Tampereen yliopisto

Briitta Korsulainen

KIINALAINEN JÄÄNNÖSLAUSE JA POLYNOMIKONGRUENSSIT

Informaatioteknologian ja viestinnän tiedekunta
Kandidaattitutkielma
Marraskuu 2020

Tiivistelmä

Briitta Korsulainen: Kiinalainen jäännöslause ja polynomikongruenssit
Kandidaattitutkielma
Tampereen yliopisto
Matematiikan ja tilastotieteen tutkinto-ohjelma
Marraskuu 2020

Tutkielma kuuluu matematiikassa lukuteorian osa-alueeseen. Lukuteoria tarkastelee erityisesti positiivisten kokonaislukujen ominaisuuksia, joista tärkein on jaollisuus. Sen lisäksi tarkastellaan myös alkulukuja. Jaollisuuden avulla voidaan edelleen määritellä kongruenssi, jonka ominaisuuksiin tämä tutkielma pitkälti painottuu.

Kongruenssilla on matematiikassa useita hyödyllisiä sovelluksia esimerkiksi tietojen salausta käsittelevässä kryptografiassa, mutta myös arkitodellisuudessa. Tässä tutkielmassa perehdytään kongruenssin ja polynomikongruenssien teoreettiseen taustaan ja esitellään eräs menetelmä muotoa $f(x) \equiv 0$ modulo m olevien polynomikongruenssien ratkaisemiseen. Apuna käytetään kiinalaista jäännöslausetta sekä Henselin lemmaa. Tutkielma nojaa vahvasti kirjallisuuteen, jonka pohjalta lauseet on esitetty. Lukijalta odotetaan jonkin verran lukuteorian alkeiden tuntemusta, vaikkakin työn kannalta keskeisimpiä käsitteitä on esitelty tutkielman alussa myöhempiä lauseita ja todistuksia varten.

Kiinalainen jäännöslause on kätevä työkalu arkistenkin matemaattisten ongelmien ratkaisemisessa. Tunnettu esimerkki lauseen soveltamisesta on vanha kiinalainen ongelma, jossa pyritään ratkaisemaan sotilaiden lukumäärä, kun tiedetään sen jakojäännökset eri luvuilla jaettaessa. Näistä tiedoista muodostetaan kongruenssiryhmä, joka voidaan ratkaista kiinalaisen jäännöslauseen avulla.

Polynomikongruenssi $f(x) \equiv 0$ modulo m voidaan ratkaista suoraan kiinalaisen jäännöslauseen avulla, jos modulona oleva luku m on yhdistetty luku, joka voidaan jakaa pareittain suhteellisiin alkulukuihin. Jos taas luku m on muotoa p^2, missä p on alkuluku, niin ratkaisu löydetään Henselin lemman avulla etsimällä ensin ratkaisu modulo p. Nostoperiaatteen avulla saadaan ratkaisut modulo p^k, kun tiedetään ratkaisut modulo p^{k-1}. Näitä eri tapauksia käsitellään tutkielman lopussa havainnollistavin esimerkein.

Avainsanat: kongruenssi, kiinalainen jäännöslause, Henselin lemma,
polynomikongruenssit, lukuteoria

Sisällys

1 Johdanto

Lukuteorialla on useita käytännön sovelluksia niin tieteessä kuin arkielämässäkin. Tärkein käsite lukuteoriassa on (erityisesti positiivisten kokonaislukujen) jaollisuus, jonka ominaisuuksiin tämäkin työ pohjautuu. Arjessa esimerkiksi karamellien jakaminen ystävien kesken perustuu jaollisuuden määritelmään, vaikkei sitä todennäköisesti tulekaan ajatelleeksi. Karamellien jakaja voi havaita, että tietyillä karamellimäärillä karamellejä ei koskaan voi jakaa tasan useammalle kuin yhdelle ystävälle, ellei ystäviä sitten ole täsmälleen yhtä monta kuin karamelleja. Tällöin on kyse alkuluvuista. Jako menee tasan, jos karamellien lukumäärä on jaollinen ystävien lukumäärällä, mutta mikäli näin ei ole, jää osa karamelleista jakamatta tai kaikki eivät saa samaa määrää karamelleja. Tällöin jää yli jakojäännös, mistä päästään erääseen tämän tutkielman pääkäsitteistä, nimittäin kongruenssiin. Tässä tutkielmassa keskitytään kuitenkin tarkastelemaan erilaisia kongruensseja hieman teoreettisemmasta näkökulmasta.

Tutkielman aluksi luvussa 2 käydään läpi kertauksenomaisesti muutamia lukuteorian peruskäsitteitä, mutta lukijan oletetaan tuntevan joitakin lukuteorian perustuloksia, kuten kahden kokonaisluvun suurimman yhteisen tekijän määrittämisen Eukleideen algoritmin avulla.

Luvussa 3 esitellään vanhaa kiinalaista alkuperää oleva kiinalainen jäännöslause ja todistetaan se. Lauseen käyttöä yhden muuttujan kongruenssiryhmien ratkaisemisessa havainnollistetaan tunnetun esimerkin avulla.

Tutkielman viimeinen luku keskittyy polynomikongruenssiyhtälöiden ratkaisumenetelmään. Luvussa todistetaan tutkijansa Kurt Henselin mukaan nimetty Henselin lemma, joka tarjoaa oivan keinon ratkaista muotoa $f(x) \equiv 0$ modulo m olevia kongruenssiyhtälöitä, kun $f(x)$ on kokonaislukukertoiminen polynomi ja m jokin positiivinen kokonaisluku.

Tutkielmassa esitetyt määritelmät, lauseet ja todistukset pohjautuvat melko suoraan Kenneth H. Rosenin kirjaan *Elementary number theory and its applications* joitakin poikkeuksia lukuunottamatta. Esimerkit ovat tekijän keksimiä tai lähteistä poimittuja harjoitustehtäviä, jotka tekijä on ratkaissut ellei muuta ole mainittu.

2 Peruskäsitteitä

Luvussa 2 esitetään lyhyesti joitakin myöhemmin tarvittavia määritelmiä ja lauseita. Näiden esitietoina olevien lauseiden todistukset ohitetaan.

2.1 Alkuluvut ja yhdistetyt luvut

Määritelmä 2.1 (vrt. [3, s. 66])**.** Kokonaisluku $p > 1$ on *alkuluku*, jos sillä ei ole muita positiivisia kokonaislukutekijöitä kuin triviaalit tekijät 1 ja p.

Esimerkki 2.1. Luvut 2, 5, 11, 23 ja 37 ovat alkulukuja.

Määritelmä 2.2 (vrt. [3, s. 66])**.** Lukua 1 suurempi kokonaisluku on *yhdistetty luku*, jos se ei ole alkuluku.

Esimerkki 2.2. Luvut $6 = 2 \cdot 3$, $142 = 2 \cdot 71$ ja $250 = 2 \cdot 5^3$ ovat yhdistettyjä lukuja.

2.2 Jaollisuus ja suurin yhteinen tekijä

Määritelmä 2.3 (vrt. [1, s. 20])**.** Olkoot $a, b \in \mathbb{Z}$. Tällöin luku a on luvun b *tekijä*, jos

$$b = ka$$

jollakin kokonaisluvulla k. Voidaan myös sanoa, että luku b on *jaollinen* luvulla a. Tätä merkitään $a \mid b$. Jos luku b ei ole jaollinen luvulla a, merkitään $a \nmid b$.

Esimerkki 2.3. Luku 9 on jaollinen luvulla 3 eli $3 \mid 9$, mutta luku 7 ei ole jaollinen luvulla 5 eli $5 \nmid 7$.

Määritelmä 2.4 (Suurin yhteinen tekijä, vrt. [3, s. 80])**.** Olkoot $a \neq 0$ tai $b \neq 0$. Tällöin kokonaislukujen a ja b *suurin yhteinen tekijä* on suurin kokonaisluku, joka jakaa sekä luvun a että luvun b. Tässä tutkielmassa lukujen a ja b suurimmalle yhteiselle tekijälle käytetään notaatiota $\text{syt}(a, b)$.

Esimerkki 2.4. Lukujen 25 ja 15 suurin yhteinen tekijä on 5, sillä $25 = 5^2$ ja $15 = 3 \cdot 5$.

Määritelmä 2.5 (vrt. [3, s. 80])**.** Kokonaislukujen a ja b sanotaan olevan *suhteellisia alkulukuja*, jos niille pätee $\text{syt}(a, b) = 1$.

Esimerkki 2.5. Luvut 36 ja 49 ovat suhteellisia alkulukuja, sillä $36 = 2^2 \cdot 3^2$ ja $49 = 7^2$, joten siis niiden suurin yhteinen tekijä on $\text{syt}(36, 42) = 1$.

2.3 Kongruenssi

Määritelmä 2.6 (vrt. [3, s. 128])**.** Olkoot a ja b kokonaislukuja ja m positiivinen kokonaisluku. Nyt jos $m \mid (a - b)$, niin sanotaan, että luku a on *kongruentti* luvun b kanssa modulo m. Tätä merkitään notaatiolla $a \equiv b \pmod{m}$. Jos $m \nmid (a - b)$, niin merkitään $a \not\equiv b \pmod{m}$.

Esimerkki 2.6. Luku 14 on kongruentti luvun 2 kanssa modulo 4, sillä $4 \mid (14 - 2)$. Voidaan siis merkitä $14 \equiv 2 \pmod{4}$.

Lause 2.1. *Olkoot a, b, c ja m sellaisia kokonaislukuja, että $m > 0$, $d = \text{syt}(c, m)$ ja $ac \equiv bc \pmod{m}$. Tällöin*

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

Todistus. Ks. [3, s. 131]. □

Lause 2.2. *Jos a ja b ovat kokonaislukuja, niin $a \equiv b \pmod{m}$, jos ja vain jos on olemassa sellainen kokonaisluku k, että $a = b + km$.*

Todistus. Ks. [3, s.129]. □

Lause 2.3 (Kongruenssin perusominaisuuksia)**.** *Olkoon $n > 1$ kiinteä ja olkoot a, b, c, d mielivaltaisia kokonaislukuja. Tällöin kongruenssilla on voimassa seuraavat ominaisuudet:*

(a) $a \equiv a \pmod{n}$.

(b) *Jos* $a \equiv b \pmod{n}$, *niin* $b \equiv a \pmod{n}$.

(c) *Jos* $a \equiv b \pmod{n}$ *ja* $b \equiv c \pmod{n}$, *niin* $a \equiv c \pmod{n}$.

(d) *Jos* $a \equiv b \pmod{n}$ *ja* $b \equiv c \pmod{n}$, *niin* $a + c \equiv b + d \pmod{n}$ *ja* $ac \equiv bd \pmod{n}$.

(e) *Jos* $a \equiv b \pmod{n}$, *niin* $a + c \equiv b + c \pmod{n}$ *ja* $ac \equiv bc \pmod{n}$.

(f) *Jos* $a \equiv b \pmod{n}$, *niin* $a^k \equiv b^k \pmod{n}$ *jokaisella* $k \geq 0$.

Todistus. Ks. [1, s. 66–67]. □

Määritelmä 2.7 (vrt. [3, s. 140])**.** Oletetaan, että luvut a ja m ovat kokonaislukuja. Tällöin kongruenssin

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

kokonaislukuratkaisua x kutsutaan luvun *käänteisluvuksi* modulo m.

Lause 2.4. *Olkoon p alkuluku. Tällöin positiivinen kokonaisluku a on itsensä käänteisluku modulo p, jos ja vain jos $a \equiv 1 \pmod{p}$ tai $a \equiv -1 \pmod{p}$.*

Todistus. Ks. [3, s. 141]. □

Lause 2.5. *Olkoot a, b ja m sellaisia kokonaislukuja, että $m > 0$ ja $\mathrm{syt}(a, m) = d$. Jos $d \nmid b$, niin kongruenssilla $ax \equiv b \pmod{m}$ ei ole ratkaisuja. Jos $d \mid b$, niin kongruenssilla $ax \equiv b \pmod{m}$ on täsmälleen d kappaletta epäkongruentteja ratkaisuja modulo m.*

Todistus. Ks. [3, s.139–140]. □

3 Kiinalainen jäännöslause

3.1 Historiaa

Kiinalainen jäännöslause tarjoaa menetelmän, jolla voidaan ratkaista vanha kiinalainen ongelma, jossa pohditaan kiinalaisten sotilaiden jakamista riveihin. Haluttiin siis selvittää sotilaiden lukumäärä, kun tiedetään, että jaettaessa sotilaiden lukumäärä kolmella jakojäännös on yksi, jaettaessa viidellä jakojäännös on kaksi ja jaettaessa seitsemällä jäännös on kolme. Tämä voidaan esittää kongruenssiyhtälönä

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

Esitetään seuraavaksi lause ja todistus, joiden avulla ongelma voidaan ratkaista ja sen jälkeen esimerkkilaskussa vastaus kysymykseen.

3.2 Kiinalainen jäännöslause

Lause 3.1. *Olkoot $m_1, m_2, \ldots, m_r (\geq 2)$ pareittain suhteellisia positiivisia alkulukuja. Silloin kongruenssiryhmällä*

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

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

Todistus (vrt. [3, s. 144–145] ja [2, s. 9]). Todistetaan lause kahdessa osassa. Ensin kohdassa 1 konstruoidaan ratkaisu ja sen jälkeen kohdassa 2 osoitetaan ratkaisun olevan yksikäsitteinen.

1. Merkitään $M_k = \frac{M}{m_k} = m_1 m_2 \cdots m_{k-1} m_{k+1} \cdots m_r$, kun $1 \leq k \leq r$. Nyt $\text{syt}(M_k, m_k) = 1$, sillä luvut $m_1, m_2, \ldots, m_r$ ovat oletuksen nojalla pareittain suhteellisia alkulukuja. Siis luvulla M_k on olemassa lauseen 2.4 mukainen käänteisluku y_k, jolla $M_k y_k \equiv 1 \pmod{m_k}$.

Osoitetaan nyt, että kongruenssiryhmän ratkaisu on

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_r M_r y_r. \tag{3.1}$$

Kokonaisluku x on yhtäaikainen ratkaisu kaikille alkuperäisille kongruenssille, joita on r kappaletta. Tämä käy ilmi, kun osoitetaan, että $x \equiv a_k \pmod{m_k}$. Koska $m_k \mid M_j$ aina, kun $j \neq k$, niin $M_j \equiv 0 \pmod{m_k}$ jaollisuuden ja kongruenssin määritelmien nojalla. Edellä todettiin, että $M_k y_k \equiv 1 \pmod{m_k}$, joten $x \equiv a_k \pmod{m_k}$. Siis x on kongruenssiryhmän ratkaisu.

2. Tehdään vastaoletus eli oletetaan, että lauseen 3.1 kongruenssiryhmällä on kaksi ratkaisua x_0 ja x_1. Tällöin $x_0 \equiv x_1 \equiv a_k \pmod{m_k}$ jokaisella luvulla $k = 1, 2, \ldots, r$ ja voidaan merkitä kongruenssin määritelmän nojalla, että jokaisella luvulla k pätee $m_k \mid (x_0 - x_1)$. Siis $M \mid (x_0 - x_1)$ eli $x_0 \equiv x_1 \pmod{M}$. Tämä on ristiriita sen oletuksen kanssa, että ratkaisuja olisi kaksi, joten siis ratkaisun on oltava yksikäsitteinen.

□

Esimerkki 3.1 (Sotilaiden lukumäärän selvittäminen, vrt. [3, s. 145])**.** Ratkaistaan kongruenssiyhtälö

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

Havaitaan, että luvut 3, 5 ja 7 ovat pareittain suhteellisia alkulukuja, joten voidaan hyödyntää kiinalaista jäännöslausetta. Sen mukaan kongruenssiryhmällä on yksikäsitteinen ratkaisu modulo $3 \cdot 5 \cdot 7$ eli modulo 105. Nyt kiinalaisen jäännöslauseen todistuksen avulla saadaan

$$\begin{aligned} M &= 3 \cdot 5 \cdot 7 = 105, \\ M_1 &= \frac{105}{3} = 35, \\ M_2 &= \frac{105}{5} = 21, \\ M_3 &= \frac{105}{7} = 15. \end{aligned}$$

Lisäksi luvuilla on M_k on olemassa sellaiset käänteisluvut y_k, että

$$35y_1 \equiv 1 \pmod 3 \Leftrightarrow 70y_1 \equiv 2 \pmod 3 \Leftrightarrow y_1 \equiv 2 \pmod 3,$$
$$21y_2 \equiv 1 \pmod 5 \Leftrightarrow y_2 \equiv 1 \pmod 5 \quad \text{ja}$$
$$15y_3 \equiv 1 \pmod 7 \Leftrightarrow y_3 \equiv 1 \pmod 7.$$

Nyt saadaan ratkaisu

$$\begin{aligned} x &\equiv a_1M_1y_1 + a_2M_2y_2 + a_3M_3y_3 \pmod{105} \\ &\equiv 1 \cdot 35 \cdot 2 + 2 \cdot 21 \cdot 1 + 3 \cdot 12 \cdot 1 \pmod{105} \\ &\equiv 157 \pmod{105} \\ &\equiv 52 \pmod{105}. \end{aligned}$$

Sotilaita on siis 52 kappaletta.

4 Polynomikongruenssit

Tutkitaan seuraavaksi muotoa $f(x) \equiv 0 \pmod{m}$ olevien kongruenssiyhtälöiden ratkaisemista, kun funktio $f(x)$ on määritelmän 4.1 mukainen kokonaislukukertoiminen polynomi. Kongruenssiyhtälöitä voidaan ratkaista esimerkiksi keksijänsä, saksalaisen matemaatikko Kurt Henselin (1891-1941) mukaan nimetyn Henselin lemman avulla. Lemma esitetään aliluvussa 4.2. Määritellään aluksi funktio $f(x)$ ja sen derivaattafunktio $f'(x)$.

Määritelmä 4.1. Olkoon f sellainen funktio, että

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

missä a_i on reaaliluku ja $i = 1, 2, \ldots, n$. Tällöin funktion $f(x)$ derivaattafunktio $f'(x)$ voidaan esittää muodossa

$$f'(x) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + a_1.$$

Määritellään myös, että merkintä $f^{(k)}(x)$ tarkoittaa polynomin $f(x)$ k. derivaattaa.

4.1 Aputuloksia

Esitetään seuraavaksi kolme apulausetta, joita tarvitaan myöhemmin Henselin lemman todistuksen yhteydessä. Kahden ensimmäisen lauseen todistukset sivuutetaan. Kolmannen lauseen todistuksessa on korjattu lähteessä ollut painovirhe.

Apulause 4.1. Olkoot $f(x)$ ja $g(x)$ polynomeja ja c vakio. Tällöin

$$(f+g)'(x) = f'(x) + g'(x) \text{ ja} \tag{4.1}$$

$$(cf)'(x) = c(f'(x)). \tag{4.2}$$

Oletetaan edelleen, että k on positiivinen kokonaisluku, jolloin

$$(f+g)^{(k)}(x) = f^{(k)}(x) + g^{(k)}(x) \text{ ja} \tag{4.3}$$

$$(cf)^{(k)}(x) = c(f^{(k)}(x)). \tag{4.4}$$

Todistus. Sivuutetaan. □

Apulause 4.2. Jos m ja k ovat positiivisia kokonaislukuja ja $f(x) = x^m$, niin

$$f^{(k)}(x) = m(m-1)\cdots(m-k+1)x^{m-k}.$$

Todistus. Sivuutetaan. □

Apulause 4.3. Jos $f(x)$ on kokonaislukukertoiminen, astetta n oleva polynomi, niin silloin

$$f(a+b) = f(a) + f'(a)b + \frac{f''(a)}{2!}b^2 + \cdots + \frac{f^{(n)}(a)}{n!}b^n,$$

missä kertoimet 1, $f'(a)$, $\frac{f''(a)}{2!}$, ..., $\frac{f^{(n)}(a)}{n!}$ ovat kokonaislukuja.

Todistus (vrt. [3, s. 156]). Todistetaan lause binomikaavan (ks. [3, s. 521-522]) avulla. Jokainen astetta n oleva polynomi f on funktioiden x^m ($m \leq n$) monikertojen summa. Koska lauseen 4.1 nojalla

$$(f+g)^{(k)}(x) = f^{(k)}(x) + g^{(k)}(x),$$

niin riittää osoittaa, että väite pätee myös polynomeilla $f_m(x) = x^m$. Binomikaavasta saadaan

$$(a+b)^m = \sum_{j=0}^{m} \binom{m}{j} a^{m-j}b^j.$$

Lisäksi lauseen 4.2 nojalla tiedetään, että

$$f_m^{(j)}(a) = m(m-1)\cdots(m-j+1)a^{m-j}.$$

Näin ollen

$$\frac{f_m^{(j)}(a)}{j!} = \binom{m}{j} a^{m-j}.$$

Koska kombinaatio $\binom{m}{j}$ on kokonaisluku aina, kun m ja j ovat sellaisia kokonaislukuja, että $0 \leq j \leq m$, niin myös kertoimet $\frac{f_m^{(j)}(a)}{j!}$ ovat kokonaislukuja. □

Nyt voidaan esittää Henselin lemmana tunnettu lause, jonka avulla voidaan ratkaista polynomikongruenssiyhtälöitä.

4.2 Henselin lemma

Lause 4.1 (Henselin lemma)**.** *Oletetaan, että $f(x)$ on kokonaislukukertoiminen polynomi, k (≥ 2) on kokonaisluku, p on alkuluku ja r on kongruenssin $f(x) \equiv 0 \pmod{p^{k-1}}$ ratkaisu. Tällöin*

1. *jos* $f'(r) \not\equiv 0 \pmod{p}$*, niin on olemassa sellainen yksikäsitteinen kokonaisluku* t *(*$0 \leq t < p$*), että*

$$f(r + tp^{k-1}) \equiv 0 \pmod{p^k},$$

kun

$$t \equiv -\overline{f'(r)}\frac{f(r)}{p^{k-1}} \pmod{p}.$$

Tässä merkintä $\overline{f'(r)}$ *tarkoittaa luvun f'(r) käänteislukua modulo p.*

2. *jos* $f'(r) \equiv 0 \pmod{p}$ *ja* $f(r) \equiv 0 \pmod{p^k}$*, niin jokaisella kokonaisluvulla t pätee*

$$f(r + tp^{k-1}) \equiv 0 \pmod{p^k}.$$

3. *jos* $f'(r) \equiv 0 \pmod{p}$ *ja* $f(r) \not\equiv 0 \pmod{p^k}$*, niin kongruenssiyhtälöllä* $f(x) \equiv 0 \pmod{p^k}$ *ei ole sellaisia ratkaisuja, että kongruenssi* $x \equiv r \pmod{p^{k-1}}$ *olisi voimassa.*

Todistus (vrt. [3, s. 156–157]). Määritetään ensin luku t. Jos s on kongruenssin $f(r) \equiv 0 \pmod{p^k}$ ratkaisu, niin se on myös kongruenssin $f(r) \equiv 0 \pmod{p^{k-1}}$ ratkaisu. Silloin on olemassa kongruenssin $f(x) \equiv 0 \pmod{p^{k-1}}$ sellainen ratkaisu r, että $s \equiv r \pmod{p^{k-1}}$. Tällöin $s = r + tp^{k-1}$ jollakin kokonaisluvulla t. Määritetään siis ehdot luvulle t. Lauseesta 4.3 seuraa, että

$$f(r + tp^{k-1}) = f(r) + f'(r)tp^{k-1} + \frac{f''(r)}{2!}(tp^{k-1})^2 + \cdots + \frac{f^{(n)}(r)}{n!}(tp^{k-1})^n, \tag{4.5}$$

missä $\frac{f^{(k)}(r)}{k!}$ on kokonaisluku ja $k = 1, 2, \ldots, n$. Oletuksen nojalla $k \geq 2$, mistä seuraa, että $k \leq m(k-1)$ ja $p^k \mid p^{m(k-1)}$ aina, kun $2 \leq m \leq n$. Siis yhtälöstä (4.5) supistuvat pois kaikki termit lukuunottamatta kahta ensimmäistä modulo p^k, joten saadaan kongruenssiyhtälö

$$f(r + tp^{k-1}) \equiv f(r) + f'(r)tp^{k-1} \pmod{p^k}. \tag{4.6}$$

Tiedetään myös, että $r + tp^{k-1}$ on kongruenssin $f(x) \equiv 0 \pmod{p^{k-1}}$ ratkaisu, joten sijoittamalla ja järjestämällä termit uudelleen saadaan yhtälö (4.6) muotoon

$$f(r) + f'(r)tp^{k-1} \equiv 0 \pmod{p^k} \tag{4.7}$$

$$f'(r)tp^{k-1} \equiv -f(r) \pmod{p^k}. \tag{4.8}$$

Kongruenssi (4.8) voidaan edelleen jakaa luvulla p^{k-1}, sillä alussa todettiin, että $f(r) \equiv 0 \pmod{p^{k-1}}$. Tällöin saadaan kongruenssi

$$\frac{f'(r)tp^{k-1}}{p^{k-1}} \equiv \frac{-f(r)}{p^{k-1}} \pmod{\frac{p^k}{p^{k-1}}} \tag{4.9}$$

$$f'(r)t \equiv \frac{-f(r)}{p^{k-1}} \pmod{p} \tag{4.10}$$

$$t \equiv \frac{-f(r)}{p^{k-1}} \cdot \overline{f'(r)} \pmod{p}. \tag{4.11}$$

Tässä merkintä $\overline{f'(r)}$ tarkoittaa luvun $f'(r)$ käänteislukua modulo p.

Tarkastellaan sitten erikseen lauseen tapaukset 1–3 tutkimalla kongruenssin (4.11) ratkaisuja modulo p.

Oletetaan ensin, että $f'(r) \not\equiv 0 \pmod{p}$. Tästä seuraa, että $\text{syt}(f'(r), p) = 1$ ja lauseen 2.5 nojalla kongruenssilla (4.11) on yksikäsitteinen ratkaisu modulo p. Siis kohta 1 on todistettu.

Oletetaan sitten, että $f'(r) \equiv 0 \pmod{p}$ ja $f(r) \equiv 0 \pmod{p^k}$. Tällöin ensimmäisestä oletuksesta seuraa, että $\text{syt}(f'(r), p) = p$. Lisäksi luku p jakaa luvun $\frac{f(r)}{p^{k-1}}$, jos ja vain jos $f(r) \equiv 0 \pmod{p^k}$, mikä on oletuksen nojalla voimassa. Tällöin lauseen 2.5 nojalla kaikki parametrin t saamat arvot ovat kongruenssin (4.10) ratkaisuja. Tämä tarkoittaa, että $x = r + tp^{k-1}$ on ratkaisu, kun $t = 0, 1, \ldots, p-1$. Siis kohta 2 pätee.

Lopuksi oletetaan, että $f'(r) \equiv 0 \pmod{p}$, mutta luku p ei jaa lukua $\frac{f(r)}{p^{k-1}}$. Jälleen $\text{syt}(f'(r), p) = p$, mutta $f(r) \not\equiv 0 \pmod{p^k}$, jolloin lauseen 2.5 nojalla kongruenssilla ei ole ratkaisuja millään luvulla t. Siis myös kohta 3 on todistettu. □

Henselin lemmasta seuraa niin sanottu nostoperiaate, jonka avulla saadaan nostettua kongruenssiyhtälön ratkaisu modulo p^k, kun tiedetään ratkaisu modulo p^{k-1}.

Seuraus 4.1 (Nostoperiaate)**.** *Oletetaan, että p on alkuluku ja r_1 polynomikongruenssin $f(x) \equiv 0 \pmod{p}$ ratkaisu. Jos $f'(r_1) \not\equiv 0 \pmod{p}$, niin on olemassa sellainen yksikäsitteinen ratkaisu r_k modulo p^k, missä $k = 2, 3, \ldots$, että*

$$r_k = r_{k-1} - f(r_{k-1})\overline{f'(r_1)}$$

missä luku $\overline{f'(r_1)}$ on luvun $f'(r_1)$ käänteisluku modulo p.

Todistus ([3, s. 157]). Oletetaan, että $f'(r_1) \not\equiv 0 \pmod{p}$, jolloin Henselin lemman kohdan 1) nojalla ratkaisu r_1 nostaa yksikäsitteisen ratkaisun r_2 modulo p^2 ja $r_2 =$

$r_1 + tp$, missä $t = -\overline{f'(r_1)}\frac{f(r_1)}{p}$. Sijoittamalla saadaan

$$r_2 = r_1 + tp = r_1 + (-\overline{f'(r_1)}\frac{f(r_1)}{p})p = r_1 - \overline{f'(r_1)}f(r_1).$$

Koska $r_2 \equiv r_1$, niin tästä seuraa suoraan, että $f'(r_2) \equiv f'(r_1) \not\equiv 0 \pmod{p}$. Käyttämällä uudelleen Henselin lemmaa, havaitaan, että on olemassa myös yksikäsitteinen ratkaisu r_3 modulo p^3, joka on jälleen muotoa

$$r_3 = r_2 + tp^2 = r_2 + (-\overline{f'(r_2)}\frac{f(r_2)}{p^2}).$$

Koska edellä todettiin, että $f'(r_2) \equiv f'(r_1) \not\equiv 0 \pmod{p}$, niin ratkaisu r_3 saadaan muotoon

$$r_3 = r_2 + (-\overline{f'(r_1)}\frac{f(r_2)}{p^2})p^2 = r_2 - \overline{f'(r_1)}f(r_2).$$

Jatkamalla tätä havaitaan seurauksen pätevän jokaisella kokonaisluvulla $k \geq 2$. □

4.3 Esimerkkejä

Seuraavat esimerkit havainnollistavat kiinalaisen jäännöslauseen ja Henselin lemman käyttöä polynomikongruenssiyhtälöiden ratkaisemisessa. Aluksi käsitellään tapausta, jossa modulona on yhdistetty luku.

Esimerkki 4.1 (vrt. [3, s. 159], teht. 6)**.** Ratkaistaan kongruenssiyhtälö

$$x^8 - x^4 + 1001 \equiv 0 \pmod{539}. \tag{4.12}$$

Luku 539 voidaan esittää muodossa $7^2 \cdot 11$, joten yhtälö (4.12) voidaan jakaa kahteen yhtälöön, joissa on eri modulot. Nämä voidaan yhdistää kongruenssiryhmäksi

$$\begin{aligned} x^8 - x^4 + 1001 &\equiv 0 \pmod{49} \\ x^8 - x^4 + 1001 &\equiv 0 \pmod{11}. \end{aligned}$$

Olkoon funktio $f(x) = x^8 - x^4 + 1001$, ja muodostetaan sen derivaatta $f'(x) = 8x^7 - 4x^3$. Ylemmän kongruenssin ratkaisuiksi r_1 saadaan kokeilemalla $r_1 = 0, 1, 6$. Tutkitaan seuraavaksi funktion f derivaattafunktiota luvun r_1 arvoilla 0, 1, 6. Kun $r_1 = 0$, niin $f'(0) = 0 \equiv 0 \pmod{7}$ ja $f(0) = 1001 \not\equiv 0 \pmod{49}$, joten Henselin lemman kohdan 3 nojalla kongruenssiyhtälöllä ei ole ratkaisuja. Kun $r_1 = 1$, saadaan derivaatan arvoksi $f'(1) = 4$ ja luku 4 ei ole kongruentti luvun 0 kanssa modulo 7,

joten Henselin lemman kohdan 1 nojalla yhtälöllä on muotoa $x = 1 + 7t_1$ oleva ratkaisu. Luku t_1 saadaan ratkaistua kongruenssista

$$t_1 \equiv -\overline{f'(1)}\frac{f(1)}{7} = -\bar{4}\frac{1001}{7} = -2 \cdot \frac{1001}{7} \equiv 8 \equiv 1 \pmod 7.$$

Siis yksi ratkaisu on $x = 1 + 7 \equiv 8 \pmod{49}$. Lopuksi tutkitaan tapausta $r_1 = 6$. Nyt derivaataksi saadaan $f'(6) \equiv 3 \not\equiv 0 \pmod 7$, joten jälleen Henselin lemman kohdan 1 nojalla yhtälöllä on ratkaisu $x = 6 + 7t_2$, jossa

$$t_2 \equiv -\overline{f'(6)}\frac{f(6)}{7} \equiv 5 \pmod 7$$

Näin ollen yhtälön toinen ratkaisu on $x = 6 + 7 \cdot 5 = 41 \pmod{49}$.

Kokeilemalla saadaan alemman yhtälön ratkaisuiksi $x = 0, 1, 10 \pmod{11}$. Muuta tarkastelua ei tässä tarvita, sillä modulona oleva luku 11 on jo valmiiksi alkuluku ja kertoo suoraan yhtälön ratkaisun.

Koska luvut 11 ja 49 ovat pareittain suhteellisia alkulukuja, niin voidaan hyödyntää lausetta 3.1 (kiinalainen jäännöslause). Saadaan kongruenssiryhmä

$$\begin{aligned} &x \equiv 8 \text{ tai } x \equiv 41 \pmod{49} \\ &x \equiv 0 \text{ tai } x \equiv 1 \text{ tai } x \equiv 10 \pmod{11}. \end{aligned}$$

Luku $M = 49 \cdot 11 = 539$ ja luvut M_k ovat

$$\begin{aligned} M_1 &= \frac{539}{49} = 11, \\ M_2 &= \frac{539}{11} = 49. \end{aligned}$$

Lukujen M_k käänteisluvut y_k ovat

$$\begin{aligned} &11y_1 \equiv 1 \pmod{49} \Leftrightarrow 99y_1 \equiv 9 \pmod{49} \Leftrightarrow y_1 \equiv 9 \pmod{49}, \\ &49y_2 \equiv 1 \pmod{11} \Leftrightarrow y_2 \equiv 9 \pmod{11}. \end{aligned}$$

Nyt saadaan ratkaisu

$$\begin{aligned} x \equiv\ & 8 \cdot 11 \cdot 9 + 0 \cdot 49 \cdot 9, 8 \cdot 11 \cdot 9 + 1 \cdot 49 \cdot 9, \\ & 8 \cdot 11 \cdot 9 + 10 \cdot 49 \cdot 9, 41 \cdot 11 \cdot 9 + 0 \cdot 49 \cdot 9, \\ & 41 \cdot 11 \cdot 9 + 1 \cdot 49 \cdot 9, 41 \cdot 11 \cdot 9 + 10 \cdot 49 \cdot 9 \pmod{539} \\ \equiv\ & 253, 155, 351, 286, 188, 384 \pmod{539}. \end{aligned}$$

Siis kongruenssiyhtälön (4.12) ratkaisut ovat $x = 155, 188, 253, 286, 351, 384$ modulo 539.

Tutkitaan sitten tapausta, jossa modulona on muotoa p^k oleva luku, kun p on alkuluku ja $k = 2, 3, \ldots$.

Esimerkki 4.2 (vrt. [3, s. 159], teht. 3)**.** Ratkaistaan kongruenssiyhtälö

$$x^2 + x + 47 \equiv 0 \pmod{2401}. \tag{4.13}$$

Huomataan, että modulo 2401 voidaan esittää muodossa $2401 = 7^4$. Olkoon funktio $f(x) = x^2 + x + 47$, jolloin sen derivaatta $f'(x)$ on määritelmän 4.1 nojalla $f'(x) = 2x + 1$. Tutkitaan aluksi, milloin kongruenssiyhtälö $f(x) \equiv 0 \pmod 7$ on voimassa. Kokeilemalla saadaan ratkaisuiksi $r_{11} = 1$ ja $r_{12} = 5$. Lisäksi todetaan, että derivaatat $f'(1) = 3$ ja $f'(5) = 11$ eivät ole kongruentteja luvun 0 kanssa modulo 7. Lisäksi luvuille $f'(1)$ ja $f'(5)$ saadaan käänteisluvut $\overline{f'(1)} = \overline{3} = 5 \pmod 7$ ja $\overline{f'(5)} = \overline{4} = 2 \pmod 7$. Nyt seurauksen 4.1 avulla saadaan ratkaisut

$$r_{21} = r_{11} - f(r_{11})\overline{f'(r_{11})} = 1 - f(1)\overline{f'(1)} = 1 - 49 \cdot 5 = -244 \equiv 1 \pmod{49} \text{ ja}$$
$$r_{22} = r_{12} - f(r_{12})\overline{f'(r_{12})} = 5 - f(5)\overline{f'(5)} = 5 - 77 \cdot 2 = -149 \equiv 47 \pmod{49}.$$

Käyttämällä seurausta uudelleen saadaan ratkaisut

$$r_{31} = r_{21} - f(r_{21})\overline{f'(r_{11})} = 1 - f(1)\overline{f'(1)} \equiv 99 \pmod{343} \text{ ja}$$
$$r_{32} = r_{22} - f(r_{22})\overline{f'(r_{12})} = 47 - f(47)\overline{f'(5)} \equiv 243 \pmod{343}.$$

Edelleen

$$r_{41} = r_{31} - f(r_{31})\overline{f'(r_{11})} = 99 - f(99)\overline{f'(1)} \equiv 785 \pmod{2401} \text{ ja}$$
$$r_{42} = r_{32} - f(r_{32})\overline{f'(r_{12})} = 243 - f(243)\overline{f'(5)} \equiv 1615 \pmod{2401}.$$

Siis kongruenssiyhtälön (4.13) ratkaisut ovat 785 ja 1615 modulo 2401.

Kongruenssiyhtälöillä ei kuitenkaan aina ole ratkaisuja. Tutkitaan lopuksi vielä esimerkkiä tällaisesta tapauksesta.

Esimerkki 4.3 (vrt. [3, s. 159], teht. 4)**.** Tarkastellaan kongruenssiyhtälöä

$$x^2 + x + 34 \equiv 0 \pmod{81}. \tag{4.14}$$

Olkoon funktio $f(x) = x^2 + x + 34$. Funktion f derivaatta on tällöin $f'(x) = 2x + 1$ ja kongruenssin $f(x) \equiv 0 \pmod 3$ ratkaisuiksi saadaan kokeilemalla $x = 1$. Koska $f'(1) = 3 \equiv 0 \pmod 3$ ja $f'(1) = 36 \not\equiv 0 \pmod{81}$, niin Henselin lemman kohdan 3 nojalla kongruenssilla (4.14) ei ole ratkaisuja.

Lähteet

[1] Burton, D. *Elementary Number Theory*. 5. painos. New York: McGraw-Hill, 2002.

[2] Haukkanen, P. *Lukuteoriaa*. Luentomoniste. Tampereen yliopisto.

[3] Rosen, K. *Elementary Number Theory and its Applications*. 4. painos. Addison-Wesley, 2000.