf{B}_1 \equiv \mathbf{I} \pmod{m}$, niin kongruenssista $\mathbf{B}_1\mathbf{A}\mathbf{B}_1 \equiv \mathbf{B}_2\mathbf{A}\mathbf{B}_1 \pmod{m}$ päätellään, että $\mathbf{B}_1 \equiv \mathbf{B}_2 \pmod{m}$.

Seuraava lause antaa helpon tavan löytää 2×2 -matriisin käänteismatriisi.

Lause 4.2. *Olkoon* $\boldsymbol{A} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, *olkoon* $m \in \mathbb{Z}_+$, $\Delta = \det \boldsymbol{A} = ad - bc$ *ja* $\operatorname{syt}(\Delta, m) = 1$. *Silloin matriisi*

$$\boldsymbol{A}^{-1} = \Delta^{-1} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

on matriisin $\boldsymbol{A}$ *käänteismatriisi modulo* m.

Todistus (vrt. [3, s. 182–183]). Määritelmän 4.2 perusteella riittää osoittaa, että $\mathbf{A}\mathbf{A}^{-1} \equiv \mathbf{A}^{-1}\mathbf{A} \equiv \mathbf{I} \pmod{m}$. Koska $\operatorname{syt}(\Delta, m) = 1$, niin luvun Δ käänteisluku modulo m on olemassa. Täten saadaan

$$\mathbf{A}\mathbf{A}^{-1} \equiv \begin{bmatrix} a & b \\ c & d \end{bmatrix} \Delta^{-1} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \equiv \Delta^{-1} \begin{bmatrix} ad - bc & 0 \\ 0 & -bc + ad \end{bmatrix}$$

$$\equiv \Delta^{-1} \begin{bmatrix} \Delta & 0 \\ 0 & \Delta \end{bmatrix} \equiv \begin{bmatrix} \Delta^{-1}\Delta & 0 \\ 0 & \Delta^{-1}\Delta \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \mathbf{I} \pmod{m}$$

ja

$$\mathbf{A}^{-1}\mathbf{A} \equiv \Delta^{-1} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \Delta^{-1} \begin{bmatrix} ad - bc & 0 \\ 0 & -bc + ad \end{bmatrix}$$

$$\equiv \Delta^{-1} \begin{bmatrix} \Delta & 0 \\ 0 & \Delta \end{bmatrix} \equiv \begin{bmatrix} \Delta^{-1}\Delta & 0 \\ 0 & \Delta^{-1}\Delta \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \mathbf{I} \pmod{m}.$$

Matriisi $\mathbf{A}^{-1}$ on täten matriisin $\mathbf{A}$ käänteismatriisi modulo m. □

Esitetään lauseen 4.2 käytöstä esimerkki.

Esimerkki 4.2. Olkoon matriisi $\mathbf{A} = \begin{bmatrix} 7 & 2 \\ 9 & 3 \end{bmatrix}$. Silloin $\det \mathbf{A} = 7 \cdot 3 - 9 \cdot 2 = 3$. Koska $\operatorname{syt}(3, 11) = 1$, niin luvulla 3 on käänteisluku modulo 11. Koska $3 \cdot 4 \equiv 1 \pmod{11}$, niin luku 4 on luvun 3 käänteisluku modulo 11. Saadaan siis, että

$$\mathbf{A}^{-1} \equiv 4 \begin{bmatrix} 3 & -2 \\ -9 & 7 \end{bmatrix} \equiv \begin{bmatrix} 12 & -8 \\ -36 & 28 \end{bmatrix} \equiv \begin{bmatrix} 1 & 3 \\ 8 & 6 \end{bmatrix} \pmod{11}.$$

Suurempien kuin 2×2-matriisien käänteismatriisien määrittämiseen tarvitaan toisenlainen menetelmä. Seuraavaksi todistetaan lause 4.3, jonka avulla pystytään todistamaan lause 4.4, joka antaa ratkaisumenetelmän käänteismatriisin $\mathbf{A}^{-1}$ löytämiselle, kun matriisi $\mathbf{A}$ on suurempi tai yhtä suuri kuin 2×2 -matriisi.

Huomautus. Lukijan oletetaan tuntevan sekä adjungoidun matriisin määritelmän että kofaktoriesityksen käsitteen (ks. [1, s. 108, 122]).

Lause 4.3. *Olkoon $\boldsymbol{A}$ $n \times n$ -matriisi ja* $\det \boldsymbol{A} \neq 0$. *Silloin* $\boldsymbol{A}(\operatorname{adj} \boldsymbol{A}) = (\det \boldsymbol{A})\boldsymbol{I}$.

Todistus (vrt. [1, s. 123–124]). Kirjoitetaan $\mathbf{A}(\operatorname{adj} \mathbf{A})$ matriisimuodossa:

$$\mathbf{A}(\operatorname{adj} \mathbf{A}) = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{i1} & a_{i2} & \dots & a_{in} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix} \begin{bmatrix} C_{11} & C_{21} & \dots & C_{j1} & \dots & C_{n1} \\ C_{12} & C_{22} & \dots & C_{j2} & \dots & C_{n2} \\ \vdots & \vdots & & \vdots & & \vdots \\ C_{1n} & C_{2n} & \dots & C_{jn} & \dots & C_{nn} \end{bmatrix}.$$

Tällöin tulomatriisin $\mathbf{A}(\operatorname{adj} \mathbf{A})$ rivin i ja sarakkeen j alkio on muodoltaan

$$a_{i1}C_{j1} + a_{i2}C_{j2} + \cdots + a_{in}C_{jn}. \tag{4.1}$$

Jos $i = j$, niin alkio (4.1) on rivin i suhteen muodostettu kofaktoriesitys, eli $\det \mathbf{A}$. Jos $i \neq j$, niin tällöin matriisin $\mathbf{A}$ alkiot ja kofaktorit tulevat matriisin $\mathbf{A}$ eri riveiltä, joten arvoksi tulee nolla. Täten

$$\mathbf{A}(\operatorname{adj} \mathbf{A}) = \begin{bmatrix} \det \mathbf{A} & 0 & \dots & 0 \\ 0 & \det \mathbf{A} & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & \det \mathbf{A} \end{bmatrix} = (\det \mathbf{A})\mathbf{I}.$$

□

Lause 4.4. *Olkoon $\boldsymbol{A}$ $n \times n$ -matriisi, olkoon $m \in \mathbb{Z}_+$ ja* $\operatorname{syt}(\det \boldsymbol{A}, m) = 1$. *Silloin matriisi $\boldsymbol{A}^{-1} = \Delta^{-1}(\operatorname{adj} \boldsymbol{A})$ on matriisin $\boldsymbol{A}$ käänteismatriisi modulo m, missä Δ^{-1} on luvun $\Delta = \det \boldsymbol{A}$ käänteisluku modulo m.*

Todistus (vrt. [3, s. 183–184]). Jos syt$(\det \mathbf{A}, m) = 1$, niin $\det \mathbf{A} \neq 0$. Tällöin lauseen 4.3 perusteella $\mathbf{A}(\operatorname{adj} \mathbf{A}) = (\det \mathbf{A})\mathbf{I} = \Delta\mathbf{I}$. Koska syt $(\det \mathbf{A}, m) = 1$, niin luvun Δ käänteisluku Δ^{-1} modulo m on olemassa. Täten

$$\mathbf{A}(\Delta^{-1} \operatorname{adj} \mathbf{A}) \equiv \mathbf{A} \cdot (\operatorname{adj} \mathbf{A})\Delta^{-1} \equiv \Delta\Delta^{-1}\mathbf{I} \equiv \mathbf{I} \pmod{m}$$

ja

$$\Delta^{-1}(\operatorname{adj} \mathbf{A})\mathbf{A} \equiv \Delta^{-1}((\operatorname{adj} \mathbf{A})\mathbf{A}) \equiv \Delta^{-1}\Delta\mathbf{I} \equiv \mathbf{I} \pmod{m}.$$

Siis $\mathbf{A}^{-1} = \Delta^{-1}(\operatorname{adj} \mathbf{A})$ on matriisin $\mathbf{A}$ käänteismatriisi modulo m. □

Kuten jo aikaisemmin todettiin, matriisin $\mathbf{A}$ käänteismatriisin $\mathbf{A}^{-1}$ avulla saadaan ratkaistua kongruenssiyhtälö

$$\mathbf{AX} \equiv \mathbf{B} \pmod{m},$$

missä syt$(\det \mathbf{A}, m) = 1$. Lauseen 4.1 perusteella, kun kerrotaan kongruenssiyhtälön molemmat puolet matriisin $\mathbf{A}$ käänteismatriisilla $\mathbf{A}^{-1}$, saadaan

$$\begin{aligned} \mathbf{A}^{-1}(\mathbf{AX}) &\equiv \mathbf{A}^{-1}\mathbf{B} \pmod{m} \\ (\mathbf{A}^{-1}\mathbf{A})\mathbf{X} &\equiv \mathbf{A}^{-1}\mathbf{B} \pmod{m} \\ \mathbf{X} &\equiv \mathbf{A}^{-1}\mathbf{B} \pmod{m}. \end{aligned}$$

Ollaan siis saatu johdettua lineaarisen kongruenssiryhmän ratkaisumenetelmä matriisien avulla.

Esimerkki 4.3. Tarkastellaan lineaarista kongruenssiryhmää

$$\begin{aligned} 3x_1 + 2x_2 + 2x_3 &\equiv 3 \pmod{5} \\ 3x_1 + 2x_2 + x_3 &\equiv 2 \pmod{5} \\ 4x_2 + 3x_3 &\equiv 1 \pmod{5}. \end{aligned}$$

Lineaarinen kongruenssiryhmä on täten matriisimuodossa

$$\begin{bmatrix} 3 & 2 & 2 \\ 3 & 2 & 1 \\ 0 & 4 & 3 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} \equiv \begin{bmatrix} 3 \\ 2 \\ 1 \end{bmatrix} \pmod{5}.$$

Merkitään $\mathbf{A} = \begin{bmatrix} 3 & 2 & 2 \\ 3 & 2 & 1 \\ 0 & 4 & 3 \end{bmatrix}$. Tällöin $\det \mathbf{A} = 12$. Koska syt$(12, 5) = 1$, niin luvulla 12 on käänteisluku modulo 5. Koska $12 \cdot 3 \equiv 1 \pmod{5}$, niin luku 3 on

luvun 12 käänteisluku modulo 5. Tällöin saadaan, että

$$\mathbf{A}^{-1} = 3(\operatorname{adj}\mathbf{A}) = 3\begin{bmatrix} 2 & 2 & -2 \\ -9 & 9 & 3 \\ 12 & -12 & 0 \end{bmatrix} = \begin{bmatrix} 6 & 6 & -6 \\ -27 & 27 & 9 \\ 36 & -36 & 0 \end{bmatrix} \equiv \begin{bmatrix} 1 & 1 & 4 \\ 3 & 2 & 4 \\ 1 & 4 & 0 \end{bmatrix} \pmod 5.$$

Tällöin

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 4 \\ 3 & 2 & 4 \\ 1 & 4 & 0 \end{bmatrix} \begin{bmatrix} 3 \\ 2 \\ 1 \end{bmatrix} = \begin{bmatrix} 9 \\ 17 \\ 11 \end{bmatrix} \equiv \begin{bmatrix} 4 \\ 2 \\ 1 \end{bmatrix} \pmod 5.$$

Siis

$$\begin{aligned} x_1 &\equiv 4 \pmod 5 \\ x_2 &\equiv 2 \pmod 5 \\ x_3 &\equiv 1 \pmod 5 \end{aligned}$$

on lineaarisen kongruenssiryhmän yksikäsitteinen ratkaisu.

Lähteet

[1] Anton, H., Rorres, C. *Elementary Linear Algebra: Applications version.* 11. painos. Wiley, 2013.

[2] Koshy, T. *Elementary Number Theory with Applications.* 2. painos. Elsevier, 2007.

[3] Rosen, K. H. *Elementary Number Theory and its Applications.* 6. painos. Addison-Wesley, 2011.