TAMPEREEN YLIOPISTO
Pro gradu -tutkielma

Harri Lehtinen

# Kongruenssista

Matematiikan, tilastotieteen ja filosofian laitos
Matematiikka
Helmikuu 2006

Tampereen yliopisto
Matematiikan, tilastotieteen ja filosofian laitos
LEHTINEN, HARRI: Kongruenssista
Pro gradu –tutkielma, 44 s.
Matematiikka
Helmikuu 2006

---

# Tiivistelmä

Tässä tutkielmassa perehdytään kongruensseihin ja niiden ominaisuuksiin. Luvussa yksi käydään läpi lukuteorian perusteita, joita tarvitaan myöhemmin. Esitetään kokonaislukujen jaollisuuteen liittyviä lauseita ja jakoalgoritmi, määritellään alkuluvut, kokonaislukujen suurin yhteinen tekijä ja pienin yhteinen monikerta. Esitetään Eukleideen algoritmi, jonka avulla voidaan löytää kahden kokonaisluvun suurin yhteinen tekijä. Luvun yksi lopussa esitetään ratkaisutapa lineaariselle Diofantoksen yhtälölle. Luvussa 2 käydään läpi kongruenssin perusominaisuuksia. Määritellään lineaarinen kongruenssiyhtälö ja esitetään ratkaisutapa lineaaristen kongruenssiyhtälöiden ryhmille. Esitetään ratkaisutapa myös polynomien kongruensseille. Luvun 2 lopussa käsitellään matriisien kongruensseja. Luvussa 3 esitetään ja todistetaan Wilsonin lause, Fermat´n pieni lause ja Eulerin lause. Tutkielman rakenne noudattelee pääosin Kenneth H. Rosenin teosta Elementary Number Theory and Its Applications, joka on ollut myös tärkein lähdeteos.

# Sisältö

## Johdanto

Tässä tutkielmassa perehdytään kongruensseihin ja niiden ominaisuuksiin. Luvussa 1 käydään läpi lukuteorian perusteita, joita tarvitaan myöhemmin. Pykälässä 1.1 esitetään kokonaislukujen jaollisuuteen liittyviä lauseita ja jakoalgoritmi, sekä määritellään alkuluvut. Pykälässä 1.2 määritellään kokonaislukujen suurin yhteinen tekijä ja pienin yhteinen monikerta, sekä esitetään Eukleideen algoritmi, jonka avulla voidaan löytää kahden kokonaisluvun suurin yhteinen tekijä. Pykälässä 1.3 määritellään lineaarinen Diofantoksen yhtälö ja esitetään sille ratkaisutapa. Luvussa 1 monet todistuksista on sivuutettu, koska niiden oletetaan olevan lukijalle tuttuja ja helppoja ratkaista.

Luvussa 2 siirrytään pääaiheeseen eli käydään läpi kongruenssiin liittyviä ominaisuuksia.. Pykälässä 2.1 esitetään kongruenssin perusominaisuuksia. Pykälässä 2.2 määritellään lineaarinen kongruenssiyhtälö ja esitetään sille ratkaisutapa. Lisäksi määritellään käänteisluvut. Pykälässä 2.3 esitetään kiinalainen jäännöslause, jonka avulla voidaan ratkaista lineaaristen kongruenssiyhtälöiden ryhmiä. Pykälässä 2.4 tarkastellaan polynomien kongruensseja ja esitetään niille ratkaisutapa. Pykälässä 2.5 käsitellään useamman muuttujan lineaarisia kongruenssiyhtälöiden ryhmiä ja esitetään niille ratkaisutapa. Pykälässä 2.6 perehdytään matriisien kongruensseihin ja niiden ominaisuuksiin.

Luvussa 3 esitetään ja todistetaan Wilsonin lause, Fermat´n pieni lause ja Eulerin lause. Pykälässä 3.1 todistetaan Wilsonin lause. Pykälässä 3.2 todistetaan Fermat´n pieni lause ja etsitään sen avulla jakojäännös. Pykälässä 3.3 todistetaan Eulerin lause, joka on Fermat´n pienen lauseen yleistys. Sitä voidaan käyttää käänteislukujen etsimiseen.

Tutkielman rakenne noudattelee pääosin Kenneth H. Rosenin teosta Elementary Number Theory and Its Applications, joka on ollut myös tärkein lähdeteos. Lukijalta odotetaan perustietoja lineaarialgebrasta.

# LUKU 1 Lukuteorian perusteita

## *1.1 Jaollisuus, jakoalgoritmi ja alkuluvut*

**Määritelmä 1.1 (Hyvinjärjestysominaisuus)** Jokaisessa positiivisten kokonaislukujen epätyhjässä joukossa on pienin alkio.

**Määritelmä 1.2** Olkoot $a$ ja $b$ kokonaislukuja ja olkoon $a \neq 0$. Jos on olemassa sellainen kokonaisluku $c$, että $b = ac$, niin luku $a$ *jakaa* luvun $b$. Jos luku $a$ jakaa luvun $b$, niin sanotaan, että luku $a$ on luvun $b$ *jakaja* tai *tekijä* ja että luku $b$ on luvun $a$ *monikerta*. Jos luku $a$ jakaa luvun $b$, niin merkitään $a \mid b$, ja jos luku $a$ ei jaa lukua $b$, merkitään $a \nmid b$.

**Lause 1.1** *Olkoot a, b ja c kokonaislukuja. Jos* $a \mid b$ *ja* $b \mid c$*, niin tällöin* $a \mid c$.

*Todistus.* Vrt. [2], s. 31. Koska $a \mid b$ ja $b \mid c$, niin on olemassa sellaiset kokonaisluvut $e$ ja $f$, että $ae = b$ ja $bf = c$. Nyt $c = bf = (ae)f = a(ef)$, jolloin määritelmän 1.2 mukaan $a \mid c$.

□

**Lause 1.2** *Olkoot a, b, c, m ja n kokonaislukuja. Jos* $c \mid a$ *ja* $c \mid b$*, niin* $c \mid (ma + nb)$.

*Todistus.* Vrt. [2], s. 32. Koska $c \mid a$ ja $c \mid b$, niin on olemassa sellaiset kokonaisluvut $e$ ja $f$, että $a = ce$ ja $b = cf$. Nyt $ma + nb = mce + ncf = c(me + nf)$, jolloin määritelmän 1.2 mukaan $c \mid (ma + nb)$.

□

**Lause 1.3 Jakoalgoritmi** *Jos a ja b ovat kokonaislukuja ja* $b > 0$*, niin on olemassa sellaiset yksikäsitteiset kokonaisluvut q ja r, että* $a = bq + r$*, missä* $0 \leq r < b$.

*Todistus.* Vrt. [2], s. 32. Olkoon joukko S = $\{a - bk \mid a, b, k \in \mathbf{Z}\}$. Olkoon joukko T kaikkien niiden joukkoon S kuuluvien kokonaislukujen joukko, jotka eivät ole negatiivisia. Joukko T ei ole tyhjä joukko, koska $a - bk$ on positiivinen aina, kun $k < a/b$. Hyvinjärjestysominaisuuden mukaan joukossa T on olemassa pienin alkio $r$. Siis $r = a - bq$ jollakin tietyllä luvulla $q \in \mathbf{Z}$. Koska $r \in$ T, niin $r \geq 0$. Jos $r \geq b$, niin $r > r - b = a - bq - b = a - b(q + 1) \geq 0$. Siis $r > a - b(q + 1) \in$ T. Tämä on ristiriidassa sen kanssa, että $r$ on joukon T pienin alkio. Siis $0 \leq r < b$. Todistetaan vielä, että luvut $q$ ja $r$ ovat yksikäsitteiset. Oletetaan, että $a = bq_1 + r_1$ ja $a = bq_2 + r_2$, missä $0 \leq r_1 < b$ ja $0 \leq r_2 < b$. Vähentämällä ensimmäisestä yhtälöstä toinen yhtälö saadaan $0 = b(q_1 - q_2) + (r_1 - r_2)$ ja edelleen $r_2 - r_1 = b(q_1 - q_2)$. Siis luku $b$ jakaa erotuksen $r_2 - r_1$. Koska $0 \leq r_1 < b$ ja $0 \leq r_2 < b$, niin $-b < r_2 - r_1 < b$. Luku $b$ voi olla jakajana ainoastaan, jos $r_2 - r_1 = 0$ eli jos $r_2 = r_1$. Koska $bq_1 + r_1 = bq_2 + r_2$ ja $r_1 = r_2$, niin $q_1 = q_2$. Siis luvut $q$ ja $r$ ovat yksikäsitteiset.

□

**Esimerkki 1.1** Olkoon $a = 146$ ja $b = 33$. Tällöin $q = 4$ ja $r = 14$, koska $146 = 33 \cdot 4 + 14$.

**Määritelmä 1.3** Olkoon $p$ lukua 1 suurempi kokonaisluku. Jos luku $p$ on jaollinen ainoastaan itsellään ja luvulla 1, niin tällöin lukua $p$ kutsutaan *alkuluvuksi*.

**Määritelmä 1.4** Olkoon $p$ lukua 1 suurempi kokonaisluku. Jos luku $p$ ei ole alkuluku, niin se on *yhdistetty luku*.

**Esimerkki 1.2** Luvut 2, 3, 5, 7, 11 ja 13 ovat alkulukuja ja luvut $4 = 2 \cdot 2$, $6 = 2 \cdot 3$, $8 = 2 \cdot 4$, $9 = 3 \cdot 3$, $10 = 2 \cdot 5$ ja $12 = 2 \cdot 6 = 3 \cdot 4$ ovat yhdistettyjä lukuja.

### *1.2 Suurin yhteinen tekijä, pienin yhteinen monikerta ja Eukleideen algoritmi*

**Määritelmä 1.5** Olkoot *a* ja *b* kokonaislukuja ja olkoon joko $a \neq 0$ tai $b \neq 0$. Lukujen *a* ja *b suurin yhteinen tekijä* on suurin kokonaisluku *c*, joka jakaa sekä luvun *a*, että luvun *b* ts.

(*i*) $c \mid a$ ja $c \mid b$

(*ii*) jos *d* on kokonaisluku, $d \mid a$ ja $d \mid b$, niin $d \leq c$.

Tällöin merkitään $(a, b) = c$. Lisäksi määritellään $(0, 0) = 0$.

**Esimerkki 1.3** Lukujen 12 ja 56 yhteisiä tekijöitä ovat $\pm 1$, $\pm 2$, $\pm 4$, $\pm 6$, jolloin $(12, 56) = 6$

**Määritelmä 1.6** Olkoot *a* ja *b* kokonaislukuja. Jos $(a, b) = 1$, niin luvut *a* ja *b* ovat *keskenään jaottomia*. Tällöin niitä kutsutaan myös *suhteellisiksi alkuluvuiksi*.

**Esimerkki 1.4** Koska $(15, 62) = 1$, niin luvut 15 ja 62 ovat keskenään jaottomia ja siis suhteellisia alkulukuja.

**Lause 1.4** *Olkoot a ja b kokonaislukuja. Jos* $(a, b) = d$, *niin* $(a/d\ ,\ b/d) = 1$.

*Todistus.* Ks. [2], s.80.

**Esimerkki 1.5** Tarkastellaan lukuja 8 ja 12. Nyt $(8, 12) = 4$, jolloin $(8/4, 12/4) = (2, 3) = 1$.

**Lause 1.5** *Olkoot a, b ja c kokonaislukuja. Tällöin* $(a + cb, b) = (a, b)$.

*Todistus.* Ks. [2], s.81.

**Huomautus 1.1** Ks. [2], s.81. Kirjassa lauseen 1.5 todistuksessa on viittaus kirjan lauseeseen 1.5. Viittaus pitäisi olla kirjan lauseeseen 1.6.

**Esimerkki 1.6** Tarkastellaan lukuja 8, 12 ja 6. Nyt $(8 + 6 \cdot 12, 12) = (80, 12) = 4 = (8, 12)$.

**Määritelmä 1.7** Olkoot *a* ja *b* kokonaislukuja. Tällöin summaa $ma + nb$, missä *m* ja *n* ovat kokonaislukuja, kutsutaan lukujen *a* ja *b lineaarikombinaatioksi*.

**Lause 1.6** *Olkoot a ja b kokonaislukuja ja olkoon joko* $a \neq 0$ *tai* $b \neq 0$. *Tällöin on olemassa sellaiset kokonaisluvut x ja y, että*

$$(a, b) = ax + by.$$

*Todistus*. Ks. [1], s.22.

**Lause 1.7** *Olkoot a ja b kokonaislukuja ja olkoon joko* $a \neq 0$ *tai* $b \neq 0$. *Luvut a ja b ovat suhteellisia alkulukuja, jos ja vain jos on olemassa sellaiset kokonaisluvut x ja y, että*

$$1 = ax + by.$$

*Todistus*. Ks. [1], s.23.

**Esimerkki 1.7** Mitä ovat lineaarikombinaatiot $8m + 12n$, missä *m* ja *n* ovat kokonaislukuja? Niitä ovat mm. $\mathbf{-8} = 8 \cdot (-1) + 12 \cdot 0$; $\mathbf{-4} = 8 \cdot 1 + 12 \cdot (-1)$; $\mathbf{0} = 8 \cdot (-3) + 12 \cdot 2$; $\mathbf{4} = 8 \cdot 2 + 12 \cdot (-1)$; $\mathbf{8} = 8 \cdot 1 + 12 \cdot 0$; $\mathbf{12} = 8 \cdot 0 + 12 \cdot 1$ jne. Voidaan osoittaa, että lukujen 8 ja 12 kaikkien lineaarikombinaatioiden joukko on $\{\dots, -12, -8, -4, 0, 4, 8, 12, \dots\}$. Tämä selviää kahdesta seuraavasta lauseesta.

**Lause 1.8** *Olkoot a ja b kokonaislukuja ja olkoon joko* $a \neq 0$ *tai* $b \neq 0$. *Tällöin lukujen a ja b suurin yhteinen tekijä on pienin positiivinen kokonaisluku, joka on lukujen a ja b lineaarikombinaatio.*

*Todistus*. Ks. [2], s.81.

**Huomautus 1.2** Ks. [2], s.81. Kirjassa lauseen 1.8 todistuksessa on viittaus kirjan lauseeseen 1.5. Viittaus pitäisi olla kirjan lauseeseen 1.6.

**Lause 1.9** *Olkoot a ja b positiivisia kokonaislukuja. Tällöin lukujen a ja b lineaarikombinaatioiden joukko on lukujen a ja b suurimman yhteisen tekijän monikertojen muodostama joukko.*

*Todistus.* Ks. [2], s.82.

**Määritelmä 1.8** Olkoot $a_1, a_2, \ldots, a_n$ kokonaislukuja, joista ainakin yksi $a_k \neq 0$, missä $1 \leq k \leq n$. Kokonaislukujen $a_1, a_2, \ldots, a_n$ *suurin yhteinen tekijä* $(a_1, a_2, \ldots, a_n)$ on suurin kokonaisluku, joka jakaa kaikki luvut $a_1, a_2, \ldots, a_n$.

**Esimerkki 1.8** Nähdään, että (6, 15, 21) = 3 ja (−7, 28, −35) = 7.

Seuraavaa apulausetta voidaan käyttää etsittäessä useamman kuin kahden kokonaisluvun suurinta yhteistä tekijää.

**Apulause 1.1** *Olkoot* $a_1, a_2, \ldots, a_n$ *kokonaislukuja, joista ainakin yksi* $a_k \neq 0$, *missä* $1 \leq k \leq n$. *Tällöin* $(a_1, a_2, \ldots, a_{n-1}, a_n) = (a_1, a_2, \ldots, a_{n-2}, (a_{n-1}, a_n))$.

*Todistus.* Ks. [2], s.83.

**Esimerkki 1.9** Etsitään kokonaislukujen 24, 64, 288 suurin yhteinen tekijä käyttämällä apulausetta 1.1, jolloin (24, 64, 288) = (24, (64, 288)) = (24, 32) = 8.

**Esimerkki 1.10** Tarkastellaan lukuja 10, 18 ja 45. Nähdään, että näiden kokonaislukujen suurin yhteinen tekijä on 1, koska (10, 18, 45) = (10, (18, 45)) = (10, 9) = 1. Kuitenkin näistä kolmesta luvusta muodostetuilla pareilla suurin yhteinen tekijä on suurempi kuin 1, sillä (10, 18) = 2, (10, 45 ) = 5 ja (18, 45) = 9.

Esimerkki 1.10 johtaa seuraavaan määritelmään.

**Määritelmä 1.9** Kokonaisluvut $a_1$, $a_2$,…, $a_n$ ovat *keskenään suhteellisia alkulukuja*, jos $(a_1, a_2, \ldots, a_n) = 1$. Joukon $a_1$, $a_2$,…, $a_n$ luvut ovat *pareittain suhteellisia alkulukuja*, jos kaikilla luvuilla $a_i$ ja $a_j$ on voimassa $(a_i, a_j) = 1$, missä $1 \leq i \leq n$, $1 \leq j \leq n$ ja $i \neq j$.

**Määritelmä 1.10** Olkoot $a$ ja $b$ kokonaislukuja. Lukujen $a$ ja $b$ *pienin yhteinen monikerta* on pienin positiivinen kokonaisluku $c$, joka on jaollinen sekä luvulla $a$, että luvulla $b$ ts.

($i$) $a \mid c$, $b \mid c$ ja

($ii$) jos $d$ on positiivinen kokonaisluku, $a \mid d$ ja $b \mid d$, niin $c \leq d$.

Tällöin merkitään $[a, b] = c$.

**Esimerkki 1.11** Lukujen 4 ja 6 pienin yhteinen monikerta on 12 eli $[4, 6] = 12$.

**Apulause 1.2** *Olkoot a, b ja c positiivisia kokonaislukuja. Jos* $(a, b) = 1$ *ja* $a \mid bc$, *niin* $a \mid c$.

*Todistus.* Vrt. [2], s.97. Koska $(a, b) = 1$, niin lauseen 1.7 perusteella on olemassa sellaiset kokonaisluvut $x$ ja $y$, että $ax + by = 1$. Kerrotaan yhtälön molemmat puolet luvulla $c$, jolloin $acx + bcy = c$. Koska $a \mid a$ ja $a \mid bc$, niin lauseen 1.2 perusteella $a \mid acx + bcy$ ja siis $a \mid c$.

□

**Esimerkki 1.12** Tarkastellaan lukuja 3, 7 ja 504. Selvästi $(3, 7) = 1$. Koska $504 = 168 \cdot 3$, niin $3 \mid 504$. Koska $504 = 7 \cdot 72$, niin apulauseen 1.2 perusteella $3 \mid 72$.

**Apulause 1.3** *Olkoot e, d, q* ja *r kokonaislukuja. Jos* $e = dq + r$, *niin* $(e, d) = (d, r)$.

*Todistus.* Vrt. [2], s.87. Olkoon $a = r$, $b = d$ ja $c = q$. Nyt $(e, d) = (dq + r, d) = (bc + a, b)$, jolloin lauseen 1.5 perusteella $(bc + a, b) = (a, b) = (r, d)$. Siis $(e, d) = (d, r)$.

□

**Lause 1.10 Eukleideen algoritmi** *Olkoon* $r_0 = a$ *ja* $r_1 = b$, *missä* $a \geq b > 0$. *Jos toistetaan lauseen* 1.3 *jakoalgoritmia, niin* $r_j = r_{j+1} q_{j+1} + r_{j+2}$, *missä* $0 \leq r_{j+2} < r_{j+1}$ *ja* $j = 0, 1, 2, \ldots, n-2$. *Jos* $r_{n+1} = 0$, *niin viimeinen nollasta poikkeava jakojäännös* $r_n = (a, b)$.

*Todistus.* Vrt. [2], s.87. Todistetaan, että Eukleideen algoritmi tuottaa kahden kokonaisluvun suurimman yhteisen tekijän. Olkoon $r_0 = a$ ja $r_1 = b$, missä $a \geq b > 0$. Toistamalla jakoalgoritmia saadaan yhtälöryhmä

$$\begin{aligned}
r_0 &= r_1 q_1 + r_2 && 0 \leq r_2 < r_1 \\
r_1 &= r_2 q_2 + r_3 && 0 \leq r_3 < r_2 \\
&\vdots \\
r_j &= r_{j+1} q_{j+1} + r_{j+2} && 0 \leq r_{j+2} < r_{j+1} \\
&\vdots \\
r_{n-2} &= r_{n-1} q_{n-1} + r_n && 0 \leq r_n < r_{n-1} \\
r_{n-1} &= r_n q_n .
\end{aligned}$$

Koska $a = r_0 \geq r_1 > r_2 > \cdots \geq 0$ ja koska jakojäännökset ovat kokonaislukuja, niin jakojäännöksiä voi olla korkeintaan $a$ kappaletta. Tämän perusteella voidaan olettaa, että jakojäännös $r_{n+1} = 0$. Apulauseen 1.3 perusteella $(a, b) = (r_0, r_1) = (r_1, r_2) = (r_2, r_3) = \cdots = (r_{n-3}, r_{n-2}) = (r_{n-2}, r_{n-1}) = (r_{n-1}, r_n) = (r_n, 0) = r_n$. Siis $(a, b) = r_n$.

□

**Esimerkki 1.13** Etsitään lukujen 352 ja 288 suurin yhteinen tekijä käyttämällä Eukleideen algoritmia. Saadaan yhtälöryhmä

$$\begin{aligned}
352 &= 288 \cdot 1 + 64 \\
288 &= 64 \cdot 4 + 32 \\
64 &= 32 \cdot 2 + 0.
\end{aligned}$$

Viimeinen nollasta poikkeava jakojäännös on 32, jolloin (352, 288) = 32.

**Lause 1.11 Aritmetiikan peruslause** *Jokainen lukua* 1 *suurempi kokonaisluku voidaan esittää yksikäsitteisesti alkulukujen tulona.*

*Todistus.* Ks. [2], s.97.

**Huomautus 1.3** Lauseen 1.11 perusteella jokainen lukua 1 suurempi kokonaisluku $n$ voidaan esittää muodossa $n = p_1^{k_1} p_2^{k_2} \cdot \cdot \cdot p_r^{k_r}$, missä $i = 1, 2, \ldots, r$ ja $k_i$ on positiivinen kokonaisluku sekä $p_i$ on alkuluku ja $p_1 < p_2 < \cdots < p_r$. Esitystä sanotaan *kanoniseksi alkutekijäesitykseksi*.

**Lause 1.12** *Olkoot $a$ ja $b$ positiivisia kokonaislukuja, joiden kanoniset alkutekijäesitykset ovat*

$$a = p_1^{j_1} p_2^{j_2} \cdots p_n^{j_n}, \qquad b = p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n},$$

*missä jotkut exponenteista $j_1, j_2, \ldots, j_n$ ja $k_1, k_2, \ldots, k_n$ voivat olla nollia. Olkoon $m_i$ minimi luvuista $j_i$ ja $k_i$ ja olkoon $M_i$ maksimi luvuista $j_i$ ja $k_i$, missä $i = 1, 2, \ldots, n$. Tällöin*

(*i*) $a \mid b$, *jos ja vain jos* $j_i \leq k_i$ *kaikilla* $i = 1, 2, \ldots, n$,

(*ii*) $(a, b) = p_1^{m_1} p_2^{m_2} \cdots p_n^{m_n}$,

(*iii*) $[a, b] = p_1^{M_1} p_2^{M_2} \cdots p_n^{M_n}$.

*Todistus.* Ks. [3], s.60.

**Apulause 1.4** *Olkoot $x$ ja $y$ reaalilukuja. Tällöin* $\max(x, y) + \min(x, y) = x + y$.

*Todistus.* Ks. [2], s.100.

**Lause 1.13** *Olkoot $a$ ja $b$ positiivisia kokonaislukuja. Tällöin* $[a, b] = \dfrac{ab}{(a,b)}$.

*Todistus.* Vrt. [2], s.100. Lukujen $a$ ja $b$ kanoniset alkutekijäesitykset ovat

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}, \qquad b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}.$$

Olkoon $M_j = \max(a_j, b_j)$ ja $m_j = \min(a_j, b_j)$, missä $1 \leq j \leq n$. Nyt

$$[a, b] \cdot (a, b) = p_1^{M_1} p_2^{M_2} \cdots p_n^{M_n} \cdot p_1^{m_1} p_2^{m_2} \cdots p_n^{m_n}$$
$$= p_1^{M_1+m_1} p_2^{M_2+m_2} \cdots p_n^{M_n+m_n}.$$

Apulauseen 1.4 perusteella $M_j + m_j = a_j + b_j$, jolloin

$$p_1^{M_1+m_1} p_2^{M_2+m_2} \cdots p_n^{M_n+m_n} = p_1^{a_1+b_1} p_2^{a_2+b_2} \cdots p_n^{a_n+b_n}$$
$$= p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n} \cdot p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$$
$$= ab.$$

□

### *1.3 Lineaarinen Diofantoksen yhtälö*

**Määritelmä 1.11** Yhtälöä $ax + by = c$, missä $a$, $b$ ja $c$ ovat kokonaislukuja, sanotaan *kahden muuttujan lineaariseksi Diofantoksen yhtälöksi*.

Lause 1.14 osoittaa milloin kahden muuttujan lineaarisella Diofantoksen yhtälöllä on kokonaislukuratkaisuja ja mitkä ne ovat.

**Lause 1.14** *Olkoot $a$ ja $b$ kokonaislukuja ja $(a, b) = d$. Kahden muuttujan lineaarisella Diofantoksen yhtälöllä $ax + by = c$ on kokonaislukuratkaisu, jos ja vain jos $d \mid c$. Jos $x_0$ ja $y_0$ toteuttavat yhtälön $ax + by = c$, niin yhtälöllä on ääretön määrä kokonaislukuratkaisuja ja ne ovat ovat muotoa*

$$x = x_0 + (b/d)t, \quad y = y_0 - (a/d)t,$$

*missä $t \in Z$.*

*Todistus.* Vrt. [1], s.34. Oletetaan ensin, että yhtälöllä $ax + by = c$ on kokonaislukuratkaisu $x = x_0$, $y = y_0$. Koska $(a, b) = d$, niin on olemassa sellaiset kokonaisluvut $r$ ja $s$, että $a = dr$ ja $b = ds$. Tällöin

$$c = ax + by = ax_0 + by_0 = drx_0 + dsy_0 = d(rx_0 + sy_0),$$

ja siis $d \mid c$.

Oletetaan nyt, että $d \mid c$, jolloin on olemassa sellainen kokonaisluku $t$, että $c = dt$. Lauseen 1.6 perusteella on olemassa sellaiset kokonaisluvut $x_0$ ja $y_0$, että $d = ax_0 + by_0$. Kerrotaan yhtälö luvulla $t$, jolloin

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

Siis yhtälöllä $ax + by = c$ on kokonaislukuratkaisu $x = tx_0$, $y = ty_0$.

Todistetaan nyt lauseen loppuosa. Olkoon $x_0$, $y_0$ yhtälön $ax + by = c$ yksi ratkaisu ja olkoon $x, y$ yhtälön $ax + by = c$ mielivaltainen ratkaisu. Nyt

$$c = ax + by = ax_0 + by_0$$

eli

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

Koska $(a, b) = d$, niin on olemassa sellaiset kokonaisluvut $r$ ja $s$, että $a = dr$ ja $b = ds$. Sijoitetaan $a = dr$ ja $b = ds$ edelliseen yhtälöön ja jaetaan luvulla $d$, jolloin

$$r(x - x_0) = s(y_0 - y).$$

Siis $r \mid s(y_0 - y)$. Koska $(a, b) = d$, niin lauseen 1.4 perusteella $(r, s) = 1$ ja tällöin apulauseen 1.2 perusteella $r \mid (y_0 - y)$. On siis olemassa sellainen kokonaisluku $t$, että $y_0 - y = rt$. Tällöin $r(x - x_0) = srt$ ja edelleen $x - x_0 = st$. Siis

$$x = x_0 + st = x_0 + (b/d)t,$$

$$y = y_0 - rt = y_0 - (a/d)t,$$

missä $t \in \boldsymbol{Z}$.

Todistetaan vielä, että $x$ ja $y$ toteuttavat yhtälön huolimatta luvun $t$ arvosta. Nyt

$$\begin{aligned} ax + by &= a(x_0 + (b/d)t) + b(y_0 - (a/d)t) \\ &= (ax_0 + by_0) + (ab/d - ab/d)t \\ &= c + 0 \cdot t \\ &= c. \end{aligned}$$

□

**Huomautus 1.4** Ks. [2], s.121. Kirjassa lauseen 1.14 todistuksessa on viittaus kirjan lauseeseen 3.7. Viittaus pitäisi olla kirjan lauseeseen 3.6.

**Esimerkki 1.14** Tarkastellaan kahden muuttujan lineaarista Diofantoksen yhtälöä $12x + 4y = 9$. Koska $(12, 4) = 4$ ja $4 \nmid 9$, niin lauseen 1.14 perusteella yhtälöllä ei ole kokonaislukuratkaisuja.

**Esimerkki 1.15** Vrt. [2], s.123. Tehtävä 1.c. Tarkastellaan kahden muuttujan lineaarista Diofantoksen yhtälöä $21x + 14y = 147$. Etsitään lukujen 21 ja 14 suurin yhteinen tekijä käyttämällä Eukleideen algoritmia.

$$21 = 14 \cdot 1 + 7$$
$$14 = 7 \cdot 2$$

Siis $(21, 14) = 7$. Koska $7 \mid 147$, niin lauseen 1.14 perusteella yhtälöllä on ääretön määrä kokonaislukuratkaisuja. Kerrotaan yhtälön $21 \cdot 1 + 14 \cdot (-1) = 7$ molemmat puolet luvulla 21, jolloin

$$21 \cdot (21) + 14 \cdot (-21) = 147.$$

Nyt yhtälön $21x + 14y = 147$ yksi ratkaisu on $x_0 = 21$, $y_0 = -21$. Koska $a/d = 21/7 = 3$ ja $b/d = 14/7 = 2$, niin kaikki muut kokonaislukuratkaisut ovat

$$x = 21 + 2t,$$
$$y = -21 - 3t,$$

missä $t \in \boldsymbol{Z}$.

**Seuraus 1.1** *Olkoot $a$ ja $b$ kokonaislukuja ja $(a, b) = 1$. Jos $x_0$ ja $y_0$ toteuttavat Diofantoksen yhtälön $ax + by = c$, niin yhtälöllä on ääretön määrä kokonaislukuratkaisuja ja ne ovat ovat muotoa*

$$x = x_0 + bt, \qquad y = y_0 - at,$$

*missä $t \in \boldsymbol{Z}$.*

*Todistus.* Seuraa suoraan lauseesta 1.14.

**Esimerkki 1.16** Tarkastellaan kahden muuttujan lineaarista Diofantoksen yhtälöä $5x + 6y = 16$. Nähdään, että $(5, 6) = 1$. Koska $x_0 = 2$ ja $y_0 = 1$ toteuttavat yhtälön, niin seurauksen 1.1 perusteella yhtälön $5x + 6y = 16$ kaikki muut kokonaislukuratkaisut ovat

$$x = 2 + 6t, \qquad y = 1 - 5t,$$

*missä $t \in \boldsymbol{Z}$.*

**Lause 1.15** *Olkoot* $a_1, a_2, \ldots, a_n \in \boldsymbol{Z}^+$ *ja* $(a_1, a_2, \ldots, a_n) = d$. *Yhtälöllä* $a_1x_1 + a_2x_2 + \ldots + a_nx_n = c$ *on kokonaislukuratkaisu, jos ja vain jos* $d \mid c$.

*Todistus.* Ks. [2], s.122.

**Esimerkki 1.17** Tarkastellaan yhtälöä $16x_1 + 12x_2 + 20x_3 = 5$. Nyt $(16, 12, 20) = 4$ ja $4 \nmid 5$, jolloin lauseen 1.15 perusteella yhtälöllä ei ole ratkaisua.

# Luku 2 Kongruenssi

## *2.1 Kongruenssin perusominaisuuksia*

**Määritelmä 2.1** Olkoon $m$ positiivinen kokonaisluku ja olkoot $a$ ja $b$ kokonaislukuja. Sanotaan, että luku $a$ on *kongruentti* luvun $b$ kanssa modulo $m$, jos $m \mid (a - b)$. Jos luku $a$ on kongruentti luvun $b$ kanssa modulo $m$, niin merkitään

$$a \equiv b \pmod{m}.$$

Jos $m \nmid (a - b)$, niin luku $a$ ei ole kongruentti luvun $b$ kanssa modulo $m$ ja merkitään

$$a \not\equiv b \pmod{m}.$$

**Esimerkki 2.1** Koska $9 \mid (12 - 3)$, niin $12 \equiv 3 \pmod{9}$ ja $35 \equiv 2 \pmod{3}$, sillä $3 \mid (35 - 2)$. Luku 2 ei ole kongruentti luvun 7 kanssa modulo 9, koska $9 \nmid (2 - 7)$ ja merkitään $2 \not\equiv 7 \pmod{9}$.

**Lause 2.1** *Olkoot a, b ja m kokonaislukuja. Tällöin* $a \equiv b \pmod{m}$, *jos ja vain jos on olemassa sellainen kokonaisluku k, että*

$$a = b + km.$$

*Todistus.* Vrt. [2], s.129. Jos $a \equiv b \pmod{m}$, niin määritelmän 2.1 mukaan $m \mid (a - b)$. Määritelmän 1.2 mukaan on olemassa sellainen kokonaisluku $k$, että $km = a - b$, jolloin $a = b + km$. Jos on olemassa sellainen kokonaisluku $k$, että $a = b + km$, niin $km = a - b$. Tällöin määritelmän 1.2 mukaan $m \mid (a - b)$, ja määritelmän 2.1 mukaan $a \equiv b \pmod{m}$.

□

**Esimerkki 2.2** Koska $11 = 2 + 3 \cdot 3$, niin $11 \equiv 2 \pmod{3}$.

**Lause 2.2** *Olkoot a, b ja c kokonaislukuja ja olkoon m positiivinen kokonaisluku. Tällöin kongruenssi modulo m toteuttaa ehdot*

(*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*. Vrt. [2], s.129.

(*i*) Koska $m \mid (a - a) = 0$, niin $a \equiv a \pmod{m}$.

(*ii*) Jos $a \equiv b \pmod{m}$, niin $m \mid (a - b)$. Määritelmän 1.2 mukaan on olemassa sellainen kokonaisluku $k$, että $km = a - b$. Tällöin $(-k)m = b - a$, joten $m \mid b - a$. Määritelmän 2.1 mukaan $b \equiv a \pmod{m}$.

(*iii*) Jos $a \equiv b \pmod{m}$ ja $b \equiv c \pmod{m}$, niin $m \mid (a - b)$ ja $m \mid (b - c)$. Määritelmän 1.2 mukaan on olemassa sellaiset kokonaisluvut $k$ ja $l$, että $km = a - b$ ja $lm = b - c$. Nyt $a - c = (a - b) + (b - c) = km + lm = (k + l)m$. Siis $m \mid a - c$, jolloin määritelmän 2.1 mukaan $a \equiv c \pmod{m}$.

□

**Määritelmä 2.2 ( Jäännösluokka modulo *m*)** *Jäännösluokka modulo m* sisältää kokonaisluvut, jotka ovat keskenään kongruentteja modulo *m*.

**Esimerkki 2.3** Jäännösluokat modulo 3 ovat

$$\{\ldots -6, -3, 0, 3, 6, \ldots\},$$
$$\{\ldots -5, -2, 1, 4, 7, \ldots\},$$
$$\{\ldots -4, -1, 2, 5, 8, \ldots\}.$$

**Huomautus 2.1** Kokonaislukujen joukko voidaan jakaa joukkoihin, joita on *m* kappaletta. Joukot ovat jäännösluokkia modulo *m* ja niiden yhdiste muodostaa kokonaislukujen joukon.

**Määritelmä 2.3** Oletetaan, että $m$ on positiivinen kokonaisluku ja $a$ ja $b$ ovat kokonaislukuja. Lauseen 1.3 jakoalgoritmin mukaisesti jaettaessa saadaan, että

$$a = bm + r,$$

missä $0 \leq r \leq m - 1$. Lukua $r$ sanotaan luvun *a jäännökseksi modulo m.*

**Huomautus 2.2** Yhtälöstä $a = bm + r$ seuraa, että $a \equiv r \pmod{m}$. Tämän perusteella jokainen kokonaisluku on kongruentti joukon $\{0, 1, \ldots, m - 1\}$ yhden kokonaisluvun kanssa modulo $m$. Koska mitkään kaksi joukon $\{0, 1, \ldots, m - 1\}$lukua eivät ole keskenään kongruentteja modulo $m$, niin jokainen kokonaisluku on kongruentti täsmälleen yhden joukon $\{0, 1, \ldots, m - 1\}$ luvun kanssa.

**Määritelmä 2.4** *Täydellinen jäännössysteemi modulo m* on sellaisten kokonaislukujen joukko, että jokainen kokonaisluku on kongruentti modulo $m$ täsmälleen yhden joukkoon kuuluvan luvun kanssa.

**Esimerkki 2.4** Kokonaislukujen joukko $\{0, 1, \ldots, m - 1\}$ on täydellinen jäännössysteemi modulo $m$.

**Lause 2.3** *Olkoot a, b ja c kokonaislukuja ja olkoon m positiivinen kokonaisluku. 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.* Vrt. [2], s.130.

($i$) Koska $a \equiv b \pmod{m}$, niin $m \mid (a - b)$. Koska $a - b = (a + c) - (b + c)$, niin m $\mid ((a + c) - (b + c))$, jolloin määritelmän 2.1 mukaan $a + c \equiv b + c \pmod{m}$.

($ii$) Koska $a \equiv b \pmod{m}$, niin $m \mid (a - b)$. Koska $a - b = (a - c) - (b - c)$, niin m $\mid ((a - c) - (b - c))$, jolloin määritelmän 2.1 mukaan $a - c \equiv b - c \pmod{m}$.

(*iii*) Koska $a \equiv b \pmod{m}$, niin $m \mid (a - b)$. Koska $m \mid (a - b)$, niin $m \mid c(a - b) = (ac - bc)$, jolloin määritelmän 2.1 mukaan $ac \equiv bc \pmod{m}$.

□

**Esimerkki 2.5** Koska $32 \equiv 4 \pmod 7$, niin lauseen 2.3 perusteella

(*i*) $37 = 32 + 5 \equiv 4 + 5 = 9 \pmod 7$,

(*ii*) $30 = 32 - 2 \equiv 4 - 2 = 2 \pmod 7$,

(*iii*) $96 = 32 \cdot 3 \equiv 4 \cdot 3 = 12 \pmod 7$.

**Esimerkki 2.6** Tarkastellaan kongruenssia $30 \equiv 10 \pmod 5$. Jos kongruenssin molemmat puolet jaetaan luvulla 5, niin saadaan $30/5 = 6 \not\equiv 10/5 = 2 \pmod 5$. Tämä johtaa seuraavaan lauseeseen.

**Lause 2.4** *Olkoot* $a, b, c \in \boldsymbol{Z}$ *ja olkoon* $m \in \boldsymbol{Z}^+$. *Jos* $d = (c, m)$ *ja* $ac \equiv bc \pmod m$, *niin* $a \equiv b \pmod{m/d}$.

*Todistus.* Vrt. [2], s.131. Jos $ac \equiv bc \pmod m$, niin $m \mid (ac - bc) = c(a - b)$. Määritelmän 1.2 mukaan on olemassa sellainen kokonaisluku $k$, että $km = c(a - b)$. Jaetaan yhtälön molemmat puolet luvulla $d$, jolloin $(c/d)(a - b) = k(m/d)$. Lauseen 1.4 perusteella $(m/d, c/d) = 1$, jolloin apulauseen 1.2 perusteella $m/d \mid (a - b)$. Määritelmän 2.1 mukaan $a \equiv b \pmod{m/d}$.

□

**Esimerkki 2.7** Koska $20 \equiv 8 \pmod 6$ ja $(4, 6) = 2$, niin $20/4 \equiv 8/4 \pmod{6/2}$ eli $5 \equiv 2 \pmod 3$.

**Seuraus 2.1** *Olkoot* $a, b, c \in \boldsymbol{Z}$ *ja olkoon* $m \in \boldsymbol{Z}^+$. *Jos* $(c, m) = 1$ *ja* $ac \equiv bc \pmod m$, *niin* $a \equiv b \pmod m$.

*Todistus.* Seuraa suoraan lauseesta 2.4.

□

**Esimerkki 2.8** Koska $45 \equiv 10 \pmod 7$ ja $(5, 7) = 1$, niin seurauksen 2.1 perusteella $45/5 = 9 \equiv 10/5 = 2 \pmod 7$.

**Lause 2.5** *Olkoot* $a, b, c, d \in \boldsymbol{Z}$ *ja olkoon* $m \in \boldsymbol{Z}^+$. *Jos* $a \equiv b \pmod m$ *ja* $c \equiv d \pmod m$, *niin*

(*i*) $a + c \equiv b + d \pmod m$,

(*ii*) $a - c \equiv b - d \pmod m$,

(*iii*) $ac \equiv bd \pmod m$.

*Todistus.* Vrt. [2], s.131.

Koska $a \equiv b \pmod m$ ja $c \equiv d \pmod m$, niin $m \mid (a - b)$ ja $m \mid (c - d)$. Määritelmän 1.2 mukaan on olemassa sellaiset kokonaisluvut $k$ ja $l$, että $km = a - b$ ja $lm = c - d$.

(*i*) Koska $(a + c) - (b + d) = (a - b) + (c - d) = km + lm = (k + l)m$, niin m $\mid ((a + c) - (b + d))$, jolloin määritelmän 2.1 mukaan $a + c \equiv b + d \pmod m$.

(*ii*) Koska $(a - c) - (b - d) = (a - b) - (c - d) = km - lm = (k - l)m$, niin m $\mid ((a - c) - (b - d))$, jolloin määritelmän 2.1 mukaan $a - c \equiv b - d \pmod m$.

(*iii*) Koska $ac - bd = ac - bc + bc - bd = c(a - b) + b(c - d) = ckm + blm = m(ck + bl)$, niin $m \mid (ac - bd)$, jolloin määritelmän 2.1 mukaan $ac \equiv bd \pmod m$.

□

**Esimerkki 2.9** Koska $15 \equiv 3 \pmod 6$ ja $8 \equiv 2 \pmod 6$, niin lauseen 2.5 perusteella

(*i*) $15 + 8 = 23 \equiv 3 + 2 = 5 \pmod 6$,

(*ii*) $15 - 8 = 7 \equiv 3 - 2 = 1 \pmod 6$,

(*iii*) $15 \cdot 8 = 90 \equiv 3 \cdot 2 = 6 \pmod 6$.

**Lause 2.6** *Olkoot* $a, b \in \boldsymbol{Z}$ *ja olkoot* $k, m \in \boldsymbol{Z}^+$. *Jos* $a \equiv b \pmod m$, *niin* $a^k \equiv b^k \pmod m$.

*Todistus.* Vrt. [2], s.133. Koska $a \equiv b \pmod{m}$, niin $m \mid (a - b)$. Koska $a^k - b^k = (a-b)(a^{k-1} + a^{k-2}b + \cdots + ab^{k-2} + b^{k-1})$, niin $(a-b) \mid (a^k - b^k)$. Lauseen 1.1 perusteella $m \mid (a^k - b^k)$, jolloin määritelmän 2.1 mukaan $a^k \equiv b^k \pmod{m}$.

□

**Huomautus 2.3** Ks. [2], s.133. Kirjassa lauseen 2.6 todistuksessa on viittaus kirjan lauseeseen 1.4. Viittaus pitäisi olla kirjan lauseeseen 1.5.

**Esimerkki 2.10** Koska $8 \equiv 4 \pmod{4}$, niin lauseen 2.6 perusteella $8^4 = 4096 \equiv 4^4 = 256 \pmod{4}$.

**Apulause 2.1** *Jos* $a_1, a_2, \ldots, a_k$ *ja* $b$ *ovat kokonaislukuja, niin* $[a_1, a_2, \ldots, a_k] \mid b$*, jos ja vain jos* $a_1 \mid b, a_2 \mid b, \ldots, a_k \mid b$.

*Todistus.* Vrt. [2], s.106, Tehtävä 39. Oletetaan, että $[a_1, a_2, \ldots, a_k] \mid b$. Koska $a_1 \mid [a_1, a_2, \ldots, a_k]$, $a_2 \mid [a_1, a_2, \ldots, a_k]$, $\ldots$, $a_k \mid [a_1, a_2, \ldots, a_k]$, niin lauseen 1.1 perusteella $a_1 \mid b$, $a_2 \mid b$, $\ldots$, $a_k \mid b$. Käänteisesti oletetaan, että $a_1 \mid b$, $a_2 \mid b$, $\ldots$, $a_k \mid b$. Luvut $a_1, a_2, \ldots, a_k$ ja $b$ voidaan esittää muodossa $a_1 = p_1^{a_{1_1}} p_2^{a_{1_2}} \cdots p_n^{a_{1_n}}$, $a_2 = p_1^{a_{2_1}} p_2^{a_{2_2}} \cdots p_n^{a_{2_n}}$, $\ldots$, $a_k = p_1^{a_{k_1}} p_2^{a_{k_2}} \cdots p_n^{a_{k_n}}$ ja $b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$. Koska $a_1 \mid b$, $a_2 \mid b$, $\ldots$, $a_k \mid b$, niin lauseen 1.12 perusteella $a_{1_i} \leq b_i$, $a_{2_i} \leq b_i$, $\ldots$, $a_{k_i} \leq b_i$, missä $i = 1, 2, \ldots, n$. Nyt $\max(a_{1_i}, a_{2_i}, \ldots, a_{k_i}) \leq b_i$, jolloin lauseen 1.12 perusteella $[a_1, a_2, \ldots, a_k] \mid b$.

□

**Apulause 2.2** *Jos* $m_1, m_2, \ldots, m_k$ *ovat pareittain suhteellisia alkulukuja, niin*

$$[m_1, m_2, \ldots, m_k] = m_1 m_2 \cdots m_k .$$

*Todistus.* Todistetaan apulause induktiolla. Olkoon $k = 2$. Nyt lauseen 1.13 perusteella $[m_1, m_2] = \frac{m_1 m_2}{(m_1, m_2)}$. Koska $m_1$ ja $m_2$ ovat suhteellisia alkulukuja, niin $(m_1, m_2) = 1$, jolloin $[m_1, m_2] = m_1 m_2$. Siis apulause on tosi, kun $k = 2$.

Tehdään induktio-oletus, että apulause on tosi, kun $k = n$, jolloin $[m_1, m_2, \ldots, m_n] = m_1 m_2 \cdots m_n$. Tehdään induktioväite, että apulause on tosi, kun $k = n + 1$. Nyt $[m_1, m_2, \ldots, m_n, m_{n+1}] = [[m_1, m_2, \ldots, m_n], m_{n+1}]$, jolloin induktio-oletuksen perusteella $[[m_1, m_2, \ldots, m_n], m_{n+1}] = [(m_1 m_2 \cdots m_n), m_{n+1}]$. Koska $m_1, m_2, \ldots, m_n, m_{n+1}$ ovat pareittain suhteellisia alkulukuja, niin nähdään, että $((m_1 m_2 \cdots m_n), m_{n+1}) = 1$, jolloin lauseen 1.13 perusteella $[m_1, m_2, \ldots, m_n, m_{n+1}] = m_1 m_2 \cdots m_n \cdot m_{n+1}$. Induktioperiaatteen mukaan apulause on tosi.

□

**Lause 2.7** *Olkoot* $a, b \in \boldsymbol{Z}$ *ja olkoot* $m_1, m_2, \ldots, m_k \in \boldsymbol{Z}^+$. *Jos* $a \equiv b \pmod{m_1}$, $a \equiv b \pmod{m_2}$, ... , $a \equiv b \pmod{m_k}$, *niin* $a \equiv b \pmod{[m_1, m_2, \ldots, m_k]}$.

*Todistus.* Vrt. [2], s.133. Koska $a \equiv b \pmod{m_1}$, $a \equiv b \pmod{m_2}$, ... , $a \equiv b \pmod{m_k}$, niin $m_1 \mid (a - b)$, $m_2 \mid (a - b)$, ... , $m_k \mid (a - b)$. Apulauseen 2.1 perusteella $[m_1, m_2, \ldots, m_k] \mid (a - b)$, jolloin määritelmän 2.1 mukaan $a \equiv b \pmod{[m_1, m_2, \ldots, m_k]}$.

□

**Seuraus 2.2** *Olkoot* $a, b \in \boldsymbol{Z}$ *ja olkoot* $m_1, m_2, \ldots, m_k$ *pareittain suhteellisia alkulukuja. Jos* $a \equiv b \pmod{m_1}$, $a \equiv b \pmod{m_2}$, ... , $a \equiv b \pmod{m_k}$, *niin* $a \equiv b \pmod{m_1 m_2 \cdots m_k}$.

Todistus. Vrt. [2], s.133. Koska $m_1, m_2, \ldots, m_k$ ovat pareittain suhteellisia alkulukuja, niin apulauseen 2.2 perusteella $[m_1, m_2, \ldots, m_k] = m_1 m_2 \cdots m_k$. Lauseen 2.7 perusteella $a \equiv b \pmod{m_1 m_2 \cdots m_k}$.

□

## *2.2 Lineaarinen kongruenssiyhtälö*

**Määritelmä 2.5** Kongruenssia

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

sanotaan *yhden muuttujan lineaarikongruenssiksi*. Toisin sanoen lineaarikongruenssit ovat ensimmäisen asteen kongruenssiyhtälöitä.

Lause 2.8 osoittaa milloin yhden muuttujan lineaarisella kongruenssiyhtälöllä on ratkaisu. Jos kongruenssiyhtälö on ratkeava, niin lause 2.8 kertoo kuinka monta epäkongruenttia ratkaisua on olemassa.

**Lause 2.8** *Olkoot* $a, b \in \boldsymbol{Z}$ *ja olkoon* $m \in \boldsymbol{Z}^+$. *Olkoon* $(a, m) = d$. *Jos luku b ei ole jaollinen luvulla d, niin kongruenssiyhtälöllä*

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

*ei ole ratkaisua. Jos luku b on jaollinen luvulla d, niin kongruenssiyhtälöllä*

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

*on täsmälleen d kappaletta keskenään epäkongruenttia ratkaisua.*

*Todistus.* Vrt. [2], s.139. Lauseen 2.1 perusteella lineaarinen kongruenssiyhtälö $ax \equiv b \pmod{m}$ on ekvivalentti lineaarisen Diofantoksen yhtälön $ax - my = b$ kanssa. Kokonaisluku $x$ on kongruenssiyhtälön $ax \equiv b \pmod{m}$ ratkaisu, jos ja vain jos on olemassa sellainen kokonaisluku $y$, että $ax - my = b$. Jos $d \nmid b$, niin lauseen 1.14 perusteella yhtälöllä $ax - my = b$ ei ole ratkaisuja. Jos $d \mid b$, niin yhtälöllä on ääretön määrä ratkaisuja ja ne ovat muotoa

$$x = x_0 + (m/d)t, \quad y = y_0 - (a/d)t,$$

missä $x_0$ ja $y_0$ ovat yhtälön $ax - my = b$ yksi ratkaisu. Luvun $x$ arvot

$$x = x_0 + (m/d)t$$

ovat kongruenssiyhtälön $ax \equiv b \pmod{m}$ ratkaisut ja niitä on ääretön määrä.

Tutkitaan nyt ratkaisuja $x_1 = x_0 + (m/d)t_1$ ja $x_2 = x_0 + (m/d)t_2$. Jos ne ovat keskenään kongruentteja modulo $m$, niin

$$x_0 + (m/d)t_1 \equiv x_0 + (m/d)t_2 \pmod{m}$$

eli

$$(m/d)t_1 \equiv (m/d)t_2 \pmod{m}.$$

Koska $m/d \mid m$, niin $(m, m/d) = m/d$, jolloin lauseen 2.4 perusteella

$$t_1 \equiv t_2 \pmod{d}.$$

Nyt kaikki keskenään epäkongruentit ratkaisut saadaan yhtälöstä $x = x_0 + (m/d)t$, missä luku $t$ saa kaikki täydellisen jäännössysteemin modulo $d$ arvot. Koska 0, 1, 2, … , $d - 1$ on yksi täydellinen jäännössysteemi modulo $d$, niin ratkaisut saadaan yhtälöstä

$$x = x_0 + (m/d)t,$$

missä $t = 0, 1, 2, \ldots, d - 1$.

□

**Esimerkki 2.11** Etsitään kongruenssinyhtälön $3x \equiv 6 \pmod 9$ kaikki ratkaisut. Koska $(3, 9) = 3$ ja $3 \mid 6$, niin on olemassa kolme keskenään epäkongruenttia ratkaisua.Tarkastellaan lineaarista Diofantoksen yhtälöä $3x - 9y = 6$. Yksi yhtälön ratkaisuista on $x_0 = -1$, $y_0 = -1$. Siis kongruenssinyhtälön $3x \equiv 6 \pmod 9$ ratkaisut ovat muota $x = x_0 + (m/d)t$, eli $x = -1 + 3t$, missä $t = 0,1,2$. Sijoitetaan luvun $t$ arvot yhtälöön, jolloin

$$x = -1 + 3 \cdot 0 = -1 \equiv 8 \pmod 9$$
$$x = -1 + 3 \cdot 1 \equiv 2 \pmod 9$$
$$x = -1 + 3 \cdot 2 \equiv 5 \pmod 9.$$

Siis kongruenssiyhtälön $3x \equiv 6 \pmod 9$ ratkaisut ovat $x \equiv 2, 5, 8 \pmod 9$.

**Määritelmä 2.6** Olkoon $a$ kokonaisluku ja $m$ positiivinen kokonaisluku. Jos $(a, m) = 1$, niin kongruenssiyhtälön

$$ax \equiv 1 \pmod{m}$$

ratkaisua kutsutaan *luvun a käänteisluvuksi* modulo $m$. Tällöin merkitään $x = \overline{a}$.

**Huomautus 2.4** Jos $\overline{a}$ on luvun $a$ käänteisluku modulo $m$, niin $a\overline{a} \equiv 1 \pmod{m}$.

**Huomautus 2.5** Kongruenssiyhtälöllä $ax \equiv 1 \pmod{m}$ on lauseen 2.8 perusteella ratkaisu, jos ja vain jos $(a, m) = 1$. Tällöin kaikki ratkaisut ovat kongruentteja modulo $m$.

**Esimerkki 2.12** Tarkastellaan kongruenssiyhtälöä $5x \equiv 1 \pmod{11}$. Koska $(5, 11) = 1$, niin kongruenssiyhtälöllä on ratkaisu. Nähdään, että $x = 9$ on yksi ratkaisu. Tällöin kaikki ratkaisut ovat $x \equiv 9 \pmod{11}$ ja ne ovat luvun 5 käänteislukuja modulo $m$.

**Huomautus 2.6** Kun tunnetaan luvun $a$ käänteisluku modulo $m$, niin sitä voidaan käyttää apuna ratkaistaessa konruenssiyhtälöä $ax \equiv b \pmod{m}$. Kerrotaan kongruenssiyhtälön molemmat puolet luvulla $\bar{a}$, jolloin $\bar{a}(ax) \equiv \bar{a}\,b \pmod{m}$ ja siis $x \equiv \bar{a}\,b \pmod{m}$.

**Esimerkki 2.13** Tarkastellaan kongruenssiyhtälöä $5x \equiv 13 \pmod{11}$. Esimerkin 2.12 perusteella luvun 5 käänteisluku modulo 11 on 9. Kerrotaan kongruenssiyhtälön molemmat puolet luvulla 9, jolloin $9 \cdot 5x \equiv 9 \cdot 13 \pmod{11}$. Siis kongruenssiyhtälön $5x \equiv 13 \pmod{11}$ ratkaisu on $x \equiv 117 \equiv 7 \pmod{11}$.

**Lause 2.9** *Olkoon $p$ alkuluku ja $a$ positiivinen kokonaisluku. Tällöin luku $a$ on itsensä käänteisluku, jos ja vain jos*

$$a \equiv 1 \pmod{p} \text{ tai } a \equiv -1 \pmod{p}.$$

*Todistus.* Vrt. [2], s.141. Jos $a$ on itsensä käänteisluku modulo $p$, niin $a^2 = a \cdot a \equiv 1 \pmod{p}$. Siis $p \mid (a^2 - 1)$. Koska $a^2 - 1 = (a - 1) \cdot (a + 1)$, niin joko $p \mid (a - 1)$ tai $p \mid (a + 1)$. Siis joko $a \equiv 1 \pmod{p}$ tai $a \equiv -1 \pmod{p}$.

Oletetaan, että $a \equiv 1 \pmod{p}$. Kerrotaan kongruenssin molemmat puolet luvulla $a + 1$, jolloin

$$a(a + 1) \equiv a + 1 \pmod{p}$$
$$a^2 + a \equiv a + 1 \pmod{p}$$
$$a^2 \equiv 1 \pmod{p}.$$

Oletetaan, että $a \equiv -1 \pmod{p}$. Kerrotaan kongruenssin molemmat puolet luvulla $a - 1$, jolloin

$$a(a-1) \equiv -(a-1) \pmod{p}$$
$$a^2 - a \equiv -a + 1 \pmod{p}$$
$$a^2 \equiv 1 \pmod{p}.$$

Siis jos $a \equiv 1 \pmod{p}$ tai $a \equiv -1 \pmod{p}$, niin luku $a$ on itsensä käänteisluku modulo $p$.

□

### *2.3 Kiinalainen jäännöslause*

Siirrytään tarkastelemaan yhden muuttujan kongruenssiyhtälöryhmiä. Tällainen ryhmä on esimerkiksi

$$x \equiv 1 \pmod{3}$$
$$x \equiv 2 \pmod{5}$$
$$x \equiv 3 \pmod{7}.$$

Kongruenssiyhtälöryhmälle esitetään kaksi ratkaisutapaa, joista ensimmäinen on kiinalainen jäännöslause.

**Lause 2.10 (Kiinalainen jäännöslause)** *Olkoot $a_1, a_2, \ldots, a_r$ kokonaislukuja ja olkoot $n_1, n_2, \ldots, n_r$ pareittain suhteellisia positiivisia alkulukuja. Olkoon $N = n_1 n_2 \cdots n_r$. Tällöin kongruenssiyhtälöryhmällä*

$$x \equiv a_1 \pmod{n_1}$$
$$x \equiv a_2 \pmod{n_2}$$
$$\vdots$$
$$x \equiv a_r \pmod{n_r}$$

*on olemassa yksikäsitteinen ratkaisu* modulo *N*.

*Todistus*. Vrt. [1], s.78. Olkoon $N_k = \dfrac{N}{n_k} = n_1 n_2 \cdots n_{k-1} n_{k+1} \cdots n_r$, missä $k = 1, 2, \ldots, r$. Koska luvut $n_1, n_2, \ldots, n_r$ ovat pareittain suhteellisia alkulukuja, niin $(N_k, n_k) = 1$. Lauseen 2.8 perusteella kongruenssiyhtälöllä $N_k x \equiv 1 \pmod{n_k}$ on ratkaisu $x = x_k$. Todistetaan, että kokonaisluku

$$x = a_1 N_1 x_1 + a_2 N_2 x_2 + \cdots + a_r N_r x_r$$

on kongruenssiyhtälöryhmän yksikäsitteinen ratkaisu.

Koska $n_k \mid N_i$, niin $N_i \equiv 0 \pmod{n_k}$, missä $i \neq k$. Tällöin

$$x = a_1 N_1 x_1 + a_2 N_2 x_2 + \cdots + a_r N_r x_r \equiv a_k N_k x_k \pmod{n_k}.$$

Koska $x_k$ on kongruenssiyhtälön $N_k x \equiv 1 \pmod{n_k}$ ratkaisu, niin

$$x \equiv a_k \cdot 1 \equiv a_k \pmod{n_k}.$$

Siis kokonaisluku $x$ on kongruenssiyhtälöryhmän ratkaisu.

Oletetaan nyt, että on olemassa myös toinen ratkaisu $x'$. Tällöin

$$x \equiv a_k \equiv x' \pmod{n_k}, \text{ missä } k = 1, 2, \ldots, r.$$

Siis $n_k \mid (x - x')$ kaikilla $k = 1, 2, \ldots, r$. Koska $(n_i, n_j) = 1$ aina, kun $i \neq j$, niin apulauseen 2.1 perusteella $[n_1, n_2, \ldots, n_r] \mid (x - x')$. Apulauseen 2.2 perusteella $n_1 \cdot n_2 \cdot \cdots \cdot n_r \mid (x - x')$, jolloin $x \equiv x' \pmod{N}$. Siis $x$ on kongruenssiyhtälöryhmän yksikäsitteinen ratkaisu modulo $N$.

□

**Esimerkki 2.14** Vrt. [2], s.145. Esimerkki 4.16. Tarkastellaan esitettyä kongruenssiyhtälöryhmää

$$x \equiv 1 \pmod{3}$$
$$x \equiv 2 \pmod{5}$$
$$x \equiv 3 \pmod{7}.$$

Nyt $N = 3 \cdot 5 \cdot 7 = 105$, $N_1 = 105 / 3 = 35$, $N_2 = 105 / 5 = 21$ ja $N_3 = 105 / 7 = 15$. Ratkaistaan nyt $y_1$, $y_2$ ja $y_3$ kongruenssiyhtälöistä

$$35 y_1 \equiv 1 \pmod{3}$$
$$21 y_2 \equiv 1 \pmod{5}$$
$$15 y_3 \equiv 1 \pmod{7}.$$

Ratkaisuiksi saadaan

$$y_1 \equiv 2 \pmod{3}$$
$$y_2 \equiv 1 \pmod{5}$$
$$y_3 \equiv 1 \pmod{7}.$$

Siis yhtälöryhmän ratkaisu on

$$x \equiv 1 \cdot 35 \cdot 2 + 2 \cdot 21 \cdot 1 + 3 \cdot 15 \cdot 1 \equiv 157 \equiv 52 \pmod{105}.$$

Voidaan vielä tarkistaa tulos sijoittamalla saatu ratkaisu $x$ alkuperäisiin kongruenssiyhtälöihin, jolloin

$$52 \equiv 1 \pmod 3$$
$$52 \equiv 2 \pmod 5$$
$$52 \equiv 3 \pmod 7.$$

Siis $x \equiv 52 \pmod{105}$ on oikea ratkaisu.

On olemassa myös toinen tapa ratkaista kongruenssiyhtälöryhmä, mikä esitetään seuraavassa esimerkissä.

**Esimerkki 2.15** Vrt. [2], s.145 Esimerkki 4.17. Tarkastellaan kongruenssiyhtälöryhmää

$$x \equiv 1 \pmod 5$$
$$x \equiv 2 \pmod 6$$
$$x \equiv 3 \pmod 7.$$

Lauseen 2.1 perusteella ryhmän ensinmäinen yhtälö voidaan kirjoittaa muodossa $x = 5t + 1$, missä $t$ on kokonaisluku. Sijoitetaan tämä ryhmän toiseen yhtälöön, jolloin

$$5t + 1 \equiv 2 \pmod 6.$$

Yhtälön ratkaisu on $t \equiv 5 \pmod 6$. Tämä voidaan kirjoittaa muodossa $t = 6u + 5$, missä $u$ on kokonaisluku. Sijoitetaan tämä yhtälöön $x = 5t + 1$, jolloin $x = 5(6u + 5) + 1 = 30u + 26$. Sijoitetaan tämä ryhmän kolmanteen yhtälöön, jolloin

$$30u + 26 \equiv 3 \pmod 7.$$

Tämän yhtälön ratkaisu on $u \equiv 6 \pmod 7$, mikä lauseen 2.1 perusteella voidaan kirjoittaa muodossa $u = 7v + 6$, missä $v$ on kokonaisluku. Sijoitetaan tämä yhtälöön $x = 30u + 26$, jolloin

$$x = 30(7v + 6) + 26 = 210v + 206.$$

Lauseen 2.1 perusteella tämä voidaan kirjoittaa muodossa

$$x \equiv 206 \pmod{210},$$

joka on yhtälöryhmän ratkaisu.

### *2.4 Polynomien kongruenssit*

Tarkastellaan kokonaislukukertoimisten polynomien kongruensseja, joissa polynomien asteluku on suurempi kuin yksi. Tässä pykälässä esitetään ratkaisutapa kongruenssille $f(x) \equiv 0 \pmod{m}$, missä $f(x)$ on kokonaislukukertoiminen polynomi. Tällainen kongruenssi on esimerkiksi $2x^3 + 7x - 4 \equiv 0 \pmod{200}$.

Aritmetiikan peruslauseen perusteella luvun $m$ kanoninen alkutekijäesitys on $m = p_1^{a_1} p_2^{a_2} \cdot \cdot \cdot p_k^{a_k}$. Tällöin kongruenssin $f(x) \equiv 0 \pmod{m}$ ratkaisu saadaan ratkaisemalla ensin kongruenssiyhtälöryhmä

$$f(x) \equiv 0 \pmod{p_i^{a_i}},$$

missä $i = 1, 2, \ldots, k$. Kun kaikki yhtälöryhmän kongruenssit on ratkaistu, niin käytetään kiinalaista jäännöslausetta, jonka perusteella saadaan kongruenssin $f(x) \equiv 0 \pmod{m}$ ratkaisu. Tätä ratkaisutapaa käytettään esimerkissä 2.17.

**Esimerkki 2.16** Vrt. [2], s.154 Esimerkki 4.20 Tarkastellaan kongruenssia $2x^3 + 7x - 4 \equiv 0 \pmod{25}$. Ratkaisut saadaan käymällä läpi kaikki luvut $x = 0, 1, 2, \ldots, 24$. On kuitenkin toinen tapa löytää ratkaisut.

Kongruenssin $2x^3 + 7x - 4 \equiv 0 \pmod{25}$ ratkaisut ovat myös kongruenssin $2x^3 + 7x - 4 \equiv 0 \pmod{5}$ ratkaisuja. Käymällä läpi kaikki luvut $x = 0, 1, 2, 3, 4$ nähdään, että kongruenssin $2x^3 + 7x - 4 \equiv 0 \pmod{5}$ ratkaisu on $x \equiv 1 \pmod{5}$, joka voidaan esittää muodossa

$$x = 1 + 5t.$$

Sijoitetaan tämä kongruenssiin $2x^3 + 7x - 4 \equiv 0 \pmod{25}$, jolloin

$$2(1 + 5t)^3 + 7(1 + 5t) - 4 \equiv 0 \pmod{25}$$

eli

$$65t + 5 \equiv 15t + 5 \equiv 0 \pmod{25}.$$

Tämä voidaan lauseen 2.4 perusteella sieventää muotoon

$$3t + 1 \equiv 0 \pmod{5},$$

jonka ratkaisu on $t \equiv 3 \pmod{5}$. Siis kongruenssin $2x^3 + 7x - 4 \equiv 0 \pmod{25}$ ratkaisu on $x \equiv 1 + 5t \equiv 1 + 5 \cdot 3 \equiv 16 \pmod{25}$.

**Esimerkki 2.17** Vrt. [2], s.153 Esimerkki 4.19 Tarkastellaan kongruenssia $2x^3 + 7x - 4 \equiv 0 \pmod{200}$. Koska $200 = 2^3 5^2$, niin ratkaistavaksi tulee kongruenssiyhtälöryhmä

$$2x^3 + 7x - 4 \equiv 0 \pmod{8}$$
$$2x^3 + 7x - 4 \equiv 0 \pmod{25}.$$

Käymällä läpi kaikki luvut $x = 0, 1, 2, \ldots, 7$ nähdään, että kongruenssin $2x^3 + 7x - 4 \equiv 0 \pmod{8}$ ratkaisu on $x \equiv 4 \pmod{8}$. Esimerkin 2.16 perusteella kongruenssin $2x^3 + 7x - 4 \equiv 0 \pmod{25}$ ratkaisu on $x \equiv 16 \pmod{25}$. Saatiin kongruenssiyhtälöryhmä

$$x \equiv 4 \pmod{8}$$
$$x \equiv 16 \pmod{25}.$$

Käytetään kiinalaista jäännöslausetta. Nyt $N = 8 \cdot 25 = 200$, $N_1 = 25$ ja $N_2 = 8$. Ratkaistaan $y_1$ ja $y_2$ kongruenssiyhtälöistä

$$25\,y_1 \equiv 1 \pmod{8}$$
$$8\,y_2 \equiv 1 \pmod{25}.$$

Ratkaisuiksi saadaan

$$y_1 \equiv 1 \pmod{8}$$
$$y_2 \equiv 22 \pmod{25}.$$

Tällöin yhtälöryhmän ratkaisu on

$$x \equiv 4 \cdot 25 \cdot 1 + 16 \cdot 8 \cdot 22 \equiv 100 + 2816 \equiv 2916 \equiv 116 \pmod{200}.$$

Siis kongruenssin $2x^3 + 7x - 4 \equiv 0 \pmod{200}$ ratkaisu on $x \equiv 116 \pmod{200}$.

Lause 2.11 esittää tavan ratkaista kongruenssiyhtälö $f(x) \equiv 0 \pmod{p^k}$, missä $p$ on alkuluku ja $k$ on kokonaisluku.

**Lause 2.11 (Henselin Lemma)** *Olkoon $f(x)$ kokonaislukukertoiminen polynomi. Olkoot $k$, $p \in \boldsymbol{Z}$ ja olkoon lisäksi $k \geq 2$. Oletetaan, että $r$ on kongruenssin $f(x) \equiv 0 \pmod{p^{k-1}}$ ratkaisu. Tällöin*

(*i*) *jos $f'(r) \not\equiv 0 \pmod{p}$, niin on olemassa sellainen yksikäsitteinen kokonaisluku $t$, että $0 \leq t < p$ ja $f(r + tp^{k-1}) \equiv 0 \pmod{p^k}$, missä $t \equiv -\overline{f'(r)}\ (f(r)/p^{k-1}) \pmod{p}$,*

(*ii*) *jos* $f'(r) \equiv 0 \pmod{p}$ *ja* $f(r) \equiv 0 \pmod{p^k}$, *niin kaikilla kokonaisluvuilla t on voimassa* $f(r + tp^{k-1}) \equiv 0 \pmod{p^k}$,

(*iii*) *jos* $f'(r) \equiv 0 \pmod{p}$ *ja* $f(r) \not\equiv 0 \pmod{p^k}$, *niin kongruenssilla* $f(x) \equiv 0 \pmod{p^k}$, *missä* $x \equiv r \pmod{p^{k-1}}$, *ei ole ratkaisuja.*

*Todistus.* Ks. [2], s.156.

**Esimerkki 2.18** Vrt. [2], s.157 Esimerkki 4.21. Etsitään kongruenssin $x^3 + x^2 + 29 \equiv 0 \pmod{25}$ ratkaisut. Olkoon $f(x) = x^3 + x^2 + 29$. Kokeilemalla nähdään, että kongruenssin $f(x) \equiv 0 \pmod{5}$ ratkaisu on $x \equiv 3 \pmod{5}$. Koska $f'(x) = 3x^2 + 2x$ ja $f'(3) = 33 \equiv 3 \not\equiv 0 \pmod{5}$, niin Henselin Lemman perusteella on olemassa muotoa $3 + 5t$ oleva yksikäsitteinen ratkaisu modulo 25, missä $t \equiv -\overline{f'(3)}\ (\ f(3)/5\ ) \pmod{5}$. Nähdään, että $f(3)/5 = 65/5 = 13$ ja $\overline{f'(3)} = \bar{3} = 2$, koska $\bar{3} = 2 \pmod{5}$. Nyt $t \equiv -2 \cdot 13 \equiv 4 \pmod{5}$ ja kongruenssin $f(x) \equiv 0 \pmod{25}$ ratkaisu on $x \equiv 3 + 5 \cdot 4 = 23 \pmod{25}$.

### *2.5 Lineaariset kongruenssiryhmät*

Seuraavaksi tarkastellaan kongruenssiyhtälöiden ryhmiä, joissa tuntemattomia muuttujia on yhtä monta kuin kongruenssiyhtälöitä ja kaikilla kongruenssiyhtälöillä on sama modulo.

**Lause 2.12** *Olkoot a, b, c, d, e, f kokonaislukuja. Olkoon m sellainen positiivinen kokonaisluku, että* $(\Delta, m) = 1$, *missä* $\Delta = ad - bc$. *Tällöin kongruenssiyhtälöryhmällä*

$$ax + by \equiv e \pmod{m}$$
$$cx + dy \equiv f \pmod{m}$$

*on yksikäsitteinen ratkaisu modulo m, joka saadaan kongruensseista*

$$x \equiv \bar{\Delta}(de - bf) \pmod{m}$$
$$y \equiv \bar{\Delta}(af - ce) \pmod{m},$$

*missä* $\bar{\Delta}$ *on luvun* $\Delta$ *käänteisluku modulo m.*

*Todistus.* Vrt. [2], s.161. Kerrotaan ryhmän ensimmäinen kongruenssi luvulla $d$ ja toinen luvulla $b$, jolloin

$$adx + bdy \equiv de \pmod{m}$$
$$bcx + bdy \equiv bf \pmod{m}.$$

Vähennetään sitten toinen kongruenssi ensimmäisestä, jolloin

$$(ad - bc)x \equiv de - bf \pmod{m}.$$

Koska $\Delta = ad - bc$, niin

$$\Delta x \equiv de - bf \pmod{m}.$$

Kerrotaan tämän kongruenssin molemmat puolet luvulla $\overline{\Delta}$, jolloin

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

Kerrotaan vastaavasti alkuperäisen kongruenssiyhtälöryhmän ensimmäinen kongruenssi luvulla $c$ ja toinen luvulla $a$, jolloin

$$acx + bcy \equiv ce \pmod{m}$$
$$acx + ady \equiv af \pmod{m}.$$

Vähennetään ensimmäinen kongruenssi toisesta, jolloin

$$(ad - bc)y \equiv af - ce \pmod{m}.$$

Koska $\Delta = ad - bc$, niin

$$\Delta y \equiv af - ce \pmod{m}.$$

Kerrotaan kongruenssin molemmat puolet luvulla $\overline{\Delta}$, jolloin

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

Näin on osoitettu, että kongruenssiyhtälöryhmän ratkaisu on

$$x \equiv \overline{\Delta}(de - bf) \pmod{m} \text{ ja } y \equiv \overline{\Delta}(af - ce) \pmod{m}.$$

Voidaan tarkistaa, että mikä tahansa tällainen pari $(x, y)$ on kongruenssiyhtälöryhmän ratkaisu. Olkoot

$$x \equiv \overline{\Delta}(de - bf) \pmod{m} \text{ ja } y \equiv \overline{\Delta}(af - ce) \pmod{m}.$$

Tällöin

$$\begin{aligned} ax + by &\equiv a\overline{\Delta}(de - bf) + b\overline{\Delta}(af - ce) \\ &\equiv \overline{\Delta}(ade - abf + abf - bce) \\ &\equiv \overline{\Delta}(ad - bc)e \\ &\equiv \overline{\Delta}\,\Delta e \\ &\equiv e \pmod{m}, \end{aligned}$$

ja

$$
\begin{aligned}
cx + dy &\equiv c\overline{\Delta}(de - bf) + d\overline{\Delta}(af - ce) \\
&\equiv \overline{\Delta}(cde - bcf + adf - cde) \\
&\equiv \overline{\Delta}(ad - bc)f \\
&\equiv \overline{\Delta}\,\Delta f \\
&\equiv f \pmod{m}.
\end{aligned}
$$

□

**Esimerkki 2.19** Tarkastellaan kongruenssiyhtälöryhmää

$$
\begin{aligned}
x + 2y &\equiv 1 \pmod 5 \\
2x + y &\equiv 1 \pmod 5.
\end{aligned}
$$

Nyt $ad - bc = 1 \cdot 1 - 2 \cdot 2 = -3 = \Delta$, jolloin $\overline{\Delta} \equiv -2 \pmod 5$ ja $(\Delta, 5) = (-3, 5) = 1$. Lauseen 2.12 perusteella kongruenssiyhtälöryhmän ratkaisut saadaan kongruensseista

$$
\begin{aligned}
x &\equiv \overline{\Delta}(de - bf) \pmod m \\
y &\equiv \overline{\Delta}(af - ce) \pmod m.
\end{aligned}
$$

Siis

$$
\begin{aligned}
x &\equiv -2(1 \cdot 1 - 2 \cdot 1) \pmod 5 \\
y &\equiv -2(1 \cdot 1 - 2 \cdot 1) \pmod 5
\end{aligned}
$$

eli

$$
\begin{aligned}
x &\equiv 2 \pmod 5 \\
y &\equiv 2 \pmod 5.
\end{aligned}
$$

## *2.6 Matriisien kongruenssit*

Tässä pykälässä ensin määritellään matriisien kongruenssi ja esitetään tärkeimmät matriisien kongruenssiin liittyvät ominaisuudet. Lopuksi esitetään kongruenssiyhtälöiden ryhmälle ratkaisutapa, jossa käytetään matriiseja. Tässä pykälässä käsiteltävien matriisien kaikki alkiot ovat kokonaislukuja.

**Määritelmä 2.7** Olkoot **A** ja **B** $n \times k$ −matriiseja. Matriisi **A** on kongruentti matriisin **B** kanssa modulo $m$, jos kaikilla pareilla $(i, j)$ on voimassa $a_{ij} \equiv b_{ij} \pmod m$, missä $1 \le i \le n$ ja $1 \le j \le k$. Tällöin merkitään $\mathbf{A} \equiv \mathbf{B} \pmod m$.

**Esimerkki 2.20** Nähdään, että

$$\begin{bmatrix} 6 & 13 \\ 17 & 24 \end{bmatrix} \equiv \begin{bmatrix} 1 & 3 \\ 2 & 4 \end{bmatrix} \pmod 5.$$

**Lause 2.13** *Olkoot* **A** *ja* **B** $n \times k$ *−matriiseja ja olkoot* **C** $k \times p$ *−matriisi ja* **D** $p \times n$ *−matriisi. Jos* **A** ≡ **B** (mod $m$), *niin* **AC** ≡ **BC** (mod $m$) *ja* **DA** ≡ **DB** (mod $m$).

*Todistus*. Vrt. [2], s.163. Matriisien **A** ja **B** alkioita ovat kokonaisluvut $a_{ij}$ ja $b_{ij}$, missä $1 \leq i \leq n$ ja $1 \leq j \leq k$. Matriisin **C** alkioita ovat kokonaisluvut $c_{ij}$, missä $1 \leq i \leq k$ ja $1 \leq j \leq p$. Nyt matriisien **AC** ja **BC** alkioita ovat kokonaisluvut

$$\sum_{t=1}^{k} a_{it}c_{tj} \text{ ja } \sum_{t=1}^{k} b_{it}c_{tj},$$

missä $1 \leq i \leq n$ ja $1 \leq j \leq p$. Koska **A** ≡ **B** (mod $m$), niin määritelmän 2.7 mukaan kaikilla pareilla ($i$, $t$) on voimassa $a_{it} \equiv b_{it} \pmod m$. Lauseen 2.3 perusteella

$$\sum_{t=1}^{k} a_{it}c_{tj} \equiv \sum_{t=1}^{k} b_{it}c_{tj} \pmod m$$

eli

$$\mathbf{AC} \equiv \mathbf{BC} \pmod m.$$

Vastaavasti voidaan todistaa, että **DA** ≡ **DB** (mod $m$), joka tässä sivuutetaan.

□

Tarkastellaan kongruenssiyhtälöryhmää

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

Kongruenssiyhtälöitä on $n$ kappaletta ja ne voidaan esittää matriisien kongruenssina **AX** ≡ **B** (mod $m$), missä

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

**Esimerkki 2.21** Kongruenssiyhtälöryhmä

$$2x + 3y \equiv 5 \pmod 7$$
$$x + 5y \equiv 6 \pmod 7$$

voidaan esittää muodossa

$$\begin{bmatrix} 2 & 3 \\ 1 & 5 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \equiv \begin{bmatrix} 5 \\ 6 \end{bmatrix} \pmod 7.$$

**Huomautus 2.7** Identiteettimatriisi **I** oletetaan tunnetuksi.

**Määritelmä 2.8** Jos **A** ja $\mathbf{A}^{-1}$ ovat $n \times n$ −matriiseja ja jos

$$\mathbf{A}^{-1}\mathbf{A} \equiv \mathbf{A}\mathbf{A}^{-1} \equiv \mathbf{I} \pmod m,$$

niin $\mathbf{A}^{-1}$ on matriisin **A** *käänteismatriisi* modulo *m*.

**Huomautus 2.8** Merkinnällä $\mathbf{A}^{-1}$ tarkoitetaan aina matriisin **A** käänteismatriisia.

**Lause 2.14** *Jos* $\mathbf{B} \equiv \mathbf{A}^{-1} \pmod m$, *niin matriisi* **B** *on matriisin* **A** *käänteismatriisi*.

*Todistus.* Vrt. [2], s.164. Oletetaan, että $\mathbf{B} \equiv \mathbf{A}^{-1} \pmod m$. Lauseen 2.13 perusteella $\mathbf{BA} \equiv \mathbf{A}^{-1}\mathbf{A} \pmod m$, jolloin $\mathbf{BA} \equiv \mathbf{I} \pmod m$. Määritelmän 2.8 mukaan matriisi **B** on matriisin **A** käänteismatriisi.

□

**Lause 2.15** *Jos matriisit* $\mathbf{B}_1$ *ja* $\mathbf{B}_2$ *ovat matriisin* **A** *käänteismatriiseja, niin* $\mathbf{B}_1 \equiv \mathbf{B}_2 \pmod m$.

*Todistus.* Vrt. [2], s.164. Koska $\mathbf{B}_1$ ja $\mathbf{B}_2$ ovat matriisin $\mathbf{A}$ käänteismatriiseja, niin määritelmän 2.8 mukaan $\mathbf{B}_1\mathbf{A} \equiv \mathbf{B}_2\mathbf{A} \equiv \mathbf{I} \pmod{m}$. Lauseen 2.13 perusteella $\mathbf{B}_1\mathbf{A}\,\mathbf{B}_1 \equiv \mathbf{B}_2\mathbf{A}\,\mathbf{B}_1 \pmod{m}$. Koska $\mathbf{A}\,\mathbf{B}_1 \equiv \mathbf{I} \pmod{m}$, niin $\mathbf{B}_1 \equiv \mathbf{B}_2 \pmod{m}$.

□

**Esimerkki 2.22** Koska

$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}\begin{bmatrix} 8 & -4 \\ -6 & 2 \end{bmatrix} = \begin{bmatrix} -4 & 0 \\ 0 & -4 \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \pmod{5}$$

ja

$$\begin{bmatrix} 8 & -4 \\ -6 & 2 \end{bmatrix}\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} = \begin{bmatrix} -4 & 0 \\ 0 & -4 \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \pmod{5},$$

niin matriisi $\begin{bmatrix} 8 & -4 \\ -6 & 2 \end{bmatrix}$ on matriisin $\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$ käänteismatriisi modulo 5.

**Huomautus 2.9** Matriisin $\mathbf{A}$ *determinantti* det($\mathbf{A}$) oletetaan tunnetuksi. Siitä käytetään myös merkintää $\Delta$.

Seuraava lause antaa helpon tavan löytää $2 \times 2$ −matriisille käänteismatriisi.

**Lause 2.16** *Olkoon* $\mathbf{A} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ *ja olkoon m positiivinen kokonaisluku. Jos* $(\Delta, m) = 1$, *niin matriisin* $\mathbf{A}$ *käänteismatriisi modulo m on*

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

*Todistus.* Vrt. [2], s.164. Koska $(\Delta, m) = 1$, niin luvun $\Delta$ käänteisluku modulo $m$ on olemassa. Nyt

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

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

ja

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

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

Määritelmän 2.8 mukaan matriisi $\mathbf{A}^{-1}$ on matriisin **A** käänteismatriisi modulo *m*.

□

**Esimerkki 2.23** Olkoon $\mathbf{A} = \begin{bmatrix} 2 & 2 \\ 1 & 2 \end{bmatrix}$. Nyt $\Delta = 2 \cdot 2 - 2 \cdot 1 = 2$. Koska luku 4 on luvun 2 käänteisluku modulo 7, niin $\overline{\Delta} = 4$. Koska (2, 7) = 1, niin lauseen 2.16 perusteella

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

**Huomautus 2.10** Matriisin **A** *adjungaatti* adj(**A**) oletetaan tunnetuksi.

**Lause 2.17** *Jos* **A** *on* $n \times n$ *−matriisi ja* $\det(\mathbf{A}) \neq 0$, *niin* $\mathbf{A}(\text{adj}\mathbf{A}) = \det(\mathbf{A})\mathbf{I}$.

*Todistus.* Ks. [4].

**Lause 2.18** *Olkoon* **A** $n \times n$ *−matriisi ja olkoon m sellainen positiivinen kokonaisluku, että* $(\Delta, m) = 1$. *Tällöin matriisin* **A** *käänteismatriisi modulo m on* $\mathbf{A}^{-1} = \overline{\Delta}(\text{adj}\mathbf{A})$.

*Todistus.* Vrt. [2], s.165. Koska $(\Delta, m) = 1$, niin $\Delta \neq 0$. Lauseen 2.17 perusteella $\mathbf{A}(\text{adj}\mathbf{A}) = \Delta\mathbf{I}$. Koska $(\Delta, m) = 1$, niin luvun $\Delta$ käänteisluku modulo *m* on olemassa. Nyt

$$\mathbf{A}(\overline{\Delta} \cdot \text{adj}\mathbf{A}) \equiv \mathbf{A} \cdot \text{adj}\mathbf{A} \cdot \overline{\Delta} \equiv \Delta \cdot \mathbf{I} \cdot \overline{\Delta} \equiv \Delta \cdot \overline{\Delta} \cdot \mathbf{I} \equiv \mathbf{I} \pmod{m}$$

ja

$$\overline{\Delta}(\text{adj}\mathbf{A})\mathbf{A} \equiv \overline{\Delta}(\text{adj}\mathbf{A} \cdot \mathbf{A}) \equiv \overline{\Delta} \cdot \Delta \cdot \mathbf{I} \equiv \mathbf{I} \pmod{m}.$$

Määritelmän 2.8 mukaan $\overline{\Delta}(\text{adj}\mathbf{A})$ on matriisin **A** käänteismatriisi modulo *m*.

□

**Esimerkki 2.24** Olkoon $\mathbf{A} = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 5 \\ 1 & 4 & 6 \end{bmatrix}$, jolloin $\Delta = -4$, $(\Delta, 7) = 1$ ja $\overline{\Delta} \equiv 5 \pmod 7$. Nyt

$$\mathbf{A}^{-1} = \overline{\Delta}(\text{adj}\mathbf{A}) = 5\begin{bmatrix} -8 & 0 & 4 \\ -1 & 3 & -2 \\ 2 & -2 & 0 \end{bmatrix} = \begin{bmatrix} -40 & 0 & 20 \\ -5 & 15 & -10 \\ 10 & -10 & 0 \end{bmatrix} \equiv \begin{bmatrix} 2 & 0 & 6 \\ 2 & 1 & 4 \\ 3 & 4 & 0 \end{bmatrix} \pmod 7.$$

Matriisin $\mathbf{A}$ käänteismatriisia $\mathbf{A}^{-1}$ voidaan käyttää ratkaistaessa kongruenssiyhtälöä

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

missä $(\det(\mathbf{A}), m) = 1$. Lauseen 2.13 perusteella voidaan yhtälön molemmat puolet kertoa matriisilla $\mathbf{A}^{-1}$, jolloin

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

**Esimerkki 2.25** Tarkastellaan kongruenssiyhtälöryhmää

$$x + 2y + 3z \equiv 1 \pmod 7$$
$$x + 2y + 5z \equiv 1 \pmod 7$$
$$x + 4y + 6z \equiv 1 \pmod 7.$$

Tämä voidaan kirjoittaa matriisien kongruenssina

$$\begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 5 \\ 1 & 4 & 6 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} \equiv \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \pmod 7.$$

Esimerkin 2.24 mukaan matriisin $\begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 5 \\ 1 & 4 & 6 \end{bmatrix}$ käänteismatriisi modulo 7 on $\begin{bmatrix} 2 & 0 & 6 \\ 2 & 1 & 4 \\ 3 & 4 & 0 \end{bmatrix}$. Nyt $\begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 2 & 0 & 6 \\ 2 & 1 & 4 \\ 3 & 4 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 8 \\ 7 \\ 7 \end{bmatrix} \equiv \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \pmod 7.$

# Luku 3 Wilsonin lause, Fermat´n pieni lause ja Eulerin lause

## *3.1 Wilsonin lause*

Vuonna 1770 julkaistussa kirjassa englantilainen matemaatikko Edward Waring väitti, että yksi hänen oppilaistaan, John Wilson, oli löytänyt tuloksen, että alkuluku $p$ jakaa luvun $(p-1)!+1$. Matemaatikko Waring oletti, että tämä Wilsonin otaksuma olisi vaikea todistaa. Kuitenkin jo vuonna 1771 Joseph Lagrange todisti tämän tuloksen ja se tunnetaan nimellä Wilsonin lause.

**Esimerkki 3.1** Olkoon $p = 7$. Nyt $(7-1)! = 6! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6$. Nähdään, että $2 \cdot 4 \equiv 1 \pmod 7$ ja $3 \cdot 5 \equiv 1 \pmod 7$. Järjestetään alkuperäisen kertoman tekijät uudelleen, jolloin $(7-1)! = 6! = 1 \cdot (2 \cdot 4) \cdot (3 \cdot 5) \cdot 6 \equiv 1 \cdot 6 \equiv -1 \pmod 7$.

**Lause 3.1 (Wilsonin lause)** *Jos p on alkuluku, niin* $(p-1)! \equiv -1 \pmod p$.

*Todistus*. Vrt. [2], s.198. Olkoon $p = 2$. Tällöin $(p-1)! = (2-1)! = 1 \equiv -1 \pmod 2$. Olkoon $p$ nyt lukua 2 suurempi alkuluku. Lauseen 2.8 perusteella kaikilla kokonaisluvuilla $a$, $1 \leq a \leq p-1$, on olemassa käänteisluku $\bar{a}$, $1 \leq \bar{a} \leq p-1$, jolla $a\bar{a} \equiv 1 \pmod p$. Lauseen 2.9 perusteella ainoat lukua $p$ pienemmät positiiviset kokonaisluvut, jotka ovat itsensä käänteislukuja, ovat luku 1 ja luku $p-1$. Nyt voidaan lukujen 2 ja $p-2$ välillä olevat kokonaisluvut järjestää $(p-3)/2$ kappaleeksi lukupareja, joiden tulot ovat kongruentteja luvun 1 kanssa modulo $p$. Tällöin

$$2 \cdot 3 \cdots (p-3) \cdot (p-2) \equiv 1 \pmod p.$$

Kerrotaan tämän kongruenssin molemmat puolet luvulla 1 ja luvulla $p-1$, jolloin

$$(p-1)! = 1 \cdot 2 \cdot 3 \cdots (p-3) \cdot (p-2) \cdot (p-1) \equiv 1 \cdot (p-1) \equiv -1 \pmod p.$$

□

**Huomautus 3.1** Seuraava lause osoittaa, että Wilsonin lause on tosi myös käänteisesti.

**Lause 3.2** *Jos $n$ on sellainen positiivinen kokonaisluku, että* $(n-1)! \equiv -1 \pmod{n}$*, niin $n$ on alkuluku.*

*Todistus.* Vrt. [2], s.199. Oletetaan, että $n$ ei ole alkuluku ja lisäksi $(n-1)! \equiv -1 \pmod{n}$. Koska $n$ ei ole alkuluku, niin $n = ab$, missä $1 < a < n$ ja $1 < b < n$. Koska $a < n$, niin $a \mid (n-1)!$, ja koska $(n-1)! \equiv -1 \pmod{n}$, niin $n \mid ((n-1)! + 1)$. Lauseen 1.1 perusteella myös luku $a$ jakaa luvun $(n-1)! + 1$. Koska $a \mid (n-1)!$ ja $a \mid ((n-1)! + 1)$, niin lauseen 1.2 perusteella $a \mid ((n-1)! + 1) - (n-1)! = 1$. Tämä on ristiriita, koska oletuksen perusteella $a > 1$.

□

**Esimerkki 3.2** Tarkastellaan lukua 11, joka on alkuluku. Nyt $(11-1)! = 10! = 3628800 = 329891 \cdot 11 - 1$. Siis $(11-1)! \equiv -1 \pmod{11}$. Tarkastellaan lukua 8. Nyt $(8-1)! = 7! = 5040 \equiv 0 \pmod{8}$. Siis luku 8 ei ole alkuluku.

### *3.2 Fermat´n pieni lause*

Pierre de Fermat esitti vuonna 1640 otaksuman, että luku $p$ jakaa luvun $a^{p-1} - 1$, jos $p$ on alkuluku ja $a$ on sellainen kokonaisluku, että $p \nmid a$. Leonhard Euler todisti otaksuman vuonna 1736 ja tulos tunnetaan nimellä Fermat´n pieni lause.

**Lause 3.3 (Fermat´n pieni lause)** *Jos $p$ on alkuluku, $a$ on positiivinen kokonaisluku ja $p \nmid a$, niin* $a^{p-1} \equiv 1 \pmod{p}$.

*Todistus.* Vrt. [2], s.199. Tarkastellaan kokonaislukujen joukkoa $\{a, 2a, 3a, \ldots, (p-2)a, (p-1)a\}$. Osoitetaan vastaoletuksella, että mikään joukon kokonaisluvuista ei ole jaollinen alkuluvulla $p$. Oletetaan, että $p \mid ja$, missä $1 \le j \le p-1$ ja $j$ on kokonaisluku. Koska $p \nmid a$, niin $(p, a) = 1$. Nyt apulauseen 1.2 perusteella $p \mid j$, mikä on mahdotonta, koska $1 \le j \le p-1$. Siis mikään joukon kokonaisluvuista ei ole jaollinen luvulla $p$ eli ne eivät ole kongruentteja luvun 0 kanssa modulo $p$. Osoitetaan lisäksi, että mitkään kaksi

joukon kokonaislukua eivät ole keskenään kongruentteja modulo $p$. Tehdään vastaoletus, että $ja \equiv ka \pmod{p}$, missä $1 \leq j < k \leq p - 1$. Koska $(a, p) = 1$, niin seurauksen 2.1 perusteella $j \equiv k \pmod{p}$. Tämä on mahdotonta, koska $1 \leq j < k \leq p - 1$. Koska joukon $\{a, 2a, 3a, \ldots, (p-2)a, (p-1)a\}$ kokonaisluvuista mikään ei ole kongruentti luvun 0 kanssa modulo $p$ ja koska mitkään kaksi joukon lukua eivät ole keskenään kongruentteja modulo $p$, niin tällöin lukujen $a, 2a, 3a, \ldots, (p-2)a, (p-1)a$ jäännösten täytyy olla luvut $1, 2, 3, \ldots, (p-2), (p-1)$ jossakin järjestyksessä. Tästä seuraa, että

$$a \cdot 2a \cdot 3a \cdots (p-2)a \cdot (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-2) \cdot (p-1) \pmod{p}.$$

Siis

$$a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}.$$

Koska $((p-1)!, p) = 1$, niin seurauksen 2.1 perusteella

$$a^{p-1} \equiv 1 \pmod{p}.$$

□

**Esimerkki 3.3** Tarkastellaan lukuja 5 ja 16. Luku 5 on alkuluku ja $5 \nmid 16$. Nyt $16^{5-1} = 16^4 = 65536 = 13107 \cdot 5 + 1$. Siis $16^{5-1} \equiv 1 \pmod{5}$.

**Esimerkki 3.4** Etsitään luvun $2^{20}$ jakojäännös modulo 7. Nähdään, että $2^{20} = (2^6)^3 \cdot 2 \cdot 2$. Koska $7 \nmid 2$, niin lauseen 3.3 perusteella $2^6 \equiv 1 \pmod{7}$. Lauseen 2.6 perusteella $(2^6)^3 \equiv 1 \pmod{7}$ ja lauseen 2.3 perusteella $(2^6)^3 \cdot 2 \cdot 2 \equiv 2 \cdot 2 \pmod{7}$. Siis $2^{20} \equiv 4 \pmod{7}$ eli luvun $2^{20}$ jakojäännös modulo 7 on 4.

**Lause 3.4** *Jos p on alkuluku ja a on positiivinen kokonaisluku, niin*

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

*Todistus.* Vrt. [2], s.200. Jos $p \nmid a$, niin lauseen 3.3 perusteella $a^{p-1} \equiv 1 \pmod{p}$. Kerrotaan kongruenssin molemmat puolet luvulla $a$, jolloin $a^p \equiv a \pmod{p}$. Jos luku $p$ jakaa luvun $a$, niin luku $p$ jakaa myös luvun $a^p$, jolloin $a^p \equiv a \equiv 0 \pmod{p}$.

□

**Esimerkki 3.5** Etsitään luvun $3^{18}$ jakojäännös modulo 17. Lauseen 3.4 perusteella $3^{17} \equiv 3 \pmod{17}$, jolloin lauseen 2.3 perusteella $3^{17} \cdot 3 \equiv 3 \cdot 3 \pmod{17}$. Siis $3^{18} \equiv 9 \pmod{17}$ eli luvun $3^{18}$ jakojäännös modulo 17 on 9.

**Lause 3.5** *Jos $p$ on alkuluku ja $a$ on sellainen kokonaisluku, että $p \nmid a$, niin $a^{p-2}$ on luvun $a$ käänteisluku modulo $p$.*

*Todistus.* Vrt. [2], s.200. Koska $p \nmid a$, niin lauseen 3.3 perusteella $a^{p-1} \equiv 1 \pmod{p}$. Koska $a^{p-1} = a \cdot a^{p-2}$, niin $a \cdot a^{p-2} \equiv 1 \pmod{p}$, jolloin määritelmän 2.6 mukaan $a^{p-2}$ on luvun $a$ käänteisluku modulo $p$.

□

**Esimerkki 3.6** Tarkastellaan lukuja 7 ja 8. Luku 7 on alkuluku ja $7 \nmid 8$. Lauseen 3.5 perusteella $8^{7-2} = 8^5 = 32768 \equiv 1 \pmod{7}$ on luvun 8 käänteisluku modulo 7, joka tosin on helppo nähdä suoraan ilman lausetta 3.5.

**Seuraus 3.1** *Olkoot $a$ ja $b$ positiivisia kokonaislukuja ja olkoon $p$ alkuluku. Jos $p \nmid a$, niin lineaarisen kongruenssiyhtälön $ax \equiv b \pmod{p}$ kokonaislukuratkaisut ovat*

$$x \equiv a^{p-2} b \pmod{p}.$$

*Todistus.* Vrt. [2], s.201. Olkoon $p$ alkuluku ja olkoot $a$ ja $b$ sellaisia positiivisia kokonaislukuja, että $p \nmid a$ ja $ax \equiv b \pmod{p}$. Kerrotaan kongruenssin molemmat puolet luvulla $a^{p-2}$, jolloin

$$a^{p-2} ax \equiv a^{p-2} b \pmod{p}.$$

Koska $p \nmid a$, niin lauseen 3.5 perusteella $a^{p-2}$ on luvun $a$ käänteisluku modulo $p$, jolloin

$$x \equiv a^{p-2} b \pmod{p}.$$

□

**Esimerkki 3.7** Tarkastellaan lineaarista kongruenssiyhtälöä $5x \equiv 13 \pmod{11}$. Koska luku 11 on alkuluku ja $11 \nmid 5$, niin seurauksen 3.1 perusteella kongruenssiyhtälön ratkaisu on $x \equiv 5^{11-2} \cdot 13 = 25390625 \equiv 7 \pmod{11}$. Sama tulos saatiin jo esimerkissä 2.13.

### *3.3 Eulerin lause*

Leonhard Euler esitti yleistyksen Fermat´n pienestä lauseesta. Fermat´n pienessä lauseessa luvun $p$ oli oltava alkuluku. Euler laajensi tarkastelun myös yhdistettyihin lukuihin ja todisti lauseen vuonna 1760. Ennen lauseen esitystä täytyy määritellä Eulerin phi-funktio, jota käytetään Eulerin lauseessa.

**Määritelmä 3.1 (Eulerin phi-funktio)** Olkoon $n$ positiivinen kokonaisluku. *Eulerin phi-funktio* $\phi(n)$ on niiden positiivisten kokonaislukujen $r$ ($\leq n$) määrä, jotka ovat suhteellisia alkulukuja luvun $n$ kanssa.

**Esimerkki 3.8** Tarkastellaan lukua 16. Luvut $r$ = 1, 3, 5, 7, 9, 11, 13 ja 15 toteuttavat ehdon $(r, 16) = 1$, jolloin $\phi(16) = 8$.

**Määritelmä 3.2 (Supistettu jäännössysteemi)** *Supistettu jäännössysteemi modulo n* on sellainen $\phi(n)$ kokonaisluvun joukko, että jokainen joukon alkio on suhteellinen alkuluku luvun $n$ kanssa ja mitkään kaksi joukon alkiota eivät ole keskenään kongruentteja modulo $n$.

**Esimerkki 3.9** Luvut $r$ = 1,5 toteuttavat ehdon $(r, 6) = 1$. Supistetussa jäännössysteemissä modulo 6 on $\phi(6) = 2$ alkiota. Siis joukko {1, 5} on supistettu jäännössysteemi modulo 6.

**Lause 3.6** *Jos* $\{r_1, r_2, \ldots, r_{\phi(n)}\}$ *on supistettu jäännössysteemi modulo n, a on positiivinen kokonaisluku ja* $(a, n) = 1$, *niin joukko* $\{ar_1, ar_2, \ldots, ar_{\phi(n)}\}$ *on myös supistettu jäännössysteemi modulo n.*

*Todistus.* Vrt. [2], s.216. Osoitetaan, että jokainen kokonaisluku $ar_j$, missä $1 \leq j \leq \phi(n)$, on suhteellinen alkuluku luvun $n$ kanssa. Tehdään vastaoletus, että $(ar_j, n) > 1$. Tällöin on olemassa sellainen alkuluku $p$, että $p \mid (ar_j, n)$. Siis $p \mid a$ ja $p \mid n$ tai $p \mid r_j$ ja $p \mid n$. Kuitenkaan ehdot $p \mid a$ ja $p \mid n$ eivät voi molemmat olla voimassa, koska oletuksen mukaan $(a, n) = 1$, eivätkä ehdot $p \mid r_j$ ja $p \mid n$ voi molemmat olla voimassa, koska $r_j$ kuuluu supistettuun jäännössysteemiin modulo $n$ eli $(r_j, n) = 1$. Siis jokainen kokonaisluku $ar_j$, missä $1 \leq j \leq \phi(n)$, on suhteellinen alkuluku luvun $n$ kanssa. Osoitetaan vielä, että mitkään kaksi luvuista $ar_j$ eivät ole keskenään kongruentteja modulo $n$. Tehdään vastaoletus, että $ar_j \equiv ar_k \pmod{n}$, missä $j$ ja $k$ ovat kokonaislukuja, $j \neq k$, $1 \leq j \leq \phi(n)$ ja $1 \leq k \leq \phi(n)$. Koska $(a, n) = 1$, niin seurauksen 2.1 perusteella $r_j \equiv r_k \pmod{n}$. Tämä ei kuitenkaan ole mahdollista, koska $r_j$ ja $r_k$ kuuluvat samaan supistettuun jäännössysteemiin modulo $n$, jolloin $r_j \not\equiv r_k \pmod{n}$. Siis mitkään kaksi luvuista $ar_j$ eivät ole keskenään kongruentteja modulo $n$.

□

**Esimerkki 3.10** Joukko {1, 2, 3, 4, 5, 6} on supistettu jäännössysteemi modulo 7. Koska (3, 7) = 1, niin lukujen $3 \cdot 1 = 3$, $3 \cdot 2 = 6$, $3 \cdot 3 = 9$, $3 \cdot 4 = 12$, $3 \cdot 5 = 15$ ja $3 \cdot 6 = 18$ muodostama joukko {3, 6, 9, 12, 15, 18} on myös supistettu jäännössysteemi modulo 7.

**Lause 3.7 (Eulerin lause)** *Jos m on positiivinen kokonaisluku ja a on sellainen kokonaisluku, että* $(a, m) = 1$, *niin*

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

*Todistus.* Vrt. [2], s.217. Olkoon $\{r_1, r_2, \ldots, r_{\phi(m)}\}$ supistettu jäännössysteemi modulo $m$. Koska $(a, m) = 1$, niin lauseen 3.6 perusteella joukko $\{ar_1, ar_2, \ldots, ar_{\phi(m)}\}$ on myös supistettu jäännössysteemi modulo $m$. Lukujen $ar_1, ar_2, \ldots, ar_{\phi(m)}$ jäännösten modulo $m$ on oltava luvut $r_1, r_2, \ldots, r_{\phi(m)}$ jossakin järjestyksessä. Tällöin

$$ar_1 ar_2 \cdots ar_{\phi(m)} \equiv r_1 r_2 \cdots r_{\phi(m)} \pmod{m},$$

eli

$$a^{\phi(m)} r_1 r_2 \cdots r_{\phi(m)} \equiv r_1 r_2 \cdots r_{\phi(m)} \pmod{m}.$$

Koska $(r_1, r_2, \ldots, r_{\phi(m)}, m) = 1$, niin seurauksen 2.1 perusteella $a^{\phi(m)} \equiv 1 \pmod{m}$.

□

Eulerin lausetta voidaan käyttää käänteislukujen modulo $m$ etsimiseen. Jos $a$ ja $m$ ovat suhteellisia alkulukuja, niin $a \cdot a^{\phi(m)-1} = a^{\phi(m)} \equiv 1 \pmod{m}$. Siis luvun $a$ käänteisluku modulo $m$ on $a^{\phi(m)-1}$.

**Esimerkki 3.11** Luvun 3 käänteisluku modulo 16 on $3^{\phi(16)-1} = 3^{8-1} = 3^7 = 2187 \equiv 11 \pmod{16}$.

Lineaarisen konruenssiyhtälön ratkaisemisessa voidaan käyttää hyväksi tätä ominaisuutta. Olkoon $ax \equiv b \pmod{m}$, missä $(a, m) = 1$. Kerrotaan kongruenssin molemmat puolet luvulla $a^{\phi(m)-1}$, jolloin

$$a^{\phi(m)-1} ax \equiv a^{\phi(m)-1} b \pmod{m}.$$

Kongruenssin $ax \equiv b \pmod{m}$ ratkaisuja ovat siis kaikki kokonaisluvut $x$, jotka toteuttavat yhtälön

$$x \equiv a^{\phi(m)-1} b \pmod{m}.$$

**Esimerkki 3.12** Vrt. [2], s.218, Tehtävä 11 a) Etsitään lineaarisen kongruenssiyhtälön $5x \equiv 3 \pmod{14}$ ratkaisut. Koska $\phi(14) = 6$, niin $x \equiv 5^{\phi(14)-1} \cdot 3 = 5^5 \cdot 3 = 9375 \equiv 9 \pmod{14}$.

## Lähteet

[1] Burton David M. Elementary number theory, Fifth Edition, The McGraw-Hill Companies, New York, 2005.

[2] Rosen Kenneth H. Elementary number theory and its applications, Fourth edition, Addison Wesley Longman, Reading, Massachusetts, 2000.

[3] Vanden Eynden Charles. Elementary Number Theory, Second edition, The McGraw-Hill Companies, Boston, 2001

[4] Pesonen Martti. Lineaarialgebra, luentomoniste, Joensuun yliopisto, 2006 [Verkkodokumentti]. URL http://www.joensuu.fi/matematiikka/kurssit/Lineaarialgebra/Kurssimateriaali/LAText/LinAlgMoniste.pdf [Viitattu 6.2.2006].