TAMPEREEN YLIOPISTO

Pro gradu -tutkielma

Jussi Tervaniemi

Primitiiviset juuret

Matematiikan, tilastotieteen ja filosofian laitos

Matematiikka

Heinäkuu 2006

Sisältö

Tampereen yliopisto

Matematiikan, tilastotieteen ja filosofian laitos

TERVANIEMI, JUSSI: Primitiiviset juuret

Pro gradu -tutkielma, 45 s.

Matematiikka

Heinäkuu 2006

Tiivistelmä

Tutkielmassa käsitellään lukuteoriaa eli kokonaislukuja ja niiden ominaisuuksia. Pääaiheena on kokonaislukujen primitiiviset juuret. Tutkielman alussa esitellään lukuteorian peruskäsitteitä, kuten esimerkiksi jaollisuus, jakoalgoritmi, alkuluku, aritmetiikan peruslause ja kongruenssi. Luvussa 2 päästään käsiksi tutkielman pääaiheeseen, tutkielma onkin painottunut juuri lukuun 2. Aluksi esitellään kokonaisluvun kertaluvun käsite, jonka avulla päästään tarkastelemaan kokonaislukujen primitiivisiä juuria. Luvun, ja koko tutkielman, yksi tärkeimmistä tavoitteista on määrittää kaikki kokonaisluvut, joilla on primitiivisiä juuria. Tämä osa tutkielmaa on tarkkaa ja suhteellisen vaativaa matematiikkaa. Tutkielman lopuksi esitellään vielä lyhyesti primitiivisten juurien sovelluksen, diskreetin logaritmin, käyttömahdollisuuksia kongruenssien ratkaisemisessa. Lähdekirjoista näkyvimmissä rooleissa ovat kirjat: Burton, David M., *Elementary Number Theory*, fifth edition ja Rosen, Kenneth H., *Elementary number theory and its applications*, 4th edition.

Johdanto

Matematiikka on täynnä toinen toistaan hämmästyttävämpiä tuloksia, mutta erityisen hämmästyttävää on huomata millaisia ominaisuuksia ja käyttömahdollisuuksia jo pelkästään kokonaisluvuilla voi olla. Yksinkertainen on kaunista. Tässä tutkielmassa paneudutaankin nimenomaan kokonaislukuihin ja niiden ominaisuuksiin, toisin sanoen lukuteoriaan. Lukuteorialla on pitkä ja rikas historia matematiikassa, siksi sitä pidetäänkin suuressa arvossa. Viime vuosien saatossa lukuteoria ei ole kiinnostanut matemaatikkoja ainoastaan historiallisista syistä, vaan myös sen tarjoamien sovellusmahdollisuuksien tähden. Lukuteorian eri sovellusmahdollisuuksia, kuten esimerkiksi kryptausta, ei tutkielmassa kuitenkaan käsitellä.

Tutkielman luku 1 toimii lukuteorian peruskäsitteiden esittelijänä. Alaluvussa 1.1 käsitellään jaollisuutta, alkulukuja ja niihin liityviä muita kokonaislukujen ominaisuuksia. Alaluvussa 1.2 puolestaan esittellään merkittävä matemaattinen lause: aritmetiikan peruslause. Alaluvussa 1.3 esitellään erilaisia kongruensseja, joiden tuntemus on ehdoton edellytys luvulle 2. Luvun 1 rooli tutkielmassa on selkeästi alustava, joten siinä esiintyviä lauseita ei ole kaikkia todistettu.

Luvussa 2 päästään tutkielman varsinaiseen aiheeseen eli kokonaislukujen primitiivisiin juuriin. Alaluvussa 2.1 esitellään käsite: kokonaisluvun kertaluku. Alaluvussa 2.2 omistaudutaan kokonaan primitiivisille juurille ja niiden ominaisuuksille. Luku 2.3, joka käsittelee primitiivisten juurten olemassaoloa, nousee tutkielman tärkeimmäksi luvuksi. Tutkielman päätavoitteena onkin määrittää kaikki ne kokonaisluvut, joilla on primitiivinen juuri. Alaluku 2.4 käy lyhyesti läpi yhden primitiivisten juurten sovelluksista: diskreetin logaritmin.

Tutkielma lähtee liikkeelle lukuteorian peruskäsitteistä, joten lukijalta edellytetään joidenkin joukko-opin, logiikan sekä algebran perusasioiden tuntemusta, esimerkiksi hyvinjärjestysperiaate oletetaan tunnetuksi. Lisäksi yleinen binomilause edellytetään tunnetuksi. Lähdekirjoina on käytetty kirjoja: Apostol, Tom M., *Introduction to Analytic Number Theory*; Jones, Gareth A. and Jones, J. Mary, *Elementary Number Theory*; Burton, David M., *Elementary Number Theory*, fifth edition ja Rosen, Kenneth H., *Elementary number*

theory and its applications, 4th edition. Lähdekirjoista näkyvimmissä rooleissa tutkielmassa ovat kaksi viimeistä. Viimeiseksi mainitun kirjan sisältö on matemaattiseti erittäin loogista ja selvää, lukuun ottamatta useita virheitä, joita teoksesta löytyy. Tämän tutkielman tekijä on maininnut erikseen jokaisesta löytämästään virheestä.

Tutkielmassa kaikki luvut ovat kokonaislukuja ellei toisin mainita. Tutkielmassa joukkomerkintä $\mathbb{Z}$ tarkoittaa kokonaislukujen joukkoa ja merkintä $\mathbb{Z}_+$ tarkoittaa positiivisten kokonaislukujen joukkoa. Luvulla p tarkoitetaan alkulukua ellei toisin mainita.

1 Lukuteorian peruskäsitteitä

Tässä luvussa esitellään joitain tärkeitä lukuteorian peruskäsitteitä, määritelmiä, lauseita ja esimerkkejä. Osa todistuksista sivuutetaan tietoisesti, näin saadaan tutkielman painopiste siirtymään lukuun 2.

1.1 Jaollisuus ja alkuluvut

Tässä alaluvussa esitellään jaollisuuden määritelmä, joitain jaollisuuden perusominaisuuksia, jakoalgoritmi ja suurimman yhteisen tekijän sekä pienimmän yhteisen monikerran määritelmät. Alaluvun loppuosa keskittyy alkulukuihin. Esitellään alkuluvun ja yhdistetyn luvun määritelmät, todistetaan alkulukujen määrän äärettömyys ja lopuksi vielä määritellään käsite suhteelliset alkuluvut.

Määritelmä 1.1. Luku a on luvun b *tekijä*, jos on olemassa sellainen $c \in \mathbb{Z}$, että $b = ac$. Jos luku a jakaa luvun b, niin merkitään $a \mid b$, muutoin merkitään $a \nmid b$.

Esimerkki 1.1. Selvästi nähdään, että $4 \mid 12$, sillä $4 \cdot 3 = 12$. Vastaavasti nähdään, että $4 \nmid 11$, sillä ei ole olemassa lukua $c \in \mathbb{Z}$ siten , että $4 \cdot c = 11$.

Esitetään seuraavaksi joitain jaollisuuden perusominaisuuksia

Lause 1.1. *Olkoot luvut a, b, c, m ja n kokonaislukuja. Silloin pätee*

1. $a \mid b$ *ja* $a \mid c \Rightarrow a \mid (b - c)$,

2. $a \mid b \Rightarrow a \mid bd$,

3. $a \mid b$ *ja* $b \mid c \Rightarrow a \mid c$,

4. $a \mid b$ *ja* $a \mid c \Rightarrow a \mid (mb + nc)$.

Todistus. 1. Koska $a \mid b$ ja $a \mid c$, niin on olemassa sellaiset luvut d ja e, että $b = ad$ ja $c = ae$. Nyt

$$b - c = (ad - ae) = a(d - e), \quad \text{missä } (d - e) \in \mathbb{Z}.$$

Koska $a \mid a(d - e)$, niin $a \mid (b - c)$.

2. Koska $a \mid b$, niin on olemassa sellainen kokonaisluku e, että $b = ae$. Nyt

$$bd = aed, \quad \text{missä } (ed) \in \mathbb{Z}.$$

Tämä tarkoittaa, että $a \mid bd$.

3. Koska $a \mid b$ ja $b \mid c$, niin on olemassa sellaiset luvut d ja f, että $b = ad$ ja $c = be$. Nyt

$$c = be = (ad)e = a(de), \quad \text{missä } (de) \in \mathbb{Z}.$$

Koska $a \mid a(de)$, niin $a \mid c$.

4. Koska $a \mid b$ ja $a \mid c$, on olemassa sellaiset luvut d ja e, että $b = ad$ ja $c = ae$. Nyt

$$mb + nc = mad + nae = a(md + ne), \quad \text{missä } (md + ne) \in \mathbb{Z}.$$

Koska $a \mid a(md + ne)$, niin $a \mid (mb + nc)$.
Kaikki lauseen neljä kohtaa on näin todistettu. □

Lause 1.2 (**Jakoalgoritmi**). *Olkoot* a *ja* $b(> 0)$ *kokonaislukuja. Silloin on olemassa sellaiset yksikäsitteiset kokonaisluvut* q *ja* r*, että*

$$a = bq + r, \quad \textit{missä} \quad 0 \leq r < b.$$

Huomautus. Lukua a sanotaan *jaettavaksi*, lukua b *jakajaksi*, lukua q *osamääräksi* ja lukua r *jakojäänökseksi*.

Lauseen 1.2 todistus (vrt. [4, s. 32]). Osoitetaan aluksi lukujen q ja r olemassaolo. Tarkastellaan joukkoa $S = \{a - bk | k \in \mathbb{Z}\}$. Olkoon T joukon S ei-negatiivisten lukujen muodostama joukko. Koska $a - bk$ on positiivinen, kun $k < a/b$, niin T on epätyhjä.

Olkoon nyt $k = q$ joukon T pienin alkio. Olkoon lisäksi $r = a - bq$, joka vastaa lauseen merkintöjä. Tiedetään, että $r \geq 0$, ja lisäksi on helppo nähdä, että $r < b$. Jos nimittäin olisi $r \geq b$, niin $r > r - b = a - bq - b = a - b(q+1) \geq 0$, mikä on ristiriidassa sen kanssa, että $r = a - bq$ on pienin ei-negatiivinen luku, joka on muotoa $a - bk$. Näin ollen $0 \leq r < b$, joten on todistettu lukujen q ja r olemassaolo.

Seuraavaksi osoitetaan, että luvut r ja q ovat yksikäsitteisiä. Tarkastellaan yhtälöitä $a = bq_1 + r_1$ ja $a = bq_2 + r_2$, missä $0 \leq r_1 < b$ sekä $0 \leq r_2 < b$. Yhdistämällä yhtälöt saadaan

$$bq_1 + r_1 = bq_2 + r_2.$$

Järjestämällä termejä uudelleen saadaan yhtälö

$$r_2 - r_1 = b(q_1 - q_2).$$

On siis osoitettu, että $b \mid (r_2 - r_1)$. Koska $0 \leq r_1 < b$ ja $0 \leq r_2 < b$, niin $-b < r_2 - r_1 < b$. Näin ollen b jakaa luvun $r_2 - r_1$ vain, jos $r_2 - r_1 = 0$ eli jos $r_1 = r_2$. Lisäksi, koska $bq_1 + r_1 = bq_2 + r_2$ ja $r_1 = r_2$, niin saadaan myös, että $q_1 = q_2$. On siis osoitettu, että luvut q ja r ovat yksikäsitteisiä, joten lause on näin todistettu. □

Esimerkki 1.2. Olkoon $a = 89$ ja $b = 13$, niin silloin $q = 6$ ja $r = 11$, sillä $89 = 13 \cdot 6 + 11$.

Olkoot a ja b ovat sellaisia lukuja, että ainakin toinen on $\neq 0$. Tällöin lukujen a ja b yhteisten tekijöiden joukko on äärellinen joukko lukuja, joka sisältää aina luvut 1 ja -1. Ollaan kiinnostuneita suurimmasta luvusta, joka löytyy kahden luvun yhteisten tekijöiden joukosta.

Määritelmä 1.2. Olkoot a ja b kokonaislukuja, joista ainakin toinen on $\neq 0$. Niiden *suurin yhteinen tekijä* on suurin kokonaisluku, joka jakaa sekä luvun a että luvun b.

Suurimman yhteisen tekijän merkitsemistapoja on olemassa useita, mutta nyt käytetään symbolia (a, b).

Huomautus. Määritellään, että $(0, 0) = 0$. Ja huomataan, että $(a, b) = (|a|, |b|)$.

Esimerkki 1.3. Lukujen 12 ja 76 yhteiset tekijät ovat $\pm 1, \pm 2, \pm 3, \pm 4$ ja ± 6. Näin ollen $(12, 76) = 6$. Vastaavasti $(6, -21) = 3$, $(11, 31) = 1$ ja $(8, 64) = 8$.

Lause 1.3. *Olkoot a ja b sellaiset kokonaisluvut, että $(a, b) = d$. Tällöin $(a/d, b/d) = 1$.*

Todistus (kts. [4, s. 80]). Olkoon e sellainen kokonaisluku, että $e \mid (a/d)$ ja $e \mid (b/d)$. Nyt on olemassa sellaiset kokonaisluvut k ja s, että $a/d = ke$ ja $b/d = se$, joten $a = dek$ ja $b = des$. Nyt siis luku de on lukujen a ja b yhteinen tekijä. Koska oletuksen mukaan d on lukujen a ja b suurin yhteinen tekijä, niin $de \leq d$, joten $e = 1$. Siis $(a/d, b/d) = 1$. Lause on näin todistettu. □

Määritellään myös kokonaislukujen pienin yhteinen monikerta.

Määritelmä 1.3. Kahden positiivisen kokonaisluvun a ja b *pienin yhteinen monikerta* on pienin sellainen positiivinen kokonaisluku d, että $a \mid d$ ja $b \mid d$. Käytetään merkintää $[a, b]$.

Esimerkki 1.4. Selvästi $[2, 3] = 6$, $[2, 40] = 40$, $[26, 65] = 130$ ja $[7, 13] = 91$.

Kokonaisluvulla 1 on vain yksi positiivinen tekijä, luku itse. Jokaisella muulla positiivisella kokonaisluvulla on ainakin kaksi positiivista tekijää, sillä luku on jaollinen itsellään sekä luvulla 1. Luvut, joilla on täsmälleen kaksi positiivista tekijää ovat tärkeässä asemassa lukuteoriassa, niitä lukuja sanotaan *alkuluvuiksi*.

Määritelmä 1.4. Luku p (> 1) on *alkuluku*, jos sen ainoat positiiviset tekijät ovat 1 ja p eli luku itse.

Esimerkki 1.5. Luvut $2, 3, 11, 31, 79$ ja 151 ovat alkulukuja.

Määritelmä 1.5. Luku a on *yhdistetty luku*, jos se ei ole alkuluku.

Seuraavaksi todistetaan, että alkulukuja on ääretön määrä. Todistukseen tarvitaan seuraava apulause.

Apulause 1.4. *Jokainen luku a (> 1) on jaollinen alkuluvulla.*

Todistus (kts. [4, s. 66]). Sivuutetaan.

Lause 1.5 (**Eukleides**)**.** *Alkulukuja on ääretön määrä.*

Todistus (vrt. [2, s. 47]). Tehdään vastaoletus, jonka mukaan alkulukuja on äärellinen määrä. Olkoot $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$, ... alkulukuja kasvavassa järjestyksessä, ja oletetaan alkuluvun p_n olevan viimeinen eli suurin alkuluku. Merkitään

$$P = p_1 p_2 p_3 \cdots p_n + 1, \quad P \in \mathbb{Z}.$$

Koska $P > 1$, niin apulauseen 1.4 mukaan P on jaollinen jollain alkuluvulla p. Ainoat alkuluvut ovat p_1, p_2,..., p_n, joten $p = p_i$, kun $i = 1, 2,...,n$. Nyt $p \mid p_1 p_2 \cdots p_n$ ja $p \mid P$, joten jaollisuuden ominaisuuksien mukaan p jakaa niiden erotuksen eli $p \mid (P - p_1 p_2 \cdots p_n)$, siis $p \mid 1$. Tämä on mahdotonta, sillä $p > 1$, joten vastaoletus on väärin ja lause on näin todistettu. □

Määritelmä 1.6. Olkoot a ja b kokonaislukuja, joista ainakin toinen on $\neq 0$. Jos $(a, b) = 1$, niin luvut a ja b ovat *suhteellisia alkulukuja.*

Esimerkki 1.6. Koska $(4, 9) = 1$, niin luvut 4 ja 9 ovat suhteellisia alkulukuja.

1.2 Aritmetiikan peruslause

Alkuluvut ovat kiehtoneet matemaatikkoja kautta aikojen, ja aritmetiikan peruslause on yksi merkittävimmistä lauseista liittyen alkulukuihin. Tässä alaluvussa esitellään aritmetiikan peruslause ja todistetaan se. Lauseen todistamiseen tarvitaan apulauseita, joiden todistukset kuitenkin sivuutetaan.

Apulause 1.6. *Jos p on alkuluku ja $p \mid ab$, niin $p \mid a$ tai $p \mid b$.*

Todistus (kts. [2, s. 41]). Sivuutetaan.

Apulause 1.7. *Jos p on alkuluku ja $p \mid a_1 a_2 \cdots a_n$, niin on olemassa sellainen $k = 1, 2, \ldots, n$, että $p \mid a_k$.*

Todistus (kts. [2, s. 41]). Sivuutetaan.

Apulause 1.8. *Jos $p_1, p_2, \ldots, p_n$ ovat alkulukuja ja $p \mid p_1 p_2 \cdots p_n$, niin on olemassa sellainen $k = 1, 2, \ldots, n$, että $p = p_k$.*

Todistus (kts. [2, s. 41]). Sivuutetaan.

Lause 1.9 (**Aritmetiikan peruslause**)**.** *Jokainen kokonaisluku a (> 1) voidaan esittää alkulukujen tulona ja tämä tulo on yksikäsitteinen lukuun ottamatta tekijöiden järjestystä.*

Todistus (kts. [2, s. 42]). Luku a on joko alkuluku tai yhdistetty luku. Jos luku a on alkuluku, niin mitään todistettavaa ei ole. Jos a on yhdistetty luku, niin silloin on olemassa sellainen luku d, että $d \mid a$ ja $1 < d < a$. Hyvinjärjestysperiaatteen mukaan voidaan valita pienin luku, luvun a jakajista, ja merkitään sitä luvulla p_1. Nyt luvun p_1 on oltava alkuluku, sillä muuten sillä olisi jakaja ja niin ollen se ei olisi pienin mahdollinen luvun a jakaja. Nyt voidaan merkitä $a = p_1 a_1$, missä p_1 on alkuluku ja $1 < a_1 < a$. Jos luku a_1 on alkuluku, niin silloin luku a on esitetty alkulukujen tulona. Jos a_1 on yhdistetty luku, niin merkitään $a_1 = p_2 a_2$, missä p_2 on alkuluku ja $1 < a_2 < a_1$. Alkutekijäesitykseen saadaan näin toinen alkuluku, sillä nyt

$$a = p_1 p_2 a_2, \quad 1 < a_2 < a_1.$$

Jos a_2 on alkuluku, niin pidemmälle ei tarvitse jatkaa, alkutekijäesitys on saatu. Muuten jatketaan edelleen ja merkitään $a_2 = p_3 a_3$, missä p_3 on alkuluku ja $1 < a_3 < a_2$. Nyt

$$a = p_1 p_2 p_3 a_3, \quad 1 < a_3 < a_2.$$

Vähenevä jono

$$a > a_1 > a_2 > \cdots > 1$$

ei voi jatkua äärettömästi, joten äärellisen määrän jälkeen vastaavia askelia luku a_{k-1} on alkuluku. Merkitään sitä luvulla p_k. Näin ollaan saatu luvun a alkutekijäesitys kokonaan, sillä

$$a = p_1 p_2 p_3 \cdots p_k.$$

Seuraavaksi todistetaan lauseen loppuosa eli alkutekijäesityksen yksikäsitteisyys. Oletetaan, että luvulla a on kaksi alkutekijäesitystä, merkitään

$$a = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s, \quad \text{missä } r \leq s.$$

Kirjoitetaan alkutekijäesityksien termit uuteen, kasvavaan järjestykseen

$$p_1 \leq p_2 \leq \ldots \leq p_r \quad ja \quad q_1 \leq q_2 \leq \ldots \leq q_s.$$

Koska $p_1 \mid q_1 q_2 \cdots q_s$, niin apulauseen 1.8 mukaan $p_1 = q_k$, missä $k = 1, 2, \ldots, s$, joten $p_1 \geq q_1$. Vastaavalla päättelyllä saadaan $q_1 \geq p_1$, joten $p_1 = q_1$. Supistamalla yhteiset tekijät saadaan

$$p_2 p_3 \cdots p_r = q_2 q_3 \cdots q_s.$$

Toistetaan päättelyketju, saadaan $p_2 = q_2$. Supistetaan yhteiset tekijät. Nyt

$$p_3 p_4 \cdots p_r = q_3 q_4 \cdots q_s.$$

Jos $r < s$, niin jatkamalla samaan tapaan, saadaan lopulta

$$1 = q_{r+1} q_{r+2} \cdots q_s.$$

Tämä on kuitenkin mahdotonta, sillä $q_i > 1$, missä $i = 1, 2, \ldots, s$, joten $r = s$. Siis

$$p_1 = q_1, p_2 = q_2, \ldots, p_r = q_s$$

eli luvun a kaksi alkutekijäesitystä ovat identtiset. Lause on näin todistettu. □

Esimerkki 1.7. Luvun 32620 alkutekijäesitys on $32620 = 2 \cdot 2 \cdot 5 \cdot 7 \cdot 233$. Alkutekijäesitys voidaan kirjoittaa muodossa

$$32620 = 2^2 \cdot 5 \cdot 7 \cdot 233.$$

1.3 Kongruenssi

Tämä alaluku käsittelee lyhyesti lukuteorian käsitettä kongruenssi, ja sen perusominaisuuksia. Käsitteen alunperin esitteli saksalainen matemaatikko Karl Friedrich Gauss ($1777 - 1855$), vuonna 1801 ilmestyneessä teoksessaan *Disquisitiones Arithmeticae*.

Määritelmä 1.7. Olkoon m positiivinen kokonaisluku. Jos a ja b ovat kokonaislukuja, niin 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 merkitään $a \not\equiv b \pmod{m}$ ja sanotaan, että luku a on epäkongruentti luvun b kanssa modulo m. Kokonaislukua m sanotaan *moduliksi*.

Esimerkki 1.8. Luku $17 \equiv 5 \pmod{4}$, sillä $4 \mid (17-5) = 12$. Vastaavasti $17 \not\equiv 8 \pmod{4}$, sillä $4 \nmid (17-8) = 9$.

Lause 1.10. *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 (vrt. [4, s. 128,129]). Jos $a \equiv b \pmod{m}$, niin $m \mid (a-b)$. Tämä tarkoittaa sitä, että on olemassa kokonaisluku k siten, että $km = a-b$, joten $a = b + km$.
Toisaalta, jos on olemassa kokonaisluku k siten, että $a = b + km$, niin $km = a - b$. Siis $m \mid (a-b)$, ja tästä seuraa $a \equiv b \pmod{m}$. Lause on näin todistettu. □

Esimerkki 1.9. Luku $16 \equiv 27 \pmod{11}$ ja $16 = 27 + (-1 \cdot 11)$.

Apulause 1.11. *Olkoot luvut a, b ja c kokonaislukuja ja olkoon $(a,b) = 1$. Jos $a \mid bc$, niin $a \mid c$*

Todistus (vrt. [2, s. 24]). Suurimman yhteisen tekijän ominaisuuksien mukaan voidaan nyt kirjoittaa $1 = ax + by$, missä luvut x ja y ovat joitain kokonaislukuja. Kertomalla yhtälö molemmin puolin luvulla c saadaan

$$c = 1 \cdot c = (ax + by)c = acx + bcy.$$

Koska $a \mid acx$ ja $a \mid bcy$, niin jaollisuuden ominaisuuksien perusteella $a \mid (acx + bcy)$ eli $a \mid c$. Lause on näin todistettu. □

Lause 1.12. *Jos $ab \equiv ac \pmod{m}$, niin $b \equiv c \pmod{m/d}$, missä $d = (a,m)$.*

Todistus (vrt. [2, s. 67]). Oletuksesta saadaan suoraan

$$a(b-c) = ab - ac = km, \text{ missä } k \in \mathbb{Z}.$$

Koska $(a, m) = d$, niin on olemassa sellaiset kokonaisluvut r ja s, että $a = dr$ ja $m = ds$. Nyt merkitään $dr(b-c) = kds$, ja supistamalla yhtälön molemmilta puolilta luku d saadaan yhtälö muotoon

$$r(b-c) = ks.$$

Nyt $s \mid r(b-c)$ ja $(r, s) = 1$, joten lauseen 1.11 mukaan $s \mid (b-c)$. Toisin sanoen $b \equiv c \pmod{s}$ eli $b \equiv c \pmod{m/d}$. Lause on näin todistettu. □

Lause 1.13. *Jos luvut a, b, $m(>0)$ ja $k(>0)$ ovat kokonaislukuja ja $a \equiv b \pmod{m}$, niin silloin $a^k \equiv b^k \pmod{m}$.*

Todistus (kts. [4, s. 133]). Koska $a \equiv b \pmod{m}$, niin $m \mid (a-b)$. Ja koska

$$a^k - b^k = (a-b)(a^{k-1} + a^{k-2}b + ... + ab^{k-1} + b^{k-1}),$$

niin $(a-b) \mid (a^k - b^k)$. Nyt jaollisuuden transitiivisuuden perusteella $m \mid (a^k - b^k)$. Siis $a^k \equiv b^k \pmod{m}$. Lause on näin todistettu. □

Huomautus. Lähdekirjan lauseen 1.13 todistuksessa on viittausvirhe.

Seuraavaksi esitellään lineaarinen kongruenssi. Kongruenssia, joka on muotoa

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

missä x on tuntematon kokonaisluku, sanotaan yhden muuttujan *lineaarikongruenssiksi.*
Huomataan, että jos $x = x_0$ on kongruenssin $ax \equiv b \pmod{m}$ ratkaisu ja jos $x_1 \equiv x_0 \pmod{m}$, niin $ax_1 \equiv ax_0 \equiv b \pmod{m}$, joten x_1 on myös ratkaisu.

Esitellään apulause, jota tarvitaan myöhemmin lauseen todistamiseen.

Apulause 1.14. *Yhtälö (Diofantoksen yhtälö) $ax + by = c$ on ratkeava, jos ja vain jos $(a, b) \mid c$.*

Todistus (kts. [2, s. 34]). Sivuutetaan.

Lause 1.15. *Kongruenssi*

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

on ratkeava silloin ja vain silloin, kun $(a, m) \mid b$.

Todistus. Todistetaan lause ekvivalenssiketjulla.

$$\begin{aligned} &\text{Kongruenssi } ax \equiv b \pmod{m} \text{ on ratkeava} \\ &\Leftrightarrow \exists x \in \mathbb{Z} : ax \equiv b \pmod{m} \\ &\Leftrightarrow \exists x \in \mathbb{Z} : m \mid (ax - b) \\ &\Leftrightarrow \exists x, y \in \mathbb{Z} : ax - b = my \\ &\Leftrightarrow \exists x, y \in \mathbb{Z} : ax - my = b. \end{aligned}$$

Nyt apulauseen 1.14 mukaan Diofantoksen yhtälö $ax - my = b$ on ratkeava, jos ja vain jos $(a, -m) \mid b$. Lause on näin todistettu. □

Esimerkki 1.10. Ratkaistaan kongruenssi $22x = 14 \pmod{12}$. Koska $(22, 12) \mid 14$, niin kongruenssi on ratkeava. Ratkaistaan kongruenssi. Koska

$$22x = 2 \cdot 11 \equiv 2 \cdot 7 = 14 \pmod{12},$$

niin lauseen 1.12 mukaan voidaan supistaa luvulla 2, ja saadaan

$$11x \equiv 7 \pmod{6}.$$

Seuraavaksi korvataan kongruenteilla luvuilla ja saadaan

$$-1x \equiv 1 \pmod{6}.$$

Nyt supistetaan luvulla -1 ja näin kongruenssi tulee muotoon

$$x \equiv -1 \pmod{6}.$$

Lopuksi vielä korvataan kongruentilla luvulla, joten

$$x \equiv 5 \pmod{6}.$$

Nyt ollaan saatu kongruenssin ratkaisu modulo 6 eli $x \equiv 5 \pmod{6}$. Koska kongruenssilla on yksi ratkaisu kokonaislukuvälillä $[0, 6]$, niin kokonaislukuvälille $[0, 12]$ mahtuu kaksi ratkaisua, joten kaikki erisuuret ratkaisut alkuperäiselle kongruenssille ovat

$$x \equiv 5 \pmod{12} \text{ ja } x \equiv 11 \pmod{12}.$$

Huomautus 1. Kongruenssilla $ax \equiv b \pmod{m}$ on täsmälleen (a, m) kappaletta erisuuria ratkaisuja modulo m. Jos $(a, m) = 1$, niin ratkaisu on yksikäsitteinen modulo m. Jos $(a, m) = b > 1$, niin kongruenssilla on yksikäsitteinen ratkaisu modulo m/b ja erisuuria ratkaisuja modulo m on b kappaletta, kuten esimerkistä 1.10 hyvin nähdään. Ominaisuutta ei kuitenkaan todisteta.

Seuraavaksi esitellään keskeisiä ja jatkon kannalta erittäin tärkeitä määritelmiä.

Määritelmä 1.8. Kokonaislukujoukko, jossa on m lukua, on *täydellinen jäännössysteemi modulo* m, jos jokainen kokonaisluku on kongruentti täsmälleen joukon yhden luvun kanssa modulo m, toisin sanoen, jos joukon mitkään kaksi lukua eivät ole kongruentteja toistensa kanssa modulo m.

Esimerkki 1.11. Joukko

$$\{18, 39, -5, 28, -1, 20\}$$

on täydellinen jäännössysteemi modulo 6, sillä

$$18 \equiv 0, \quad 39 \equiv 3, \quad -5 \equiv 1, \quad 28 \equiv 4, \quad -1 \equiv 5 \quad \text{ja} \quad 20 \equiv 2,$$

missä kaikki on modulo 6. Tästä on helppo nähdä, etteivät luvut ole kongruentteja toistensa kanssa modulo 6.

Määritelmä 1.9 (**Eulerin funktio**)**.** Olkoon $n \geq 1$. Eulerin phi-funktio $\phi(n)$ ilmoittaa niiden, lukua n pienempien tai sen kanssa yhtäsuurien, positiivisten kokonaislukujen määrän, jotka ovat suhteellisia alkulukuja luvun n kanssa.

Huomautus. Jos luku n on alkuluku, niin jokainen luku $a < n$ on suhteellinen alkuluku luvun n kanssa, joten $\phi(n) = n - 1$.

Esimerkki 1.12. $\phi(6) = 2$, sillä $(1, 6) = 1$, $(5, 6) = 1$ ja $(r, 6) > 1$, kun $r = 2, 3, 4, 6$.

Lause 1.16. *Olkoon p alkuluku ja $k > 0$. Tällöin*

$$\phi(p^k) = p^k - p^{k-1} = p^k \left(1 - \frac{1}{p}\right).$$

Todistus (kts. [2, s. 130]). Selvästi $(n, p^k) = 1$, jos ja vain jos $p \nmid n$. Lukujen 1 ja p^k välissä on p^{k-1} lukua, jotka ovat jaollisia luvulla p, nimittäin luvut

$$p, 2p, 3p, ..., (p^{k-1})p.$$

Koska nyt joukkossa $\{1, 2, 3, ..., p^k\}$ on täsmälleen $p^k - p^{k-1}$ lukua, jotka ovat suhteellisia alkulukuja luvun p^k kanssa, niin suoraan phi-funktion määritelmästä seuraa, että $\phi(p^k) = p^k - p^{k-1}$. Lause on näin todistettu. □

Esimerkki 1.13. Selvästi $\phi(25) = \phi(5^2) = 5^2 - 5^{(2-1)} = 5^2 - 5 = 20$.

Määritelmä 1.10. Kokonaislukujoukko, jossa on $\phi(m)$ lukua, on *supistettu jäännössysteemi modulo m*, jos jokainen luku on suhteellinen alkuluku luvun m kanssa eikä mitkään joukon kaksi lukua ole kongruentteja toistensa kanssa modulo m.

Esimerkki 1.14. Joukko

$$\{1, 2, 4, 7, 8, 11, 13, 14\}$$

on supistettu jäännössysteemi modulo 15, sillä

$$(r_i, 15) = 1 \quad \text{ja} \quad r_i \not\equiv r_j \pmod{15}, \text{kun } r_i \neq r_j,$$

missä $r_{i,j} = 1, 2, 4, 7, 8, 11, 13, 14$.

Lause 1.17. *Olkoon $\{r_1, r_2, ..., r_{\phi(m)}\}$ supistettu jäännössysteemi modulo m, ja olkoon a sellainen kokonaisluku, että $(a, m) = 1$. Silloin*

$$\{ar_1, ar_2, ..., ar_{\phi(m)}\}$$

on myös supistettu jäännössysteemi modulo m.

Todistus (kts. [4, s. 216]). Ensiksi todistetaan, että jokainen kokonaisluku ar_i on suhteellinen alkuluku luvun m kanssa. Tehdään vastaoletus ja oletetaan, että $(ar_i, m) > 1$. Nyt on siis olemassa sellainen alkuluku p, että $p \mid a$ tai $p \mid r_i$. Siis joko $p \mid a$ ja $p \mid m$, tai $p \mid r_i$ ja $p \mid m$. Nyt jos $p \mid r_i$ ja $p \mid m$, niin $(r_i, m) > 1$. Tämä ei kuitenkaan ole mahdollista, sillä $\{r_1, r_2, ..., r_{\phi(m)}\}$ on oletuksen mukaan supistettu jäännössysteemi modulo m eli pitää olla $(r_i, m) = 1$. Jos taas $p \mid a$ ja $p \mid m$, niin $(a, m) > 1$. Tämäkin on ristiriidassa

oletuksen kanssa, sillä $(a, m) = 1$. Näin ollen jokainen kokonaisluku ar_i on suhteellinen alkuluku luvun m kanssa, kun $i = 1, 2, ..., \phi(m)$.

Toiseksi osoitamme, ettei mitkään kaksi lukua ar_i ole kongruentteja modulo m. Tehdään vastaoletus, että on olemassa sellaiset luvut i ja j, että $ar_i \equiv ar_j \pmod{m}$, missä $1 \leq i, j \leq \phi(m)$ ja $i \neq j$. Koska $(a, m) = 1$, niin lauseen 1.12 mukaan $r_i \equiv r_j \pmod{m}$. Tämä on ristiriidassa oletuksen kanssa, sillä $\{r_1, r_2, ..., r_{\phi(m)}\}$ on supistettu jäännössysteemi modulo m eli pitää olla $r_i \not\equiv r_j \pmod{m}$ aina, kun $i \neq j$. Siis mitkään kaksi lukua ar_i eivät ole keskenään kongruentteja modulo m. Lause on näin todistettu. □

Seuraavaksi esitetään erittäin keskeinen lause, joka on saanut nimensä sveitsiläisen matemaatikon Leonhard Eulerin (1707−1783) mukaan, kyseessä on *Eulerin lause*. Eulerin lauseen todistuksessa tarvitaan kuitenkin seuraavaa apulausetta.

Apulause 1.18. *Olkoot a, b ja c kokonaislukuja. Silloin $(a, bc) = 1$, jos ja vain jos $(a, b) = 1$ ja $(a, c) = 1$.*

Todistus (kts. [2, s. 130]). Sivuutetaan.

Lause 1.19 (**Eulerin lause**)**.** *Olkoot $m(\geq 1)$ ja a sellaiset kokonaisluvut, että $(a, m) = 1$. Silloin $a^{\phi(m)} \equiv 1 \pmod{m}$.*

Todistus (kts. [4, s. 217]). Olkoon $\{r_1, r_2, ..., r_{\phi(m)}\}$ supistettu jäännössysteemi modulo m. Nyt lauseen 1.17 mukaan myös $\{ar_1, ar_2, ..., ar_{\phi(m)}\}$ on supistettu jäännössysteemi modulo m. Nyt siis jokaista lukua ar_j kohti on olemassa sellainen yksikäsitteinen luku r_i, että $r_i \equiv ar_j \pmod{m}$. Kertomalla molempien jäännössysteemien termit keskenään, saadaan

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

Siis

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

Koska $(r_i, m) = 1$, jokaisella arvolla $i = 1, 2, ..., \phi(m)$, niin apulauseen 1.18 mukaan $(r_1 r_2 \cdots r_{\phi(m)}, m) = 1$. Nyt supistamalla saadaan

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

Lause on näin todistettu. □

Lukuteorian yksi merkittävimmistä vaikuttajista on ollut ehdottomasti ranskalainen Pierre de Fermat ($1601 - 1665$). Fermat kehitti erittäin tärkeitä lauseita, joilla on myös lukuisia hienoja sovelluksia lukuteorian parissa. Tunnetuimpia lauseita ovat *Fermat'n lause* ja *Fermat'n pieni lause*, joka esitellään seuraavaksi. On syytä huomata, että tässä tutkielmassa lauseen todistukseen käytetään apuna Eulerin lausetta, joka oikeastaan on myöhemmin todistettu Fermat'n lauseen yleistys.

Lause 1.20 (**Fermat'n pieni lause**)**.** *Jos p on alkuluku ja a on sellainen kokonaisluku, että $p \nmid a$, niin $a^{p-1} \equiv 1 \pmod{p}$.*

Todistus. Koska p on alkuluku, niin $\phi(p) = p - 1$. Nyt $(a, m) = 1$, joten Eulerin lauseesta seuraa suoraan, että $a^{p-1} \equiv 1 \pmod{p}$, sillä

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

Lause on näin todistettu. □

Seuraus 1.21. *Jos p on alkuluku ja a on positiivinen kokonaisluku, niin*

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

Todistus (kts. [4, s. 200])*.* Jaetaan todistus kahteen osaan. Jos $p \nmid a$, niin Fermat'n pienen lauseen mukaan $a^{p-1} \equiv 1 \pmod{p}$. Nyt kertomalla kongruenssin molemmat puolet luvulla a saadaan $a^p \equiv a \pmod{p}$. Jos $p \mid a$, niin selvästi $a \mid a^p$, joten $a^p \equiv a \equiv 0 \pmod{p}$. Kummassakin tapauksessa saadaan $a^p \equiv a \pmod{p}$. Lause on näin todistettu. □

Seuraavista esimerkeistä ilmenee hyvin Fermat'n lauseen käyttökelpoisuus ratkastaessa vaativampia kongruensseja tai testattaessa ovatko luvut alkulukuja.

Esimerkki 1.15. Todistetaan, että luvut 6^{76} ja 9 ovat kongruentteja modulo 13. Fermat'n pienen lauseen mukaan tiedetään, että $6^{12} \equiv 1 \pmod{13}$, joten

$$\begin{aligned} 6^{76} = 6^{12 \cdot 6 + 4} &= (6^{12})^6 \cdot (6^2)^2 \\ &\equiv 1^6 \cdot 10^2 \equiv 100 \equiv 9 \pmod{13}. \end{aligned}$$

Esimerkki 1.16. Tarkastellaan onko luku 241 alkuluku. Valitaan luvuksi a mahdollisimman helppo luku, olkoon $a = 2$. Koska

$$2^{241} = 2^{8 \cdot 30+1} = (2^8)^{30} \cdot 2$$

ja $2^8 = 256 \equiv 15 \pmod{241}$, niin saadaan

$$2^{241} \equiv 15^{30} \cdot 2 \equiv (15^3)^{10} \cdot 2 \pmod{241}.$$

Nyt koska $15^3 = 3375 \equiv 1 \pmod{241}$, niin lopulta saadaan

$$2^{241} \equiv 1^{10} \cdot 2 \equiv 2 \pmod{241}.$$

Siis luku 241 on alkuluku.

Lopuksi vielä kongruensseista esitellään yksi hyvin tärkeä käsite: *modulaarinen käänteisluku*. Erityismuotoa oleva kongruenssi $ax \equiv 1 \pmod{m}$ on lauseen 1.15 mukaan ratkeava, jos ja vain jos $(a, m) = 1$.

Määritelmä 1.11. Olkoon luku a sellainen kokonaisluku, että $(a, m) = 1$. Silloin kongruenssin $ax \equiv 1 \pmod{m}$ ratkaisua x sanotaan luvun a *käänteisluvuksi modulo* m.

Esimerkki 1.17. Ratkaistaan kongruenssi $8x \equiv 13 \pmod{19}$. Nyt $(8, 19) = 1$, joten yksikäsitteinen ratkaisu on olemassa. Koska $8 \cdot 12 = 96 \equiv 1 \pmod{19}$, niin luku 12 on luvun 8 käänteisluku modulo 19. Kerrotaan kongruenssin molemmat puolet luvulla 12 ja saadaan $12 \cdot 8x \equiv 12 \cdot 13 \pmod{19}$. Siis

$$x \equiv 12 \cdot 13 \equiv 156 \equiv 4 \pmod{19}.$$

Huomataan, että vastaavasti luku 8 on luvun 12 käänteisluku modulo 19.

Lause 1.22. *Olkoon p alkuluku. Silloin luku a on itsensä käänteisluku modulo p, jos ja vain jos $a \equiv 1 \pmod{p}$ tai $a \equiv -1 \pmod{p}$.*

Todistus (vrt. [4, s. 141]). Jos $a \equiv 1 \pmod{p}$ tai $a \equiv -1 \pmod{p}$, niin lauseen 1.13 mukaan $a^2 \equiv 1 \pmod{m}$. Näin ollen luku a on itsensä käänteisluku modulo p.

Jos taas a on itsensä käänteisluku modulo p, niin $a^2 = a \cdot a \equiv 1 \pmod{p}$. Siis $p \mid (a^2 - 1) = (a - 1)(a + 1)$. Nyt apulauseen 1.7 mukaan $p \mid (a - 1)$ tai $p \mid (a + 1)$. Siis $a \equiv 1 \pmod{p}$ tai $a \equiv -1 \pmod{p}$ □

Esitellään vielä nopeasti eräs käytännöllinen työkalu kongruenssiryhmän yhteisen ratkaisun löytämiseen. Kahden tai useamman yhden muuttujan lineaarikongruenssien, joilla on eri modulit, yhteisen ratkaisun löytämiseen käytetään *kiinalaista jäännöslausetta*.

Lause 1.23 (**kiinalainen jäännöslause**). *Olkoot luvut* $m_1, m_2, ..., m_r (\geq 2)$ *pareittain suhteellisia alkulukuja. Tällöin 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 (kts. [4, s. 144]). Sivuutetaan.

2 Primitiiviset juuret

Tässä luvussa paneudutaan tutkielman pääaiheeseen, kokonaislukujen primitiivisiin juuriin. Termin *primitiivinen juuri* keksi alunperin Leonhard Euler vuonna 1773. Tästä huolimatta, hänen todistuksensa, että jokaisella alkuluvulla on primitiivinen juuri ei kuitenkaan ollut oikein. Italialainen matemaatikko Joseph Louis Lagrange (1736 − 1813) todisti väitteen ensimmäisenä täsmällisesti vuonna 1769, tämä esitellään alaluvussa 2.3. Koko tutkielman päätavoite on kuitenkin määrittää kaikki luvut, joilla on primitiivisiä juuria, tämä huipennus saavutetaan aivan alaluvun 2.3 lopuksi.

Primitiivisillä juurilla on useita eri sovelluksia matematiikassa, niiden avulla voidaan esimerkiksi määritellä diskreetit logarimit, jotka puolestaan helpottavat tietynlaisten kongruenssien ratkaisemisessa.

Aluksi kuitenkin esitellään käsite *kokonaisluvun kertaluku modulo* m.

2.1 Kokonaisluvun kertaluku

Tiedetään, että Eulerin lauseen mukaan kongruenssi $a^{\phi(m)} \equiv 1 \pmod{m}$ on ratkeava, kun $(a, m) = 1$, joten on olemassa sellainen kokonaisluku x, että

$a^x \equiv 1 \pmod{m}$.

Määritelmä 2.1. Olkoot a ja m (> 1) keskenään jaottomia kokonaislukuja. Silloin luvun a *kertaluku* modulo m on pienin sellainen positiivinen kokonaisluku x, että $a^x \equiv 1 \pmod{m}$. Merkitään $x = \mathrm{ord}_m a$.

Huomautus. Olkoot $m > 1$ ja $k > 1$ kokonaislukuja. Nyt selvästi $1^k \equiv 1 \pmod{m}$, mutta $\mathrm{ord}_m 1 \neq k$, sillä luku 1 on pienin sellainen luku, että $1^1 \equiv 1 \pmod{m}$.

Esimerkki 2.1. Etsitään luvun 2 kertaluku modulo 9. Nyt selvästi

$$2^1 \equiv 2 \pmod{9}, \quad 2^2 \equiv 4 \pmod{9}, \quad 2^3 \equiv 8 \pmod{9}, \quad 2^4 \equiv 16 \equiv 7 \pmod{9},$$
$$2^5 \equiv 32 \equiv 5 \pmod{9}, \quad 2^6 \equiv 64 \equiv 1 \pmod{9},$$

joten $\mathrm{ord}_9 2 = 6$.
Vastaavasti löytyy $\mathrm{ord}_9 5$. Koska

$$5^1 \equiv 5 \pmod{9}, \quad 5^2 \equiv 25 \equiv 7 \pmod{9}, \quad 5^3 \equiv 125 \equiv 8 \pmod{9},$$
$$5^4 \equiv 625 \equiv 4 \pmod{9}, \quad 5^5 \equiv 3125 \equiv 2 \pmod{9}, \quad 5^6 \equiv 15625 \equiv 1 \pmod{9},$$

niin $\mathrm{ord}_9 5 = 6$.

Huomautus. Jos kaksi kokonaislukua ovat kongruentteja modulo m, niin niillä on sama kertaluku modulo m. Koska, jos $a \equiv b \pmod{m}$ ja $a^x \equiv 1 \pmod{m}$, niin lauseen 1.13 mukaan $a^x \equiv b^x \pmod{m}$, joten $b^x \equiv 1 \pmod{m}$. Jotta löydetään kongruenssin $a^x \equiv 1 \pmod{m}$ kaikki ratkaisut, niin tarvitaan seuraava lause.

Lause 2.1. *Olkoot luvut a ja $m(> 1)$ suhteellisia alkulukuja. Nyt positiivinen kokonaisluku x on kongruenssin $a^x \equiv 1 \pmod{m}$ ratkaisu, jos ja vain jos $\mathrm{ord}_m a \mid x$.*

Todistus (vrt. [4, s. 308, 309]). Jos $\mathrm{ord}_m a \mid x$, niin $x = k \cdot \mathrm{ord}_m a$, missä k on positiivinen kokonaisluku. Näin ollen

$$a^x = (a^{\mathrm{ord}_m a})^k \equiv 1^k \equiv 1 \pmod{m}. \tag{2.1}$$

Nyt todistetaan vielä toiseen suuntaan. Oletetaan, että $a^x \equiv 1 \pmod{m}$. Jakoalgoritmin mukaan merkitään

$$x = q \cdot \mathrm{ord}_m a + r, \quad 0 \leq r < \mathrm{ord}_m a.$$

Näin ollen

$$a^x = a^{q \cdot \mathrm{ord}_m a + r} = (a^{\mathrm{ord}_m a})^q a^r \equiv a^r \pmod{m}.$$

Koska $a^x \equiv 1 \pmod{m}$, niin $a^r \equiv 1 \pmod{m}$. Koska luku $\mathrm{ord}_m a = y$ on pienin kokonaisluku, että $a^y \equiv 1 \pmod{m}$, ja $0 \leq r < y$, niin $r = 0$. Näin ollen $x = q \cdot \mathrm{ord}_m a + r = q \cdot \mathrm{ord}_m a$ eli $\mathrm{ord}_m a \mid x$. Lause on näin todistettu. □

Huomautus. Lähdekirjan todistuksen yhtälöä (2.1) vastaavassa yhtälössä on virhe.

Esimerkki 2.2. Esimerkissä 2.1 saatiin, että $\mathrm{ord}_9 2 = 6$. Nyt esimerkiksi $x = 24$ on kongruenssin $2^x \equiv 1 \pmod{9}$ ratkaisu, sillä $6 \mid 24$. Vastaavasti $x = 15$ ei ole kyseisen kongruenssin ratkaisu, koska $6 \nmid 15$.

Seuraavaa lause, joka itse asiassa on lauseen 2.1 seuraus, on jatkossa erittäin tärkeä. Se helpottaa huomattavasti työtä etsittäessä kokonaislukujen primitiivisiä juuria.

Seuraus 2.2. *Jos a ja $m(> 0)$ ovat suhteellisia alkulukuja, niin* $\mathrm{ord}_m a \mid \phi(m)$.

Todistus (vrt. [4, s. 309]). Koska $(a, m) = 1$, niin Eulerin lauseesta saadaan

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

Nyt lauseesta 2.1 seuraa suoraan, että $\mathrm{ord}_m a \mid \phi(m)$. □

Esimerkki 2.3. Esimerkissä 2.1 etsittiin luvun 2 kertalukua modulo 9 nöyrästi koittamalla läpi kaikki luvut $1, 2, 3, 4, 5, 6$. Nyt seurauksen 2.2 mukaan voidaan helpottaa etsimistä. Koska $\phi(9) = 6$, niin kertaluku löytyy luvun 6 jakajista eli luvuista $1, 2, 3$ tai 6. Luvun 2 kertaluku modulo 9 on luku 6, joka on yksi luvun 6 jakajista.

Vastaavasti etsittäessä luvun 4 kertalukua modulo 23, määritetään ensiksi luvun 23 phi-funktio eli $\phi(23) = 22$. Luvun $\mathrm{ord}_{23} 4$ ainoat mahdolliset arvot ovat siis luvut $1, 2, 11$ tai 22. Nyt

$$4^1 \equiv 4 \pmod{23}, \quad 4^2 \equiv 16 \pmod{23}, \quad 4^{11} \equiv 4194304 \equiv 1 \pmod{23},$$

joten $\mathrm{ord}_{23} 4 = 11$.

Lause 2.3. *Olkoot a ja $m(>0)$ suhteellisia alkulukuja ja luvut $i, j \geq 0$. Nyt $a^i \equiv a^j \pmod{m}$, jos ja vain jos $i \equiv j \pmod{\mathrm{ord}_m a}$.*

Todistus (vrt. [4, s. 310]). Oletetaan, että $i \equiv j \pmod{\mathrm{ord}_m a}$ ja yleisyyttä menettämättä $0 \leq j \leq i$. Näin ollen kongruenssin määritelmän mukaan voidaan merkitä $i = j + k \cdot (\mathrm{ord}_m a)$, missä $k \in \mathbb{Z}$. Siis

$$a^i = a^{j+k\cdot \mathrm{ord}_m a} = a^j (a^{\mathrm{ord}_m a})^k \equiv a^j \pmod{m},$$

koska $a^{\mathrm{ord}_m a} \equiv 1 \pmod{m}$.
Todistetaan vielä toiseen suuntaan. Oletetaan nyt $a^i \equiv a^j \pmod{m}$, missä $i \geq j$. Koska $(a, m) = 1$, niin $(a^j, m) = 1$. Koska

$$a^i = a^j a^{i-j} \equiv a^j \pmod{m},$$

niin lauseesta 1.12 seuraa, että

$$a^{i-j} \equiv 1 \pmod{m}.$$

Täten lauseen 2.1 mukaan $\mathrm{ord}_m a \mid (i - j)$ eli $i \equiv j \pmod{\mathrm{ord}_m a}$. Lause on näin todistettu. □

Esimerkki 2.4. Olkoot $a = 7$ ja $m = 12$. Koska $\phi(12) = 4$, niin $7^3 \equiv 7^7 \pmod{12}$, sillä $3 \equiv 7 \pmod{4}$. Vastaavasti $7^{12} \not\equiv 7^{23}$, sillä $12 \not\equiv 23 \pmod{4}$.

Seuraus 2.4. *Jos luvun a kertaluku on luku k modulo m, niin kokonaisluvut $a, a^2, ..., a^k$ ovat epäkongruentteja modulo m.*

Todistus (vrt. [2, s. 159]). Jos $a^i \equiv a^j \pmod{m}$, kun $1 \leq i \leq j \leq k$, niin silloin lauseen 2.3 mukaan on oltava $i \equiv j \pmod{k}$. Tämä on kuitenkin mahdollista vain, jos $i = j$, joka on ristiriidassa oletuksen kanssa. Lause on näin todistettu. □

2.2 Primitiiviset juuret

Tämä alaluku käsittelee tutkielman varsinaista aihetta. Keskitytään kokonaisluvun a kaikkein suurimpaan mahdolliseen kertalukuun modulo m.

Määritelmä 2.2. Olkoot r ja ja m (> 1) keskenään suhteellisia alkulukuja. Jos $\mathrm{ord}_m r = \phi(m)$, niin sanotaan, että r on *primitiivinen juuri modulo m*.

Esimerkki 2.5. Esimerkissä 2.1 saatiin, että $\text{ord}_9 2 = 6$ ja $\text{ord}_9 5 = 6$. Koska $\phi(9) = 6$, niin luvut 2 ja 5 ovat primitiivisiä juuria modulo 9.

Esimerkki 2.6. Etsitään kaikki primitiiviset juuret modulo 11. Koska $\phi(11) = 10$, niin mahdolliset kertaluvut ovat luvut $1, 2, 5$ ja 10. Luku 11 on alkuluku, joten joudutaan tutkimaan kaikkien lukua 11 pienempien lukujen kertaluvut. Saadaan

$$\text{ord}_{11} 1 = 1 \neq 10,$$

$$\text{ord}_{11} 10 = 2 \neq 10,$$

$$\text{ord}_{11} 3 = \text{ord}_{11} 4 = \text{ord}_{11} 5 = \text{ord}_{11} 9 = 5 \neq 10 \text{ ja}$$

$$\text{ord}_{11} 2 = \text{ord}_{11} 6 = \text{ord}_{11} 7 = \text{ord}_{11} 8 = 10.$$

Siis luvut $2, 6, 7$ ja 8 ovat primitiivisiä juuria modulo 11.

Huomautus. Primitiivisiä juuria etsiessä on syytä olla tarkkana ja muistaa kertaluvun määritelmä. Esimerkiksi, vaikka $\phi(7) = 6$ ja $2^6 = 64 \equiv 1 \pmod 7$, niin luku 2 ei ole primitiivinen juuri modulo 7, sillä $\text{ord}_7 2 = 3$.

Huomautus. (vrt. [4, s. 310, 311]). Tutkielmassa tullaan osoittamaan millä kokonaisluvuilla on olemassa primitiivisiä juuria, joten kaikilla kokonaisluvuilla ei niitä siis ole. Esimerkiksi ei ole olemassa primitiivisiä juuria modulo 12. Luvun 12 kanssa suhteelliset alkuluvut (< 12) ovat luvut 1, 5, 7 ja 11. Nyt $\text{ord}_{12} 1 = 1$ ja $\text{ord}_{12} 5 = \text{ord}_{12} 7 = \text{ord}_{12} 11 = 2$, mutta $\phi(12) = 4$. Luku 8 on ensimmäinen kokonaisluku, jolla ei ole primitiivisiä juuria. Esimerkiksi kolmenkymmenen ensimmäisen kokonaisluvun joukossa olevat muut luvut, joilla ei ole primitiivisiä juuria, ovat luvut $15, 16, 20, 21, 24, 28$ ja 30. Tässä vaiheessa voidaankin vain arvailla lukuja, joilla on primitiivisiä juuria. Kolmenkymmenen ensimmäisen luvun perusteella näyttäisi siltä, että esimerkiksi jokaisella alkuluvulla ja parittoman alkuluvun potenssilla niitä olisi. Myöhemmin selviää pitävätkö arvelut paikkansa.

Apulause 2.5. *Olkoot $a_1, a_2, ..., a_n$ ja b sellaisia kokonaislukuja, että $(a_1, b) = (a_2, b) \cdots (a_n, b) = 1$. Tällöin $(a_1 a_2 \cdots a_n, b) = 1$*

Todistus. Tehdään vastaoletus $(a_1 a_2 \cdots a_n, b) = d > 1$. Koska $d > 1$, niin se on apulauseen 1.4 mukaan jaollinen jollain alkuluvulla p. Koska $d \mid a_1 a_2 \cdots a_n$,

niin jaollisuuden transitiivisuuden mukaan $p \mid a_1 a_2 \cdots a_n$. Nyt apulauseen 1.6 mukaan $p \mid a_1$, $p \mid a_2$, ... , $p \mid a_{n-1}$ tai $p \mid a_n$. Jos $p \mid a_1$, niin $(a_1, b) \geq p > 1$, mikä on ristiriidassa oletuksen kanssa. Jos $p \mid a_2$, niin $(a_2, b) \geq p > 1$, mikä on myös ristiriita. Samalla tapaa myös muut luvut $a_3, a_4, ..., a_n$ johtavat ristiriitaan oletuksen kanssa, joten $d = 1$. Lause on näin todistettu. □

Lause 2.6. *Olkoot r ja m ($m > 1$) suhteellisia alkulukuja, ja olkoon r primitiivinen juuri modulo m. Silloin kokonaislukujoukko*

$$\left\{r^1, r^2, ..., r^{\phi(m)}\right\}$$

on supistettu jäännössysteemi modulo m.

Todistus (vrt. [4, s. 311]). Ensiksi osoitetaan, että jokainen joukon luku on suhteellinen alkuluku luvun m kanssa. Oletuksesta seuraa suoraan, että $(r, m) = 1$. Nyt apulauseen 2.5 mukaan $(r^k, m) = 1$ aina, kun $k = 1, 2, ..., \phi(m)$.

Osoitetaan vielä, etteivät mitkään luvuista r^1, r^2, ..., $r^{\phi(m)}$ ole kongruentteja keskenään modulo m. Koska luku r on primitiivinen juuri modulo m, niin $\mathrm{ord}_m r = \phi(m)$, joten seurauksen 2.4 mukaan mitkään luvuista r^1, r^2, ..., $r^{\phi(m)}$ eivät ole kongruentteja keskenään modulo m. Lause on näin todistettu. □

Esimerkki 2.7. Esimerkissä 2.6 todettiin, että luku 2 on primitiivinen juuri modulo 11. Koska $\phi(11) = 10$, niin lauseen 2.6 perusteella kokonaislukujoukko $\{2^1, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8, 2^9, 2^{10}\}$ eli $\{2, 4, 8, 5, 10, 9, 7, 3, 6, 1\}$ on supistettu jäännössysteemi modulo 11.

Tässä vaiheessa on lukijalle voinut herätä joitain kysymyksiä aiheesta. Kuinka monta primitiivistä juurta kullakin luvulla on? Onko mahdollista ilmaista luvun a^u, missä $u \in \mathbb{Z}_+$, kertaluku modulo m luvun a kertaluvun modulo m avulla? Seuraavaksi tarkastellaan näitä ongelmia.

Lause 2.7. *Olkoon u positiivinen kokonaisluku. Jos $\mathrm{ord}_m a = t$, niin*

$$\mathrm{ord}_m(a^u) = \frac{t}{(t, u)}.$$

Todistus (vrt. [4, s. 312]). Merkitään $s = \mathrm{ord}_m(a^u)$, $v = (t, u)$, $t = t_1 v$ ja $u = u_1 v$. Lauseen 1.3 perusteella tiedetään, että $(t_1, u_1) = 1$.

Koska $t_1 = t/(t,u)$, niin osoitetaan, että $\mathrm{ord}_m(a^u) = t_1$. Täytyy siis osoittaa, että $(a^u)^{t_1} \equiv 1 \pmod{m}$ ja että jos $(a^u)^s \equiv 1 \pmod{m}$, niin $t_1 \mid s$. Huomataan, että

$$(a^u)^{t_1} = (a^{u_1 v})^{(t/v)} = (a^{u_1})^{v(t/v)} = (a^{u_1})^t = (a^t)^{u_1} \equiv 1 \pmod{m},$$

koska oletuksen mukaan $\mathrm{ord}_m a = 1$. Nyt lauseen 2.1 mukaan $s \mid t_1$.

Toisaalta, koska

$$(a^u)^s = a^{us} \equiv 1 \pmod{m},$$

tiedetään, että $t \mid us$. Siis

$$t \mid u_1 vs, \tag{2.2}$$

ja edelleen $t_1 \mid u_1 s$. Koska $(t_1, u_1) = 1$, niin apulauseen 1.11 mukaan $t_1 \mid s$. Nyt $s \mid t_1$ ja $t_1 \mid s$, joten $s = t_1 = t/v = t/(t,u)$. Lause on näin todistettu. □

Huomautus. Lauseen 2.7 lähdekirjan todistuksen relaatiota (2.2) vastaavassa relaatiossa on indeksivirhe.

Esimerkki 2.8. Esimerkissä 2.1 osoitettiin, että $\mathrm{ord}_9 2 = 6$. Nyt lauseen 2.7 mukaan on helppo todeta, että

$$\mathrm{ord}_9 2^4 = 6/(6,4) = 6/2 = 3.$$

Tämä tulos on helppo tarkistaa. Koska $2^4 = 16 \equiv 7 \pmod{9}$, niin

$$7^1 \equiv 7 \pmod{9}, \quad 7^2 = 49 \equiv 4 \pmod{9}, \quad 7^3 = 343 \equiv 1 \pmod{9},$$

joten $\mathrm{ord}_9 2^4 = 3$.

Seuraava, lauseen 2.7 seuraus, on erittäin hieno ja käytännöllinen matemaattinen oivallus. Se kertoo, mitkä primitiivisen juuren potensseista ovat myös primitiivisiä juuria.

Seuraus 2.8. *Olkoon r primitiivinen juuri modulo $m(>1)$. Silloin r^u on primitiivinen juuri modulo m, jos ja vain jos $(u, \phi(m)) = 1$.*

Todistus (vrt. [4, s. 312]). Lauseen 2.7 perusteella tiedetään, että

$$\mathrm{ord}_m(r^u) = \mathrm{ord}_m r/(\mathrm{ord}_m r, u).$$

Koska r on oletuksen mukaan primitiivinen juuri modulo m, niin voidaan merkitä

$$\mathrm{ord}_m(r^u) = \phi(m)/(\phi(m), u).$$

Näin ollen $\mathrm{ord}_m(r^u) = \phi(m)$, jos ja vain jos $(u, \phi(m)) = 1$. Lause on näin todistettu. □

Esimerkki 2.9. Etsitään seurauksen 2.8 avulla kaikki primitiiviset juuret modulo 7. Koska $\phi(7) = 6$ ja $\mathrm{ord}_7 3 = 6$, niin luku 3 on primitiivinen juuri modulo 7. Luvun 6 kanssa suhteellisia alkulukuja ovat luvut 1 ja 5, joten kaikki primitiiviset juuret modulo 7 ovat luvut $3^1 \equiv 3 \pmod 7$ ja $3^5 = 243 \equiv 5 \pmod 7$.

Seuraava lause ilmoitaa täsmällisesti luvun primitiivisten jurten kokonaislukumäärän.

Lause 2.9. *Jos positiivisella kokonaisluvulla m on primitiivinen juuri, niin primitiivisten juurten modulo m kokonaislukumäärä on $\phi(\phi(m))$.*

Todistus (vrt. [4, s. 312]). Olkoon r primitiivinen juuri modulo m. Lauseen 2.6 mukaan luvut $r^1, r^2, ..., r^{\phi(m)}$ muodostavat supistetun jäännössysteemin modulo m. Nyt seurauksen 2.8 mukaan luku r^u on primitiivinen juuri modulo m, jos ja vain jos $(u, \phi(m)) = 1$. Luvun $\phi(m)$ kanssa suhteellisia alkulukuja on Eulerin phi-funktion määritelmän mukaan $\phi(\phi(m))$ kappaletta. Täten primitiivisten juurten kokonaislukumäärä on $\phi(\phi(m))$. Lause on näin todistettu. □

Esimerkki 2.10. Koska $\phi(\phi(11)) = \phi(10) = 4$, joten luvulla 11 on 4 kappaletta primitiivisiä juuria. Esimerkin 2.6 mukaan primitiiviset juuret modulo 11 ovat luvut $2, 6, 7$ ja 8.

2.3 Primitiivisten juurten olemassaolo

Tämän alaluvun tarkoitus on määrittää kaikki kokonaisluvut, joilla on primitiivinen juuri. Tullaan huomaamaan, että on enemmän poikkeus kuin sääntö, että luvuilla on primitiivinen juuri. Ensiksi todistetaan, että jokaisella alkuluvulla on primitiivinen juuri. Seuraavaksi osoitetaan, että jokaisella parittoman alkuluvun potenssilla on primitiivinen juuri. Lopulta tiedetään ainoas-

taan luvuilla, jotka ovat muotoa $2, 4, p^k$ ja $2p^k$, missä p on pariton alkuluku ja k on positiivinen kokonaisluku, olevan primitiivisiä juuria.

Alaluvussa 1.3 on esitelty erilaisia kongruensseja, luvusta on silti jätetty pois yksi kokonaisuus: *polynomikongruenssit*. Esitetään polynomikongruenseista nyt vain jatkon kannalta tarvittavat asiat.

Määritelmä 2.3. Olkoon $f(x)$ kokonaislukukertoiminen polynomi. Kokonaislukua c sanotaan polynomin $f(x)$ *juureksi modulo* m, jos $f(c) \equiv 0 \pmod{m}$. Huomataan, että jos luku c on $f(x)$:n juuri modulo m, niin silloin kaikki luvun c kanssa kongruentit luvut modulo m ovat myös $f(x)$:n juuria modulo m.

Esimerkki 2.11. Polynomikongruenssilla $x^2 + 2x - 3 \equiv 0 \pmod{6}$ on täsmälleen kaksi juurta, nimittäin luvut 1 ja 3, sillä $1 + 2 \cdot 1 - 3 \equiv 0 \pmod{6}$ ja $3^2 + 2 \cdot 3 - 3 \equiv 12 \equiv 0 \pmod{6}$.

Huomautus. (vrt. [4, s. 315, esim. 9.12]). Olkoon p alkuluku ja $(x, p) = 1$. Fermat'n pienen lauseen mukaan $x^{p-1} \equiv 1 \pmod{p}$. Siis polynomilla $f(x) = x^{p-1} - 1$ on täsmälleen $p - 1$ kappaletta epäkongruentteja juuria modulo p, nimittäin $x \equiv 1, 2, ..., p - 1 \pmod{p}$.

Tarvitaan seuraavaa tärkeää lausetta koskien polynomikongruenssien juuria modulo p, missä p on alkuluku.

Lause 2.10 (Lagrangen lause). *Olkoon* $f(x) = a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0$ *kokonaislukukertoiminen* n*-asteinen polynomi, jossa* $n \geq 1$ *ja* $(a_n, p) = 1$. *Tällöin polynomilla* $f(x)$ *on enintään* n *kappaletta epäkongruentteja juuria modulo* p.

Todistus (vrt. [4, s. 315,316]). Todistetaan lause induktiolla. Kun $n = 1$, niin $f(x) = a_1 x + a_0$, missä $p \nmid a_1$. Polynomin $f(x)$ juuri modulo p on lineaarikongruenssin $a_1 \equiv a_0 \pmod{p}$ ratkaisu. Koska $(a_1, p) = 1$, niin huomautuksen 1 (s. 14) mukaan kyseisellä kongruenssilla on täsmälleen yksi ratkaisu, joten polynomin $f(x)$ juuria modulo p on täsmälleen yksi kappale. Väite pätee, kun $n = 1$.

Tehdään induktio-oletus, että väite pätee astetta $n - 1$ oleville polynomeille. Tehdään vastaoletus ja oletetaan, että polynomilla $f(x)$ on $n+1$ kappaletta epäkongruentteja juuria modulo p. Merkitään juuria $c_0, c_1, ..., c_n$, nyt

siis $f(c_t) \equiv 0 \pmod{p}$, missä $t = 0, 1, ..., n$. Nyt

$$\begin{aligned} f(x) - f(c_0) &= a_n(x^n - c_0^n) + a_{n-1}(x^{n-1} - c_0^{n-1}) + ... + a_1(x - c_0) \\ &= a_n(x - c_0)(x^{n-1} + x^{n-2}c_0 + ... + xc_0^{n-2} + c_0^{n-1}) \\ &\quad + a_{n-1}(x - c_0)(x^{n-2}c_0 + x^{n-3}c_0 + ... + xc_0^{n-3} + c_0^{n-2}) \\ &\quad + ... + a_1(x - c_0) \\ &= (x - c_0)g(x), \end{aligned}$$

missä $g(x)$ on astetta $n - 1$ oleva polynomi, jonka suurinta astetta olevan muuttujan kerroin on a_n. Osoitetaan, että kaikki luvuista $c_1, c_2, ..., c_n$ on polynomin $g(x)$ juuria modulo p. Olkoon t sellainen kokonaisluku, että $1 \leq t \leq n$. Koska $f(c_t) \equiv f(c_0) \equiv 0 \pmod{p}$, niin saadaan

$$f(c_t) - f(c_0) = (c_t - c_0)g(c_t) \equiv 0 \pmod{p}.$$

Tästä seuraa, että $g(c_t) \equiv 0 \pmod{p}$, koska $c_t - c_0 \not\equiv 0 \pmod{p}$. Siis c_t on polynomin $g(x)$ juuri modulo p. Nyt siis $n - 1$-asteisella polynomilla $g(x)$, missä $a_n \nmid p$, on n kappaletta epäkongruentteja juuria modulo p. Tämä on kuitenkin ristiriidassa induktio-oletuksen kanssa. Polynomilla $f(x)$ ei siis voi olla enempää juuria, kuin n kappaletta, vastaoletus on näin ollen väärin ja väite oikein. Lause on näin todistettu. □

Seuraavan lauseen todistamiseen tullaan tarvitsemaan Lagrangen lausetta.

Lause 2.11. *Olkoon p alkuluku ja olkoon d luvun $p - 1$ tekijä. Tällöin polynomilla $p(x) = x^d - 1$ on täsmälleen d kappaletta epäkongruentteja juuria modulo p.*

Todistus (vrt. [4, s. 316]). Merkitään $p - 1 = de$. Silloin

$$\begin{aligned} f(x) = x^{p-1} - 1 = x^{de} - 1 &= (x^d - 1)(x^{d(e-1)} + x^{d(e-2)} + ... + x^d + 1) \\ &= (x^d - 1)g(x) \\ &= p(x)g(x). \end{aligned}$$

Nyt Fermat'n pienen lauseen mukaan polynomilla $f(x)$ on $p - 1$ kappaletta epäkongruentteja juuria modulo p. Jokainen polynomin $f(x)$ juuri on, jomman kumman polynomin $p(x)$ tai $g(x)$ juuri modulo p.

Lagrangen lauseen mukaan polynomilla $g(x)$ on enintään $d(e-1) = de - d = p - 1 - d$ kappaletta juuria modulo p. Jokainen polynomin $f(x)$ juuri modulo p, joka ei ole polynomin $g(x)$ juuri modulo p, on oltava polynomin $p(x)$ juuri modulo p. Näin ollen polynomilla $p(x)$ on vähintään $(p-1)-(p-1-d) = d$ kappaletta juuria modulo p. Toisaalta Lagrangen lauseen mukaan polynomilla $p(x)$ on enintään d kappaletta epäkongruentteja juuria modulo p. Siis polynomilla $p(x)$ on täsmälleen d kappaletta juuria modulo p. Lause on näin todistettu. □

Lause 2.11 on tarpeellinen työkalu todistettaessa kuinka monella keskenään epäkongruentilla kokonaisluvulla on jokin tietty kertaluku modulo p. Ennen kyseistä lausetta, esitellään vielä apulause ja määritellään uusi funktio. Kun p alkuluku, niin jokaiselle luvun $p-1$ jakajalle, luvulle d, voidaan määriteellä funktio $F(d)$, joka ilmoittaa sellaisten lukujen a määrän, että $\mathrm{ord}_p a = d$, missä $1 \leq a < p$.

Määritelmä 2.4. Olkoon p alkuluku. Funktio $F(d)$ määritellään kaavalla

$$F(d) = \mid \{a : 1 \leq a < p, \mathrm{ord}_p a = d\} \mid, \text{ missä } d \mid p-1.$$

Esimerkki 2.12. Olkoon $p = 7$, joten $p - 1 = 7 - 1 = 6$. Nyt $F(2) = 1$, sillä $\mathrm{ord}_7 6 = 2$ ja $\mathrm{ord}_7 1, 2, 3, 4, 5 \neq 2$. Vastaavasti $F(3) = 2$, sillä $\mathrm{ord}_7 2, 4 = 3$ ja $\mathrm{ord}_7 1, 3, 5, 6 \neq 3$.

Apulause 2.12. *Olkoon p alkuluku ja olkoon d luvun $p-1$ positiivinen tekijä. Tällöin $F(d) \leq \phi(d)$.*

Todistus (vrt. [4, s. 316, 317]). Jos $F(d) = 0$, niin selvästi $F(d) \leq \phi(d)$. Muulloin on olemassa kokonaisluku a siten, että $\mathrm{ord}_p a = d$. Koska $\mathrm{ord}_p a = d$, niin kokonaisluvut

$$a^k, \text{ missä } k = 1, 2, ..., d,$$

ovat epäkongruentteja keskenään modulo p. Edelleen jokainen näistä kokonaisluvuista on polynomin $x^d - 1$ juuri modulo p, sillä $(a^k)^d = (a^d)^k \equiv 1 \pmod{p}$, kaikilla positiivisilla kokonaisluvuilla k. Lauseen 2.11 perusteella tiedetään, että polynomilla $x^d - 1$ on täsmälleen d kappaletta epäkongruentteja juuria modulo p, joten jokainen näistä juurista modulo p on kongruentti

yhden luvuista a^k kanssa. Lauseen 2.7 perusteella tiedetään, että luvun a^k kertaluku on luku d, jos $(k, d) = 1$. Tällaisia lukuja on täsmälleen $\phi(d)$ kappaletta kokonaislukuvälillä $[1, d]$. Siis jos on olemassa yksi sellainen luku a, että $\mathrm{ord}_p a = d$ ja $1 \leq a < p$, niin sellaisia lukuja on olemassa täsmälleen $\phi(d)$ kappaletta. Siis $F(d) \leq \phi(d)$. Lause on näin todistettu. □

Lause 2.13. *Olkoon p alkuluku ja olkoon d luvun $p-1$ positiivinen tekijä. Tällöin on olemassa täsmälleen $\phi(d)$ kappaletta keskenään epäkongruenttia kokonaislukua, joiden kertaluku on d modulo p.*

Todistus (vrt. [4, s. 317]). Koska kokonaisluvun kertaluku d modulo p ei ole jaollinen luvulla p, mutta jakaa luvun $p-1$, niin saadaan

$$p - 1 = \sum_{d|p-1} F(d)$$

Toisaalta, koska mielivaltaiselle positiiviselle kokonaisluvulle n pätee, että

$$\sum_{d|n} \phi(d) = \sum_{d|n} \phi(n/d) = n, \tag{2.3}$$

niin voidaan merkitä

$$p - 1 = \sum_{d|p-1} \phi(d).$$

Apulauseesta 2.12 ja yhtälöstä

$$\sum_{d|p-1} F(d) = \sum_{d|p-1} \phi(d)$$

seuraa, että $F(d) = \phi(d)$, jokaisella luvulla d, kun $d \mid p-1$. Siis kertaluvulla d on täsmälleen $\phi(d)$ kappaletta keskenään epäkongruentteja kantalukuja modulo p. Lause on näin todistettu. □

Huomautus. Lauseen 2.13 todistuksen kaavan 2.3 ominaisuutta ei tutkielmassa erikseen todisteta. (kts. [4, s. 226]). Lähdekirjan todistuksessa kyseisen ominaisuuden kohdalla viitataan kirjan aiempaan lauseeseen, joka esittelee ja todistaa väitteen. Viittaus on osoitettu kuitenkin väärään lauseeseen. Myös seuraavan lauseen lähdekirjan todistuksessa on samanlainen viittausvirhe.

Lause 2.14. *Jokaisella alkuluvulla on primitiivinen juuri.*

Todistus (vrt. [4, s. 317]). Olkoon p alkuluku. Tällöin lauseen 2.13 mukaan on olemassa täsmälleen $\phi(p-1)$ kappaletta keskenään epäkongruenttia kokonaislukua, joiden kertaluku on $p-1$ modulo p. Nyt jokainen näistä kokonaisluvuista on primitiivisen juuren määritelmän mukaan primitiivinen juuri modulo p, joten primitiivisiä juuria on olemassa $\phi(p-1)$ kappaletta. Siis jokaisella alkuluvulla p on $\phi(p-1)$ kappaletta primitiivisiä juuria. Lause on näin todistettu. □

Seuraavaksi osoitetaan, että jokaisella parittoman alkuluvun potenssilla on primitiivinen juuri. Tämän väitteen todistamisessa ensiaskel on osoittaa, että jokaisella parittoman alkuluvun neliöllä on primitiivinen juuri.

Lause 2.15. *Jos p on pariton alkuluku ja r sen primitiivinen juuri, niin silloin r tai $r+p$ on primitiivinen juuri modulo p^2.*

Todistus (vrt. [4, s. 321, 322]). Koska r on primitiivinen juuri modulo p, niin tiedetään, että

$$\mathrm{ord}_p r = \phi(p) = p-1.$$

Olkoon $n = \mathrm{ord}_{p^2} r$, joten

$$r^n \equiv 1 \pmod{p^2}.$$

Koska selvästi $p \mid p^2$, niin saadaan

$$r^n \equiv 1 \pmod{p}.$$

Koska r on primitiivinen juuri modulo p, niin lauseesta 2.1 seuraa, että

$$p-1 \mid n. \tag{2.4}$$

Toisaalta seurauksesta 2.2 seuraa, että

$$n \mid \phi(p^2).$$

Koska lauseen 1.16 mukaan $\phi(p^2) = p(p-1)$, niin tästä seuraa, että $n \mid p(p-1)$. Nyt koska $n \mid p(p-1)$ ja $p-1 \mid n$, niin $n = p-1$ tai $n = p(p-1)$. Jos $n = p(p-1)$, niin r on primitiivinen juuri modulo p^2, sillä $\mathrm{ord}_{p^2} r = p(p-1) = \phi(p^2)$. Jos $n = p-1$, niin

$$r^{p-1} \equiv 1 \pmod{p^2}.$$

Olkoon nyt $s = r + p$. Tällöin luku s on myös primitiivinen juuri modulo p, sillä $s \equiv r \pmod{p}$. Siis $\mathrm{ord}_{p^2} s = p - 1$ tai $\mathrm{ord}_{p^2} s = p(p-1)$. Näistä kahdesta vaihtoehdosta eliminoidaan ensimmäinen, jolloin jälkimmäinen vaihtoehto jää voimaan. Osoitettaessa, että $\mathrm{ord}_{p^2} s \neq p - 1$, käytetään aluksi hyväksi binomilausetta. Koska yleinen binomi lause on muotoa

$$\begin{aligned}(x+y)^n =& \binom{n}{0}x^n + \binom{n}{1}x^{n-1}y + \binom{n}{2}x^{n-2}y^2 + ... \\ &+ \binom{n}{n-2}x^2y^{n-2} + \binom{n}{n-1}xy^{n-1} + \binom{n}{n}y^n,\end{aligned}$$

missä $x, y \in \mathbb{Z}$ ja $n \in \mathbb{Z}_+$, niin nyt

$$\begin{aligned}s^{p-1} = (r+p)^{p-1} &= r^{p-1} + (p-1)r^{p-2}p + \binom{p-1}{2}r^{p-3}p^2 + ... + p^{p-1} \\ &\equiv r^{p-1} + (p-1)p \cdot r^{p-2} \pmod{p^2}.\end{aligned}$$

Nyt koska $r^{p-1} \equiv 1 \pmod{p^2}$, niin saadaan

$$\begin{aligned}s^{p-1} \equiv 1 + (p-1)p \cdot r^{p-2} &\equiv 1 + \underbrace{p^2 r^{p-2}}_{\equiv 0 \pmod{p^2}} - pr^{p-2} \\ &\equiv 1 - pr^{p-2} \pmod{p^2}.\end{aligned}$$

Nyt viimeisen kongruenssin muodosta on helppo osoittaa, että $s^{p-1} \not\equiv 1 \pmod{p^2}$, sillä jos niin olisi, niin silloin $pr^{p-2} \equiv 0 \pmod{p^2}$. Edellisestä seuraa, että $r^{p-2} \equiv 0 \pmod{p}$, mikä on mahdotonta, sillä selvästi $p \nmid r$.

Siis koska $\mathrm{ord}_{p^2} s \neq p - 1$, niin $\mathrm{ord}_{p^2} s = p(p-1) = \phi(p^2)$. Siis $s = r + p$ on primitiivinen juuri modulo p^2. Lause on näin todistettu. □

Huomautus. Lauseen 2.15 todistuksessa apuna käytetty binomilause oletetaan lukijalta tunnetuksi. Lähdekirjan todistuksen kaavaa (2.4) vastaavassa kaavassa on painovirhe.

Esimerkki 2.13. Esimerkin 2.6 mukaan luku 2 on primitiivinen juuri modulo 11. Nyt lauseen 2.15 todistuksessa käytettävien sääntöjen mukaan pätee joko $\mathrm{ord}_{121} 2 = 10$ tai $\mathrm{ord}_{121} 2 = 110$. Koska

$$r^{p-1} = 2^{10} = 1024 \not\equiv 1 \pmod{121},$$

niin pätee $\mathrm{ord}_{121} 2 = 110$. Siis luku 2 on primitiivinen juuri myös modulo 121.

Huomautus. Erittäin harvoin on se tilanne , että

$$r^{p-1} \equiv 1 \pmod{p^2},$$

missä p on alkuluku ja r on primitiivinen juuri modulo p. Tällöin siis $\mathrm{ord}_{p^2} r = p - 1$ eli r ei olekaan silloin primitiivinen juuri modulo p^2. Täten toinen vaihtoehto eli luku $r + p$ on lauseen 2.15 mukaan primitiivinen juuri modulo p^2.

Esitellään vielä yksi tarvittava apulause.

Apulause 2.16. *Olkoon p pariton alkuluku ja olkoon r sellainen luvun p primitiivinen juuri, että $r^{p-1} \not\equiv 1 \pmod{p^2}$. Tällöin kaikille kokonaisluvuille $k \geq 2$ pätee*

$$r^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}.$$

Todistus (vrt. [4, s. 323, 324] ja [2, s. 170, 171]). Aluksi pitää huomata, että lauseen 2.15 todistuksen eri välivaiheiden perusteella tiedetään, että luvulla p ylipäätään on olemassa sellainen primitiivinen juuri r, että

$$r^{p-1} \not\equiv 1 \pmod{p^2}.$$

Nyt osoitetaan, että tälle primitiiviselle juurelle r pätee

$$r^{\phi(p^{k-1})} = r^{p^{k-1}-p^{k-2}} = r^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k},$$

kaikilla kokonaisluvuilla $k \geq 2$. Tehdään todistus induktiolla luvun k suhteen. Selvästi väite pätee, kun $k = 2$. Tehdään induktio-oletus, että väite pätee mielivaltaisella arvolla $k \geq 2$. Todistetaan, että väite on totta myös arvolla $k + 1$. Koska $(r, p) = 1$, niin lauseen 2.5 perusteella $(r, p^{k-1}) = (r, p^k) = 1$. Täten Eulerin lauseesta seuraa, että

$$r^{p^{k-2}(p-1)} = r^{\phi(p^{k-1})} \equiv 1 \pmod{p^{k-1}}.$$

Siis kongruenssin määritelmän mukaan on olemassa sellainen kokonaisluku a, että

$$r^{p^{k-2}(p-1)} = 1 + ap^{k-1},$$

missä induktio-oletuksen perusteella $p \nmid a$. Korotetaan nyt yhtälön molemmat puolet potenssiin p, ja binomilauseen avulla saadaan

$$\begin{aligned} r^{p^{k-1}(p-1)} &= (1 + ap^{k-1})^p \\ &\equiv 1 + ap^k \pmod{p^{k+1}}. \end{aligned}$$

Koska $p \nmid a$, niin

$$r^{p^{k-1}(p-1)} = r^{p^k - p^{k-1}} = r^{\phi(p^k)} \not\equiv 1 \pmod{p^{k+1}}.$$

Väite pätee arvolla $k+1$, joten väite pätee kaikilla kokonaisluvuilla $k \geq 2$. Lause on näin todistettu. □

Lause 2.17. *Jos p on pariton alkuluku ja luku k on positiivinen kokonaisluku, niin luvulla p^k on primitiivinen juuri.*

Todistus (vrt. [4, s. 323] ja [2, s. 171]). Apulauseen 2.16 perusteella voidaan valita luvun p primitiivinen juuri r siten, että

$$r^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}.$$

Nyt siis osoitetaan, että tällainen luku r on primitiivinen juuri modulo p^k, $\forall k \in \mathbb{Z}_+$. Olkoon

$$n = \operatorname{ord}_{p^k} r.$$

Lauseen 2.1 mukaan tiedetään, että

$$n \mid \phi(p^k) = p^{k-1}(p-1). \tag{2.5}$$

Toisaalta tiedetään, että koska

$$r^n \equiv 1 \pmod{p^k},$$

niin

$$r^n \equiv 1 \pmod{p}.$$

Nyt koska r on primitiivinen juuri modulo p, niin $\operatorname{ord}_p r = p-1$, joten seurauksen 2.2 perusteella $p-1 \mid n$. Koska $p-1 \mid n$ ja $n \mid p^{k-1}(p-1)$, niin luvun n on oltava muotoa $p^t(p-1)$, missä $0 \leq t \leq k-1$. Jos $n = p^t(p-1)$ siten, että $t \leq k-2$, niin

$$r^{p^{k-2}(p-1)} = r^{p^t(p-1)\cdot p^{k-2-t}} = (r^{p^t(p-1)})^{p^{k-2-t}} \equiv 1 \pmod{p^k}, \tag{2.6}$$

mikä on ristiriita. Siis

$$\text{ord}_{p^k} r = p^{k-1}(p-1) = \phi(p^k). \tag{2.7}$$

Siis luku r on primitiivinen juuri myös modulo p^k. Lause on näin todistettu. □

Huomautus. Lauseen 2.17 lähdekirjan [4] todistuksessa on useita eri virheitä. Kaavoja 2.5, 2.6 ja 2.7 vastaavissa kaavoissa olevat virheet/painovirheet ovat suhteellisen isoja. Lisäksi todistuksessa viitataan vielä väärään aiempaan lauseeseen. Lähdekirjan [2] todistuksesta on jätetty tarkastelematta sellaiset t:n arvot, että $t < k - 2$.

Lause 2.18. *Olkoon luku p pariton alkuluku. Jos luku r on primitiivinen juuri modulo p^2, niin se on primitiivinen juuri myös modulo p^k, kaikilla positiivisilla kokonailuvuilla k.*

Todistus. Tulos seuraa aivan suoraan edellisistä lauseista. Lauseen 2.15 todistuksen eri välivaiheiden nojalla voidaan valita sellainen luvun p^2 primitiivinen juuri, että

$$r^{p-1} \not\equiv 1 \pmod{p^2}.$$

Nyt apulauseen 2.16 mukaan kyseiselle luvulle r pätee

$$r^{p^{k-2}(p-1)} \not\equiv 1 \pmod{p^k}, \forall k \in \mathbb{Z}_+.$$

Lopulta lauseen 2.17 mukaan r on primitiivinen juuri modulo p^k. Lause on näin todistettu. □

Esimerkki 2.14. Esimerkin 2.13 mukaan $r = 2$ on primitiivinen juuri modulo 11^2. Siis lauseen 2.18 mukaan $r = 2$ on primitiivinen juuri myös modulo 11^k, $\forall k \in \mathbb{Z}_+$.

Seuraavaksi perehdytään luvun 2 potenssien primitiivisiin juuriin. Huomataan, että $\text{ord}_2 1 = 1 = \phi(2)$ ja $\text{ord}_4 3 = 2 = \phi(4)$, joten luvuilla 2^1 ja 2^2 on primitiiviset juuret. Jos luvun 2 potenssit ovat suurempia kuin luku 2, niin tilanne on toinen, kuten seuraava lause osoittaa.

Lause 2.19. *Luvulla 2^k ei ole primitiivisiä juuria, kun $k \geq 3$.*

Todistus (vrt. [2, s. 168]). Aluksi osoitamme, että jos a on pariton kokonaisluku, niin

$$a^{2^{k-2}} \equiv 1 \pmod{2^k}, \text{ kun } k \geq 3.$$

Todistetaan induktiolla luvun k suhteen. Jos $k = 3$, niin kongruenssi on muotoa $a^2 \equiv 1 \pmod 8$. Selvästi $1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod 8$. Tehdään induktio-oletus, että väite pätee, kun $k > 3$. Kongruenssi $a^{2^{k-2}} \equiv 1 \pmod{2^k}$ on suoraan kongruenssin määritelmän mukaan ekvivalentti yhtälölle

$$a^{2^{k-2}} = 1 + 2^k b,$$

missä b on kokonaisluku. Korotetaan yhtälön molemmat puolet toiseen, saadaan

$$\begin{aligned}(a^{2^{k-2}})^2 = a^{2^{k-1}} &= (1 + 2^k b)^2 \\ &= 1 + 2(2^k b) + (2^k b)^2 \\ &= 1 + 2^{k+1}(b + b^2 2^{k-1}) \\ &\equiv 1 \pmod{2^{k+1}},\end{aligned}$$

joten kongruenssi $a^{2^{k-2}} \equiv 1 \pmod{2^k}$ pätee arvolla $k+1$. Siis induktiotodistuksen perusteella kyseinen kongruenssi pätee kaikilla kokonaisluvuilla $k \geq 3$.

Nyt kokonaisluvut, jotka ovat suhteellisia alkulukuja luvun 2^k kanssa, ovat kaikki parittomat luvut. Siis ainoat mahdolliset kokonaisluvut, jotka voivat olla primittiivisiä juuria modulo 2^k, ovat parittomia, mutta edellisen todistuksen perusteella, kun $k \geq 3$, niin kaikille parittomille kokonaisluvuille a pätee

$$a^{2^{k-2}} = a^{2^{k-1-1}} = a^{2^{k-1} \cdot 2^{-1}} = a^{2^{k-1}/2} = a^{\phi(2^k)/2} \equiv 1 \pmod{2^k}.$$

Täten $\operatorname{ord}_{2^k} a \neq \phi(2^k)$, joten ei ole olemassa primitiivisiä juuria modulo 2^k, kun $k \geq 3$. Lause on näin todistettu. □

Nyt on osoitettu, että jokaisella alkuluvulla ja parittoman alkuluvun potenssilla on primitiivinen juuri. On myös todistettu, että luvun 2 potensseista ainoastaan luvuilla 2 ja 4 on primitiivinen juuri. Jäljelle jää vielä tapaus, kun luku on muotoa $2p^k$, missä p on pariton alkuluku ja k on kokonaisluku. Seuraavaksi määritetäänkin kaikki ne yhdistetyt luvut, jotka eivät ole alkuluvun

potensseja, mutta jotka silti omaavat primitiivisiä juuria. Osoitetaan, että näistä kokonaisluvuista ainoastaan muotoa $2p^k$ olevilla kokonaisluvuilla on primitiivisiä juuria.

Lause 2.20. *Jos p on pariton alkuluku ja luku k on positiivinen kokonaisluku, niin luvulla $2p^k$ on primitiivinen juuri.*

Todistus (vrt. [2, s. 171]). Lauseen 2.17 perusteella voidaan valita seuraavasti: olkoon luku r primitiivinen juuri modulo p^k. Voidaan olettaa, että luku r on pariton luku, sillä jos r on parillinen, niin luku $r + p^k$, joka myös on primitiivinen juuri modulo p^k, on pariton. Siis $(r, 2p^k) = 1$. Olkoon $n = \mathrm{ord}_{2p^k} r$. Nyt Eulerin lauseesta seuraa, että

$$r^{\phi(2p^k)} \equiv 1 \pmod{2p^k}.$$

Nyt seurauksen 2.2 mukaan

$$n = \mathrm{ord}_{2p^k} r \mid \phi(2p^k) = \phi(2)\phi(p^k) = \phi(p^k). \tag{2.8}$$

Toisaalta $r^n \equiv 1 \pmod{2p^k}$, joten $r^n \equiv 1 \pmod{p^k}$. Edelleen seurauksen 2.2 perusteella $\mathrm{ord}_{p^k} r = \phi(p^k) \mid n$, sillä r on primitiivinen juuri modulo p^k. Nyt koska $n \mid \phi(p^k)$ ja $\phi(p^k) \mid n$, niin

$$n = \phi(2p^k). \tag{2.9}$$

Siis luku r on primitiivinen juuri modulo $2p^k$. Lause on näin todistettu. □

Huomautus. Lauseen 2.20 todistuksen kaavat 2.8 ja 2.9 perustuvat Eulerin phi-funktion multiplikatiivisuusominaisuuteen, jonka esittelyä ei ole katsottu tarpeelliseksi tutkielman aiheen kannalta.(kts. [2, s. 171]).

Jos yhdistetty luku ei ole alkuluvun potenssi, niin se on selvästi jaollinen kahdella tai useammalla alkuluvulla. Seuraavaksi todistetaan, että tällaisella kokonaisluvulla, paitsi lauseen 2.20 tapauksessa, ei ole primitiivisiä juuria.

Lause 2.21. *Jos luku n on positiivinen yhdistetty kokonaisluku, joka ei ole parittoman alkuluvun potenssi tai kaksi kertaa parittoman alkuluvun potenssi, niin luvulla n ei ole priimitiivistä juurta.*

Todistus (vrt. [4, s. 326, 327]). Luvun n alkutekijäesitys on muotoa

$$n = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}. \tag{2.10}$$

Tehdään vastaoletus ja oletetaan, että luvulla n on primitiivinen juuri r. Täten $(r, n) = 1$ ja $\mathrm{ord}_n r = \phi(n)$. Koska $(r, n) = 1$, niin $(r, p^k) = 1$, aina kun luku p^k on yksi luvun n alkutekijäesityksen termi. Nyt Eulerin lauseesta seuraa, että

$$r^{\phi(p^k)} \equiv 1 \pmod{p^k}.$$

Merkitään nyt

$$U = [\phi(p_1^{k_1}), \phi(p_2^{k_1}), ..., \phi(p_m^{k_m})].$$

Koska pienimmän yhteisen monikerran määritelmän mukaan $\phi(p_1^{k_1}) \mid U$, niin

$$r^U \equiv 1 \pmod{p_i^{k_i}}, \tag{2.11}$$

kaikilla $i = 1, 2, ..., m$. Koska kiinalaisen jäännöslauseen perusteella

$$r^U \equiv 1 \pmod{n},$$

niin saadaan

$$\mathrm{ord}_n r = \phi(n) \leq U.$$

Toisaalta phi-funktion multiplikatiivisuudesta seuraa, että

$$\phi(n) = \phi(p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}) = \phi(p_1^{k_1})\phi(p_2^{k_2}) \cdots \phi(p_m^{k_m}).$$

Nyt siis saadaan

$$\phi(p_1^{k_1})\phi(p_2^{k_2}) \cdots \phi(p_m^{k_m}) \leq [\phi(p_1^{k_1}), \phi(p_2^{k_1}), ..., \phi(p_m^{k_m})].$$

Jotta tämä järjestysrelaatio pätee, on kokonaislukujen $\phi(p_1^{k_1}), \phi(p_2^{k_2}), ..., \phi(p_m^{k_m})$ oltava pareittain suhteellisia alkulukuja.

Lauseen 1.16 mukaan $\phi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$, joten $\phi(p^k)$ on parillinen, jos p on pariton tai $p = 2$ ja $k \geq 2$. Siis kokonaisluvut $\phi(p_1^{k_1}), \phi(p_2^{k_2}), ..., \phi(p_m^{k_m})$ eivät ole pareittain suhteellisia alkulukuja, ellei $m = 1$ ja n alkuluvun potenssi, tai $m = 2$ ja $n = 2p^t$, missä p on pariton alkuluku ja k on positiivinen kokonaisluku. Täten positiivisella yhdistetyllä kokonaisluvulla, joka ei ole parittoman alkuluvun potenssi tai kaksi kertaa parittoman alkuluvun potenssi, ei ole priimitiivistä juurta. Lause on näin todistettu. □

Huomautus. Lähdekirjan lauseen 2.21 todistuksen yhtälöä 2.10 vastaavassa yhtälössä ja kongruenssia 2.11 vastaavassa kongruenssissa on indeksi- ja painovirheet.

Nyt kerätään palaset yhteen ja saadaan yksi tutkielman päätavoitteista lauseen muodossa.

Lause 2.22. *Positiivisella kokonaisluvulla* $n(>1)$ *on primitiivinen juuri, jos ja vain jos*

$$n = 2, 4, p^k \text{ tai } 2p^k,$$

missä p *on pariton alkuluku ja* k *on positiivinen kokonaisluku.*

Todistus. Tulos seuraa suoraan lauseista 2.14, 2.17, 2.19, 2.20 ja 2.21. Lause on näin todistettu. □

2.4 Diskreetti logaritmi

Tässä alaluvussa esitellään lyhyesti yksi primitiivisten juurten sovelluksista, jolle on käyttöä modulääriaritmetiikassa. Olkoon r primitiivinen juuri modulo m. Nyt lauseen 2.6 mukaan kokonaisluvut

$$r^1, r^2, ..., r^{\phi(m)}$$

muodostavat supistetun jäännössysteemin modulo m. Siis jos luku a on suhteellinen alkuluku luvun m kanssa, niin tiedetään, että on olemassa sellainen yksikäsitteinen kokonaisluku x, että $1 \leq x \leq \phi(m)$ ja

$$r^x \equiv a \pmod{m}.$$

On siis mielekästä määritellä seuraavasti.

Määritelmä 2.5. Olkoon r primitiivinen juuri modulo m ja $(a, m) = 1$. Tällöin yksikäsitteistä lukua x, jolle pätee $1 \leq x \leq \phi(m)$ ja $r^x \equiv a \pmod{m}$, sanotaan luvun a *r-kantaiseksi logaritmiksi modulo m (eli indeksiksi)* ja merkitään $x = \text{ind}_r a$.

On huomattava, että vaikka merkinnässä $x = \text{ind}_r a$ ei esiinny modulia m, niin silti luku $\text{ind}_r a$ riippuu modulista m.

Huomautus. Selvästi määritelmä sanoo, että $1 \leq \text{ind}_r a \leq \phi(m)$ ja $r^{\text{ind}_r a} \equiv a \pmod{m}$. On myös huomattava, että keskenään kongruenteilla luvuilla modulo m on samat indeksit. Täsmennetään hieman. Olkoot $(a, m) = (b, m) = 1$ ja $a \equiv b \pmod{m}$. Koska $r^{\text{ind}_r a} \equiv a \pmod{m}$ ja $r^{\text{ind}_r b} \equiv b \pmod{m}$, niin $r^{\text{ind}_r a} \equiv r^{\text{ind}_r b} \pmod{m}$. Koska luku r on primitiivinen juuri modulo m, niin lauseen 2.3 mukaan $\text{ind}_r a \equiv \text{ind}_r b \pmod{\phi(m)}$. Nyt koska $1 \leq \text{ind}_r a \leq \phi(m)$ ja $1 \leq \text{ind}_r b \leq \phi(m)$, niin $\text{ind}_r a = \text{ind}_r b$.

Esimerkki 2.15. Olkoon $m = 5$. Luku 2 on primitiivinen juuri modulo 5, sillä $\text{ord}_5 2 = \phi(5)$. Nyt $2^1 \equiv 2 \pmod{5}$, $2^2 \equiv 4 \pmod{5}$, $2^3 \equiv 3 \pmod{5}$ ja $2^4 \equiv 1 \pmod{5}$. Siis modulo 5 pätee

$$\text{ind}_2 1 = 4, \text{ind}_2 2 = 1, \text{ind}_2 3 = 3 \text{ ja } \text{ind}_2 4 = 2.$$

Koska $\text{ord}_5 3 = \phi(5)$, niin myös luku 3 on primitiivinen juuri modulo 5. Nyt saadaan eri indeksien arvot, modulo 5 pätee

$$\text{ind}_3 1 = 4, \text{ind}_3 2 = 3, \text{ind}_3 3 = 1 \text{ ja } \text{ind}_3 4 = 2.$$

Indeksien laskusäännöt muistuttavat logaritmien laskusääntöjä. Logaritmien kantalukua vastaa nyt primitiivinen juuri r ja yhtäsuuruus korvataan käsitteellä kongruenssi modulo $\phi(m)$.

Lause 2.23. *Olkoot m positiivinen kokonaisluku ja luku r primitiivinen juuri modulo m. Olkoon $(a, m) = (b, m) = 1$. Tällöin*

1. $\text{ind}_r 1 \equiv 0 \pmod{\phi(m)}$,
2. $\text{ind}_r(ab) \equiv \text{ind}_r a + \text{ind}_r b \pmod{\phi(m)}$,
3. $\text{ind}_r(a^k) \equiv k \cdot \text{ind}_r a \pmod{\phi(m)}$, *jos* $k \in \mathbb{Z}_+$.

Todistus (vrt. [4, s. 330, 331]). 1) Eulerin lauseen perusteella tiedetään, että $r^{\phi(m)} \equiv 1 \pmod{m}$. Primitiivisen juuren määritelmän mukaan luku $\phi(m)$ on pienin positiivinen kokonaisluku siten, että $r^{\phi(m)} \equiv 1 \pmod{m}$. Siis $\text{ind}_r 1 = \phi(m) \equiv 0 \pmod{\phi(m)}$.
2) Diskreetin logaritmin määritelmän mukaan

$$r^{\text{ind}_r(ab)} \equiv ab \pmod{m}$$

ja

$$r^{\mathrm{ind}_r a+\mathrm{ind}_r b} = \underbrace{r^{\mathrm{ind}_r a}}_{\equiv a \pmod m} \cdot \underbrace{r^{\mathrm{ind}_r b}}_{\equiv b \pmod m} \equiv ab \pmod m.$$

Siis

$$r^{\mathrm{ind}_r(ab)} \equiv r^{\mathrm{ind}_r a+\mathrm{ind}_r b} \pmod m.$$

Nyt lauseen 2.3 perusteella saadaan

$$\mathrm{ind}_r(ab) \equiv \mathrm{ind}_r a + \mathrm{ind}_r b \pmod{\phi(m)}.$$

3) Olkoon k positiivinen kokonaisluku. Nyt diskreetin logaritmin määritelmästä saadaan, että

$$r^{\mathrm{ind}_r a^k} \equiv a^k \pmod m.$$

Koska exponenttien laskusääntöjen perusteella

$$r^{k\cdot\mathrm{ind}_r a} = \underbrace{(r^{\mathrm{ind}_r a})^k}_{\equiv a^k \pmod m},$$

niin selvästi

$$r^{\mathrm{ind}_r a^k} \equiv r^{k\cdot\mathrm{ind}_r a} \pmod m.$$

Jälleen käytetään lausetta 2.3 ja saadaan

$$\mathrm{ind}_r(a^k) \equiv k \cdot \mathrm{ind}_r a \pmod{\phi(m)}.$$

Lauseen kaikki 3 kohtaa on näin todistettu. □

Esimerkki 2.16. Olkoon $m = 5$, joten $\phi(5) = 4$. Esimerkissä 2.15 saatiin, että $\mathrm{ind}_2 2 = 1$ ja $\mathrm{ind}_2 3 = 3$. Nyt lauseen 2.23 mukaan

$$\mathrm{ind}_2 4 = \mathrm{ind}_2(2 \cdot 2) = \mathrm{ind}_2 2 + \mathrm{ind}_2 2 = 1 + 1 \equiv 2 \pmod 4,$$

kuten on saatu myös esimerkissä 2.15.
Havainnollistetaan vielä lauseen 2.23 kohtaa 3. Selvästi

$$\mathrm{ind}_2(3^3) = 3 \cdot \mathrm{ind}_2 3 \equiv 3 \cdot 3 = 9 \equiv 1 \pmod 4$$

ja sama pätee, kun lasketaan suoraan, sillä

$$\mathrm{ind}_2(3^3) = \mathrm{ind}_2 27 = \mathrm{ind}_2 2 = 1.$$

Aiemmin on todettu diskreettien logaritmien helpottavan tietynlaisten kongruenssien ratkaisemista. Näytetään hyvä esimerkki aiheesta.

Esimerkki 2.17. Ratkaistaan diskreettien logaritmien avulla kongruenssi $5x^{13} \equiv 9 \pmod{11}$. Esimerkissä 2.6 todettin luvun 2 olevan primitiivinen juuri modulo 11. Laaditaan taulukko 1, josta ilmenevät 2-kantaiset diskreetit logaritmit modulo 11.

a	1	2	3	4	5	6	7	8	9	10
$\text{ind}_2 a$	10	1	8	2	4	9	7	3	6	5

Taulukko 1: 2-kantaiset diskreetit logaritmit modulo 11.

Otetaan kongruenssin kummastakin puolesta 2-kantainen diskreetti logaritmi modulo 11, joten saadaan

$$\text{ind}_2(5x^{13}) \equiv \text{ind}_2 9 = 6 \pmod{10}.$$

Seuraavaksi käytetään lausetta 2.23 ja saadaan

$$\text{ind}_2(5x^{13}) \equiv \text{ind}_2 5 + \text{ind}_2(x^{13}) \equiv 4 + 13 \cdot \text{ind}_2 x \equiv 4 + 2 \cdot \text{ind}_2 x \pmod{10}.$$

Siis

$$4 + 2 \cdot \text{ind}_2 x \equiv 6 \pmod{10}$$

eli

$$2 \cdot \text{ind}_2 x \equiv 2 \pmod{10}.$$

Kun ratkaistaan kyseinen lineaarinen kongruenssi, niin saadaan

$$\text{ind}_2 x \equiv 1 \pmod{5}.$$

Siis

$$\text{ind}_2 x \equiv 1, 6 \pmod{10}.$$

Näin ollen diskreetin logaritmin määritelmän mukaan

$$x \equiv 2^1, 2^6 \pmod{11} \quad \text{eli} \quad x \equiv 2, 9 \pmod{11}.$$

Koska edellisen laskennan jokainen vaihe on voimassa myös käänteisesti, niin on saatu kongruenssin $5x^{13} \equiv 9 \pmod{11}$ ratkaisu.

Jos valitaan luvun 11 joku toinen primitiivinen juuri, niin luonnollisesti indeksitaulukon arvot muuttuvat, mutta annetun kongruenssin ratkaisemiseen tällä ei ole merkitystä. Esimerkin 2.6 mukaan myös luvut $6, 7$ ja 8 ovat primitiivisiä juuria modulo 11. Nyt taulukossa 2 on esitetty 6-kantaiset diskreetit logaritmit modulo 11.

a	1	2	3	4	5	6	7	8	9	10
$\text{ind}_6 a$	10	9	2	8	6	1	3	7	4	5

Taulukko 2: 6-kantaiset diskreetit logaritmit modulo 11.

Nyt kongruenssin $5x^{13} \equiv 9 \pmod{11}$ kummastakin puolesta otetaan 6-kantainen diskreetti logaritmi modulo 11, joten saadaan

$$\text{ind}_6(5x^{13}) \equiv \text{ind}_6 9 = 4 \pmod{10}.$$

Nyt

$$\text{ind}_6(5x^{13}) \equiv \text{ind}_6 5 + \text{ind}_6(x^{13}) \equiv 6 + 13 \cdot \text{ind}_6 x \equiv 6 + 2 \cdot \text{ind}_2 x \pmod{10}.$$

Siis

$$6 + 2 \cdot \text{ind}_2 x \equiv 4 \pmod{10}$$

eli

$$2 \cdot \text{ind}_2 x \equiv 8 \pmod{10}.$$

Kun ratkaistaan kyseinen lineaarinen kongruenssi, niin saadaan

$$\text{ind}_2 x \equiv 4 \pmod{5}.$$

Siis

$$\text{ind}_2 x \equiv 4, 9 \pmod{10}.$$

Näin ollen diskreetin logaritmin määritelmän mukaan

$$x \equiv 6^4, 6^9 \pmod{11} \quad \text{eli} \quad x \equiv 9, 2 \pmod{11}.$$

Saatiin siis täsmälleen samat ratkaisut kuin aiemminkin.

Lause 2.24. *Olkoon r primitiivinen juuri modulo m ja $(a, m) = 1$. Tällöin kongruenssilla $x^k \equiv a \pmod{m}$ on ratkaisu, jos ja vain jos*

$$a^{\phi(m)/d} \equiv 1 \pmod{m},$$

missä $d = (k, \phi(m))$. Jos ratkaisu on olemassa, niin silloin niitä on olemassa täsmälleen d kappaletta.

Todistus (vrt. [2, s. 176]). Nyt diskreettien logaritmien laskusääntöjen mukaan kongruenssi $a^{\phi(m)/d} \equiv 1 \pmod{m}$ saadaan muotoon

$$\frac{\phi(m)}{d} \cdot \operatorname{ind}_r a \equiv 0 \pmod{\phi(m)}.$$

Tämä kongruenssi pätee, jos ja vain jos $d \mid \operatorname{ind}_r a$. Toisaalta kongruenssi $x^k \equiv a \pmod{m}$ saadaan muotoon

$$k \cdot \operatorname{ind}_r x \equiv \operatorname{ind}_r a \pmod{\phi(m)},$$

mikä on lauseen 1.15 mukaan ratkeava, jos ja vain jos $(k, \phi(m)) = d \mid \operatorname{ind}_r a$. Siis kongruenssi $x^k \equiv a \pmod{m}$ on ratkeava, jos ja vain jos $a^{\phi(m)/d} \equiv 1 \pmod{m}$.

Lauseen jälkimmäinen osa palautuu kongruenssiin $ax \equiv b \pmod{m}$ ja sen ratkaisujen määrään, tämä ominaisuus esitellään huomautuksessa 1 (s. 14). Lause on näin todistettu. □

Esimerkki 2.18. Ratkaistaan kongruenssi $x^5 \equiv 7 \pmod{11}$. Aluksi tarkastellaan kongruenssin ratkeavuutta lauseen 2.24 avulla. Nyt $d = (5, \phi(11)) = (5, 10) = 5$, joten $\phi(11)/5 = 2$. Koska $7^2 \equiv 49 \not\equiv 1 \pmod{11}$, niin kongruenssi ei ole ratkeava.

Toisaalta lauseen 2.24 mukaan kongruenssi $x^5 \equiv 10 \pmod{11}$ on ratkeava, sillä $10^2 \equiv 99 \equiv 1 \pmod{11}$. Nyt kongruenssin $x^5 \equiv 10 \pmod{11}$ kummastakin puolesta otetaan 2-kantainen diskreetti logaritmi modulo 11, joten saadaan

$$5 \cdot \operatorname{ind}_2 x \equiv 5 \pmod{10}.$$

Siis

$$\operatorname{ind}_2 x \equiv 1 \pmod{2}.$$

Siis

$$\text{ind}_2 x \equiv 1, 3, 5, 7, 9 \pmod{10}.$$

Lopulta ratkaisuksi saadaan

$$x \equiv 2^1, 2^3, 2^5, 2^7, 2^9 \pmod{11} \quad \text{eli} \quad x \equiv 2, 8, 10, 7, 6 \pmod{11}.$$

Viitteet

[1] Apostol, Tom M., *Introduction to Analytic Number Theory*, Springer-Verlag, New York, 1976.

[2] Burton, David M., *Elementary Number Theory*, fifth ed., McGraw-Hill, New York, 2002.

[3] Jones, Gareth A. and Jones, J. Mary, *Elementary Number Theory*, Spriger, London, 1998.

[4] Rosen, Kenneth H., *Elementary number theory and its applications*, 4th ed., Addison-Wesley, Reading, Massachusetts, 2000.