Diofantoksen yhtälöt

Pro gradu -tutkielma
Pasi Juopperi
Matematiikan ja tilastotieteen laitos
Helsingin yliopisto
Syksy 2013

HELSINGIN YLIOPISTO
HELSINGFORS UNIVERSITET
UNIVERSITY OF HELSINKI

Tiedekunta/Osasto Fakultet/Sektion – Faculty Matemaattis- luonnontieteellinen tiedekunta	Laitos/Institution– Department Matemaatiikan ja tilastotieteen laitos	
Tekijä/Författare – Author Pasi Juopperi		
Työn nimi / Arbetets titel – Title Diofantoksen yhtälöt		
Oppiaine /Läroämne – Subject Matematiikka		
Työn laji/Arbetets art – Level Pro gradu -tutkielma	Aika/Datum – Month and year 12/2013	Sivumäärä/ Sidoantal – Number of pages 33

Tiivistelmä/Referat – Abstract

Tämä pro gradu –tutkielma käsittelee Diofantoksen yhtälöitä. Diofantoksen yhtälöt on nimetty kreikkalaisen matemaatikon Diofantoksen mukaan. Diofantos eli 200 -luvulla ja häntä kutsutaan kreikkalaisen algebran isäksi.

Tutkielman tarkoitus on laajentaa ja syventää lukion Lukuteoria ja logiikka -kurssin sisältöjä. Jotta tutkielman asiat voi käsittää, tarvitaan pohjatiedoiksi yllämainitun kurssin tiedot. Tarkoituksena on, että tätä tutkielmaa voi käyttää lisämateriaalina Lukuteoria ja logiikka -kurssilla.

Diofanktoksen yhtälöt ovat kokonaislukukertoimisia kahden tai useamman muuttujan polynomiyhtälöitä. Keskeisiä matemaattisia käsitteitä tässä tutkielmassa ovat luonnolliset luvut ja kokonaisluvut, suurin yhteinen tekijä, pienin yhteinen jaettava, Diofantoksen yhtälö ja kongruenssi. Tutkielmassa käydään läpi joitain määritelmiä ja lauseita, joiden avulla Diofantoksen yhtälöitä voidaan ratkaista. Lauseiden teoriaa ja todistuksia selvennetään esimerkkien avulla. Osat todistuksista on hyvin suoraviivaisia ja osat todistuksista voivat olla lukiolaiselle haastavia, mutta esimerkkien kautta kaikki lauseet ovat helposti ymmärrettävissä. Tutkielmassa käydään aluksi läpi joitain määritelmiä, jotka voivat olla jo tuttuja lukio-opinnoista. Määritelmien jälkeen käydään pulmatehtävän avulla läpi Diofantoksen yhtälöihin liittyvää teoriaa ja lauseita, joiden avulla pulmatehtävä lopulta ratkeaa. Lopuksi tutkielmassa tarkastellaan lineaarisia kongruensseja ja niiden yhteyttä Diofantoksen yhtälöihin.

Avainsanat – Nyckelord – Keywords
Diofantoksen yhtälö

Säilytyspaikka – Förvaringställe – Where deposited

Muita tietoja – Övriga uppgifter – Additional information

Sisältö

Johdanto

Tässä pro gradu -tutkielmassa tullaan käsittelemään Diofantoksen yhtälöitä. Diofantoksen yhtälöt on nimetty kreikkalaisen matemaatikon Diofantoksen mukaan. Diofantos eli 200 -luvulla ja häntä kutsutaan kreikkalaisen algebran isäksi.

Tämän tutkielman tarkoitus on laajentaa ja syventää lukion Lukuteoria ja logiikka -kurssin sisältöjä. Jotta tutkielman asiat voi käsittää, tarvitaan pohjatiedoiksi yllämainitun kurssin tiedot. Tarkoituksena on, että tätä tutkielmaa voi käyttää lisämateriaalina Lukuteoria ja logiikka -kurssilla.

Diofanktoksen yhtälöt ovat kokonaislukukertoimisia kahden tai useamman muuttujan polynomiyhtälöitä. Tutkielmassa käydään läpi joitain määritelmiä ja lauseita, joiden avulla Diofantoksen yhtälöitä voidaan ratkaista. Lauseiden teoriaa ja todistuksia selvennetään esimerkkien avulla. Osat todistuksista on hyvin suoraviivaisia ja osat todistuksista voivat olla lukiolaiselle haastavia, mutta esimerkkien kautta kaikki lauseet ovat helposti ymmärrettävissä. Tutkielmassa käydään aluksi läpi joitain määritelmiä, jotka voivat olla jo tuttuja lukio-opinnoista. Määritelmien jälkeen käydään pulmatehtävän avulla läpi Diofantoksen yhtälöihin liittyvää teoriaa ja lauseita, joiden avulla pulmatehtävä lopulta ratkeaa. Lopuksi tutkielmassa tarkastellaan lineaarisia kongruensseja ja niiden yhteyttä Diofantoksen yhtälöihin.

1 Pohjatietoa

Tavoitteena on, että lukijalle jää selkeä kuva mitä Diofantoksen yhtälöillä tarkoitetaan ja miten niihin liittyviä tehtäviä ratkaistaan. Ennenkuin mennään varsinaisesti Diofantoksen yhtälöiden pariin, niin perehdytään joihinkin algebran perusmääritelmiin, joita tullaan tarvitsemaan myöhemmin, kun käsitellään tarkemmin Diofantoksen yhtälöitä ja niihin liittyvää teoriaa.

1.1 Luonnolliset ja kokonaisluvut

Määritelmä 1.1. Luonnollisiin lukuihin luetaan luvut {1,2,3 ...} . Luonnollisten lukujen joukkoa merkitään kirjaimella $\mathbb{N}$. Joissakin tapauksissa luonnolliset luvut määritellään siten, että mukaan otetaan myös luku 0. Tässä työssä käytetään ensimmäiseksi mainittua määritelmää.

Määritelmä 1.2. Kokonaislukuihin luetaan luvut $\{\ldots -3, -2, -1, 0, 1, 2, 3 \ldots\}$. Kokonaislukujen joukon merkintään käytetään kirjainta $\mathbb{Z}$.

1.2 Suurin yhteinen tekijä

Määritelmä 1.3. Kahden kokonaisluvun a ja b suurin yhteinen tekijä tarkoittaa suurinta kokonaislukua, joka jakaa molemmat luvut a ja b. Luvuista a tai b toisen täytyy olla erisuuri kuin 0. Kokonaislukujen a ja b suurinta yhteistä tekijää merkitään $syt(a, b)$. Jos toinen luvuista on nolla, niin $syt(a, 0) = a$.

Toisinaan voi olla työlästä jakaa kokonaisluvut alkutekijöihin. Tällöin suurimman yhteisen tekijän etsimiseen kannattaa käyttää Eukleiden algoritmia.

Lause 1.4. *Olkoon annettu kaksi kokonaislukua a ja b. Nyt* $syt(a, b)$ *löydetään Eukleideen algoritmin avulla.*

Todistus. Olkoot $a, b \in \mathbb{Z}, a \neq 0, b \neq 0$. Tällöin jakoalgoritmin avulla saadaan

$$\begin{aligned}
a &= q_1 b + r_1, \text{missä } 0 < r_1 < |b| \\
b &= q_2 r_1 + r_2, \text{missä } 0 < r_2 < r_1 \\
r_1 &= q_3 r_2 + r_3, \text{missä } 0 < r_3 < r_2 \\
&\vdots \\
r_{n-2} &= q_n + r_{n-1}, \text{missä } 0 < r_n < r_{n-1} \\
r_{n-1} &= q_{n+1} r_n
\end{aligned}$$

Tämä menettely päättyy, sillä jono $r_1, r_2, \ldots$ on aidosti vähenevä $\mathbb{N}$:ssä ja alhaalta rajoitettu. Havaitaan nyt, että

$$r_n | \; r_{n-1} \Rightarrow r_n | \; r_{n-2} \Rightarrow \ldots \Rightarrow r_n | \; b \Rightarrow r_n | \; a.$$

Eli toisin sanoen r_n jakaa sekä luvun a ja b. Ja edelleen havaitaan, että

$$c | \; a \text{ ja } c | \; b \Rightarrow c | \; r_1 \Rightarrow c | \; r_2 \Rightarrow \ldots \Rightarrow c | \; r_n.$$

Siis r_n on lukujen a ja b suurin yhteinen tekijä. □

Esimerkki 1.5. Etsitään suurin yhteinen tekijä luvuille 382 ja 26:

$$\begin{aligned} 382 &= 14 \cdot 26 + 18, & 0 < 18 < 26, \\ 26 &= 1 \cdot 18 + 8, & 0 < 8 < 18, \\ 18 &= 2 \cdot 8 + 2, & 0 < 2 < 8, \\ 8 &= 4 \cdot 2. \end{aligned}$$

Eli $syt(382, 26) = 2$.

Lause 1.6. *Pienin positiivinen kokonaisluku n, joka on muotoa*

$$n = ax + by,$$

ja missä x ja y ovat kokonaislukuja, on suurin yhteinen tekijä positiivisille kokonaisluvuille a ja b.

Todistus. Tarkastellaan kokonaislukujoukkoa G, jossa luvut ovat muotoa $ax+by$ ja missä x ja y ovat myös kokonaislukuja. Koska

$$a = a \cdot 1 + b \cdot 0$$

ja

$$b = a \cdot 0 + b \cdot 1,$$

niin näemme, että luvut a ja b kuuluvat joukkoon G. Siis joukko G on epätyhjä ja n on pienin positiivinen kokonaisluku tässä joukossa. Nyt määritelmä joukolle G kertoo, että n on muotoa:

$$n = ax + by,$$

joillakin kokonaisluvuilla x ja y. Näin ollen on olemassa positiivinen n millä tahansa positiivisilla kokonaisluvuilla a ja b.

Seuraavaksi meidän täytyy osoittaa, että $syt(a, b) = n$. Voimme merkitä suurinta yhteistä tekijää kirjaimella d ja tiedetään, että

$$a = dr$$

ja

$$b = ds,$$

joillakin kokonaisluvuilla r ja s, koska a ja b ovat luvun d monikertoja. Nyt saadaan, että

$$n = ax + by = drx + dsy = d(rx + sy).$$

Koska d on nyt luvun n positiivinen tekijä, niin $d \leq n$.

Osoitetaan, että n on yhteinen tekijä luvuille a ja b. Voidaan esittää a muodossa

$$a = qn + r, \text{missä } 0 \leq r < n.$$

Nyt, jos $r \neq 0$, niin r kuuluu joukkoon G, koska

$$r = a - qn = a - q(ax + by) = a(1 - qx) + b(-qy).$$

Tämä on kuitenkin mahdotonta, koska n on pienin luku joukossa G. Tästä syystä

$$a = qn$$

ja n on luvun a tekijä. Samalla tavalla kuin edellä osoitetaan, että n on luvun b tekijä:

$$b = q'n + r' \text{ missä } 0 \leq r' < n.$$

Jos $r' \neq 0$, niin

$$r' = b - q'n = b - q'(ax + by) = a(-q'x) + b(1 - q'y)$$

ja r' on joukon G alkio. Koska n on pienin alkio joukossa G, niin tämä on mahdotonta ja luvun r' täytyy olla nolla. Siis

$$b = q'n$$

ja n on siis yhteinen tekijä luvuille a ja b. Tämä tarkoittaa, että

$$n \leq d,$$

koska d on suurin yhteinen tekijä. Epäyhtälöistä

$$d \leq n \text{ ja } n \leq d$$

saadaan, että

$$n = d.$$

□

1.3 Pienin yhteinen jaettava

Ennen murtolukujen yhteen- tai vähennyslaskua täytyy murtoluvut muuttaa samannimisiksi. Yhteinen nimittäjä valitaan usein siten, että se on nimittäjien pienin yhteinen jaettava.

Kahden tai useamman kokonaisluvun pienin yhteinen jaettava on pienin kokonaisluku, joka on jaollinen jokaisella annetuista kokonaisluvuista.

Määritelmä 1.7. Olkoot $a, b \in \mathbb{Z}$ Pienintä positiivista kokonaislukua t, jonka luku a ja luku b jakaa, sanotaan lukujen a ja b pienimmäksi yhteiseksi jaettavaksi. Kokonaislukujen a ja b pienintä yhteistä jaettavaa merkitään $pyj(a, b)$.

Pienin yhteinen jaettava löydetään siten, että luvut jaetaan ensin alkutekijöihin. Jokainen esiintyvä alkutekijä otetaan korotettuna korkeimpaan potenssiin, mikä lukujen alkutekijäesityksistä esiintyy ja näiden tulona saadaan pienin yhteinen jaettava. Selvennetään tätä vielä esimerkillä.

Esimerkki 1.8. Määritetään $pyj(156, 104)$
Jaetaan aluksi luvut alkutekijöihin:

$$156 = 2^2 \cdot 3 \cdot 13$$

$$104 = 2^3 \cdot 13$$

Ja pienin yhteinen jaettava on siis $2^3 \cdot 3 \cdot 13 = 312$, $pyj(156, 104) = 312$.

Lause 1.9. *Olkoot a ja b positiivisia kokonaislukuja, tällöin pätee*

$$syt(a, b) \cdot pyj(a, b) = ab.$$

Todistus. Merkitään, että $syt(a, b) = d$ ja $pyj(a, b) = m$. Nyt meidän täytyy todistaa, että $md = ab$. Todistetaan aluksi, että md jakaa luvun ab. Olkoon

$$n = \frac{ab}{d}.$$

Tämä kokonaisluku voidaan esittää eri tavoilla:

$$n = \frac{a}{d} \cdot b$$

ja

$$n = a \cdot \frac{b}{d}.$$

Luku n on siis luvun a monikerta ja myös luvun b monikerta. Koska n on nyt yhteinen monikerta luvuille a ja b, niin luvun m täytyy jakaa luku n. Siis md jakaa luvun

$$nd = \frac{ab}{d} \cdot d = ab.$$

Osoitetaan seuraavaksi, että ab jakaa luvun md. Lauseen 1.6 nojalla luku d voidaan kirjoittaa muodossa:

$$ax + by = d$$

ja kertomalla molemmat puolet luvulla m saadaan

$$max + mby = md.$$

Koska m on luvun b monikerta, niin max luvun ab monikerta. Samoin m on luvun a monikerta ja mby on monikerta luvulle ab. Siis $max + mby$ on monikerta luvulle ab ja $max + mby = md$ on luvun ab monikerta. Koska md jakaa luvun ab ja ab jakaa luvun md, niin täytyy olla, että $md = ab$. □

2 Lineaarinen Diofantoksen yhtälö

Tässä luvussa käydään läpi lineaaristen Diofantoksen yhtälöihin liittyvää teoriaa. Käydään tämä teoria läpi käyttämällä apuna tyypillistä pulmapähkinää, joka voi esiintyä esimerkiksi aikakausilehdessä.

Pulmapähkinä Maanviljelijä Matti osti markkinnoilta 100 eläintä. Nämä 100 eläintä maksoivat täsmälleen 2000 euroa. Maanviljelijä osti lehmiä, jotka maksoivat 50 euroa kappaleelta. Hän osti myös lampaita ja sikoja. Lampaat maksoivat 20 euroa ja siat maksoivat 5 euroa kappaleelta. Kuinka monta lehmää, lammasta ja sikaa maanviljelijä osti?

Pyritään nyt löytämään tehokas tapa ratkaista tämä pulmapähkinä. Tottakai pähkinän voi ratkaista kokeilemalla eri ratkaisuja ja päätyä siten oikeaan tulokseen, mutta tässä tutkielmassa ratkaisuun käytetään apuna matemaattisia yhtälöitä.

Jos pulmapähkinään on ratkaisu, niin täytyy olla olemassa sellaiset kokonaisluvut x, y ja z, että

$$x + y + z = 100$$

ja

$$50x + 20y + 5z = 2000.$$

Lisäksi x, y ja z täytyvät olla positiivisia kokonaislukuja:

$$x > 0, y > 0, z > 0.$$

On huomioitava, että aina tällaisiin pulmiin ei ole olemassa ratkaisua.

2.1 Kokonaislukuja käsitteleviä lauseita

Ennen seuraava vaihetta pulmapähkinän ratkaisussa, todistetaan kokonaisluvuista kertovia lauseita, joiden avulla voimme myöhemmin muokata yllä olevia yhtälöitä. Jotkin lauseet voivat tuntua lukiolaiselle itsestään selviltä. Näillä lauseilla ja varsinkin niiden todistuksilla on tärkeä merkitys, jotta opitaan oikea matemaattinen esitystapa. On myös tärkeää että lauseet osataan todistaa, mikäli jotain lausetta käytetään.

Lause 2.1. *Olkoot a ja b luonnollisia lukuja siten, että $a > b$. Tällöin jokaiselle luvulle $n \in \mathbb{N}$ pätee ehdot:*

$$(1)\ a + n > b + n,$$

$$(2)\ a \cdot n > b \cdot n.$$

Todistus. Merkintä $a > b$ tarkoittaa määritelmän mukaan, että $a = b + c$, jossa c on jokin luonnollinen luku. Siten

$$a + n = (b + c) + n = b + (c + n) = b + (n + c) = (b + n) + c,$$

eli

$$a + n > b + n$$

kaikilla $n \in \mathbb{N}$.

Vastaavalla tavalla yhtälö

$$a \cdot n = (b + c) \cdot n = (b \cdot n) + (c \cdot n)$$

tarkottaa, että

$$a \cdot n > b \cdot n.$$

□

Tämän lauseen avulla voimme todistaa seuraavan lauseen, jota käytämme myöhemmin esimerkin ratkaisussa.

Lause 2.2. *Olkoot a, b ja c luonnollisia lukuja siten, että*

$$a \cdot c = b \cdot c,$$

tällöin $a = b$.

Todistus. Käytetään tässä todistuksessa vastaväitettä, joka todistetaan mahdottomaksi. Tällaista todistusta kutsutaan epäsuoraksi todistukseksi. Käytetään todistuksessa myös apuna aiemmin todistettua lausetta 2.1.

Vastaväite: $a > b$ tai $b > a$.

Nyt vastaväite voidaan kirjoittaa aiemman lauseen 2.1 perusteella muotoon:

$$a \cdot c > b \cdot c$$

tai

$$b \cdot c > a \cdot c.$$

Tästä seuraa ristiriita alkuperäisen oletuksen $a \cdot c = b \cdot c$ kanssa. Siis alkuperäinen väite $a = b$ on totta. □

Lause 2.3. *(1) Jos a, b ja k ovat kokonaislukuja, $k \neq 0$, niin $a = b$, jos ja vain jos $ka = kb$.*
(2) Jos a, b, c, d, k ja h ovat kokonaislukuja, $k \neq 0$, niin tällöin $a = b$ ja $c = d$, jos ja vain jos $a = b$ ja $ha + kc = hb + kd$.

Todistus. Lauseen ensimmäinen osa seuraa lauseesta 2.2. Lauseen toinen osa seuraa ensimmäisestä osasta ja siitä, että vähennyslasku on määritelty. Jos

$$a = b \text{ ja } c = d,$$

niin

$$a = b \text{ ja } ha + kc = hb + kd$$

Toisaalta, jos

$$a = b \text{ ja } ha + kc = hb + kd,$$

niin

$$ha = hb,$$
$$(ha + kc) - ha = (hb + kd) - hb,$$
$$kc = kd,$$

ja edelleen

$$c = d.$$

□

Lauseen 2.3 avulla voidaan muokata pulmapähkinän yhtälöä ja jatkaa sen ratkaisua. Eli pulmapähkinän yhtälö

$$50x + 20y + 5z = 2000$$

voidaan nyt aiemman teorian perusteella korvata yhtälöllä

$$10x + 4y + z = 400.$$

Eli pystyimme jakamaan yhtälön jokaisen osan viidellä ilman, että tämä vaikutti mahdollisiin arvoihin x, y ja z. Samalla tavalla voidaan korvata yhtälöt

$$x + y + z = 100 \text{ ja } 10x + 4y + z = 400$$

yhtälöillä

$$x + y + z = 100 \text{ ja } 9x + 3y = 300.$$

Viimeisin yhtälö saadaan, koska

$$9x + 3y = (10x + 4y + z) + (-1) \cdot (x + y + z) = 400 - 100.$$

Edelleen saadaan, että yhtälö

$$9x + 3y = 300$$

on nyt

$$3x + y = 100.$$

Tämä muoto yhtälöstä on yksinkertaisempi, kuin aiempi muoto minkä se korvasi. Olemme saaneet tuntemattoman tekijän z nyt eliminoitua. Suurimman yhteisen tekijän teorian, lause 1.6, ja Eukleideen algoritmin avulla voidaan ilmaista kokonaislukujen a ja b suurinta yhteistä tekijää seuraavassa muodossa:

$$syt(a, b) = am + bn,$$

joillakin kokonaisluvuilla m ja n. Koska $syt(3, 1) = 1$, niin on olemassa kokonaisluvut m ja n siten,että

$$1 = 3m + n.$$

Nyt voidaan käyttää Eukleideen algoritmia löytääksemme kokonaisluvut m ja n. Kertomalla sadalla saadaan, että

$$3 \cdot 100m + 100n = 100$$

ja tällöin sellaiset kokonaisluvut x ja y, jotka toteuttavat yhtälön

$$3x + y = 100$$

voidaan saada ratkaistua lukujen m ja n avulla.

Tällä tavalla löydetään kuitenkin vain lukuja jotka ovat sadan kerrannaisia, eikä niistä ole tässä tapauksessa hyötyä. Emme siis voi käyttää lukuja m ja n lukujen x ja y etsimiseen.

2.2 Lineaarinen Diofantoksen yhtälö: määritelmä ja lauseita

Pulmapähkinän ratkaisussa on nyt päästy hyvälle alulle. Pulman ongelma pystyttiin kirjoittamaan matemaattisina kaavoina, joita saatiin edelleen muokattua yksinkertaisempaan muotoon. Annetaan seuraavaksi matemaattinen määritelmä Diofantoksen yhtälölle ja todistetaan siihen liittyvät kaksi lausetta, joiden avulla päästään eteenpäin pulmapähkinän tehokkaassa ratkaisussa.

Määritelmä 2.4. Olkoot a, b, c, x ja y kokonaislukuja. Yhtälöä joka on muodossa

$$ax + by = c$$

kutsutaan lineaariseksi Diofantoksen yhtälöksi.

Lause 2.5. *On olemassa kokonaisluvut x ja y siten, että*

$$ax + by = c,$$

jos ja vain jos $d = syt(a, b)$ on luvun c tekijä. Tässä a, b ja c ovat nollasta poikkeavia kokonaislukuja.

Todistus. Suurimman yhteisen tekijän määritelmän ja Eukleideen algoritmin avulla nähdään, että tunnetuille kokonaisluvuille a, b ja c voi olla olemassa kokonaisluvut x ja y vain, jos $syt(a, b)$ on luvun c tekijä:

Olkoon kokonaisluku d lukujen a ja b suurin yhteinen tekijä. Tällöin

$$a = da_1 \text{ ja } b = db_1.$$

Nyt, jos kokonaisluvut x ja y ovat olemassa, niin

$$c = d(a_1x + b_1y)$$

ja d on tekijä luvulle c.

Olkoon nyt $d = syt(a, b)$ tekijä luvulle c, eli $c = dc_1$. Suurimman yhteisen tekijän teorian ja lauseen 1.6 avulla tiedetään, että on olemassa kokonaisluvut m ja n siten, että

$$d = am + bn,$$

ja nyt

$$c = dc_1 = a \cdot mc_1 + b \cdot nc_1.$$

Tämä todistaa lauseen. □

Huom! Ratkaisut x ja y ovat mitä tahansa kokonaislukuja, ei välttämättä pelkästään positiivisia tai nollasta poikkeavia kokonaislukuja.

Esimerkki 2.6. Lineaarisiin Diofantoksen yhtälöihin voi olla monia eri ratkaisuja:

$$\begin{aligned} 4 \cdot 3 + 2 \cdot (-5) &= 2 \\ 4 \cdot 6 + 2 \cdot (-11) &= 2 \\ 4 \cdot (-2) + 2 \cdot 5 &= 2. \end{aligned}$$

Lause 2.7. *Olkoot x ja y kokonaislukuja siten, että*

$$ax_1 + by_1 = c,$$

missä a, b ja c ovat nollasta poikkeavia kokonaislukuja ja

$$syt(a, b) = 1.$$

Tällöin

$$x = x_1 + qb \text{ ja } y = y_1 - qa$$

toteuttavat yhtälön

$$ax + by = c$$

kaikilla kokonaisluvuilla q. Toisaalta, jos x_2 ja y_2 ovat kokonaislukuja siten, että

$$ax_2 + by_2 = c$$

niin silloin on olemassa sellainen kokonaisluku q, että

$$x_2 = x_1 + bq \text{ ja } y_2 = y_1 - aq.$$

Todistus. Ensimmäinen väite saadaan suoraan sijoittamalla:

$$\begin{aligned} ax + by &= a(x_1 + bq) + b(y_1 - aq) \\ &= ax_1 + by_1 + abq - abq \\ &= ax_1 + by_1 \\ &= c. \end{aligned}$$

Toisen osan todistuksessa tarkastellaan yhtälöitä

$$ax_1 + by_1 = c$$

ja

$$ax_2 + by_2 = c.$$

Tästä saadaan transitiivisuus-ominaisuuden avulla, että

$$ax_1 + by_1 = ax_2 + by_2$$

ja edelleen

$$b(y_1 - y_2) = a(x_2 - x_1).$$

Koska oletuksen mukaan $syt(a, b) = 1$, niin nyt voidaan nähdä, että b on tulon $a(x_2 - x_1)$ tekijä. Tästä seuraa, että b on erotuksen $x_2 - x_1$ tekijä, joten

$$x_2 - x_1 = bq,$$

jollakin kokonaisluvulla q. Edelleen saadaan, että

$$x_2 = x_1 + bq.$$

Nyt sijoittamalla $x_2 - x_1 = bq$ yhtälöön $b(y_1 - y_2) = a(x_2 - x_1)$ saadaan, että

$$b(y_1 - y_2) = a(bq).$$

Koska oletuksen mukaan $b \neq 0$, niin ylempi yhtälö voidaan jakaa puolittain luvulla b ja tällöin saadaan, että

$$y_1 - y_2 = aq$$

ja edelleen

$$y_2 = y_1 - aq.$$

□

Nyt meillä on riittävästi työkaluja, jotta voimme palata pulmapähkinän ratkaisemiseen. Aiemmin saimme selvitettyä, että yhtälölle

$$3x + y = 100$$

löydetään ratkaisu yhtälön

$$3 \cdot 100m + 100n = 100$$

avulla.

Annetaan arvot $m = 0$ ja $n = 1$, niin saadaan yhtälölle yksi ratkaisu. Käytetään nyt apuna lausetta 2.7 ja voidaan todeta, että kaikki ratkaisut saadaan yhtälöistä:

$$x = 0 + (1)q, \quad y = 100 - 3q,$$

missä q on mielivaltainen kokonaisluku. Sijoitetaan nyt x ja y yhtälöön

$$x + y + z = 100$$

ja saadaan, että

$$q + (100 - 3q) + z = 100$$

$$z = 2q$$

Pulmapähkinän ehdot olivat, että

$$x > 0, y > 0, z > 0$$

Näiden avulla saadaan ehdot kokonaisluvulle q:

$$q > 0, \quad 100 - 3q > 0, \quad 2q > 0$$

Tarkastelemalla näitä ehtoja nähdään, että q on kokonaisluku, joka saa arvoja välillä 0 ja 34, eli pulmapähkinälle on yhteensä 33 eri ratkaisua. Eri ratkaisut saadaan, kun sijoitetaan arvot $q = 1, q = 2, \ldots, q = 33$ yhtälöihin

$$x = q,$$

$$y = 100 - 3q,$$

$$z = 2q,$$

missä x kertoo ostettujen lehmien lukumäärän, y kertoo lampaiden lukumäärän ja z kertoo sikojen lukumäärän.

Esimerkki 2.8. Etsitään sellaiset positiiviset kokonaisluvut x ja y, että

$$208x + 136y = 120.$$

Lauseen 2.3 avulla saadaan, että

$$26x + 17y = 15,$$

koska $syt(208, 136, 120) = 8$. Nyt voidaan käyttää Eukleideen algoritmia ja saadaan, että

$$26 = 1 \cdot 17 + 9,$$

$$17 = 2 \cdot 9 - 1.$$

Kuljetaan seuraavaksi Eukleideen algoritmia lopusta alkuun päin ja saadaan, että

$$1 = 2 \cdot 9 - 17 = 2(26 - 17) - 17 = 2 \cdot 26 + (-3) \cdot 17.$$

Saatiin, että $syt(26, 17) = 1$ ja yhtälöllä $26x + 17y = 15$ on siis ratkaisu. Pari

$$x_1 = 15 \cdot 2 = 30 \quad \text{ja} \quad y_1 = 15 \cdot (-3) = -45$$

antaa yhden ratkaisun yhtälölle $26x + 17y = 15$. Yleinen ratkaisu löydetään tarkastelemalla paria:

$$x = 30 + 17q \quad \text{ja} \quad y = -45 - 26q,$$

missä q on kokonaisluku. Alussa annettiin ehdoksi löytää positiiviset kokonaisluvut eli

$$30 + 17q > 0 \quad \text{ja} \quad -45 - 26q > 0.$$

Tästä seuraa, että q on kokonaisluku, joka on pienempi kuin -1 ja suurempi kuin -2 eli yhtälöllä $208x + 136y = 120$ ei ole ratkaisua positiivisilla kokonaisluvuilla.

3 Lisää lineaarisia Diofantoksen yhtälöitä

Edellä käsiteltiin lineaarisia Diofantoksen yhtälöitä, joissa oli kaksi tuntematonta muuttujaa. Nyt lineaarinen Diofantoksen yhtälö n kappaleella muuttujia: $x_1, x_2, \ldots, x_n$ on muotoa

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = c,$$

missä c ja a_i ovat nollasta poikkeavia kokonaislukuja.

Lause 3.1. *On olemassa sellaiset kokonaisluvut* $x_1, x_2, \ldots, x_n$, *että*

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = c, \quad n > 1,$$

jos ja vain jos $syt(a_1, a_2, \ldots, a_n)$ *on luvun* c *tekijä. Luvut* c *ja* a_i *ovat nollasta poikkeavia kokonaislukuja*

Todistus. Ensimmäinen osa saadaan samalla lailla kuten lausessa 2.5 todistettiin. Täytyy olla, että $syt(a_1, a_2, \ldots, a_n)$ on luvun c tekijä, jos kokonaisluvut x_i ovat olemassa. Oletetaan nyt, että

$$c = dc_1,$$

missä $d = syt(a_1, a_2, \ldots, a_n)$.

Suurimman yhteisen tekijän teoriasta saadaan, että on olemassa sellaiset kokonaisluvut $b_1, b_2, \ldots, b_n$, että

$$d = a_1b_1 + a_2b_2 + \cdots + a_nb_n.$$

Siis

$$c = c_1d = a_1(c_1b_1) + a_2(c_1b_2) + \cdots + a_n(c_1b_n),$$

ja tällä yhtälöllä on kokonaislukuratkaisu. □

Esimerkki 3.2. Etsitään sellaiset kokonaisluvut x, y ja z, joilla

$$50x + 45y + 36z = 10.$$

Ensimmäiseksi nähdään, että

$$syt(50, 45) = 5,$$

ja

$$50 \cdot 1 + 45 \cdot (-1) = 5.$$

Seuraavaksi tutkitaan lukuja 5 ja 36:

$$syt(5, 36) = 1$$

ja tästä saadaan, että

$$syt(50, 45, 36) = syt(5, 35) = 1.$$

Ja tästä seuraa aiemman lauseen perusteella, että yhtälöllä on kokonaislukuratkaisu.

Nyt

$$1 = 36 \cdot 1 + 5 \cdot (-7)$$

ja sijoittamalla saadaan, että

$$1 = 36 \cdot 1 + (-7) \cdot 50 + 7 \cdot 45$$

Edelleen, kun kerrotaan kymmenellä saadaan, että

$$50 \cdot (-70) + 45 \cdot 70 + 36 \cdot 10 = 10.$$

Yksi ratkaisu yhtälölle saatiin luvuilla $x_1 = -70, y_1 = 70$ ja $z_1 = 10$.

On selvää, että saatu ratkaisu ei ole ainoa mahdollinen ratkaisu. Haluamme tietysti löytää yhtälölle kaikki ratkaisut, eikä vain yhtä. Jotta voimme löytää muutkin ratkaisut, niin tarvitsemme avuksi seuraavan tuloksen.

Lause 3.3. *Jos b ja c ovat nollasta poikkeavia kokonaislukuja, niin tällöin voidaan löytää sellaiset kokonaisluvut h, k, r ja s, että*

$$hs - kr = 1 \quad ja \quad bk + cs = 0$$

Todistus. Oletetaan, että b ja c ovat positiivisia. Pienimmän yhteisen jaettavan teorian perusteella saadaan, että

$$syt(b, c) \cdot pyj(b, c) = bc.$$

Koska $pyj(b, c)$ on luvun b kerrannainen, niin

$$pyj(b, c) = bk, \text{ jollakin } k$$

ja valitsemalla

$$s = -b/syt(b, c)$$

saadaan, että

$$bk+cs = bk+c(-b/syt(b, c)) = bk-bc/syt(b, c) = bk-pyj(b, c) = bk-bk = 0.$$

Edelleen tästä saadaan, että

$$k = bc/(b \cdot syt(b, c)) = c/syt(b, c)$$

ja näin ollen $syt(k, s) = 1$. Suurimman yhteisen tekijän teorian ja lauseen 1.6 mukaan on olemassa kokonaisluvut h ja r siten, että

$$hs + (-k)r = 1.$$

Vaaditut kokonaisluvut ovat siis olemassa. Voimme löytää luvut h ja r käyttämällä apuna Eukleideen algoritmia. □

Esimerkki 3.4. Jos $b = 12$ ja $c = 20$, niin nähdään, että $k = 20/syt(12, 20) = 20/4 = 5$ ja $s = -12/syt(12, 20) = -12/4 = -3$. Tarkistetaan vielä, että $bk + cs = 0$

$$12 \cdot 5 + 20 \cdot (-3) = 0.$$

Nyt $syt(5, -3) = 1$ ja havaitaan, että

$$1 = (-1) \cdot 5 + (-2) \cdot (-3).$$

Voidaan valita luvut $h = -2$ ja $r = 1$ ja tällöin saadaan, että

$$hs - kr = 1.$$

Käytetään tätä tulosta apuna seuraavan lauseen todistamisessa.

Lause 3.5. *Olkoot a, b, c ja d nollasta poikkeavia kokonaislukuja ja h, k, r ja s kokonaislukuja siten, että $hs - kr = 1$ ja $bk + cs = 0$. Tällöin, jos x, y ja z ovat kokonaislukuja ja*

$$ax + by + cz = d,$$

niin kokonaisluvut $x, t = sy - kz$ ja $u = hz - ry$ toteuttavat yhtälön

$$ax + (bh + cr)t + (bk + cs)u = d.$$

Toisaalta, jos x, t ja u ovat kokonaislukuja, jotka toteuttavat viimeisimmän yhtälön, niin tällöin luvut $x, y = ht + ku$ ja $z = rt + su$ toteuttavat yhtälön

$$ax + by + cz = d$$

Todistus. Selvästi, koska $bk + cs = 0$, niin kolmen tuntemattoman yhtälö

$$ax + by + cz = d$$

muuttuu kahden tuntemattoman yhtälöksi

$$ax + (bh + cr)t = d.$$

Tämä voidaan todistaa suoraan muokkaamalla yhtälöä.

$$\begin{aligned} &ax + (bh + cr)(sy - kz) + (bk + cs)(hz - ry) \\ &= ax + by(hs - kr) + cz(hs - kr) + cy(rs - rs) + bz(hk - hk) \\ &= ax + by + cz = d. \end{aligned}$$

Vastakkaiselle oletukselle saadaan, että

$$ax + b(ht + ku) + c(rt + su) = ax + (bh + cr)t + (bk + cs)u = d.$$

Nyt jos löydetään kaikki ratkaisut tuntemattomilla x ja t yhtälölle

$$ax + (bh + cr)t = d,$$

niin mielivaltaisella kokonaisluvulla u yhtälön

$$ax + by + cz = d$$

ratkaisut saadaan kolmikosta

$$x = x, \quad y = ht + ku, \quad z = rt + su.$$

□

Esimerkki 3.6. Jatketaan nyt esimerkin 3.2 ratkaisua. Jotta voidaan ratkaista yhtälö

$$50x + 45y + 36z = 10$$

kokonaisuudessaan, niin täytyy löytää kokonaisluvut h, k, r ja s. Nämä luvut saadaan lauseen 3.3 avulla. Koska

$$syt(45, 36) = 9,$$

niin $k = 36/9 = 4$ ja $s = -45/9 = -5$. Nyt voidaan valita, että $h = -1$ ja $r = 1$. Tällöin pätee, että

$$hs - kr = (-1) \cdot (-5) - 4 \cdot (-1) = 1$$

ja

$$bk + cs = 45 \cdot 4 + 36 \cdot (-5) = 180 - 180 = 0.$$

Nyt lauseen 3.5 avulla yhtälö $50x + 45y + 36z = 10$ saadaan muotoon

$$50x - 9t = 10$$

ja tälle yleinen ratkaisu saadaan yhtälöistä

$$x = 2 + 9q \quad \text{ja} \quad t = 10 + 50q.$$

Näissä yhtälöissä q on mielivaltainen kokonaisluku. Alkuperäisen yhtälön ratkaisut saadaan seuraavista yhtälöistä:

$$x = 2 + 9q,$$

$$y = -10 - 50q + 4u,$$

$$z = 10 + 50q - 5u,$$

missä parametrit q ja u ovat mielivaltaiset kokonaislukumuuttujat.

3.1 Neljän muuttujan Dionfantoksen yhtälö

Diofantoksen yhtälö, jossa on neljä muuttujaa, on muotoa

$$ax + by + cz + dw = e.$$

Tällainen yhtälö voidaan supistaa kolmen tuntemattoman yhtälöksi käyttämällä apuna lausetta 3.3 ja lausetta 3.5 luvuille c ja d. Voimme vähentää yhtälöstä tuntemattomien määrää yhdellä ottamalla käyttöön parametrit. Neljän tuntemattoman muuttujan yhtälölle tarvitsee tehdä kaksi supistusta ja yleinen ratkaisu voidaan esittää kolmen parametrin avulla. Käydään tämä läpi vielä esimerkin avulla.

Esimerkki 3.7. Ratkaistaan Diofantoksen yhtälö

$$2x + 3y + 12z + 20w = 9.$$

Käytetään nyt apuna aiemmin ratkaistun esimerkin 3.4 tuloksia. Tuloksista nähdään, että $-2, 5, 1$ ja -3 ovat kokonaislukuja, siten että

$$12 \cdot 5 + 20 \cdot (-3) = 0$$

ja

$$-2 \cdot (-3) - 1 \cdot 5 = 0.$$

Eli kokonaisluvut $-2, 5, 1$ ja -3 vastaavat muuttujia h, k, r ja s ja siten saadaan eliminoitua $(12z + 20w)$ yhtälöstä. Nyt uusi yhtälö on muotoa

$$2x + 3y + (12 \cdot (-2) + 20 \cdot 1)t = 9$$

Eliminoidut tuntemattomat muuttujat saadaan yhtälöistä

$$z = -2t + 5u$$

ja

$$w = t - 3u,$$

joissa u on mielivaltainen kokonaisluku.

Seuraavaksi tehdään sama käsittely juuri saadulle yhtälölle

$$2x + 3y - 4t = 9.$$

Tällä kertaa eliminoidaan tekijät y ja t. Luvuille $b = 3$ ja $c = -4$ valitaan luvut $k = 3$ ja $s = 4$ ja siten voidaan valita luvut $h = 1$ ja $r = 1$. Näillä luvuilla saadaan uudeksi yhtälöksi

$$2x + (3 - 4)v = 9$$

ja eliminoidut tuntemattomat tekijät saadaan yhtälöistä

$$y = v + 3f,$$

$$t = v + 4f,$$

joissa f on mielivaltainen kokonaisluku.

Yhtälön

$$2x - v = 9$$

yleinen ratkaisu saadaan luvuista $x = 4 + q$ ja $v = -1 + 2q$, joissa q on mielivaltainen kokonaisluku. Selvitetään sitten myös muiden tuntemattomien tekijöiden parametrimuodot. Sijoitetaan $x = 4 + q$ ja $v = -1 + 2q$ yhtälöihin $y = v + 3f$ ja $t = v + 4f$. Nyt saadaan, että

$$y = (-1 + 2q) + 3f,$$

$$t = (-1 + 2q) + 4f.$$

Edelleen sijoitetaan edellä saadut yhtälöihin $z = -2t + 5u$ ja $w = t - 3u$ ja saadaan, että

$$z = -2((-1 + 2q) + 4f) + 5u,$$

$$w = ((-1 + 2q) + 4f) - 3u.$$

Mielivaltaisilla kokonaisluvuilla u, q ja f saadaan esitettyä yleinen ratkaisu alkuperäiselle yhtälölle $2x + 3y + 12z + 20w = 9$:

$$x = 4 + q$$

$$y = -1 + 2q + 3f$$

$$z = 2 - 4q - 8f + 5u$$

$$w = -1 + 2q + 4f - 3u.$$

Jos $u = q = f = 0$, niin saadaan yksittäinen ratkaisu $x = 4, y = -1, z = 2, w = -1$.

4 Lineaariset kongruenssit

4.1 Määritelmä ja yhteys Diofantoksen yhtälöön

Kongruensseja voidaan käyttää apuna ratkaistaessa Diofantoksen yhtälöitä. Kertauksena määritellään aluksi mitä kongruenssi tarkoittaa. Tämän lisäksi määritellään lineearinen kongruenssi ja tutkitaan miten se liittyy lineaarisiin Diofantoksen yhtälöihin.

Määritelmä 4.1. Jos a, b ja m ovat kokonaislukuja ja $m > 0$, niin tällöin a ja b ovat kongruentteja modulo m, jos ja vain jos erotus $a - b$ on jaollinen luvulla m. Merkitään tällöin

$$a \equiv b \bmod m.$$

Aiemmin esimerkissä 2.8 ratkaistiin kokonaisluvut x ja y, jotka toteuttivat yhtälön

$$208x - 136y = 120.$$

Ratkaisut saatiin parista $x = 30 + 17q$ ja $y = -45 - 26q$, joissa q on mielivaltainen kokonaisluku. Kongruenssin avulla ilmaistuna tämä tarkoittaa, että millä tahansa kokonaisluvulla $x = 30 + 17q$ on ominaisuus

$$208x \equiv 120 \bmod 136.$$

Ja toisaalta, jos on olemassa kokonaisluku x siten, että

$$208x \equiv 120 \bmod 136,$$

niin tällöin täytyy olla, että x on muotoa $x = 30 + 17q$. Tämä kongruenssi on yhtäpitävää yhtälön

$$208x - 120 = 136k$$

kanssa, missä k on kokonaisluku. Nyt x ja $-k$ antavat ratkaisun yhtälölle

$$208x + 136y = 120.$$

Määritelmä 4.2. Kongruenssia, joka on muotoa

$$ax \equiv c \bmod b$$

ja missä a, b ja c ovat positiivisia kokonaislukuja, kutsutaan lineaariseksi kongruenssiksi.

Ongelmana on löytää kaikki kokonaisluvut x siten, että

$$208x \equiv 120 \bmod 136.$$

Tämä ongelma on kuitenkin sama kuin, että löydettäisiin kokonaisluvut x ja y siten, että

$$208x + 136y = 120.$$

Lineaarisella Diofantoksen yhtälöllä ja lineaarisella kongruenssilla näyttäisi olevan selkeä yhteys. Todistetaan tämä seuraavassa lauseessa.

Lause 4.3. *Kokonaisluku x toteuttaa lineaarisen kongruenssin*

$$ax \equiv c \ mod \ b$$

jos ja vain jos on olemassa kokonaisluku y siten, että

$$ax + by = c.$$

Todistus. Olkoon ensin $ax \equiv c \bmod b$. Tällöin määritelmän mukaan kokonaisluku $ax - c$ on luvun b monikerta. Eli

$$ax - c = kb.$$

Valitaan, että $y = -k$ ja siten

$$ax + by = c.$$

Todistus toiseen suuntaan saadaan käymällä edelliset vaiheet käänteisessä järjestyksessä. □

Lineaaristen kongruenssien ja lineaaristen Diofantoksen yhtälöiden välinen vastavuus auttaa meitä selvittämään milloin lineaarisella kongruenssilla on ratkaisu.

4.2 Lauseita ja esimerkkejä

Lause 4.4. *Lineaarisella kongruenssilla*

$$ax \equiv c \ mod \ b$$

on ratkaisu, jos ja vain jos $d = syt(a, b)$ on tekijä luvulle c. Mikäli kongruenssilla on ratkaisu, niin ratkaisuja mod b on d kappaletta.

Todistus. Lineaarisella kongruenssilla $ax \equiv c \bmod b$ on ratkaisu, jos ja vain jos Diofantoksen yhtälöllä

$$ax + by = c$$

on ratkaisu. Nyt Diofantoksen yhtälöllä on ratkaisu, jos ja vain jos $d = syt(a, b)$ on luvun c tekijä ja tämä todistaa ensimmäisen osan lauseesta.

Lauseen 2.7 mukaan Diofantoksen yhtälön $ax + by = c$ yleinen ratkaisu on muotoa

$$x = x_0 + bq,$$

$$y = y_0 - aq,$$

missä x_0 ja y_0 ovat ratkaisu Diofantoksen yhtälölle ja q on mielivaltainen kokonaisluku. Koska lauseen 2.7 ehdoissa on, että $d = syt(a, b) = 1$ niin voidaan kirjoittaa yleinen ratkaisu muodossa:

$$x = x_0 + (b/d)q,$$

$$y = y_0 - (a/d)q.$$

On selvästi olemassa d kokonaislukua, jotka ovat

$$x_0, x_0 + b/d, x_0 + 2b/d, \ldots, x_0 + (d-1)b/d,$$

ja sijaitsevat eri ekvivalenssiluokissa modulo b. Mitkä tahansa kaksi lukua erottuvat listassa nollasta poikkeavalla kokonaisluvulla, joka on lukujen $-b$ ja b välissä:

$$(x_0 + mb/d) - (x_0 + nb/d) = (m - n)b/d,$$

missä $m - n \neq 0$ ja $-d < m - n < d$. Nyt, jos oletetaan, että kokonaisluku t on kongruentti jonkin luvun $x_0 + mb/d, 0 \leq m < d$ kanssa, niin tällöin t on ratkaisu kongruenssille. Tämä seuraa siitä, että

$$at = a(x_0 + mb/d - kb) = a(x_0 + mb/d) - kab$$

mikä tarkoittaa, että

$$at \equiv a(x_0 + mb/d) \bmod b.$$

Koska kongruenssi on transitiivinen niin saadaan, että

$$at \equiv c \bmod b.$$

Nyt jokainen kokonaisluku d luokissa modulo b

$$x_0, x_0 + b/d, x_0 + 2b/d, \ldots, x_0 + (d-1)b/d,$$

on ratkaisu kongruenssille

$$at \equiv c \bmod b.$$

Toisaalta, koska yhtälöt

$$x = x_0 + (b/d)q,$$

ja

$$y = y_0 - (a/d)q,$$

joissa q on mielivaltainen kokonaisluku, antavat kaikki ratkaisut yhtälölle $ax + by = c$, niin voidaan nähdä että jokainen kongruenssin $ax \equiv c \bmod b$ ratkaisu on muotoa

$$x = x_0 + (b/d)q.$$

Kokonaisluvun $x = x_0 + (b/d)q$ täytyy kuulua johonkin edellä mainittuihin ekvivalenssiluokkiin, joita oli d kappaletta. □

Esimerkki 4.5. Ratkaise kongruenssi $9x \equiv 12 \bmod 21$.

Koska $syt(9, 21) = 3$ ja se on myös luvun 12 tekijä, tiedämme että kongruenssilla on olemassa ratkaisu. Tutkitaan aluksi erotusta $9x - 12$ ja millä kokonaisluvuilla x tämä $9x - 12$ on luvun 12 monikerta. On helppoa löytää kokeilemalla eri ratkaisuja, esimerkiksi

$$9 \cdot (-1) - 12 = 21,$$

$$9 \cdot 6 - 12 = 42,$$

$$9 \cdot 13 - 12 = 105,$$

mutta on työlästä löytää kaikki ratkaisut, joten käytetään apuna edellä käytyä teoriaa. Mikä tahansa kokonaisluku, joka on muotoa

$$x = (-1) + ((21)/3)q$$

on ratkaisu.Tarkastellaan seuraavaksi lukuja:

q:	0	1	2	3	-1	-2	-3	6	$\cdots$
x:	-1	6	13	20	-8	-15	-22	41	$\cdots$

Nämä luvut voidaan jaotella kolmeen luokkaan modulo 21:

$$
\begin{aligned}
[-1] &= -1, 20, -22, 41, \cdots \\
[6] &= 6, -15, \cdots \\
[13] &= 13, 8, \cdots
\end{aligned}
$$

Mikäli kokonaisluvut a, b ja c ovat suuria lukuja, niin voidaan käyttää Eukleideen algoritmia apuna, jotta löydetään d ja jokin ratkaisu x_0.

Esimerkki 4.6. Ratkaise lineaarinen kongruenssi $657x \equiv 18 \bmod 963$.

Käytetään nyt Eukleideen algoritmia:

$$
\begin{aligned}
963 &= 657 \cdot 1 + 306 \\
657 &= 306 \cdot 2 + 45 \\
306 &= 45 \cdot 6 + 36 \\
45 &= 36 \cdot 1 + 9 \\
36 &= 9 \cdot 4
\end{aligned}
$$

Edellä saatiin, että $syt(963, 657) = 9$, joka on tekijä luvulle 18. Nyt siis tiedämme, että kongruenssilla on olemassa ratkaisu ja ratkaisut muodostuvat yhdeksästä ekvivalenssiluokasta modulo 963. Yllä olevasta Eukleideen algoritmista saadaan, että

$$9 = 22 \cdot 657 + (-15) \cdot 963.$$

Tästä saadaan edelleen, että

$$657 \cdot 44 \equiv 18 \bmod 963$$

eli $x = 44$ on yksi ratkaisu kongruenssille. Kaikki ratkaisut kongruenssille ovat seuraavien 9 luokan elementit:

$$[44], [44 + 107], [44 + 214], \ldots, [44 + 856].$$

Nämä luokat saatiin, koska $b/d = 963/9 = 107$.

Diofantoksen yhtälöistä saatuja tuloksia voidaan käyttää myös kahden lineaarisen kongruenssin ratkaisemiseen. Meidän täytyy siis löytää sellainen kokonaisluku x, että kongruenssit

$$ax \equiv b \bmod m$$

ja

$$cx \equiv nz \bmod n$$

pitävät paikkansa ja lauseen 4.3 mukaan tämä on yhtäpitävää sen kanssa, että etsimme kokonaisluvut x, y ja z siten, että

$$ax + my = b$$

ja

$$cx + nz = d.$$

Eli meidän täytyy ratkaista pari lineaarisia Diofantoksen yhtälöitä samanaikaisesti. Todistetaan seuraavaksi lause, joka on erityistapaus yllä olevasta.

Lause 4.7. *Olkoot a, b, m ja n positiivisia kokonaislukuja. Tällöin on olemassa sellainen kokonaisluku x siten, että*

$$x \equiv a \ mod \ m$$

ja

$$x \equiv b \ mod \ n,$$

jos ja vain jos

$$x \equiv b \ mod \ syt(m, n).$$

Mikäli x ja y toteuttavat kongruenssit, niin tällöin

$$x \equiv y \ mod \ pyj(m, n).$$

Todistus. On selvästi olemassa kokonaisluku x siten, että

$$x \equiv a \bmod m$$

ja

$$x \equiv b \bmod n,$$

jos ja vain jos on olemassa kokonaisluvut r ja s siten, että

$$x = a + rm$$

ja

$$x = b + sn.$$

Yhdistetään nyt yllä olevat kaksi yhtälöä ja saadaan, että

$$a + rm = b + sn$$

ja edelleen, että

$$rm - sn = b - a.$$

Lauseen 2.5 avulla tiedetään, että kokonaisluvut r ja s ovat olemassa, jos ja vain jos $syt(m, n)$ on tekijä luvulle $(b - a)$ eli

$$b \equiv a \bmod syt(m, n).$$

Koska kokonaisluvut r ja s määrittävät luvun x, on ensimmäinen osa lauseesta totta.

Todistetaan seuraavaksi lauseen toinen osa. Jos $x \equiv a \bmod m$ ja $y \equiv a \bmod m$, niin joillakin kokonaisluvuilla h ja k

$$x = a + km \text{ ja } y = a + hm.$$

Tästä saadaan, että

$$x - y = a + km - (a + hm) = (k - h)m,$$

tai toisin sanoen

$$x \equiv y \bmod m.$$

Jos $x \equiv b \bmod n$ ja $y \equiv b \bmod n$, niin vastaavasti kuin edellä saadaan, että

$$x \equiv y \bmod n.$$

Selvästi $x - y$ on $pyj(m, n)$ monikerta, jos se on monikerta luvuille m ja n. Tämä seuraa siitä, että $pyj(m, n)$ on tekijä kaikille lukujen m ja n monikerroille. Lopuksi voidaan todeta, että

$$x \equiv y \bmod pyj(m, n),$$

jos $x \equiv a \bmod m$, $x \equiv b \bmod n$, $y \equiv a \bmod m$ ja $y \equiv b \bmod n$. □

Lauseen 4.7 ensimmäisen osan todistuksesta nähdään, että luvun x arvot voidaan selvittää lukujen r ja s arvojen avulla ja nämä arvot saadaan ratkaisemalla lineaarinen Diofantoksen yhtälö. Käydään seuraavaksi läpi esimerkki, joka selkeyttää lauseen 4.7 käyttöä.

Esimerkki 4.8. Etsi sellainen kokonaisluku x, että

$$x \equiv 5 \bmod 12 \text{ ja } x \equiv 4 \bmod 17.$$

Kokonaisluku x on olemassa, koska

$$5 \equiv 4 \bmod syt(12, 17),$$

$$5 \equiv 4 \bmod 1.$$

Nyt täytyy siis löytää kokonaisluvut r ja s, jotka toteuttavat yhtälön

$$x = 5 + 12r = 4 + 17s.$$

Voimme siis ratkaista yhtälön $12r - 17s = 1$. Tämä voidaan ratkaista Eukleideen algoritmillä tai kokeilemalla eri ratkaisuja. Kokeilemalla löydetään, että

$$12 \cdot 7 - 17 \cdot 5 = -1,$$

eli $r = 7$ ja $s = 5$. Tästä saadaan, että

$$x = 5 + 12 \cdot 7 = 4 + 17 \cdot 5 = 89,$$

mikä on yksi ratkaisu kongruensseille.

4.3 Kiinalainen jäännöslause

Määritelmä 4.9. Kokonaislukuja $a_1, a_2, \ldots, a_n$ sanotaan keskenään jaottomiksi tai suhteellisiksi alkuluvuiksi, jos niiden suurin yhteinen tekijä on 1.

Lause 4.10. *(Kiinalainen jäännöslause) Jos n kappaletta positiivisia kokonaislukuja $m_1, m_2, \ldots, m_n$ ovat suhteellisia alkulukuja, niin tällöin joukolla kongruensseja*

$$x \equiv a_1 \ mod \ m_1, \ldots, x \equiv a_n \ mod \ m_n,$$

on olemassa ratkaisu x'. Alkiot jäännösluokassa $[x']$ modulo $m_1 m_2 \ldots m_n$ ovat yllä olevan kongruenssijoukon ratkaisut.

Todistus. Todistetaan Kiinalainen jäännöslause induktiolla. Jos $n = 1$, niin väite on triviaalisti tosi, sillä kongruenssilla

$$x \equiv a_1 \bmod m_1$$

on olemassa ratkaisut ja ne ovat luvut luokassa $[a_1] \bmod m_1$. Kun $n = 2$, niin väite on lauseen 4.7 mukaan tosi. Oletetaan nyt, että väite on tosi positiivisilla kokonaisluvuilla lukuun k saakka. Tarkastellaan seuraavasti joukkoa, jossa kongruensseja on $k + 1$ kappaletta eli

$$x \equiv a_1 \bmod m_1, \ldots, x \equiv a_k \bmod m_k, x \equiv a_{k+1} \bmod m_{k+1},$$

missä $syt(m_i, m_j) = 1, i \neq j$. Induktio-oletuksen mukaan joukolla k kongruensseja

$$x \equiv a_2 \bmod m_2, \ldots, x \equiv a_{k+1} \bmod m_{k+1}$$

on olemassa ratkaisu r. Elementit luokassa $[r]$ modulo m, missä $m = m_2 m_3 \cdots m_{k+1}$, ovat ratkaisut joukolle k kongruensseja.

Tarkastellaan seuraavaksi paria kongruensseja

$$x \equiv r \bmod m \text{ ja } x \equiv a_1 \bmod m_1.$$

Nyt nähdään, että kokonaisluvut m ja m_1 ovat suhteellisia alkulukuja, koska luvun m alkutekijä on välttämättä tekijä yhdelle luvuista $m_2, \cdots, m_{k+1}$. Siis $syt(m, m_1) = 1$. Lauseen 4.7 mukaan tällä parilla kongruensseja on olemassa ratkaisu x' ja kaikki ratkaisut ovat luvut jäännösluokassa $[x']$ modulo mm_1. Tällöin x' on ratkaisu $k+1$ kongruenssille

$$x \equiv a_1 \bmod m_1, \ldots, x \equiv a_{k+1} \bmod m_{k+1}$$

ja on helppo nähdä, että joukko ratkaisuja näille $k+1$ kappaleelle kongruensseja on tarkalleen luokka $[x']$ modulo $m_1 m_2 \cdots m_{k+1}$. Ratkaisu näille $k+1$ kongruensseille on myös ratkaisu k kongruenseille

$$x \equiv a_2 \bmod m_2, \ldots, x \equiv a_{k+1} \bmod m_{k+1}$$

ja ratkaisu myös kongruenssille

$$x \equiv a_1 \bmod m_1.$$

Ja näin induktion nojalla lause on tosi. □

Kiinalaisen jäännöslauseen avulla voidaan ratkaista systemaattisesti tietyntyyppisiä pulmatehtäviä ja aivopähkinöitä. Ratkaistaan seuraavaksi esimerkkinä eräs pulmatehtävä Kiinalaisen jäännöslauseen avulla.

Esimerkki 4.11. Kolmentoista merirosvon joukkio sai haltuunsa aarrearkun, jossa on x kultakolikkoa. Kun kolikot jaettiin tasan kaikkien merirosvojen kanssa, jäljelle jäi 8 kolikkoa. Kaksi merirosvoa kuoli ja tasaisen jaon jälkeen kolikkoja jäi jakamatta 3 kappaletta. Kolikot jaettiin vielä kerran, kun kolme merirosvoa lisää oli kuollut ja jäljelle jäi 5 kolikkoa. Mikä on pienin määrä kolikkoja, jolla jaot voidaan tehdä?

Pulma voidaan esittää kongruenssien avulla. Toisin sanoen meidän täytyy löytää ratkaisu joukolle kongruensseja:

$$x \equiv 8 \bmod 13, x \equiv 3 \bmod 11, x \equiv 5 \bmod 8.$$

Koska $syt(13, 11) = syt(13, 8) = syt(11, 8) = 1$, niin Kiinalaisen jäännöslauseen avulla tiedetään, että tällä joukolla on täsmälleen yksi ratkaisu välillä 0 ja 8(11)(13). Ratkaistaan aluksi kongruenssipari

$$x \equiv 8 \bmod 13, x \equiv 3 \bmod 11.$$

Meidän täytyy siis löytää kokonaisluvut r ja s siten, että

$$x = 8 + 13r = 3 + 11s,$$

tai

$$11s - 13r = 5.$$

Koska

$$11 \cdot 6 - 13 \cdot 5 = 1,$$

niin voimme valita, että

$$s = 30 \text{ ja } r = 25.$$

Tällöin

$$8 + 13 \cdot 25 = 3 + 11 \cdot 30 = 333$$

on yksi ratkaisu kongruenssiparille. Jäännösluokat $[333] = [47]$ modulo 143 antavat kaikki ratkaisut kongruenssiparille.

Tarkastellaan seuraavaksi kongruenssiparia

$$x \equiv 47 \bmod 143, x \equiv 5 \bmod 8.$$

Tämän ratkaisua varten tarvitsee löytää kokonaisluvut u ja v siten, että

$$x = 47 + 143u = 5 + 8v$$

eli

$$143u - 8v = -42$$

Koska

$$143 \cdot 7 - 8 \cdot 125 = 1,$$

voimme valita, että

$$u = 7 \cdot (-42) \text{ ja } v = 125 \cdot (-42).$$

Tällöin saadaan, että

$$47 + 143 \cdot 7 \cdot (-42) = 5 + 8 \cdot 125 \cdot (-42) = -41995$$

on ratkaisu tälle kongruenssiparille. Koska kaikki tämän kongruenssiparin ja alkuperäisten kolmen kongruenssin ratkaisut kuuluvat jäännösluokkaan $[-41995]$ modulo 1144 ja koska 333 on pienin positiivinen kokonaisluku kyseisessä luokassa,

$$-41995 = -37 \cdot 1144 + 333,$$

niin 333 on tämän pulmatehtävän ratkaisu.

Lähdeluettelo

[1] W. E. Deskins: *Abstract algebra*. The Macmillan Company, New York, 1964.

[2] L. J. Mordell: *Diophantine Equations*. Academic Press, London, 1969.

[3] P. Jäppinen, A. Kupiainen, M. Räsänen: *Lukion Calculus 6, Lukuteoria ja logiikka*. Otava, Helsinki, 2005.