TAMPEREEN TEKNILLINEN YLIOPISTO
TAMPERE UNIVERSITY OF TECHNOLOGY

MAIJU NIEMINEN

KIINALAINEN JÄÄNNÖSLAUSE

Kandidaatintyö

Tarkastaja: Mika Mattila
09.10.2018

TIIVISTELMÄ

MAIJU NIEMINEN: Kiinalainen jäännöslause
Tampereen teknillinen yliopisto
Kandidaatintyö, 17 sivua
lokakuu 2018
Teknis-luonnontieteellinen koulutusohjelma
Pääaine: Matematiikka
Tarkastajat: Yliopisto-opettaja Mika Mattila
Avainsanat: Kiinalainen jäännöslause

SISÄLLYS

LYHENTEET JA MERKINNÄT

syt	Suurin yhteinen tekijä
mod	Modulo

1. JOHDANTO

Matematiikka on tieteiden kuningatar ja lukuteorian sanotaan olevan matematiikan kuningas. Lukuteoria on vanhimpia matematiikan aloja. Siinä tutkitaan paljon kokonaislukuja ja niiden jaollisuutta. Kiinalainen jäännöslause on lukuteorian lause, joka on kirjoitettu ylös nimensä mukaan Kiinassa. Sen alkuperäinen ongelma oli selvittää kiinalaisten sotilaiden määrä sotilaiden riveihin jakautumisen avulla.

Kiinalainen jäännöslause perustuu moniin lukuteorian määritelmiin. Työssä tutkitaan kiinalaisen jäännöslauseeseen tarvittavia määritelmiä ja taustoja sekä tutustutaan sen käyttökohteisiin. Kiinalaisen jäännöslauseen sovelluksista kerrotaan vielä lyhyesti lopussa.

Vaikka kiinalainen jäännöslause on vanha keksintö, sillä on useita nykyaikaisia sovelluksia. Yksi tärkeimmistä sovelluksista on salausjärjestelmä RSA. RSA:ssa lukujonot voidaan salata ja vastaanottaja purkaa salauksen siihen saadulla avaimella. Salaaminen perustuu siihen, että kahden suuren alkuluvun tulon tekijät ovat vaikeasti selvitettävissä.

Työn alussa kerrotaan perustietoja lukuteoriasta ja määritellään keskeisiä käsitteitä, kuten jaollisuutta. Jaollisuutta tai jaottomuutta voidaan esittää kongruenssin avulla. Kongruenssin avulla tutkitaan eri jäännösluokkia, jotka ovat myös kongruenssiyhtälöiden ratkaisuja. Kiinalaisessa jäännöslauseessa on kyse kongruenssiyhtälöryhmän ratkaisemisesta.

Kiinalainen jännöslauseessa tarkastellaan sen sisältöä ja todistusta. Esimerkin kautta tutkitaan kiinalaisen jäännöslauseen käyttämistä. Viimeisenä katsotaan käytännön sovellusta kiinalaiselle jäännöslauseelle.

2. KONGRUENSSI

2.1 Jakoyhtälö

Lukuteoriassa käsitellään paljon kokonaislukuja. Kokonaislukujen tärkein ominaisuus lukuteoriassa on jaollisuus.

Määritelmä 2.1.1. Kokonaisluku b on jaollinen kokonaisluvulla a, jos on olemassa sellainen kokonaisluku c, että $b = ac$. Jos a jakaa luvun b, voidaan sanoa, että a on kokonaisluvun b jakaja ja b on luvun a monikerta.

Luvun b jaollisuus luvulla a voidaan merkitä $a \mid b$. Jos a ei jaa kokonaislukua b, kirjoitetaan $a \nmid b$. Jakohtälö on lause, jonka nojalla mistä tahansa kokonaisluvusta voidaan yksikäsitteisellä tavalla erottaa etukäteen valitun jakajan q monikerta. [1, s. 36-37]

Lause 2.1.1 (Jakoyhtälö)**.** Positiivisille kokonaisluvuille a ja b on olemassa sellaiset yksikäsitteiset kokonaisluvut q ja r, että $a = bq + r$, missä $0 \leq r < b$.

Jakoyhtälöllä [1, s. 37] voidaan kirjoittaa jokainen kokonaisluku minkä tahansa luvun avulla. Esimerkiksi jokainen luku voidaan ilmoittaa luvun 4 avulla muodossa $4q, 4q+1, 4q+2$ tai $4q+3$.

Määritelmä 2.1.2 (Suurin yhteinen tekijä)**.** Olkoot a ja b kokonaislukuja. Lukujen a ja b suurin yhteinen tekijä $d > 0$ on suurin sellainen positiivinen kokonaisluku, että $d \mid a$ ja $d \mid b$.

Lukujen a ja b suurinta yhteistä tekijää merkitään $\text{syt}(a, b) = d$. Jakoyhtälön avulla voidaan etsiä lukujen suurin yhteinen tekijä Eukleideen algoritmilla. Jos luvut ovat jaollisia, luvuista pienempi on suurin yhteinen tekijä. Luvut $a_1, a_2, \ldots, a_n$ ovat keskenään jaottomia, jos $\text{syt}(a_1, a_2, \ldots, a_n) = 1$. Luvut ovat pareittain suhteellisia alkulukuja eli pareittain jaottomia, jos $\text{syt}(a_i, a_j) = 1$, kun $i \neq j$.

Lause 2.1.2. Olkoot a ja b positiivisia kokonaislukuja. Oletetaan, että $a = bq + r$ joillakin kokonaisluvuilla q ja $0 < r \neq b$. Tällöin kokonaisluku c on lukujen a ja b tekijä, jos ja vain jos luku c on myös lukujen b ja r tekijä.

Todistus. Ks. [1, s. 94]. □

Lause 2.1.3. Olkoot a ja b kokonaislukuja ja $a = bq + r$, missä $r \neq 0$ ja $b > r$. Tällöin $\text{syt}(a, b) = \text{syt}(b, r)$

Todistus. Ks. [1, s. 103] □

Lauseen 2.1.3 [1, s.103] avulla voidaan etsiä kahdelle luvulle suurin yhteinen tekijä jakoyhtälön avulla. Jos Lausetta 2.1.3 käytetään usemman kerran peräkkäin, saadaan algoritmi suurimman yhteisen tekijän löytämiselle.

Lause 2.1.4 (Eukleideen algoritmi)**.** Olkoot $a = r_0$ ja $b = r_1$ sellaiset kokonaisluvut, että $a \geq b > 0$. Algoritmissa sovelletaan jakoyhtälöä n kertaa peräkkäin, jolloin saadut yhtälöt ovat muotoa $r_j = r_{j+1}q_{j+1} + r_{j+2}$, missä $0 < r_{j+2} < r_{j+1}$ jokaisella $j = 0, 1, 2, \ldots, n-2$, kunnes $r_{n+1} = 0$. Silloin saadaan $\text{syt}(a, b) = r_n$, viimeinen nollasta eroava jäkojäänös.

Todistus vrt. [1, s. 103-104]. Olkoot $r_0 = a$ ja $r_1 = b$ sellaisia positiivisia kokonaislukuja, että $a \geq b$. Koko Eukleideen algoritmi voidaan kirjoittaa auki muotoon

$$\begin{aligned}
r_0 &= r_1q_1 + r_2, \qquad 0 \leq r_2 < r_1,\\
r_1 &= r_2q_2 + r_3, \qquad 0 \leq r_3 < r_2,\\
&\vdots\\
r_{j-2} &= r_{j-1}q_{j-1} + r_j, \qquad 0 \leq r_j < r_{j-1},\\
&\vdots\\
r_{n-3} &= r_{n-2}q_{n-2} + r_{n-1}, \qquad 0 \leq r_{n-1} < r_{n-2},\\
r_{n-2} &= r_{n-1}q_{n-1} + r_n, \qquad 0 \leq r_n < r_{n-1},\\
r_{n-1} &= r_nq_n.
\end{aligned}$$

Jokaisessa tapauksessa viimeisestä jakojäännöksestä tulee nolla, sillä jono $a = r_0 \geq r_1 > r_2 > \cdots \geq 0$ ei voi sisältää enempää kuin a kappaletta lukuja ja jokainen luku on edellistä aidosti pienempi ja ei-negatiivinen. Kun hyödynnetään Lausetta 2.1.3, saadaan

$$\begin{aligned}
\text{syt}(a, b) = \text{syt}(r_0, r_1) = \text{syt}(r_1, r_2) = \text{syt}(r_2, r_3) = \cdots = \text{syt}(r_{n-3}, r_{n-2})\\
= \text{syt}(r_{n-2}, r_{n-1}) = \text{syt}(r_{n-1}, r_n) = \text{syt}(r_n, 0) = r_n.
\end{aligned}$$

Tästä seuraa, että $\text{syt}(a, b) = r_n$. □

Esimerkki 2.1.1. Etsitään suurin yhteinen tekijä luvuille 414 ja 315:

$$\begin{aligned} 414 &= 1 \cdot 315 + 99, \\ 315 &= 3 \cdot 99 + 18, \\ 99 &= 5 \cdot 18 + 9, \\ 18 &= 2 \cdot 9 + 0. \end{aligned}$$

Tällöin syt(414, 315)=9.

Diofantoksen yhtälössä tehtävä on selvittää kahden muuttujan lineaarisen yhtälön ratkaisua. Ratkaisun löytäminen perustuu suurimman yhteisen tekijän löytämiseen.

Lause 2.1.5 (Diofantoksen yhtälö)**.** Olkoot a ja b positiivia kokonaislukuja ja $d = \text{syt}(a, b)$. Yhtälölle $ax + by = c$ ei ole kokonaislukuratkaisua, jos $d \nmid c$. Jos $d \mid c$, yhtälölle on olemassa äärettömän monta kokonaislukuratkaisua.

Todistus. Diofantoksen yhtälö eli Lause 2.1.5 [1, s. 137-138] todistetaan kolmessa osassa. Ensin tutkitaan, millä ehdoin ratkaisu on olemassa. Sen jälkeen osoitetaan, että ratkaisuja on ehdon täyttyessä ääretön määrä. Lopuksi todistetaan, että kaikki ratkaisut ovat oikeaa muotoa.

Oletetaan, että pari $(x,\ y)$ on kokonaislukuratkaisu, jolloin $ax + by = c$. Koska $d \mid a$ ja $d \mid b$, niin on oltava $d \mid c$. Jos kuitenkin olisi, että $d \nmid c$, yhtälölle ei ole ratkaisua, sillä tällöin yhtälön $ax + by = c$ vasen puoli olisi jaollinen luvulla d mutta oikea puoli ei, mikä olisi ristiriita. Oletetaan siis, että $d \mid c$. Silloin on olemassa kokonaisluvut s ja t, joille on voimassa $d = as + bt$. Koska $d \mid c$, tästä seuraa, että on olemassa kokonaisluku e, jolle on voimassa $de = c$. Yhdistämällä tulokset saadaan $c = de = (as + bt)e = a(se) + b(te)$. Yhdeksi yhtälön ratkaisuksi voidaan nyt valita $x = x_0$ ja $y = y_0$, missä $x_0 = se$ ja $y_0 = te$. Ratkaisu on siis olemassa. Todistetaan seuraavaksi, että ratkaisuja on ääretön määrä. Olkoon $x = x_0 + (b/d)n$ ja $y = y_0 - (a/d)n$, missä n on jokin mielivaltainen kokonaisluku. Näytetään, että pari (x, y) on aina ratkaisu riippumatta luvusta n. Nähdään, että (x, y) on ratkaisu, sillä

$$\begin{aligned} ax + by &= ax_0 + a(b/d)n + by_0 - b(a/d)n \\ &= ax_0 + by_0 = c. \end{aligned}$$

Näytetään vielä, että mielivaltainen ratkaisu (x, y) on oikeaa muotoa, eli jokainen ratkaisu saadaan jollakin kertoimen n arvolla. Koska (x, y) ja (x_0, y_0) ovat molemmat

yhtälön ratkaisuja, voidaan kirjoittaa

$$c = (ax + by) = (ax_0 + by_0).$$

Tästä saadaan ratkaistua $a(x - x_0) = b(y_0 - y)$. Jakamalla molemmat puolet luvulla d saadaan

$$(a/d)(x - x_0) = (b/d)(y_0 - y).$$

Tiedetään, että $\text{syt}(a/d, b/d) = 1$, mistä seuraa, että $(a/d) \mid (y_0 - y)$. Tämän avulla kirjoitetaan $(a/d)n = y_0 - y$ eli $y = y_0 - (a/d)n$. Samoin voidaan toimia myös ratkaisun x kanssa, jolloin saadaan $a(x - x_0) = b(a/d)n$ eli $x = x_0 + (b/d)n$. □

Diofantoksen yhtälön ratkaisujen äärettömys voidaan ajatella esimerkiksi suoran avulla. Esimerkiksi yhtälö $2x + 3y = 5$ voidaan esittää muodossa $y = -2/3x + 5/3$, joka on suoran yhtälö. Jos suoralle löydetään yksi kokonaislukupiste, niin suoralla on ääretön määrä kokonaislukupisteitä. Esimerkiksi piste $(1, 0)$ on suoralla, ja siten sillä on myös äärettömön monta muuta kokonaislukuratkaisua.

2.2 Kongruenssi

Kongruenssi kertoo kahden luvun välisestä yhteydestä ja jaksollisuudesta. Luonnossa on monia asioita, jotka ovat kongruentteja keskenään jollakin modulolla m. Esimerkiksi kellonaika on sama aina tasan 24 tunnin jälkeen. Kellon minuttiluku on myös kongruentti modulo 60 sekuntia. Sekunttiluku taas voidaan ilmoittaa kellossa aina pienempänä kuin 60 eli se on kongruentti modulo 60.

Määritelmä 2.2.1 (Kongruenssi)**.** Olkoon m positiviinen kokonaisluku. Kokonaisluvut a ja b ovat kongruentteja modulo m eli $a \equiv b \pmod{m}$, jos $m \mid a - b$.

Jos luvut eivät ole kongruetteja keskenään modulo m, merkitään $a \not\equiv b \pmod{m}$ [1, s. 145].

Lause 2.2.1. Kokonaisluvut a ja b ovat kongruentteja modulo m eli $a \equiv b \pmod{m}$, jos ja vain jos on olemassa sellainen kokonaisluku k, että $a = b + km$.

Todistus. Jos a ja b ovat kongruentteja modulo m eli $a \equiv b \pmod{m}$, niin $a - b$ on jaollinen luvulla m. Silloin voidaan kirjoittaa, että $km = a - b$ eli $a = b + km$. Toisaalta, jos $a = b + km$, niin $a - b = km$ eli a ja b ovat kongruentteja modulo m. □

Edellisestä Lauseesta 2.2.1 [1, s. 146] seuraa, että kokonaisluvuista a ja b jää sama jakojäännös jaettaessa luvulla m.

Esimerkiksi luvut 5 ja 8 ovat kongruentteja modulo 3, sillä niistä jää sama jakojäännös jaettaessa luvulla 3. Tällöin voidaan kirjoittaa

$$8 \equiv 5 \pmod{3}.$$

Luvut 5 ja 8 voidaan ilmoittaa muodossa $2+3k$, missä k on määrätty kokonaisluku. Kaikki muutkin niiden kanssa kongruentit luvut modulo 3 voidaan ilmoittaa muodossa $2 + 3k$. Luvuista muodostuu luvun 3 jäännösluokka, joka yleensä merkitään pienimmän positiivisen luvun mukaan, mikä saavutetaan, kun $k = 0$. Esimerkiksi luvun 3 kaikki jäännösluokat ovat kaikki $\bar{0}$, $\bar{1}$ tai $\bar{2}$. Jokainen kokonaisluku voidaan sijoittaa johonkin näistä jäännösluokista.

Yleisesti jokaiselle luvulla n on olemassa tasan n kappaletta jäännösluokkia, joissa jokaisessa on eri jakojäännös luvulla n jaettaessa. Jokaisessa luokassa on ääretön määrä numeroita. Jokainen kokonaisluku voidaan sijoittaa tasan yhteen jäännösluokkaan. Luokkien jakojännökset ovat nollasta lukuun $n - 1$.

2.3 Kongruenssiyhtälö

Kongruenssia voidaan hyödyntää myös tietynlaisten matemaattisten ongelmien ratkaisemisessa. Kongruenssi voidaan muodostaa myös kokonaislukumuuttujalle, jolloin syntyy kongruenssiyhtälö. Erityisesti kongruensille voidaan määritellä lineaarinen yhtälö, jossa muuttuja on ensimmäistä astetta. Lineaarinen kongruenssiyhtälö voidaan kirjoittaa muodossa

$$ax \equiv b \pmod{m},$$

missä x on muuttuja. Lineaarisen kongruenssiyhtälön voi ratkaista Diofantoksen yhtälön avulla. [1, s. 157]

Esimerkki 2.3.1. Etsitään kaikki ratkaisut yhtälölle $41x \equiv 3 \pmod{12}$. Tarkistetaan ensin, että vastaus on olemassa, eli, että $\text{syt}(41, 12) = 1$ ja $\text{syt}(41, 12) = 1 \mid 3$. Muodostetaan kongruenssiyhtälöstä diofantoksen yhtälö $41x - 12y = 3$.

Käytetään Eukleideen algoritmia suurimman yhteisen tekijän tarkistamiseen:

$$\begin{aligned} 41 &= 3 \cdot 12 + 5, \\ 12 &= 2 \cdot 5 + 2, \\ 5 &= 2 \cdot 2 + 1. \end{aligned}$$

Saaduista jakoyhtälöistä voidaan kirjoittaa alkuperäisen diofantoksen yhtälön kertoimien avulla ja etsiä siten jotkin käyvät arvot muuttujille x ja y. Sijoitetaan jokaisen jakojäännöksen tilalle jakoyhtälön edelliset vaiheen termit, jolloin saadaan

$$\begin{aligned} 1 &= 5 - 2 \cdot 2 \\ &= 5 - 2(12 - 2 \cdot 5) \\ &= 41 - 3 \cdot 12 - 2(12 - 2(41 - 3 \cdot 12)) \\ &= 41 - 3 \cdot 12 - 2(12 - 2 \cdot 41 + 6 \cdot 12) \\ &= 41 - 3 \cdot 12 - 2 \cdot 12 + 4 \cdot 41 - 12 \cdot 12 \\ &= 5 \cdot 41 - 17 \cdot 12. \end{aligned}$$

Kerrotaan luvulla 3 yhtälön molemmat puolet ja saadaan muutettua yhtälö muotoon $3 = 15 \cdot 41 - 51 \cdot 12$. Ratkaisuksi saadaan alkuperäisen Diofantoksen yhtälön avulla $x_0 = 15$ ja $y_0 = -51$.

Lineaarisen kongruenssiyhtälön ratkaisemiseen voidaan käyttää myös luvun a käänteislukua modulo m. Diofantoksen yhtälön kautta voidaan tietää, että ratkaisu on olemassa ja saadaan ratkaistua yhtälö. Tarvittava Diofantoksen yhtälö on muotoa $ax+my = 1$, missä $\text{syt}(a, m) = 1$. Keskenään jaottomat kertoimet a ja m sisältävälle Diofantoksen yhtälölle löytyy aina ratkaisu.

Määritelmä 2.3.1. Olkoot keskenään jaottomat kokonaisluvut a ja m, milloin $\text{syt}(a, m) = 1$. Yhtälön $ax \equiv 1 \pmod{m}$ kokonaislukuratkaisua x kutsutaan luvun a käänteisluvuksi modulo m.

Esimerkki 2.3.2. Etsitään ratkaisu yhtälölle $11x \equiv 1 \pmod{34}$. Vastaukseksi saadaan $x \equiv 31 \pmod{34}$, sillä $11 \cdot 31 \equiv 1 \pmod{34}$.

Kongruenssiyhtälöitä voi olla useampi, jolloin saadaan kongruenssiyhtälöryhmä. Kongruenssiyhtälöryhmissä on useampi lineaarinen yhtälö, joissa esiintyy muuttujia. Muuttujana voi toimia kerroin x tai moduli m.

3. KIINALAINEN JÄÄNNÖSLAUSE

Kiinalainen jäännöslause on tunnettu laajalti, mutta sen on kirjoittanut yleisessä muodossa ylös kiinalainen Ch'in Chiu-Shao kirjassaan vuonna 1247. Ensimmäiset tunnetut kirjoitukset ovat ensimmäiseltä vuosisadalta Kreikasta. Kiinalaisen jäännöslauseen alkuperäinen ongelma oli selvittää armeijan sotilaiden määrä annettujen tietojen perusteella. Ongelmassa on kerrottu kolme ehtoa, joiden avulla voidaan muodostaa kiinalaisen jäännöslauseen yhtälöryhmä. Kiinalaisessa jäännöslauseessa on lineaarinen kongruenssiyhtälöryhmä, joissa kaikissa on sama muuttuja x. [1, s. 163]

Lause 3.0.1 (Kiinalainen jäännöslause)**.** Olkoot $m_1, m_2, m_3, \ldots, m_r$ pareittain jaottomia kokonaislukuja. Silloin kongruenssiyhtälöryhmälle

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ x &\equiv a_3 \pmod{m_3} \\ &\vdots \\ x &\equiv a_r \pmod{m_r} \end{aligned}$$

on olemassa ratkaisu. Ratkaisu saadaan, kun muuttujan x jäännösluokkana, jossa modulo on $M = m_1 m_2 \ldots m_r$.

Todsitus vrt. [1, s. 162]. Merkitään

$$M_k = M/m_k = m_1 m_2 m_3 \ldots m_{k-1} m_{k+1} \ldots m_r.$$

Silloin $\text{syt}(M_k, m_k) = 1$, joten luvulla M_k on aina olemassa käänteisluku y_k modulo m_k. Silloin on voidaan kirjoittaa $M_k y_k \equiv 1 \pmod{m_k}$. Tämän avulla voidaan jokaisella $k = 1, 2, 3, \ldots, r$ kirjoittaa

$$x \equiv a_k \equiv a_k y_k M_k \pmod{m_k}.$$

Arvataan, että ratkaisu on

$$x = a_1M_1y_1 + a_2M_2y_2 + \cdots + a_rM_ry_r$$

ja todistetaan se oikeaksi. Tarkatellaan i. kongrunessiyhtälön toteutumista, missä $i \in \{1, 2, 3, \ldots, r\}$. Koska $m_i \mid M_k$ aina kun $i \neq k$, niin $M_k \equiv 0 \pmod{m_i}$. Saadaan

$$\begin{aligned} x &\equiv a_1M_1y_1 + a_2M_2y_2 + \cdots + a_iM_iy_i + \cdots + a_rM_ry_r \pmod{m_i} \\ &\equiv a_iM_iy_i \pmod{m_i} \\ &\equiv a_i \pmod{m_i}. \end{aligned}$$

Jokaisella modulilla kaikki muut summan termit ovat nollia, paitsi, kun $k = i$. Tällöin $M_iy_i \equiv 1 \pmod{m_i}$, jolloin jäljelle jää ainoastaan $x \equiv a_i \pmod{m_i}$. Oikeaksi todetun ratkaisun x on oltava yksikäsitteinen modulo M. Näytetään, että kaksi eri ratkaisua ovat kongruentteja modulo M. Olkoot kaksi ratkaisua x_0 ja x_1, jolloin jokaiselle kokonaisluvun k arvolla $x_0 \equiv x_1 \equiv a_k \pmod{m_k}$. Toisin sanoen $m_k \mid (x_0 - x_1)$. Koska luvut m_k ovat luvun M pareittain jaottomia tekijöitä, seuraa, että $M \mid (x_0 - x_1)$. Jaollisuuden avulla voidaan kirjoittaa ratkaisut taas kongruenssiksi modulo M, eli $x_0 \equiv x_1 \pmod{M}$. Kongruenteista ratkaisusta saadaan siis yksiselitteinen ratkaisujoukko. □

Kiinalaiselle jäännöslauseelle voidaan käyttää suoraa ratkaisukaavaa, jonka avulla voidaan helpottaa ratkaisun saamista. Ratkaisukaava saadaan todistuksen summalausekkeesta. Ratkaisu x saadaan siis suoraan summalausekkeesta, mutta modulon mukaan ratkaisuja on ääretön määrä. Summasta saadaan myös pienin luku modulolla, ja usein vastaus esitetään silti yhtälömuodossa. Lasketaan esimerkki lineaarisesta kongrunessiyhtälöryhmästä kiinalaisen jäännöslauseen avulla.

Esimerkki 3.0.1. Ratkaistaan yhtälöryhmä

$$\begin{aligned} x &\equiv 1 \pmod{3}, \\ x &\equiv 2 \pmod{5}, \\ x &\equiv 3 \pmod{11} \end{aligned}$$

kiinalaisen jäännöslauseen avulla. Lasketaan ensin modulien tulo $M = 3{\cdot}5{\cdot}11 = 165$. Lasketaan jokaiselle vielä luku $M_k = M/m_k$. Saadaan $M_1 = 165/3 = 55, M_2 = 165/5 = 33$ ja $M_3 = 165/11 = 15$. Ratkaisun saamiseksi tarvitaan vielä käänteisluvut y_k kaikille termeille. Luku y_1 saadaan ratkaisemalla yhtälö $55y_1 \equiv 1 \pmod{3}$.

Yhtälöä voidaan sieventää, sillä $55 \equiv 1 \pmod 3$, muotoon $y_1 \equiv 1 \pmod 3$. Tällöin $y_1 = 1 + 3k$ eli tässä tapauksessa valitaan $y_1 = 1$. Toiselle termille M_2 muodostetaan myös yhtälö $33y_2 \equiv 1 \pmod 5$ ja saadaan ratkaisuksi $y_2 = 2$, sillä $2 \cdot 33 = 66 \equiv 1 \pmod 5$. Kolmanneksi yhtälöksi saadaan $15y_3 \equiv 1 \pmod{11}$ ja ratkaisuksi saadaan $y_3 = 3$.

Nyt voidaan laskea x ratkaisukaavan avulla

$$x = 1 \cdot 55 \cdot 1 + 2 \cdot 33 \cdot 2 + 3 \cdot 15 \cdot 3 = 322.$$

Vastaus on siis $x \equiv 322 \pmod{165}$ eli $x \equiv 157 \pmod{165}$. Pienin mahdollinen positiivinen kokonaislukuratkaisu on siis 157.

Esimerkki 3.0.2. Lasketaan luvun 49^{17} kaksi viimeistä numeroa. Luodaan kaksi lineaarista kongruenssiyhtälöä, jotka ratkaisemalla saadaan luku, joka on pienempi kuin 100. Tällöin modulin tulee olla 100 eli muodostetaan kaksi kongrunessiyhtälöä, joiden modulien tulo on 100. Jotta kiinalaista jäännöslausetta voidaan käyttää, modulien tulee olla pareittain jaottomia.

$$\begin{aligned} x &\equiv 49^{17} \pmod{25}, \\ x &\equiv 49^{17} \pmod 4. \end{aligned}$$

Todetaan vielä, että $\text{syt}(25, 4) = 1$. Selvitetään luvun m_k käänteisluvut moduloilla 25 ja 4. Etsitään sellaiset luvut y_1 ja y_2, että

$$\begin{aligned} 4y_1 &\equiv 1 \pmod{25}, \\ 25y_2 &\equiv 1 \pmod 4. \end{aligned}$$

Modulien tulo $M = 25 \cdot 4 = 100$, $m_1 = 4$ ja $m_2 = 25$. Ratkaistaan käänteisluvut. Ratkaisuksi saadaan $y_1 = 19$ ja $y_2 = 1$, sillä $19 \cdot 4 = 76 \equiv 1 \pmod{25}$ ja $25 \equiv 1 \pmod 4$. Kiinalaisessa jäännöslauseessa halutaan selvittää luku $x = a_1 m_i y_1 + a_2 m_2 y_2$. Luvut a_1 ja a_2 ovat suuria, joten sievennetään niitä. Huomataan, että

$$\begin{aligned} 49^{17} &\equiv (-1)^{17} \equiv -1 \pmod{25} \text{ ja} \\ 49^{17} &\equiv 1^{17} \equiv 1 \pmod 4. \end{aligned}$$

Nyt voidaan laskea luku x. Saadaan

$$x = (-1) \cdot 4 \cdot 19 + 1 \cdot 25 \cdot 1 = -76 + 25 = -51.$$

Lasketaan vielä positiivinen arvo, joka on pienempi kuin 100, koska $x = -51 \equiv$

49 (mod 100), niin luvun 49^{17} kaksi viimeistä numeroa ovat 49.

Jos mudolit eivät ole pareittain jaottomia, yhtälöparilla voi silti olla ratkaisu. Ratkaisu on olemassa, jos $\text{syt}(m_1, m_2) \mid (a_1 - a_2)$. Tällöin löytyy yksiselitteinen ratkiasu modulo $m_1 m_2 / \text{syt}(m_1, m_2)$

Esimerkki 3.0.3. Lasketaan luku x, joka toteuttaa ehdot

$$\begin{aligned} x &\equiv 7 \pmod{200}, \\ x &\equiv 82 \pmod{375}. \end{aligned}$$

Huomataan ensin, että $\text{syt}(200, 375) = 25 \neq 1$, eli emme voi suoraan hyödyntää kiinalaista jäännöslausetta. Tälle yhtälöryhmälle voidaan löytää ratkaisu, sillä $25 \mid 175$. Ratkaistaan tehtävä pilkkomalla kongruenssi samalla tavalla kuin edellisessä esimerkissä:

$$\begin{aligned} x &\equiv 7 \pmod{25}, \\ x &\equiv 7 \pmod{8}, \\ x &\equiv 82 \equiv 1 \pmod{3}, \\ x &\equiv 82 \pmod{125}. \end{aligned}$$

Tästä voidaan huomata, että vielä $\text{syt}(25, 125) \neq 1$. Toinen kongruenssiyhtälö täytyy vielä muuttaa tai poistaa. Huomataan, että 25 ja 125 ovat molemmat luvun 5 monikertoja. Lisäksi molemmista kongrunessiyhtälöistä saadaan sama jakojäännös modulo 5. Tällöin toinen kongruenssiyhtälö voidaan poistaa, sillä suuremmalla modulilla saadaan kaikki myös pienemmän modulin ratkaisut. Kongruenssiyhtälöryhmäksi saadaan:

$$\begin{aligned} x &\equiv 7 \pmod{8} \\ x &\equiv 1 \pmod{3} \\ x &\equiv 82 \pmod{125}. \end{aligned}$$

Lasketaan kiinalaisella jäännöslauseella ratkaisu. Saadaan $M = 8 \cdot 3 \cdot 125 = 3000$, $M_1 = 375, M_2 = 100$ sekä $M_3 = 24$. Tällöin

$$\begin{aligned} x &= a_1 y_1 M_1 + a_2 y_2 M_2 + a_3 y_3 M_3 \\ &= 7 \cdot 375 \cdot 7 + 1 \cdot 1000 \cdot 1 + 82 \cdot 24 \cdot 99 = 18375 + 1000 + 194832 = 214207 \\ &\equiv 1207 \pmod{3000}. \end{aligned}$$

Saatu ratkaisu toimii alkuperäisessä kongruenssiyhtälöryhmässä, eli ratkaisu on oi-

kea. Huomataan myös vielä, että ratkaisu on yksiselitteinen modulo $\frac{m_1 m_2}{\text{syt}(m_1,m_2)}$.

On myös mahdollista, että kongruenssiyhtälöryhmälle ei ole olemassa ollenkaan ratkaisua. Esimerkiksi kongruenssiyhtälöparille

$$\begin{aligned} x &\equiv 2 \pmod 4 \\ x &\equiv 1 \pmod 6 \end{aligned}$$

ei ole olemassa ratkaisua, sillä ensimmäisen yhtälön perusteella, x on parillinen ja toisen yhtälön mukaan x on pariton.

Lause 3.0.2. Ratkaisu on olemassa kongruenssiyhtälöparille

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2}, \end{aligned}$$

kun $\text{syt}(m_1, m_2) \mid (a_1 - a_2)$. Ratkaisu x on yksiselitteinen modulo $m_1 m_2/\text{syt}(m_1, m_2)$.

Todistus vrt. [1, s. 667] . Lauseen 2.2.1 mukaan ensimmäinen yhtälö voidaan kirjoittaa $x = a_1 + km_1$ ja sijoittaa alempaan. Saadaan $a_1 + km_1 \equiv a_2 \pmod{m_2}$. Muokataan tämä muotoon $km_1 \equiv a_2 - a_1 \pmod{m_2}$. Kongruenssin määritelmästä voidaan sanoa, että $km_1 = a_2 - a_1 + tm_2$, eli $km_1 - tm_2 = a_2 - a_1$. Koska $\text{syt}(m_1, m_2) \neq 1$, voidaan se ottaa yhteiseksi tekijäksi. Kertoimelle k löytyy arvo, kun $\text{syt}(m_1, m_2) \mid (a_2 - a_1)$. Kun oletetaan, että löydetään jokin sopiva kertaluku k_0, saadaaan $k = k_0 + m_2 t/\text{syt}(m_1, m_2)$. Sijoitetaan k ja saadaan

$$\begin{aligned} x &= a_1 + km_1 \\ &= a_1 + (k_0 + m_2 t/\text{syt}(m_1, m_2)) \\ &= a_1 + k_0 m_1 + m_1 m_2 t/\text{syt}(m_1, m_2). \end{aligned}$$

Merkitään, että $x_1 = a_1 + k_0 m_1$, jolloin ratkaisu on $x = x_1 + [m_1, m_2]t$, missä $[m_1, m_2] = \frac{m_1 m_2}{\text{syt}(m_1,m_2)}$. Konguenssiyhtälönä ratkaisu on muotoa $x \equiv x_1 \pmod{[m_1, m_2]}$. □

Edellisen esimerkin modulo $3000 = \frac{200 \cdot 375}{25}$, eli ehto toteutuu. Todistuksen avulla voidaan suoraan laskea myös kongruenssiyhtälöryhmien ratkaisuja.

4. SOVELLUKSET

Tietokoneissa käytetään binäärilukuja. Luvut ovat siis pitkiä. Kiinalaisen jäännöslauseen avulla voidaan tietokoneissa kirjoittaa valtavan suuret luvut helpommin käsiteltäviksi ja muistettavaksi [1, s.164]. Kiinalaisella jäännöslauseella voidaan tehokkaasti ilmaista salausjärjestelmä RSA:n salausavain, jossa käytetään paljon suuria lukuja. RSA on käytetyin yleinen salausjärjestelmä. Sen nimi tulee matemaatikoiden Ronald Rivest, Adi Shamir ja Leonard Adleman mukaan. He julkaisivat sen 1977, vaikka todellisuudelssa RSA oli jo keksitty 1973, mutta tietoja uudesta salausjärjestelmästä ei haluttu tuolloin vielä paljastaa. RSA perustuu siihen, että on hyvin työlästä etsiä suuren luvun tekijät, kun se on kahden suuren alkuluvun tulo. RSA:n avulla voidaan salata tietoja, kun toisella osapuolella on jo purkauksen avain. Osa tiedoista on julkisia, minkä avulla haluttu viesti salataan. [1, s. 333]

Artikkelissa [2] esitellään RSA:n käyttöä. RSA:ta käytettäessä ensin valitaan kokonaislukupari (e, n). Näistä valitaan ensin luku n, joka on kahden suuren alkulukujen q ja p tulo. Luvut q ja p pidetään salassa. Luvulle n lasketaan Eulerin funktion $\varphi(n)$ arvo luvun e saamiseksi. Kahden alkuluvun tulon tapauksessa $\varphi(n) = (q-1)(p-1)$. Tämän jälkeen voidaan etsiä luku e. Luku e täytyy valita niin, että $\text{syt}(e, \varphi(n)) = 1$ ja myös $ed \equiv 1 \pmod{\varphi(n)}$. Luku e voidaan saada ratkaistua Diofantoksen yhtälöstä $ed - l\varphi(n) = 1$.

Lukupari (e, n) on julkista tietoa. Haluttu salattava luku w esitetään lukuparin (e, n) avulla. Lasketaan luku $v = w^e \pmod{n}$.

Luku v lähetetään viestin vastaanottajalle, joka tietää luvut p ja q. Hän voi selvittää alkuperäisen luvun w ratkaisemalla kongruenssin, $v^d \equiv w^{ed} = w^{1+\varphi(n)l} \equiv w \pmod{n}$.

Samaan ratkaisuun päästään hyödyntämällä kiinalaista jäännöslausetta pilkomalla modulo n sen tekijöihin ja saadaan yhtälöpari

$$\begin{aligned} w &\equiv v^d \pmod{p} \\ w &\equiv v^d \pmod{q}. \end{aligned}$$

Molemmista yhtälöistä sievennetään v^d modulo p ja modulo q, jolloin saadaan

$$\begin{aligned} w &\equiv w_p \pmod{p} \\ w &\equiv w_q \pmod{q}. \end{aligned}$$

Ratkaistaan tämä yhtälöpari kiinalaisella jäännöslauseella.[2]

Esimerkki 4.0.1. Salataan luku 123 RSA:n avulla. Ensin valitaan kaksi alkulukua, jotka ovat $p = 11$ ja $q = 17$. Seuraavaksi lasketaan luku $n = 11 \cdot 17 = 187$. Lasketaan $\varphi(n) = (p-1)(q-1) = 10 \cdot 16 = 160$. Valitaan sellainen luku e, joka toteuttaa ehdon $\text{syt}(e, \varphi(n)) = 1$. Valitaan kokonaisluvun e arvoksi jokin pieni kokonaisluku, tässä tapauksessa asetetaan $e = 7$. Nyt voidaan laskea luku d Diofantoksen yhtälön $ed - l\varphi(n) = 1$ avulla. Yhtälöksi saadaan $7d - 160l = 1$. Kun kertaluku $l = 1$, saadaan luvun arvoksi $d = 23$. Nyt kaikki tarpeelliset vakiot on selvitetty ja voidaan julkaista julkinen pari $(e, n) = (7, 187)$.

Nyt salataan viesti $w = 123$ laskemalla $v = w^e \pmod{n}$. Nyt

$$v = 123^7 \equiv 187 \equiv -4 \pmod{187}.$$

Luku v lähetetään eteenpäin vastaanottajalle, joka tietää luvut q ja p. Salaus puretaan ratkaisemalla kongrunessiyhtälö $v^d = w^d \equiv w = (-4)^{23} \pmod{187}$. Toisaalta salaus voidaan purkaa kiinalaisen jäännöslauseen avulla ratkaisemalla kongruenssiyhtälöpari $v^d = (-4)^{23} \equiv w^d \equiv w \equiv w_p \pmod{11}$ ja $v^d = (-4)^{23} \equiv w^d \equiv w \equiv w_q \pmod{17}$. Ratkaistaan yhtälöparista haluttu luku w kiinalaisella jäännöslauseella. On siis oltava

$$\begin{aligned} w &\equiv w_p = 2 \pmod{11}, \\ w &\equiv w_q = 4 \pmod{17}. \end{aligned}$$

Lasketaan $w = a_1 y_1 M_1 + a_2 y_2 M_2$, missä $a_1 = 2$ ja $a_2 = 4$. Lasketaan käänteisluvut, kun $M = 11 \cdot 17 = 187, M_1 = 17$ ja $M_2 = 11$. Käänteisluvut ovat

$$\begin{aligned} 17y_1 &\equiv 1 \pmod{11}, \\ 11y_2 &\equiv 1 \pmod{17}, \\ y_1 &= 2, \\ y_2 &= 14. \end{aligned}$$

Lasketaan $w = a_1 y_1 M_1 + a_2 y_2 M_2 = 2 \cdot 2 \cdot 17 + 4 \cdot 14 \cdot 11 = 684$. Pienin positiviinen kokonaisluku w modulo 187 on $w = 684 \equiv 123 \pmod{187}$, mikä on alkuperäinen salattu luku.

Huomataan, että salattavan luvun on oltava pienempi kuin laskettu luku n, sillä lausekkeesta $v^d = w^d \equiv w \pmod{n}$ ei saada tarkasti muita lukuja kuin pienin positiivinen luku modulo n. Tämän takia salattavan luvun w on oltava pienempi kuin luku n. Esimerkiksi, jos salataan luku 1234, eteenpäin lähetettävä luku on $v = 1234^7 \equiv 73 \pmod{187}$. Kun tämän purkaa, saadaan $v^d \equiv w^d \equiv 73^{23} \equiv 112 \pmod{187}$. Vastauksesi saadaan siis luku 112, vaikka lähdettiin luvusta 1234. Luku 1234 kuitenkin on kongruentti luvun 112 kanssa modulo 187.

Todellisuudessa RSA:n laskujen luvut ovat erittäin pitkiä ja käsin laskemisesta tulee erittäin haastavaa. Esimerkiksi tosielämässä voidaan valita toiseksi alkuluvuksi p= 1202752425547874888595622079373451212873338780368207543365389998395517985098879789986914690080913161115334681705083209602216014636634639181247 0987105415233, jossa on 154 numeroa. Näin suurta lukua on vaikea hahmottaa tai tehdä sille mitään laskutoimituksia.

5. YHTEENVETO

Kiinalainen jännöslause yhdistää lukuteorian perusmääritelmiä ja tuloksia sovellukseksi, jota voidaan oikeasti hyödyntää tekniikassa. Tietokoneiden maailmassa laskennallinen tehokkuus on tärkeää. Kiinalaisesta jäännöslauseesta tulee uusia sovelluksia ja artikkeleita jatkuvasti.

Käsitteiden kuten jaollisuus, jakoyhtälö, suurin yhteinen tekijä ja kongrunessimääritelmät ovat tuttuja jo aiemmita kouluasteilta. Niitä koskevat erilaiset lauseet kuitenkin muodostavat haastavia ja monimutkaisia kokonaisuuksia. Tässä tapauksessa kiinalainen jäännöslauseen muodostamiseen tarvitaan kaikkia mainittuja määritelmiä ja useita niistä johdettuja lauseita.

Kiinalainen jäännöslauseella voidaan ratkaista lineaarisia kongrunessiyhtälöitä. Kongruenssiyhtälöryhmiä voidaan ratkaista myös muilla tavoin, mutta kiinalainen jäännöslause on helpoin tapa käsin sekä koneellisesti.

LÄHTEET

[1] Kenneth H. Rosen, Elementary Number Theory & Its Applications, 6th edition, Pearson, 2011.

[2] Anne-Maria Ernvall-Hytönen, Kiinalainen jäännöslause ripauksella kryptografiaa, Matematiikkalehti Solmu 3/2012.