Kongruenssi

LuK-tutkielma
Jenni Limma
Matemaattisten tieteiden laitos
Oulun yliopisto
Syksy 2022

Sisällys

Johdanto

Tutkielmassa on käytetty pääasiassa teosta [1]. Ensimmäisessä luvussa esitellään kongruenssin määritelmä sekä tärkeimpiä tuloksia. Työssä käytetyt kongruenssin määritelmät ja huomautukset ovat todistettu Algebran perusteet kurssilla [2].
Kongruenssi tutkii eri jäännösluokkia, joita voidaan ratkaista myös kongruenssiyhtälöiden eli lineaaristen kongruenssien avulla. Kaikki esimerkit on itse keksittyjä, koska siten opitaan sisäistämään asia. Tällöin ei vain voi katsoa jostain suoraan, miten tämä tehtävä tehdään, vaan täytyy itse keksiä ratkaisu.
Luvussa 2 on esitelty ja todistettu Diofantoksen yhtälö. Diofantoksen yhtälö on hyödyllinen ratkaistaessa yhtälöä, jossa on kaksi muuttujaa, mutta vain yksi yhtälö. Sen avulla voidaan ratkaista myös kongruensseja. Diofantoksen yhtälö otettiin avuksi lukuun 3 lineaarisen kongruenssin todistamiseen. Lineaarinen kongruenssi on yksi tärkeimpiä asioita työssä, sillä sitä tarvitaan tulevissa esimerkeissä.
Luku 4 on työssä pääkohta. Siellä esitellään Kiinalainen jäännöslause, joka perustuu moniin lukuteorian määritelmiin. Kiinalainen jäännöslause on todella vanha keksintö, mutta todella hyödyllinen nykypäivänä salausjärjestelmissä. Ennen Kiinalaista jäännöslausetta käytettiin Kiinassa laskemaan sotilaiden lukumäärä, kun tiedettiin, kuinka paljon sotilaita oli eri riveillä, niin saatiin sen jakojäännökset eri luvuilla jaettaessa. Kiinalaisessa jäännöslauseessa ratkaistaan lineaarisia kongruensseja yhtäaikaa eli ratkaistaan lineaarista kongruenssiryhmää.
Lopuksi luvuissa 5 ja 6 perehdytään hieman Wilsonin lauseeseen sekä Ferman't pieneen lauseeseen. Näissä lauseissa tutkitaan, miten alkulukuja voi hyödyntää kongruensseissa.

1 Kongruenssin perustietoa

Kongruenssi syntyi 1800-luvun alussa Gaussin tekemänä. Kongruenssi on yksi lukuteorian tärkeimmistä kielistä.

Määritelmä 1.1. Jos a ja b ovat kokonaislukuja ja m on positiivinen kokonaisluku, sanotaan että *luku a on kongruentti luvun b kanssa modulo m*, jos $m \mid (a-b)$.

Merkitään

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

Jos $m \nmid (a-b)$, merkitään $a \not\equiv b \pmod{m}$ ja sanotaan, että a ei ole kongruentti luvun b kanssa modulo m.

Esimerkki 1.2. $17 \equiv 5 \pmod{2}$, koska $2 \mid (17-5)$. Huomataan myös, että $17 = 6 \cdot 2 + 5$.

Huomautus 1.3. Jos a ja b ovat kokonaislukuja ja m on positiivinen kokonaisluku, niin

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

jos ja vain jos on olemassa kokonaisluku k siten, että

$$a = b + km.$$

Esimerkki 1.4. $7 \equiv -1 \pmod{4}$, koska $7 = -1 + 2 \cdot 4$.

Huomautus 1.5. Olkoon a, b ja c kokonaislukuja sekä m positiivinen kokonaisluku. Tällöin toteutuvat seuraavat ehdot:

- Reflektiivisyys: $a \equiv a \pmod{m}$.
- Symmetrisyys: Jos $a \equiv b \pmod{m}$, niin $b \equiv a \pmod{m}$.
- Transitiivisuus: Jos $a \equiv b \pmod{m}$ ja $b \equiv c \pmod{m}$, niin $a \equiv c \pmod{m}$.

Huomautuksesta 1.5 huomataan, että kokonaislukujen joukko on jaettu m:ksi eri joukoksi, joita kutsutaan *kongruessiluokiksi modulo m*. Näistä joukoista jokainen sisältää kokonaislukuja, jotka ovat keskenään kongruentteja modulo m.

Lause 1.6. *Olkoon a, b ja c kokonaislukuja ja m positiivinen kokonaisluku siten, että $a \equiv b \pmod{m}$. Tällöin*

- $a + c \equiv b + c \pmod{m}$,
- $a - c \equiv b - c \pmod{m}$,
- $ac \equiv bc \pmod{m}$.

Esimerkki 1.7. Koska $25 \equiv 1 \pmod{6}$, niin lauseen 1.6 perusteella

- $28 = 25 + 3 \equiv 1 + 3 \equiv 4 \pmod{6}$
- $20 = 25 - 5 \equiv 1 - 5 \equiv -4 \pmod{6}$ ja
- $50 = 25 \cdot 2 \equiv 1 \cdot 2 \equiv 2 \pmod{6}$.

Seuraava lause on tärkeä, sillä siitä huomataan kongruenssin jakolaskusääntö, kun molemmat puolet jaetaan samalla kokonaisluvulla.

Lause 1.8. *Jos a, b ja c ovat kokonaislukuja ja m positiivinen kokonaisluku siten, että $syt(c, m) = d$ ja $ac \equiv bc \pmod{m}$, niin*

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

Todistus. Jos $ac \equiv bc \pmod{m}$, niin $m \mid (ac - bc)$ eli $m \mid c(a - b)$. Tällöin on olemassa kokonaisluku k siten, että $c(a - b) = km$. Kun molemmat puolet jaetaan luvulla d, saadaan $(c/d)(a - b) = k(m/d)$. Koska $syt(m/d, c/d) = 1$, niin $m/d \mid (a - b)$. Joten $a \equiv b \pmod{m/d}$. □

Esimerkki 1.9. Koska $40 \equiv 10 \pmod{15}$ ja $syt(10, 5) = 5$, niin huomataan, että $40/10 \equiv 10/10 \pmod{15/5}$ eli $4 \equiv 1 \pmod{3}$.

Seuraava seuraus on erikoistapaus lauseesta 1.8.

Seuraus 1.10. *Jos a, b ja c ovat kokonaislukuja ja m positiivinen kokonaisluku sekä $syt(c, m) = 1$ ja $ac \equiv bc \pmod{m}$, niin $a \equiv b \pmod{m}$.*

Esimerkki 1.11. Koska $22 \equiv 2 \pmod{5}$ ja $syt(2, 5) \equiv 1$, niin voidaan päätellä, että $22/2 \equiv 2/2 \pmod{5}$ eli $11 \equiv 1 \pmod{5}$.

Seuraava lause on yleisempi ja hyödyllisempi kuin lause 1.6.

Lause 1.12. *Olkoon a, b, c ja d kokonaislukuja ja m positiivinen kokonaisluku sekä $a \equiv b \pmod{m}$ ja $c \equiv d \pmod{m}$. Tällöin*

- $a + c \equiv b + d \pmod{m}$,
- $a - c \equiv b - d \pmod{m}$,
- $ac \equiv bd \pmod{m}$.

Esimerkki 1.13. Koska $7 \equiv -1 \pmod{4}$ ja $9 \equiv 5 \pmod{4}$, niin lauseen 1.12 perusteella $16 = 7 + 9 \equiv -1 + 5 \equiv 4 \equiv 0 \pmod{4}$, $2 = 9 - 7 \equiv 5 - 7 \equiv -2 \pmod{4}$ ja $63 = 7 \cdot 9 \equiv -1 \cdot 5 = -5 \pmod{4}$.

2 Diofantoksen yhtälö

Yhtälöä muodossa

$$ax + by = c,$$

missä a, b ja c ovat kokonaislukuja, sanotaan *lineaariseksi Diofantoksen yhtälöksi* kahdella muuttujalla. Diofantoksen yhtälö on yhtälö, jossa kertoimet ovat kokonaislukuja ja jolle etsitään kokonaislukuratkaisuja. Seuraavaksi otetaan muutama tärkeä asia huomioon ennen kuin voidaan todistaa Diofantoksen yhtälö.

Lause 2.1. *Olkoon a ja b kokonaislukuja ja ainakin toinen näistä nollasta eroava. Tällöin kokonaislukujen a ja b suurin yhteinen tekijä on olemassa yksikäsitteisenä. Lisäksi on olemassa kokonaisluvut s ja t siten, että*

$$as + bt = syt(a, b).$$

Lisäksi otetaan huomautus sekä lemma suurimpaan yhteiseen tekijään.

Huomautus 2.2. Olkoon a, b ja c kokonaislukuja siten, että $syt(a, b) = d$. Tällöin

- $syt(a/d, b/d) = 1$
- $syt(a + cb, b) = syt(a, b)$

Lemma 2.3. *Jos a, b ja c ovat sellaisia positiivisia kokonaislukuja, että $syt(a, b) = 1$ ja $a \mid bc$, niin $a \mid c$.*

Lause 2.4. ***Diofantoksen yhtälö***
Olkoon a ja b positiivisia kokonaislukuja ja $syt(a,b) = d$. Jos $d \nmid c$, niin yhtälöllä $ax+by = c$ ei ole ratkaisua. Jos $d \mid c$, niin yhtälöllä $ax+by = c$ on äärettömän monta ratkaisua. Jos $x = x_0$ ja $y = y_0$ on yhtälön $ax + by = c$ tietty ratkaisu, niin kaikki ratkaisut saadaan kaavalla

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

missä n on kokonaisluku.

Todistus. Olkoon x ja y kokonaislukuja siten, että

$$ax + by = c.$$

Koska $d \mid a$ ja $d \mid b$, niin myös $d \mid c$. Näin ollen jos $d \nmid c$, niin yhtälöllä ei ole ratkaisua.

Oletetaan, että $d \mid c$. Lauseen 2.1 perusteella

$$d = as + bt,$$

missä s ja t ovat kokonaislukuja. Koska $d \mid c$, niin on olemassa kokonaisluku e siten, että $de = c$. Kerrotaan yhtälön $d = as + bt$ molemmat puolet luvulla e, saadaan

$$c = de = (as + bt)e = a(se) + b(te).$$

Näin ollen yhtälön yksi ratkaisu on $x = x_0 = se$ ja $y = y_0 = te$.

Osoitetaan nyt, että ratkaisuja on äärettömän monta. Olkoon $x = se+(b/d)n$ ja $y = te - (a/d)n$, missä n on kokonaisluku. Huomataan, että x ja y on yhtälön ratkaisu, koska

$$ax + by = ax_0 + a(b/d)n + by_0 - b(a/d)n = ax_0 + by_0 = c.$$

Osoitetaan nyt, että yhtälön $ax+by = c$ kaikki ratkaisut täytyvät olla lauseen 2.4 väittämässä muodossa. Olkoon x ja y kokonaislukuja siten, että $ax+by = c$. Koska

$$ax_0 + by_0 = c,$$

niin vähentämällä tämän, huomataan, että

$$(ax + by) - (ax_0 + by_0) = 0.$$

Tästä saadaan

$$a(x - x_0) + b(y - y_0) = 0.$$

Siten

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

Jakamalla molemmat puolet luvulla d, saadaan

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

Huomautuksen 2.1 perusteella tiedetään, että $syt(a/d, b/d) = 1$. Lemman 2.3 perusteella $(a/d) \mid (y_0 - y)$. Tällöin on olemassa kokonaisluku n siten, että $(a/d)n = y_0 - y$ eli $y = y_0 - (a/d)n$. Nyt sijoitetaan tämä yhtälöön $a(x - x_0) = b(y_0 - y)$ luvun y paikalle, saadaan

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

Tästä ratkaisemalla luvun x, päästään tulokseen

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

□

Otetaan esimerkki havainnollistamaan, miten Diofantoksen yhtälöä voidaan käyttää.

Esimerkki 2.5. Ratkaistaan Diofantoksen yhtälö

$$60x + 18y = 96.$$

Ratkaistaan ensiksi $syt(60, 18)$ Eukleideen algoritmilla. Tällöin

$$\begin{aligned} 60 &= 3 \cdot 18 + 6 \\ 18 &= 3 \cdot 6, \end{aligned}$$

joten $syt(60, 18) = 6$. Nyt $6 \mid 96$ eli ratkaisu on olemassa.
Lineaarisella kombinaatiolla saadaan

$$6 = 60 \cdot 1 - 3 \cdot 18.$$

Kertomalla tämä yhtälö puolittain luvulla 16, saadaan

$$96 = 60 \cdot 16 + 18 \cdot (-48).$$

Diofantoksen yhtälön $60x + 18y = 96$ eräs ratkaisu on $x_0 = 16$ ja $y = -48$. Kaikki ratkaisut ovat

$$\begin{aligned} x &= x_0 + (b/d)n \\ &= 16 + (18/6)n \\ &= 16 + 3n \end{aligned}$$

ja

$$\begin{aligned} y &= y_0 - (a/d)n \\ &= -48 - (60/6)n \\ &= -48 - 10n, \end{aligned}$$

missä n on kokonaisluku.

3 Lineaarinen kongruenssi

Tässä luvussa mennään kongruensseihin, joissa on muuttuja x mukana. Keksitään myös keino, millä muuttuja x saadaan ratkaistua. Kongruenssia muodossa

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

missä x on tuntematon kokonaisluku, kutsutaan lineaariseksi kongruenssiksi, missä on vain yksi muuttuja x.

Lause 3.1. *Olkoon a ja b kokonaislukuja ja m positiivinen kokonaisluku sekä $syt(a, m) = d$. Jos $d \nmid b$, niin lineaarisella kongruenssilla*

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

ei ole ratkaisua.
Jos taas $d \mid b$, niin lineaarisella kongruenssilla

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

on ratkaisu. Lisäksi toisistaan modulo m eroavien ratkaisujen lukumäärä on d.

Todistus. Huomautuksen 1.3 mukaan lineaarinen kongruenssi $ax \equiv b \pmod{m}$ vastaa lineaarisen Diofantoksen yhtälön muotoa $ax - my = b$. Kokonaisluku x on lineaarisen kongruenssin $ax \equiv b \pmod{m}$ ratkaisu, jos ja vain jos on olemassa sellainen kokonaisluku y, että

$$ax - my = b.$$

Lauseen 2.4 perusteella tiedetään, että jos $d \nmid b$, niin yhtälöllä $ax - my = b$ ei ole ratkaisua. Jos taas $d \mid b$, niin yhtälöllä $ax - my = b$ on olemassa äärettömän monta ratkaisua. Tällöin

$$x = x_0 + (m/d)t \quad \text{ja} \quad y = y_0 + (a/d)t,$$

missä t on kokonaisluku sekä $x = x_0$ ja $y = y_0$ on yhtälön $ax - my = b$ eräs ratkaisu. Luvun x arvot

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

ovat lineaarisen kongruenssin

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

ratkaisut, joita on äärettömän monta.

Todistetaan seuraavaksi, että lineaarisen kongruenssin $ax \equiv b \pmod{m}$ kaikki ratkaisut on muotoa

$$x \equiv x_0 \pmod{m/d},$$

missä x_0 on eräs ratkaisu.
Olkoon x_0 lineaarisen kongruenssin $ax \equiv b \pmod{m}$ eräs ratkaisu ja

$$x_1 \equiv x_0 \pmod{m/d}.$$

Nyt $ax_0 \equiv b \pmod{m}$ ja $x_1 \equiv x_0 \pmod{m/d}$.
Siis

$$m/d \mid (x_1 - x_0),$$

joten

$$a \cdot m/d \mid a \cdot (x_1 - x_0).$$

Koska $d \mid a$, niin

$$a'm \mid ax_1 - ax_0,$$

missä $a' = a/d$ on kokonaisluku. Näin ollen $m \mid ax_1 - ax_0$ eli

$$ax_1 \equiv ax_0 \pmod{m}.$$

Huomautuksen 1.5 nojalla, koska $ax_0 \equiv b \pmod{m}$, saadaan

$$ax_1 \equiv b \pmod{m}.$$

Eli myös x_1 on lineaarisen kongruenssin $ax \equiv b \pmod{m}$ ratkaisu.

Todistetaan vielä, että ratkaisu on yksikäsitteinen modulo m/d.
Olkoon x_1 ja x_2 lineaarisen kongruenssin $ax \equiv b \pmod{m}$ kaksi ratkaisua, eli

$$ax_1 \equiv b \pmod{m} \text{ ja } ax_2 \equiv b \pmod{m}.$$

Huomautuksen 1.5 nojalla

$$ax_1 \equiv ax_2 \pmod{m}.$$

Nyt lauseen 1.8 perusteella

$$x_1 \equiv x_2 \pmod{m/d}.$$

Näiden todistusten perusteella lineaarisen kongruenssin $ax \equiv b \pmod{m}$ kaikki ratkaisut ovat muotoa

$$x \equiv x_0 \pmod{m/d}.$$

□

Otetaan esimerkki havainnollistamaan lineaarisen kongruenssin ratkaisua.

Esimerkki 3.2. Etsitään kaikki ratkaisut lineaariselle kongruenssille

$$12x \equiv 6 \pmod{15}.$$

Huomataan ensin, että $syt(12, 15) = 3$ ja $3 \mid 6$. Eli ratkaisu on olemassa.
Tällöin voidaan supistaa ja saadaan

$$\begin{aligned} & 12x \equiv 6 \pmod{15} \quad |: 3 \\ \Leftrightarrow \quad & 4x \equiv 2 \pmod{5}. \end{aligned}$$

Voidaan löytää ensimmäinen ratkaisu kokeilemalla. Kokeilemalla saadaan eräs ratkaisu $x_0 = 3$, koska $4 \cdot 3 \equiv 2 \pmod{5}$.
Kaikki ratkaisut ovat

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

Eli ratkaisuja ovat $\ldots -2, 3, 8, 13 \ldots$
Nyt on siis voimassa

$$x = 3 + 5k,$$

missä k on kokonaisluku.
Tai voidaan käyttää apuna Eukleideen algoritmia. Otetaan supistettu muoto

$$4x \equiv 2 \pmod{5},$$

jossa $syt(4, 5) = 1$, joten Eukleideen algoritmilla saadaan

$$\begin{aligned} 5 &= 1 \cdot 4 + 1 \\ 4 &= 4 \cdot 1. \end{aligned}$$

Tästä saadaan lineaarikombinaatiolla

$$\begin{aligned} & 1 = 5 - 1 \cdot 4 \quad | \cdot 2 \\ \Leftrightarrow \quad & 2 = 2 \cdot 5 - 2 \cdot 4. \end{aligned}$$

Tällöin yksi ratkaisu on $x_0 = -2$. Eli ratkaisuja ovat $\ldots -7, -2, 3, 8, 13 \ldots$.

Lasketaan vielä esimerkki lineaarisesta kongruenssista käyttämällä apuna Diofantoksen yhtälöä.

Esimerkki 3.3. Etsitään ratkaisu lineaariselle kongruenssille

$$15x - 3 \equiv 2x + 4 \pmod{47}.$$

Muokataan ensiksi lineaarinen kongruenssi muotoon $ax \equiv b \pmod{m}$:

$$\begin{aligned} & 15x - 3 \equiv 2x + 4 \pmod{47} \\ \Leftrightarrow \quad & 15x - 2x \equiv 4 + 3 \pmod{47} \\ \Leftrightarrow \quad & 13x \equiv 7 \pmod{47}. \end{aligned}$$

Huomataan, että $syt(13, 47) = 1$, joten ratkaisu on olemassa. Ratkaisun löytämiseksi käytetään apuna Diofantoksen yhtälöä $13x - 47y = 7$.
Eukleideen algoritmilla saadaan

$$\begin{aligned} 47 &= 3 \cdot 13 + 8 \\ 13 &= 1 \cdot 8 + 5 \\ 8 &= 1 \cdot 5 + 3 \\ 5 &= 1 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \\ 2 &= 2 \cdot 1. \end{aligned}$$

Lineaarikombinaatiolla saadaan

$$\begin{aligned} 1 &= 3 - 1 \cdot 2 \\ 1 &= 3 - (5 - 1 \cdot 3) \cdot 1 \\ 1 &= 3 \cdot 2 - 5 \cdot 1 \\ 1 &= (8 - 1 \cdot 5) \cdot 2 - 5 \cdot 1 \\ 1 &= 8 \cdot 2 - 3 \cdot 5 \\ 1 &= 8 \cdot 2 - 3 \cdot (13 - 1 \cdot 8) \\ 1 &= 8 \cdot 5 - 3 \cdot 13 \\ 1 &= (47 - 3 \cdot 13) \cdot 5 - 3 \cdot 13 \\ 1 &= 47 \cdot 5 - 18 \cdot 13 \qquad | \cdot 7 \\ 7 &= 47 \cdot 5 \cdot 7 - 18 \cdot 13 \cdot 7 \\ 7 &= 47 \cdot 35 - 126 \cdot 13 \end{aligned}$$

Näin ollen Diofantoksen yhtälön yksi ratkaisu on $x_0 = -126$ ja $y_0 = 35$. Kaikki ratkaisut lineaariselle kongruenssille ovat

$$x \equiv -126 \equiv 15 \pmod{47}.$$

Eli ratkaisuja ovat $\ldots -126, -79, -32, 15, 62, 109 \ldots$.
Nyt on siis voimassa yhtälö

$$x = 15 + 47k,$$

missä k on kokonaisluku.

Tarkastellaan nyt lineaarista kongruenssia $ax \equiv 1 \pmod{m}$. Lauseen 3.1 perusteella saadaan lineaarisen kongruenssin ratkaisu jos ja vain jos $syt(a, m) = 1$ ja nämä kaikki ratkaisut ovat kongruentteja modulo m. Annetulla kokonaisluvulla a ratkaisu lineaariselle kongruenssille $ax \equiv 1 \pmod{m}$ on luvun a *käänteisluku modulo* m eli kokonaislukuratkaisua x kutsutaan luvun a käänteisluvuksi modulo m.

4 Kiinalainen jäännöslause

Luvussa 1 käsiteltiin perustietoja, joita oli käsitelty suurinta osaa Algebran perusteet kurssilla. Tässä luvussa mennään pidemmälle ja asioihin, joita ei olla vielä käsitelty. Käsitellään lineaarista kongruenssiryhmää. Tarkastellaan myös sitä, kun yhdellä muuttujalla on kaksi tai useampi lineaarinen kongruenssi eri moduloilla.
Kiinalaisessa jäännöslauseessa on lineaarinen kongruenssiryhmä, joissa kaikissa on sama muuttuja x eli vain yksi muuttuja, mutta eri moduloja.

Lause 4.1. ***Kiinalainen jäännöslause***
Olkoon $m_1, m_2, \ldots, m_r$ positiivisia kokonaislukuja, jotka ovat pareittain keskenään jaottomia. Tällöin kongruenssiyhtälöryhmälle

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

on yksikäsitteinen ratkaisu modulo $M = m_1 m_2 \cdots m_r$.

Todistus. Merkitään

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

Tällöin $syt(M_k, m_k) = 1$. Näin ollen luvulla M_k on aina olemassa käänteisluku y_k modulo m_k. Silloin voidaan kirjoittaa $M_k y_k \equiv 1 \pmod{m_k}$. Nyt saadaan muodostettua summa

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \ldots + a_r M_r y_r.$$

Kokonaisluku x on nyt ratkaisu kongruenssiryhmälle.

Todistetaan ensin, että

$$x \equiv a_k \pmod{m_k},$$

kun $k = 1, 2, \ldots, r$.
Koska $m_k \mid M_j$, kun $j \neq k$, niin $M_j \equiv 0 \pmod{m_k}$ eli $a_j M_j y_j \equiv 0 \pmod{m_k}$.
Siten luku x jokaisella $k = 1, 2, \ldots, r$ voidaan kirjoittaa muotoon

$$x \equiv 0 + 0 + \ldots + a_k M_k y_k + \ldots + 0 + 0 \pmod{m_k}.$$

Koska $M_k y_k \equiv 1 \pmod{m_k}$, niin

$$x \equiv a_k M_k y_k \equiv 1 \cdot a_k \equiv a_k \pmod{m_k}.$$

Näin ollen x on kongruenssiryhmän ratkaisu.
Seuraavaksi todistetaan, että mitkä tahansa kaksi ratkaisua ovat kongruentteja modulolla M eli todistetaan, että ratkaisu on yksikäsitteinen modulo M. Olkoot x_0 ja x_1 kaksi ratkaisua kongruenssiryhmälle. Siten jokaista kokonaislukua k kohti on olemassa $x_0 \equiv x_1 \equiv a_k \pmod{m_k}$ eli jokaista kokonaislukua k kohti $m_k \mid (x_0 - x_1)$. Koska luvun M tulontekijät m_i ovat keskenään jaottomia, niin $M \mid (x_0 - x_1)$, joten $x_0 \equiv x_1 \pmod{M}$. Tämä siis osoittaa, että r määrälle kongruensseja on samanaikainen ratkaisu yksikäsitteisesti modulo M. Kongruenteista ratkaisuista saadaan siis yksiselitteinen ratkaisujoukko. □

Kongruenssiyhtälöryhmälle voidaan käyttää suoraa ratkaisukaavaa, joka helpottaa ratkaisun saamista. Ratkaisukaavana käytetään todistuksen summalauseketta, mutta modulon mukaan ratkaisuja on äärettömän monta. Tästä summasta voidaan saada myös pienin luku modulolla, mutta usein ratkaisu silti esitetään yhtälömuodossa. Otetaan esimerkki havainnollistamaan Kiinalaista jäännöslausetta.

Esimerkki 4.2. Ratkaistaan yhtälöryhmä

$$\begin{aligned} x &\equiv 1 \pmod{2} \\ x &\equiv 2 \pmod{5} \\ x &\equiv 3 \pmod{7} \end{aligned}$$

Kiinalaisen jäännöslauseen avulla.
Huomataan ensin, että modulot ovat keskenään jaottomia, joten tehtävä on mahdollista ratkaista Kiinalaisella jäännöslauseella.
Lasketaan ensin modulojen tulo $M = 2 \cdot 5 \cdot 7 = 70$.
Lasketaan seuraavaksi luvut $M_k = M/m_k$. Saadaan $M_1 = 70/2 = 35, M_2 = 70/5 = 14$ ja $M_3 = 70/7 = 10$.

Tarvitaan vielä kaikille luvuille M_k käänteisluvut y_k modulo m_k.
Luku y_1 saadaan ratkaisemalla yhtälö $35y_1 \equiv 1 \pmod 2$. Ratkaisuksi saadaan $y_1 \equiv 1 \pmod 2$.
Luku y_2 saadaan puolestaan ratkaisemalla yhtälö $14y_2 \equiv 1 \pmod 5$, josta saadaan $y_2 \equiv 4 \pmod 5$.
Luku y_3 saadaan yhtälöllä $10y_3 \equiv 1 \pmod 7$, josta saadaan $y_3 \equiv 5 \pmod 7$.
Nyt voidaan laskea ratkaisukaavan avulla x

$$\begin{aligned} x &= a_1y_1M_1 + a_2y_2M_2 + a_3y_3M_3 \\ &= 1 \cdot 1 \cdot 35 + 2 \cdot 4 \cdot 14 + 3 \cdot 5 \cdot 10 \\ &= 297 \end{aligned}$$

Vastaus on siis

$$x \equiv 297 \pmod{70}$$

eli

$$x \equiv 17 \pmod{70}.$$

Pienin mahdollinen positiivinen kokonaislukuratkaisu on siis 17.

On kehitetty myös iteratiivinen menetelmä, jolla voi laskea samanaikaisia kongruenssiryhmiä. Otetaan tästä seuraavaksi esimerkki.

Esimerkki 4.3. Ratkaistaan yhtälöryhmä

$$\begin{aligned} x &\equiv 1 \pmod 7 \\ x &\equiv 2 \pmod 8 \\ x &\equiv 3 \pmod 9. \end{aligned}$$

Huomautuksen 1.3 perusteella ensimmäinen kongruenssi voidaan kirjoittaa muotoon $x = 7t + 1$, missä t on kokonaisluku. Sijoitetaan tämä toiseen kongruenssiin muuttujan x paikalle. Tällöin saadaan

$$7t + 1 \equiv 2 \pmod 8,$$

josta saadaan ratkaisuksi $t \equiv 7 \pmod 8$. Taas huomautuksen 1.3 avulla saadaan $t = 8u+7$, missä u on kokonaisluku. Siten $x = 7(8u+7)+1 = 56u+50$. Sijoitetaan tämä lauseke muuttujalle x kolmanteen kongruenssiin. Näin saadaan

$$56u + 50 \equiv 3 \pmod 9.$$

Kun tämä kongruenssi ratkaistaan, saadaan $u \equiv 8 \pmod 9$. Huomautuksen 1.3 mukaan $u = 9v + 8$, missä v on kokonaisluku. Nyt

$$x = 56(9v + 8) + 50 = 504v + 498.$$

Kun tämä yhtälö käännetään kongruenssiksi saadaan

$$x \equiv 498 \pmod{504}.$$

Näin ollaan saatu ratkaistua yhtälöryhmä.

Huomataan kuitenkin, että äskeisen esimerkin menetelmää voidaan käyttää vain ratkaisemaan peräkkäisiä lineaarisia kongruensseja sekä silloin, kun kongruenssien modulot ovat keskenään jaottomia ja kongruenssien on oltava yhdenmukaisia.

5 Wilsonin lause

Tutkitaan seuraavassa kahdessa luvussa, miten alkulukuja voi hyödyntää kongruensseissa. Tässä luvussa käsitellään tärkeää kongruenssia, *Wilsonin lausetta*, joka on usein hyödyllinen lukuteoriassa. Wilsonin lause on hyödyllinen erityisesti kongruensseissa, joissa on mukana kertomia.

Otetaan ensin huomautus, jota tarvitaan Wilsonin lauseen todistuksessa.

Huomautus 5.1. Olkoon p alkuluku. Tällöin positiivinen kokonaisluku a on itsensä käänteisluku modulo p jos ja vain jos $a \equiv 1 \pmod{p}$ tai $a \equiv -1 \pmod{p}$. Eli $a \equiv 1 \pmod{p}$ tai $a \equiv p-1 \pmod{p}$.

Todistus. Jos $a \equiv 1 \pmod{p}$ tai $a \equiv -1 \pmod{p}$, niin $a^2 \equiv 1 \pmod{p}$. Tällöin huomataan, että a on itsensä käänteisluku modulo p.
Toisaalta, jos a on itsensä käänteisluku modulo p, niin $a^2 = a \cdot a \equiv 1 \pmod{p}$. Tällöin $p \mid (a^2 - 1)$. Koska $a^2 - 1 = (a-1)(a+1)$, niin joko $p \mid (a-1)$ tai $p \mid (a+1)$. Näin ollen $a \equiv 1 \pmod{p}$ tai $a \equiv -1 \pmod{p}$. □

Lause 5.2. ***Wilsonin lause***
Jos p on alkuluku, niin

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

Todistus. Kun $p = 2$, niin

$$(p-1)! \equiv 1 \equiv -1 \pmod{2}.$$

Eli Wilsonin lause toteutuu, kun $p = 2$.
Olkoon nyt p alkuluku, mikä on suurempi kuin 2. Lauseen 3.1 ja huomautuksen 5.1 perusteella jokaiselle kokonaisluvulle a, kun $1 < a < p-1$, on olemassa käänteisluku $\hat{a}$ modulo p, missä $1 < \hat{a} < p-1$. Tällöin

$$a\hat{a} \equiv 1 \pmod{p}.$$

Huomautuksen 5.1 mukaan luvun a käänteisluku modulo p on eri suuri kuin luku a itse. Siksi voidaan jakaa kokonaisluvut luvusta 2 lukuun $p-2$ erillisiin kokonaislukupareihin niin, että jokaisen parin tulo on kongruentti luvun 1 kanssa modulo p. Kertomalla nämä parit keskenään saadaan

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

Kerrotaan yhtälön molemmat puolet luvuilla 1 sekä $(p-1)$, ja huomataan, että $(p-1) = -1 \pmod{p}$. Näin saadaan

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

eli

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

□

Otetaan esimerkki Wilsonin lauseesta.

Esimerkki 5.3. Olkoon $p = 5$. Tällöin

$$4! \equiv -1 \pmod{5}.$$

Toisaalta

$$(5-1)! = 4! = 1 \cdot 2 \cdot 3 \cdot 4 = 24.$$

Järjestellään tulontekijät uudelleen ryhmittämällä ne yhteen käänteisparit modulo 5. Huomataan, että $2 \cdot 3 \equiv 1 \pmod{5}$. Tällöin

$$4! \equiv 1 \cdot (2 \cdot 3) \cdot 4 \equiv 1 \cdot 4 \equiv -1 \pmod{5}.$$

Otetaan toinen esimerkki Wilsonin lauseesta.

Esimerkki 5.4. Olkoon $p = 11$. Tällöin

$$10! \equiv -1 \pmod{11}.$$

Toisaalta

$$(11-1)! = 10! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 = 3628800.$$

Järjestellään tulontekijät uudelleen ryhmittämällä ne yhteen käänteisparit modulo 11. Huomataan, että $2 \cdot 6 \equiv 1 \pmod{11}, 3 \cdot 4 \equiv 1 \pmod{11}, 5 \cdot 9 \equiv \pmod{11}$ ja $7 \cdot 8 \equiv 1 \pmod{11}$. Tällöin

$$10! \equiv 1 \cdot (2 \cdot 6) \cdot (3 \cdot 4) \cdot (5 \cdot 9) \cdot (7 \cdot 8) \cdot 10 \equiv 1 \cdot 10 \equiv -1 \pmod{11}.$$

6 Fermat'n pieni lause

Kun kongruenssissa on eksponentteja, niin seuraava lause on todella hyödyllinen.

Lause 6.1. ***Fermat'n pieni lause***
Jos p on alkuluku ja a on positiivinen kokonaisluku siten, että $syt(a,p) = 1$ eli $p \nmid a$, niin

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

Todistus. Tarkastellaan kokonaislukuja

$$a, 2a, \ldots, (p-1)a,$$

joita on $p-1$ kappaletta. Yksikään näistä kokonaisluvuista ei ole jaollinen luvulla p, sillä jos $p \mid ja$, niin Lemman 2.3 perusteella $p \mid j$. Tämä on mahdotonta, koska $1 \leq j \leq p-1$. Lisäksi mitkään kaksi kokonaislukua $a, 2a, \ldots, (p-1)a$ eivät ole keskenään kongruentteja modulo p.
Oletetaan, että

$$ja \equiv ka \pmod{p}.$$

Seurauksen 1.10 perusteella $j \equiv k \pmod{p}$, koska $syt(a,p) = 1$. Tämä on mahdotonta, koska j ja k ovat positiivisia kokonaislukuja, jotka ovat pienempiä kuin p.
Näin ollen kokonaisluvut $a, 2a, \ldots, (p-1)a$ ovat $p-1$ kappaletta kokonaislukuja, jotka eivät ole kongruentteja nollan kanssa modulo p, eivätkä ole keskenään kongruentteja modulo p. Tästä voidaan päätellä, että varmasti

$$1 \cdot 2 \cdot \ldots \cdot (p-1) \equiv a \cdot 2a \cdot \ldots \cdot (p-1)a \pmod{p}$$

ja siten

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

Koska $syt((p-1)!, p) = 1$ eli p ei ole luvun $(p-1)!$ tekijä, niin seurauksen 1.10 perusteella voidaan supistaa kongruenssin molemmilta puolilta luku $(p-1)!$. Tällöin saadaan

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

□

Otetaan todistukselle avuksi esimerkki.

Esimerkki 6.2. Olkoon $p = 5$ ja $a = 2$. Tällöin

$$\begin{aligned} 1 \cdot 2 &\equiv 2 \pmod 5 \\ 2 \cdot 2 &\equiv 4 \pmod 5 \\ 3 \cdot 2 &\equiv 1 \pmod 5 \\ 4 \cdot 2 &\equiv 3 \pmod 5. \end{aligned}$$

Näin ollen

$$(1 \cdot 2) \cdot (2 \cdot 2) \cdot (3 \cdot 2) \cdot (4 \cdot 2) \equiv 2 \cdot 4 \cdot 1 \cdot 3 \pmod 5$$

eli

$$2^4 \cdot 1 \cdot 2 \cdot 3 \cdot 4 \equiv 2 \cdot 4 \cdot 1 \cdot 3 \pmod 5.$$

Siten

$$2^4 \cdot 4! \equiv 4! \pmod 5,$$

joten

$$2^4 \equiv 1 \pmod 5.$$

Otetaan toinen esimerkki Ferman't pienesta lauseesta.

Esimerkki 6.3. Etsitään positiivinen jakojäännös $2^{98} \pmod 7$ Fermat'n pienen lauseen avulla. Tiedetään, että

$$2^6 \equiv 1 \pmod 7.$$

Siten

$$2^{98} = (2^6)^{16} \cdot 2^2 \equiv 4 \pmod 7.$$

Joskus halutaan, että Fermat'n pieni lause pätee kaikille positiivisille kokonaisluvuille a, kun alkuluku on p. Tällöin täytyy käyttää seuraavaa lausetta, joka on seuraus Fermat'n pienestä lauseesta.

Lause 6.4. *Jos p on alkuluku ja a on positiivinen kokonaisluku, niin*

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

Todistus. Jos $p \nmid a$, niin Fermat'n pienen lauseen perusteella $a^{p-1} \equiv 1 \pmod p$. Kun kerrotaan tämän kongruenssin molemmat puolet luvulla a, saadaan $a^p \equiv a \pmod p$.
Jos $p \mid a$, niin myös $p \mid a^p$ eli $a^p \equiv a \equiv 0 \pmod p$. Tästä saadaan $a^p \equiv a \pmod p$.
Tämä viimeistelee todistuksen, koska $a^p \equiv a \pmod p$, jos $p \nmid a$ ja jos $p \mid a$. □

Esimerkki 6.5. Luvut 5 ja 7 ovat alkulukuja, niin

$$2^5 = 32 \equiv 2 \pmod{5}$$

ja

$$6^7 = 279926 \equiv 6 \pmod{7}.$$

Lähdeluettelo

[1] Kenneth H. Rosen: *Elementary Number Theory and Its Applications*, AT and T Informotion Systems Laboratories, kesäkuu 1986

[2] Kari Myllylä, Markku Niemenmaa, Topi Törmä: *Algebran perusteet*, Oulun yliopisto, Luentomoniste 2022