TAMPEREEN YLIOPISTO
Pro gradu -tutkielma

Marianna Rajala

Neliönjäännösten resiprookkilaki: todistus ja sovelluksia

Matematiikan ja tilastotieteen laitos
Matematiikka
Toukokuu 2009

Tampereen yliopisto

Matematiikan ja tilastotieteen laitos

Rajala, Marianna: Neliönjäännösten resiprookkilaki: todistus ja sovelluksia

Pro gradu -tutkielma, 55 s., 1 liites.

Matematiikka

Toukokuu 2009

Tiivistelmä

Olkoot p ja q erisuuria parittomia alkulukuja. Oletetaan silloin, että tiedetään, onko q neliönjäännös modulo p vai neliönepäjäännös modulo p. Tällöin voidaan kysyä, tiedetäänkö silloin, että p on neliönjäännös modulo q tai neliönepäjäännös modulo q.

Euler löysi kokeellisesti tähän kysymykseen myöntävän vastauksen vuonna 1783. Hän ei kuitenkaan pystynyt todistamaan vastausta oikeaksi. Vuonna 1785 Legendre muotoili Eulerin vastauksen uudelleen elegantimpaan lauseen muotoon käyttämällä omalla nimellään kulkevaa symbolia. Tämä lause tunnetaan nykyisin neliönjäännösten resiprookkilakina ja se kertoo, onko kongruenssilla $x^2 \equiv q \pmod{p}$ ratkaisuja, kun tiedetään, onko kongruenssilla $x^2 \equiv p \pmod{q}$ ratkaisuja.

Tässä tutkielmassa todistetaan neliönjäännösten resiprookkilaista muoto

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

ja todistetaan se ekvivalentiksi muodon

$$p \equiv \pm q \pmod{4a} \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$$

kanssa. Lisäksi esitetään lauseen sovelluksia.

Lukijalta edellytetään joidenkin lukuteorian perusasioiden tuntemista. Oletetaan muun muassa, että lukija tuntee jaollisuuden ja suurimman yhteisen tekijän tarkan määritelmän sekä alkuluvun käsitteen. Päälähdeteoksena käytetään Kenneth H. Rosenin kirjaa Elementary number theory and its applications.

Sisältö

1 Johdanto

Olkoot p ja q erisuuria parittomia alkulukuja. Oletetaan silloin, että tiedetään, onko q neliönjäännös modulo p vai neliönepäjäännös modulo p. Tällöin voidaan kysyä, tiedetäänkö silloin, että p on neliönjäännös modulo q tai neliönepäjäännös modulo q.

Euler löysi kokeellisesti tähän kysymykseen myöntävän vastauksen vuonna 1783. Hän ei kuitenkaan pystynyt todistamaan vastausta oikeaksi. Vuonna 1785 Legendre muotoili Eulerin vastauksen uudelleen elegantimpaan lauseen muotoon käyttämällä omalla nimellään kulkevaa symbolia. Tämä lause tunnetaan nykyisin neliönjäännösten resiprookkilakina ja se kertoo, onko kongruenssilla $x^2 \equiv q \pmod{p}$ ratkaisuja, kun tiedetään, onko kongruenssilla $x^2 \equiv p \pmod{q}$ ratkaisuja. Jatkossa tuloksesta käytetään myös lyhyempää nimitystä resiprookkilaki. Neliönjäännösten resiprookkilaki esitetään usein muodossa

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

Legendre julkaisi lauseelle myös monia todistuksia. Jokaisesta todistuksesta löydettiin kuitenkin vakavia puutteita. Ensimmäisen pitävän todistuksen esitti Gauss, joka toisten töistä tietämättömänä uudelleen keksi tuloksen 18-vuotiaana vuonna 1795. Hänen sanotaan [4] uhranneen tuloksen todistamiseen kaiken mahdollisen aikansa yhden vuoden ajan.

Sen jälkeen, kun Gauss oli esittänyt ensimmäisen todistuksensa resiprookkilaille vuonna 1796, hän jatkoi erilaisten todistusten etsimistä. Hänen tiedetään Rosenin [16] mukaan löytäneen ainakin kuusi erilaista todistusta. Tavoitteena Gaussilla oli löytää sellainen todistus, joka olisi yleistettävissä korkeammille potensseille. Tässä hän onnistui kuudennen todistuksensa kohdalla (kts.[6] tai [10]).

Gauss ei kuitenkaan ole ollut ainoa, joka on halunnut etsiä erilaisia todistustapoja resiprookkilaille. Muun muassa Cauchy, Dedekind ja Eisenstein kuuluvat siihen nimekkäiden matemaatikkojen joukkoon, joka on julkaissut todistuksen resiprookkilaille. Franz Lemmermeyer pitää internetissä[1] yllä listaa resiprookkilain todistuksista. Listalla on tällä hetkellä 224 todistusta.

Luvussa 4 tullaan esittämään resiprookkilaille todistus, jonka esitti alun perin Max Eisenstein. Tämä todistus on yksinkertaistettu muoto Gaussin kolmannesta todistuksesta. Yksinkertaistuksen tekee mahdolliseksi Eisensteinin esittämä lause, joka auttaa muuttamaan neliönjäännösten resiprookkilain todistuksen kolmion hilapisteiden (lattice point) laskemiseksi. Ennen

[1] http://www.rzuser.uni-heidelberg.de/∼ hb3/fchrono.html(haettu 10.4.2008)

resiprookkilain todistamista tullaan tekemään valmistelevia tarkasteluja luvussa 3, jossa esitetään tarvittavia käsitteitä, määritelmiä ja lauseita koskien mm. neliönjäännöstä ja Legendren symbolia.

Lukijalta edellytetään joidenkin lukuteorian perusasioiden tuntemista. Oletetaan mm., että lukija tuntee jaollisuuden ja suurimman yhteisen tekijän tarkan määritelmän sekä alkuluvun käsitteen. Päälähdeteoksena käytetään Kenneth H. Rosenin kirjaa Elementary number theory and its applications.[2]

Mainittakoon vielä, että aina, kun todistuksen kohdalla ei ole mainintaa lähdeteoksesta, kyseessä on tekijän itse todistama lause. Tämä ei tarkoita, etteikö kyseisiä lauseita olisi todistettu missään lähdeteoksista. Lähes kaikki esimerkit ovat tekijän itse tuottamia, vaikka niihin on otettu mallia lähdeteoksien vastaavista esimerkeistä.

[2]Tämän tutkielman liitteeseen on myös listattu aiheeseen liittyvää suositeltavaa luettavaa, jota ei ole käytetty lähdemateriaalina.

2 Historiaa

2.1 Gauss, neliönjäännösten resiprookkilain ensimmäinen todistaja

James Anderson ja James Bell [1, s. 224-227] esittelevät kiintoisia historian henkilöitä. Yksi heistä on Carl Friedrich Gauss, joka eli vuosina 1777-1855. Hän syntyi Saksassa ja oli tavallisen työläisperheen lapsi. Jotkut lähteet kertovat Andersonin ja Bellin mukaan, että Gaussin isä olisi ollut muurari ja toiset lähteet väittävät hänen olleen puutarhuri, kanavan esimies ja lihakauppias. Gaussin isä vastusti Gaussin koulutusta ja toivoi hänen jatkavan omaa uraansa, mikä se ikinä olikin. Andersonin ja Bellin mukaan on kerrottu, että Gaussin isä pakotti poikansa aikaisin nukkumaan talviaikaan säästääkseen valoa ja polttoainetta, mutta Gauss teki kynttilän tyhjäksi koverretusta turnipsista opiskellakseen.

Gaussin sanotaan myös olleen liian älykäs siihen, ettei häntä ja hänen tuloksiaan olisi huomattu. Hän opiskeli itsekseen esimerkiksi lukemista ja aritmetiikkaa. On myös kerrottu, että Gauss löysi kolmevuotiaana virheen isänsä tilikirjoista. Ensimmäisillä matematiikan tunneillaan Gaussin opettaja, J. G. Büttner, pyysi oppilaitaan laskemaan yhteen kokonaisluvut yhdestä sataan pitääkseen luokkansa toimeliaana. Gauss ratkaisi ongelman sekunneissa löydettyään kaavan n:n ensimmäisen kokonaisluvun summan laskemiseksi. Büttner säästi itseään määrätessään Gaussin raskaaseen työhön järjestelemään matematiikan kirjoja ja määrätessään assistenttinsa tutoroimaan Gaussia.

Gauss tuotiin Brunswickin herttuan tietoisuuteen ja herttuasta tulikin Gaussin suojelija kuolemaansa saakka. Herttualta saamansa tuen avulla Gauss pystyi osallistumaan Collegium Caroliumin opetukseen vuosina 1792-1795. Kyseessä oli yliopistoon valmistava koulu. Tämän ajanjakson aikana Gauss muodosti pienimmän neliösumman menetelmän. Vuonna 1795 hän pääsi Göttingeniin, mutta ei ollut vielä päättänyt, opiskelisiko hän filosofiaa vai matematiikkaa. Yhdeksäntoistavuotiaana Göttingenissä ollessaan Gauss keksi, että säännöllinen 17-sivuinen monikulmio voitaisiin muodostaa käyttämällä ainoastaan suoraa kulmaa ja kompassia. Tämä keksintö, joka oli ollut ratkaisematon vuosisatoja, sai Gaussin valitsemaan matematiikan. Ilmeisesti matematiikan opetus oli tähän aikaan heikkoa Göttingenissä, ja siksi Gauss työskenteli yksin todistaen joitakin suurimmista tuloksistaan. Valmistuttuaan Göttingenistä 1798 Gauss palasi Brunswickiin, missä hän työskenteli suojelijansa rahallisella avustuksella.

Gaussille myönnettiin tohtorin arvo 1801. Hänen väitöskirjansa, algebran peruslauseen todistus, oli pääosin kirjoitettu Johann Frederick Pfaffin alaisuudessa. Pfaff oli Saksan parhaiten tunnettu matemaatikko. Gauss oli tavannut hänet kirjastossa. Myöhemmin Gauss tuotti lauseelle useita todistuksia. Kun

Gaussin suojelija kuoli, Gauss hyväksyi paikan Göttingenistä. Hän päätti ottaa tuolinsa astronomiasta, jotta hänellä olisi enemmän aikaa työskennellä. Gauss ei kuitenkaan pitänyt opettamisesta vaan suosi matematiikan harrastustaan. Göttingenistä hän poistui tuolinsa vastaanottamisen jälkeen ainoastaan kaksi kertaa.

Ollessaan 24-vuotias Gauss aloitti työstämään *Disquisitiones Arithmeticae*ta. Teos vakiinnutti lukuteorian aseman matematiikan osa-alueena. Gauss loi teoksessaan lukujen kongruenssit. Hän julkaisi myös ensimmäisen todistuksen neliönjäännösten resiprookkilaille. Yhteensä Gauss esitti Andersonin ja Bellin mukaan resiprookkilaille kahdeksan todistusta 17 vuoden sisällä[3]. Hän näytti myös, että säännöllinen p sivuinen monikulmio voidaan konstruoida suorakulmalla ja kompassilla, jos p on muotoa $2^{2^n} - 1$, ja todisti Wilsonin lauseen yleistyksen. Kirja oli jaettu seitsemään kappaleeseen ja tuli tunnetuksi seitsemän sinetin kirjana, sillä sitä oli liian vaikea lukea. Kaikkien onneksi Peter Gustav Lejeune-Dirichlet onnistui rikkomaan nämä sinetit ja kirjoitti teoksen luettavampaan muotoon. Andersonin ja Bellin mukaan Gaussin kirjaa oli saatavilla vain muutama kappale julkaisijan konkurssin vuoksi. Edes kaikilla hänen oppilaillaan ei ollut sitä. Dirichlet'n sanotaan nukkuneen kyseinen kirja tyynynsä alla.

Vaikka Gauss tunnetaan yleisesti matematiikan prinssinä, hän oli yhtä tunnettu fysiikassa, mekaniikassa ja teoreettisessa astronomiassa. Esimerkkinä kerrottakoon, että Gauss keksi heliotroopin ja yhdessä Weberin kanssa, joka oli fyysikko Göttingenissä, hän keksi ja käytti lennätintä yhden mailin etäisyydellä. Mainittakoon vielä, että Gauss piti kirjaa todistuksistaan aina 19-vuoden iästä eteenpäin. Useimmat näistä todistuksista Gauss piti salassa ja julkaisi vain muutamia. Näitä muistiinpanoja ei julkaistu ennen vuotta 1901. Tästä syystä useat matemaatikkojen tänä aikana julkaisemat tulokset osoittautuivatkin Gaussin jo todistamiksi.

2.2 Euler

Anderson ja Bell [1, s. 188] esittelevät matemaatikoista myös Eulerin. Léonard Euler, 1707-1783, oli luterilaisen pastorin poika Sveitsistä. Hänen isänsä oli hänen ensimmäinen opettajansa ja halusi pojastaan pappia. Euler pääsi onnekseen Jean Bernoullin oppilaaksi. Bernoulli oli yksi Euroopan parhaista matemaatikoista. Koska Eulerin mahdollisuudet Sveitsissä olivat rajalliset, hän, useiden muiden eurooppalaisten matematiikoiden tapaan, meni vasta perustettuun Pietarin Akatemiaan. Venäjällä asuessaan Euler menetti näön toisesta silmästään. Vähän hänen saapumisensa jälkeen poliittinen tukahduttaminen alkoi Venäjällä. Neljäntoista vuoden jälkeen Euler lähti Venäjältä

[3]Huomaa, että kuten johdannossa mainittiin Rosen [16] väittää todisituksia olleen ainakin kuusi. Tarkasta lukumäärästä ei siis voida olla varmoja

Berliinin Akatemian matematiikan osaston johtajaksi. Anderson ja Bell kertovat, että ilmeisesti Saksan kuningataräidin kysyessä Eulerilta, miksi hän oli niin ujo, hän vastasi tulleensa juuri maasta, jossa puhujat hirtettiin.

Häntä pidettiin kaikesta huolimatta yhä suuressa arvossa Venäjällä. Kun Venäjä hyökkäsi Saksaan 1760, he tuhosivat Eulerin maatilan. Kun venäläiset saivat tämän tietoonsa, menetys korvattiin välittömästi ja keisarinna lisäsi mukaan ylimääräisen lahjan. Sitä, millainen lahja oli, Anderson ja Bell eivät kerro. Friedrick II kanssa syntyneiden erimielisyyksien vuoksi Euler palasi Venäjälle oltuaan 25 vuotta Saksassa ja vastaanotti Katariina suuren esittämän avokätisen tarjouksen. Neljä vuotta Venäjälle muuttamisen jälkeen Euler menetti näön toisestakin silmästä ja oli sokea viimeiset 17 vuotta elämästään. Euler ei kuitenkaan luopunut matematiikan luomisesta.

Andersonin ja Bellin mukaan vuonna 1771 syttyi tulipalo, joka tuhosi Eulerin talon. Hänen sveitsiläinen palvelijansa, Peter Grimes, syöksyi rohkeasti palavaan taloon ja kantoi sokean Eulerin ulos. Katariina rakennutti hänelle välittömästi uuden talon. Kerrotaan, että 18.päivä syyskuuta 1783 Euler käytti iltapäivän laskien lakeja pallojen nousulle ja hahmotellen laskelmia vasta löydetyn Uranuksen radalle. Myöhemmin Euler oli leikkimässä lapsenlapsensa kanssa ja polttamassa piippua, kun hän sai aivohalvauksen. Piippu tippui hänen suustaan, hän lausahti "kuolen"ja Eulerin elämä päättyi.

Myöhemmin esiteltävä ϕ -funktio on nimetty Eulerin mukaan. Anderson ja Bell väittävätkin hänen olleen tuotteliain matematiikan kirjoittaja. Hänen työnsä täyttäisivät heidän mukaansa yli 75 suurta kirjaa. Hän oli aktiivinen käytännöllisesti katsoen jokaisella matematiikan osa-alueella. Lukuteoriassa Euler teki suunnattoman määrän töitä, joihin kuuluvat muun muassa useiden Fermat'n vähäisempien lauseiden todistaminen. Hän sai ansioita topologian idean synnyttämisestä. Hän voitti myös arvokkaan Biennal-palkinnon tieteiden akatemiasta kaksitoista kertaa. Euler käytti ensimmäisenä käsitettä funktio. Wikipediassa kerrotaan, että "tämän lisäksi Euler aloitti muun muassa verkkoteorian ja variaatiolaskennan perusteiden tutkimisen. Häneltä ovat peräisin myös monet modernit merkinnät, muun muassa summa, pii ja imaginaariyksikkö. Yksi tunnetuimmista Eulerin töistä on niin sanottu Eulerin identiteetti $e^{\pi i}+1 = 0$. Sitä pidetään yleisesti matematiikan kauneimpana kaavana".

2.3 Legendre

Anderson ja Bell [1] estittelevät myös Adrien-Marie Legendren. Kuten johdannossa mainittiin, Adrien-Marie Legendre (1752-1833) oli ensimmäinen, joka esitti neliönjäännösten resiprookkilain. Legendre oli varakkaasta eteläranskalaisesta perheestä, mutta eli suurimman osan elämästään Pariisissa. Häntä koulutettiin Collége Mazarinissa Pariisissa ja hän oli matematiikan professorina Ècole Militiairessa viisi vuotta. Hän luopui paikastaan käyttääkseen enemmän aikaa tutkimukseensa. Kaksi vuotta myöhemmin hän voitti palkinnon Berliinin Akatemiassa esseestään ammusten radoista. Hänet valittiin tieteiden akatemiaan, mihin hän jäi sen sulkemiseen (10 vuotta myöhemmin) asti. Hän ei suostunut taipumaan hallitukselle, kun se yritti määrätä akatemiaa. Hän joutui luopumaan eläkkeestään ja kuoli köyhyydessä.

Legendre ei ollut erityisen pidetty ja arvostettu, vaikka hän oli suuri matemaatikko. Hän ei omasta mielestään saanut ansaitsemaansa tunnustusta ja oli Andersonin ja Bellin mielestä varmasti oikeassa. Hän oli erityisen ärtynyt Gaussista. Anderson ja Bell väittävät Gaussin olleen sitä mieltä, että jos hän oli päiväkirjassaan osoittanut lauseelle todistuksen, se oli hänen. Legendren mielestä sen henkilön, joka todistuksen oli julkaissut, kuului saada kunnia. Legendrehän esitti ensimmäisenä tässä tutkielmassa esitetyn muodon neliönjäännösten resiprookkilaista, mutta ei kyennyt todistamaan sitä. Gauss todisti sen ja jätti Legendren panoksen huomiotta. Legendre julkaisi ensimmäisen todistuksen pienimpien neliösummien metodista. Tämän todistuksen on Andersonin ja Bellin mukaan sanottu olevan ensimmäinen tyydyttävä todistus. Jälleen kerran Gauss vaati aiemman kunnian.

Parhaiten Legendre tunnetaan kirjastaan euklidisesta geometriasta, jota pidetään Andersonin ja Bellin mukaan yhtenä parhaimmista ikinä kirjoitetuista oppikirjoista. Hän työskenteli monilla alueilla, mutta on lähinnä tunnettu työstään lukuteoriassa, taivaallisessa mekaniikassa ja elliptisten funktioiden teoriassa. Neliönjäännösten resiprookkilain ja Legendren symbolin lisäksi, hänen työnsä lukuteoriassa sisälsi Fermat'n suuren lauseen todistuksen, kun $n = 5$ ja alkulukujen jakauman arvioinnin. Hän oli myös yksi kolmesta valtuutetusta, jotka tarkkailivat standardimetrin määrittämiselle välttämätöntä kolmiomittausta.

3 Valmistelevia tarkasteluja

Tässä luvussa käsitellään luvun 4 käsittelyn kannalta tärkeitä määritelmiä ja lauseita sekä tutustutaan tutkielmassa käytettäviin merkintöihin. Kaikkia määritelmiä ja lauseita ei käytetä sellaisenaan, vaan ne on tarkoitettu ajattelun kehittämiseen. Resiprookkilain ymmärtäminen vaatii tietynlaista ajattelua. Jos toisin ei mainita, lukujen oletetaan olevan kokonaislukuja. Tässä luvussa oletetaan lukijan tuntevan lukuteoria perusmerkinnät sekä jaollisuuden, alkuluvun ja suurimman yhteisen tekijän käsitteet.

3.1 Kongruenssi

Kongruenssit mahdollistavat jaollisuussuhteiden käsittelemisen jota kuinkin yhtäsuuruuden tapaan [16]. Seuraavassa esitellään muutamia kongruessin ominaisuuksia, jotka helpottavat resiprookkilain todistuksen ymmärrettävyyttä.

Määritelmä 3.1. Olkoon m positiivinen kokonaisluku. Silloin sanotaan luvun a olevan *kongruentti* luvun b kanssa modulo m, jos $m|(a-b)$. Jos luku a on kongruentti luvun b kanssa modulo m, niin merkitään $a \equiv b \pmod{m}$ [8, s. 18]. Vastaavasti, jos $m \nmid (a-b)$, merkitään $a \not\equiv b \pmod{m}$. Tällöin a ja b ovat *epäkongruentteja*. Lukua m kutsutaan kongruenssin *moduliksi*.

Esimerkki 3.1. Kongruenssin määritelmän mukaan $13 \equiv 1 \pmod{4}$, koska $4|(13-1) = 12$. Toisaalta $13 \not\equiv 4 \pmod{4}$, sillä $4 \nmid (13-4) = 9$.

Lause 3.1. *Olkoot a ja b kokonaislukuja. Silloin $a \equiv b \pmod{m}$, jos ja vain jos on olemassa sellainen kokonaisluku k, että $a = b + km$.*

Todistus. Vrt.[16, s. 142]. Jos $a \equiv b \pmod{m}$, niin $m|(a-b)$. Tästä seuraa, että on olemassa kokonaisluku k, jolle pätee $km = a-b$ siten, että $a = b+km$. Kääntäen, jos on olemassa kokonaisluku k, jolle $a = b+km$, niin $km = a-b$. Siis $m|(a-b)$ ja näin ollen $a = b + km$. □

Esimerkki 3.2. Selvästi $14 \equiv 2 \pmod{3}$.Toisaalta $14 = 2 + 3 \cdot 4$.

Lause 3.2. *Olkoot a,b,c kokonaislukuja sekä olkoon m positiivinen kokonaisluku. Olkoon $a \equiv b \pmod{m}$. Silloin*

(i) $a + c \equiv b + c \pmod{m}$

(ii) $a - c \equiv b - c \pmod{m}$

(iii) $ac \equiv bc \pmod{m}$.

Todistus. Vrt.[16, s. 144]. Koska $a \equiv b \pmod{m}$, tiedetään, että $m|(a-b)$. Yhtäsuuruudesta $(a+c)-(b+c) = a-b$, nähdään, että $m|((a+c)-(b+c))$, mistä seuraa kohta (i). Samoin kohta (ii) seuraa siitä, että $(a-c)-(b-c) = a-b$. Kohdassa (iii) tulee huomata, että $ac - bc = c(a-b)$. Siis $ac \equiv bc \pmod{m}$. □

Esimerkki 3.3. Sovelletaan lausetta kongruenssiin $13 \equiv 1 \pmod{4}$, jolloin kongruenssit

$$\begin{aligned} 15 &= 13 + 2 \equiv 1 + 2 = 3 \pmod{4}, \\ 11 &= 13 - 2 \equiv 1 - 2 = -1 \pmod{4}, \\ 26 &= 13 \cdot 2 \equiv 1 \cdot 2 = 2 \pmod{4} \end{aligned}$$

ovat voimassa.

Lause 3.3. *Olkoon m positiivinen kokonaisluku. Jos $a \equiv b \pmod{m}$ ja $c \equiv d \pmod{m}$, niin $ac \equiv bd \pmod{m}$.*

Todistus. Vrt.[16, s. 145]. Huomataan ensin, että

$$ac - bd = ac - bc + bc - bd = c(a-b) + b(c-d) = ckm + blm = m(ck + bl).$$

Siis $m|(ac - bd)$. Näin ollen $ac \equiv bd \pmod{m}$. □

Esimerkki 3.4. Selvästi $8 \equiv 3 \pmod{5}$ ja $7 \equiv 2 \pmod{5}$. Tällöin pitää myös paikkansa $56 \equiv 6 \pmod{5}$, joka voidaan sieventää vielä muotoon $56 \equiv 1 \pmod{5}$

Kongruenssin jakaminen puolittain kokonaisluvulla ei ole aivan yhtä yksinkertaista kuin kertominen. Seuraavassa lauseessa esitellään, miten puolittain jakaminen on mahdollista.

Lause 3.4. *Merkitään $(a, m) = d$. Silloin*

$$ab \equiv ac \pmod{m} \Leftrightarrow b \equiv c \pmod{m/d}.$$

[8, s. 19]

Todistus. Kongruessin ja jaollisuuden määritelmien perusteella voidaan selvästi esittää ekvivalenssiketju

$$\begin{aligned} ab \equiv ac \pmod{m} &\Leftrightarrow m|(ab - ac) \\ &\Leftrightarrow m|a(b-c) \\ &\Leftrightarrow \frac{m}{d}|\frac{a}{d}(b-c) \\ &\Leftrightarrow \frac{m}{d}|(b-c) \\ &\Leftrightarrow b \equiv c \pmod{m/d}. \end{aligned}$$

□

Korollaari 3.1. *Olkoon m positiivinen kokonaisluku ja olkoon a sellainen kokonaisluku, että $(a, m) = 1$. Silloin*

$$ab \equiv ac \pmod{m} \Leftrightarrow b \equiv c \pmod{m}.$$

Esimerkki 3.5. Selvästi $40 \equiv 16 \pmod 6$ ja $(4, 6) = 2$, joten lauseen 3.4 perusteella $10 \equiv 4 \pmod 2$.

Määritelmä 3.2. Joukko $\{r_1, r_2, \ldots, r_m\}$ on *täydellinen jäännössysteemi* modulo m, jos $r_i \not\equiv r_j \pmod m$, aina kun $i \neq j$. [7, s. 4]

Esimerkki 3.6. $\{0, 1, 2, \ldots, m-1\}$ on täydellinen jäännössysteemi modulo m.

Määritelmä 3.3. *Eulerin funktio* ϕ määritellään kaavalla

$$\phi(n) = |\{r : 1 \leq r \leq n, (r, n) = 1\}|, n \in \mathbb{Z}^+.$$

[7, s. 4]

Esimerkki 3.7. Seuraavassa taulukossa on esitetty Eulerin ϕ-funktion arvot luvun m arvoille 1-10.

m	1	2	3	4	5	6	7	8	9	10
$\phi(m)$	1	1	2	2	4	2	6	4	6	4

Taulukko 1. Eulerin ϕ-funktion arvoja.

Huomautus 3.1. $\phi(m)$ on parillinen aina, kun $m > 2$. [16, s. 243]

Huomautus 3.2. Jos p on alkuluku, niin $\phi(p) = p - 1$. Tämä pätee myös toisin päin. Jos p on positiivinen kokonaisluku ja $\phi(p) = p - 1$, niin p on alkuluku. [16, s. 242]

Huomautus 3.3. $\phi(p^a) = p^a - p^{a-1}$, kun p on alkuluku ja $a \in \mathbb{Z}^+$. [16, s. 241]

Määritelmä 3.4. Joukko $\{r_1, r_2, \ldots, r_{\phi(m)}\}$ on *supistettu jäännössysteemi* modulo m, jos
1) $(r_i, m) = 1$, kun $i = 1, 2, \ldots, \phi(m)$,
2) $r_i \not\equiv r_j \pmod m$, kun $i \neq j$.
[7, s. 4]

Esimerkki 3.8. $\{r \mid 1 \leq r \leq m, (r, m) = 1\}$ on supistettu jäännössysteemi modulo m.

Lause 3.5. *Olkoon $\{r_1, r_2, \ldots, r_{\phi(m)}\}$ supistettu jäännössysteemi modulo m ja olkoon a sellainen nollasta eroava kokonaisluku, että $(a, m) = 1$. Silloin $A = \{ar_1, ar_2, \ldots, ar_{\phi(m)}\}$ on supistettu jäännössysteemi modulo m. [7, s. 5]*

Todistus. Vrt.[9]. Joukossa A on $\phi(m)$ alkiota, joten riittää osoittaa, että supistetun jäännössysteemin määritelmän kohdat 1 ja 2 pätevät.

(1)Vastaoletus: On olemassa $i \in \{1, \ldots, \phi(m)\}$ siten, että $(ar_i, m) > 1$. Siis on olemassa alkuluku p siten, että $p|ar_i$ ja $p|m$, koska positiivinen kokonaisluku on alkulukujen tulo. Tästä seuraa, että $p|a$ ja $p|m$ tai $p|r_i$ ja $p|m$. Jos $p|a$ ja $p|m$, niin $(a, m) > 1$, mikä on ristiriita. Jos taas $p|r_i$ ja $p|m$, niin $(r_i, m) > 1$. Siis$\{r_1, r_2, \ldots, r_{\phi(m)}\}$ ei ole supistettu jäännössysteemi modulo m, mikä on ristiriita. Siis kohta 1 on voimassa.

(2)Vastaoletus: On olemassa $i, j \in \{1, \ldots, \phi(m)\}$, $i \neq j$ sekä $ar_i \equiv ar_j \pmod{m}$. Koska $(a, m) = 1$, seuraa, että $r_i \equiv r_j \pmod{m}$, mikä on ristiriita. Siis kohta 2 on voimassa. □

Lause 3.6 (Eulerin-Fermat´n lause)**.** *Olkoon m positiivinen kokonaisluku ja a sellainen kokonaisluku, että $(a, m) = 1$. Tällöin*

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

[7, s. 5]

Todistus. Vrt.[9]. Merkitään

$$R = \{r_1, r_2, \ldots, r_{\phi(m)}\} = \{r | 0 \leq r \leq m-1, (r, m) = 1\}$$

ja

$$aR = \{ar_1, \ldots, ar_{\phi(m)}\}.$$

Nyt jokaista $ar_i \in aR$ kohti on olemassa yksikäsitteinen $r_j \in R$ siten, että $r_j \equiv ar_i \pmod{m}$. Tällöin lauseen 3.3 perusteella

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

Toisin sanottuna

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

Koska supistetun jäännössysteemin määritelmän perusteella $(r_1 r_2 \cdots r_{\phi(m)}, m) = 1$, niin saadaan $a^{\phi(m)} \equiv 1 \pmod{m}$. □

Esimerkki 3.9. Eulerin-Fermat'n lauseen perusteella

$$5^{\phi(16)} = 5^8 = 390625 \equiv 1 \pmod{16},$$

sillä $(5, 16) = 1$.

Lause 3.7 (Fermat´n pieni lause)**.** *Jos p on alkuluku ja $p \not| a$, niin $a^{p-1} \equiv 1 \pmod{p}$. [16, s. 217]*

Todistus. Huomautuksen 3.3 perusteella tiedetään, että $\phi(p) = p-1$. Koska $p \nmid a$, niin jaollisuuden määritelmän perusteella $(p, a) = 1$. Täten lauseen 3.6 perusteella

$$a^{\phi(p)} \equiv 1 \pmod{p} \quad \text{eli} \quad a^{p-1} \equiv 1 \pmod{p}.$$

□

Korollaari 3.2. *Jos p on alkuluku, niin $a^p \equiv a \pmod{p}$.*

Todistus. Katso [7] tai [16]. □

Määritelmä 3.5. Olkoon $(a, m) = 1$. Silloin kongruenssin $ax \equiv 1 \pmod{m}$ ratkaisua x sanotaan luvun a *käänteisluvuksi* modulo m. [7, s. 7]

Huomautus 3.4. Kun $(a, m) = 1$, niin luvun a käänteisluku modulo m on olemassa ja se on yksikäsitteinen modulo m. [7, s. 7]

Esimerkki 3.10. Luku 9 on luvun 7 käänteisluku modulo 31, sillä $(7, 31) = 1$ ja $7 \cdot 9 = 63 \equiv 1 \pmod{31}$. [7, s. 7]

Lause 3.8. *Olkoon p alkuluku ja $p \nmid a$. Silloin luku a on itsensä käänteisluku modulo p, jos ja vain jos $a \equiv 1 \pmod{p}$ tai $a \equiv -1 \pmod{p}$. [7, s. 7]*

Todistus. Kts. [7, s. 7] □

Lause 3.9 (Wilsonin lause)**.** *Jos p on alkuluku, niin $(p-1)! \equiv -1 \pmod{p}$.*

Todistus. Vrt.[16, s. 216]. Tutkitaan ensin tapaukset $p = 2$ ja $p = 3$.

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

$$p = 3 : (3-1)! = 2! = 2 \equiv -1 \pmod{3}.$$

Oletetaan sitten, että $p > 3$. Olkoon $a \in \{2, 3, \ldots, p-2\}$. Koska $(a, p) = 1$, niin tiedetään, että luvun a käänteisluku modulo p on olemassa. Koska $p \nmid (a-1)$ ja $p \nmid (a+1)$, niin edellisen lauseen nojalla luvun a käänteisluku modulo p on eri kuin luku a itse. Siis luvut $2, 3, \ldots, p-2$ voidaan jakaa erillisiin pareihin siten, että jokaisen parin tulo on kongruentti luvun 1 kanssa modulo p. Tämä voidaan tehdä, sillä lukuja on parillinen määrä ja luvut 1 ja $p-1$ ovat itsensä käänteisalkioita modulo p.

Kertomalla nämä parit keskenään saadaan, että

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

Koska $p - 1 \equiv -1 \pmod{p}$, niin saadaan, että

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

□

Lause 3.10 (Kiinalainen jäännöslause)**.** *Olkoot $m_1, m_2, \ldots, m_r$, missä $r \geq 2$, 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 $M = m_1 \cdot m_2 \cdots m_r$.

Todistus. Kts.[7, s. 8] □

Esimerkki 3.11. Ratkaise kongruenssiryhmä

$$\begin{aligned} x &\equiv 1 \pmod{2} \\ x &\equiv 1 \pmod{5} \\ x &\equiv 0 \pmod{3}. \end{aligned}$$

Koska 2,3,5 ovat pareittain suhteellisia alkulukuja, niin kiinalaisen jäännöslauseen nojalla kongruenssiryhmällä on yksikäsitteinen ratkaisu modulo $2 \cdot 3 \cdot 5 = 30$. Tällöin

$$\begin{aligned} M_1 &= \frac{30}{2} = 15 \\ M_2 &= \frac{30}{5} = 6 \\ M_3 &= \frac{30}{3} = 10. \end{aligned}$$

Koska

$$\begin{aligned} 15 \cdot 1 &\equiv 1 \pmod{2} \\ 6 \cdot 1 &\equiv 1 \pmod{5} \\ 10 \cdot 1 &\equiv 1 \pmod{3}, \end{aligned}$$

niin

$$\begin{aligned} y_1 &\equiv 1 \pmod{2} \\ y_2 &\equiv 1 \pmod{5} \\ y_3 &\equiv 1 \pmod{3}. \end{aligned}$$

Siis $x \equiv 1 \cdot 15 \cdot 1 + 1 \cdot 6 \cdot 1 + 0 \cdot 10 \cdot 1 \equiv 21 \pmod{30}$.

3.2 Primitiivinen juuri

Aloitetaan aiheen käsittely kokonaisluvun kertaluvun käsitteestä. Olkoot a ja m suhteellisia alkulukuja ja $m > 1$. Silloin lauseen 3.6 mukaan $a^{\phi}(m) \equiv 1 \pmod{m}$. Tällöin on olemassa ainakin yksi sellainen positiivinen kokonaisluku x, että $a^x \equiv 1 \pmod{m}$. Koska kokonaisluvut ovat hyvinmääriteltyjä, voidaan todeta, että on olemassa sellainen pienin kokonaisluku x, joka totetuttaa edellä mainitun kongruenssin.

Määritelmä 3.6. Olkoot a ja m suhteellisia alkulukuja ja $m > 0$. Tällöin luvun a *kertaluku* modulo m on pienin sellainen positiivinen kokonaisluku x, että $a^x \equiv 1 \pmod{m}$. Merkitään $x = \mathrm{ord}_m a$. [7, s. 15]

Esimerkki 3.12. Etsitään $\mathrm{ord}_5 2$. Aluksi todetaan, että $(2, 5) = 1$. Nyt

$$\begin{aligned} 2^1 = 2 &\equiv 2 \pmod{5} \\ 2^2 = 4 &\equiv 4 \pmod{5} \\ 2^3 = 8 &\equiv 3 \pmod{5} \\ 2^4 = 16 &\equiv 1 \pmod{5}. \end{aligned}$$

Tämän perusteella $\mathrm{ord}_5 2 = 4$. Ei ole tarpeen laskea vaihtoehtoa 2^5, sillä etsimme pienintä sellaista positiivista kokonaislukua x, että kongruenssilla $a^x \equiv 1 \pmod{m}$ on ratkaisu.

Seuraava lause on tarpeellinen, kun etsitään kongruenssin $a^x \equiv 1 \pmod{m}$ kaikkia ratkaisuja.

Lause 3.11. *Olkoot a ja m suhteellisia alkulukuja ja $m > 0$. Silloin positiivinen kokonaisluku x on kongruenssin $a^x \equiv 1 \pmod{m}$ ratkaisu, jos ja vain jos $ord_m a | x$.*

Todistus. Vrt.[16, s. 334]. Oletetaan, että $\mathrm{ord}_m a | x$. Nyt $x = (\mathrm{ord}_m a)k$, missä $k \in \mathbb{Z}^+$. Siis

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

Oletetaan seuraavaksi, että $a^x \equiv 1 \pmod{m}$. Tällöin jakoalgoritmin mukaan on olemassa sellaiset kokonaisluvut q ja r, että

$$x = q(\mathrm{ord}_m a) + r, \quad \text{kun} \quad 0 \leq r < \mathrm{ord}_m a.$$

Tästä nähdään, että

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

Koska $a^x \equiv 1 \pmod{m}$, tiedetään, että $a^r \equiv 1 \pmod{m}$. Epäyhtälöstä $a \leq r < \mathrm{ord}_m a$ voidaan päätellä, että $r = 0$, sillä määritelmän mukaan $\mathrm{ord}_m a$ on pienin positiivinen kokonaisluku, jolle pätee $a^{\mathrm{ord}_m a} \equiv 1 \pmod{m}$. Koska $r = 0$, saadaan $x = q \cdot \mathrm{ord}_m a$. Näin ollet $\mathrm{ord}_m a | x$. □

Esimerkki 3.13. Koska $\text{ord}_5 2 = 4$, niin esimerkiksi $x = 12$ on kongruenssin $2^x \equiv 1 \pmod 5$ ratkaisu, sillä $4|12$. Toisaalta $x = 6$ ei ole kongruenssin $2^x \equiv 1 \pmod 5$ ratkaisu, sillä $4 \not| 6$.

Korollaari 3.3. *Jos a ja m ovat suhteellisia alkulukuja ja $m > 0$, niin $ord_m a|\phi m$*

Todistus. Vrt.[16, s. 335]. Koska $(a, m) = 1$, niin Eulerin-Fermat'n lauseen mukaan

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

Kuitenkin lauseen 3.11 mukaan luku x on kongruenssin $a^x \equiv 1 \pmod m$ ratkaisu, jos ja vain jos $\text{ord}_m a|x$. Nyt $x = \phi(m)$. Näin ollen $\text{ord}_m a|\phi(m)$. □

Esimerkki 3.14. Etsitään $\text{ord}_{15} 2$. Koska $\phi(15) = 8$, niin edellä mainitun seurauksen perusteella mahdollisia $\text{ord}_{15} 2$ arvoja ovat 1,2, 4 ja 8. Koska

$$\begin{aligned} 2^1 = 2 &\equiv 2 \pmod{15} \\ 2^2 = 4 &\equiv 4 \pmod{15} \\ 2^4 = 16 &\equiv 1 \pmod{15} \\ 2^8 = 256 &\equiv 1 \pmod{15}, \end{aligned}$$

niin $\text{ord}_{15} 2 = 4$.

Huomautus 3.5. Jos luvun $\phi(m)$ tekijöistä valitaan mielivaltaisesti jokin x, ei välttämättä ole olemassa sellaista lukua a, että x olisi sen kertaluku modulo m.

Jos a on sellainen luku, että $(a, m) = 1$, niin korollaarin 3.3 mukaan $\text{ord}_m a|\phi(m)$. Luvun $\text{ord}_m a$ suurin mahdollinen arvo on siis $\phi(m)$. Tästä seuraa primitiivisen juuren määritelmä.

Määritelmä 3.7. Olkoot r ja m suhteellisia alkulukuja ja $m > 1$. Jos $\text{ord}_m r = \phi(m)$, niin sanotaan, että r on *primitiivinen juuri* modulo m.

Toisin sanoen luvulla m on *primitiivinen juuri* r, jos $r^{\phi(m)} \equiv 1 \pmod m$ ja $r^k \not\equiv 1$ aina, kun $k < \phi(m)$. [7, s. 17]

Esimerkki 3.15. Koska $\text{ord}_9 2 = 6 = \phi(9)$, 2 on primitiivinen juuri modulo 9. Koska $\text{ord}_7 2 = 3 \neq \phi(7)$, 2 ei ole primitiivinen juuri modulo 7.

Huomautus 3.6. Kaikilla kokonaisluvuilla ei ole primitiivistä juurta. Tällaisia lukuja ovat muun muassa 8,12 ja 15.

3.3 Neliönjäännös

Martin J. Erickson [5] kysyy, milloin neliökongruenssit ovat ratkaistavissa. Hän kysyy myös, miten niiden ratkaisut löydetään. Tässä työssä tullaan huomaamaan, että ratkaisun avain on alkulukujen neliönjäännökset, kuten Ericksson esittää.

On olemassa kaksi lähestymistapaa ongelmalle $x^2 \equiv a \pmod{p}$, missä p on alkuluku. Voidaan valita p ja etsiä sellaisia luvun a arvoja, että sillä on neliöjuuri modulo p tai voidaan valita a ja etsiä modulia p, jolle on olemassa luvun a neliöjuuri.

Aloitetaan tämän luvun käsittely käsittelemällä yleistä neliökongruenssia,

$$ax^2 + bx + c \equiv 0 \pmod{m},$$

missä $a \not\equiv 0 \pmod{m}$. Käytetään Ericksonia [5] mukaillen neliöksi täydentämistä. Kerrotaan kongruenssi termillä $4a$:

$$4a^2x^2 + 4abx + 4ac \equiv 0 \pmod{m}.$$

Sieventämällä päästään muotoon:

$$(2ax + b)^2 \equiv b^2 - 4ac \pmod{m}.$$

Kun tehdään supistus $y^2 \equiv b^2 - 4ac \pmod{m}$, nähdään, että jos m on pariton ja $(a, m) = 1$ ylläolevalla kongruenssilla on ratkaisu, jos ja vain jos kongruenssilla $y^2 \equiv b^2 - 4ac \pmod{m}$ on ratkaisu.

Siirrytään seuraavaksi käsittelemään neliönjäännöksiä.

Määritelmä 3.8. Luku a on *neliönjäännös* modulo m, jos a on suhteellinen alkuluku luvun m kanssa ja on olemassa sellainen kokonaisluku x, että $a \equiv x^2 \pmod{m}$. Jos tällaista lukua x ei ole olemassa, a on *neliönepäjäännös*. [3, s. 180]

Koska jatkossa rajoitutaan tapauksiin, joissa m on pariton alkuluku, esitetään myös seuraava määritelmä.

Määritelmä 3.9. Olkoon p pariton alkuluku ja olkoon a sellainen kokonaisluku, että $p \nmid a$. Tällöin a on *neliönjäännös* modulo p, jos kongruenssilla

$$x^2 \equiv a \pmod{p}$$

on ratkaisu. Jos kongruenssilla ei ole ratkaisua, kutsutaan lukua a *neliönepäjäännökseksi* modulo p. Voidaan käyttää myös nimitystä epäneliönjäännös. [12, s. 100]

Huomautus 3.7. Jos $a \equiv b \pmod{p}$, niin a ja b ovat molemmat joko neliönjäännöksiä tai neliönepäjäännöksiä modulo p. Näin ollen neliönjäännöksiä tutkittaessa riittää, että tarkastellaan lukuja $1, 2, \ldots, p-1$. [17]

Esimerkki 3.16. Tutkitaan alkulukua 5. Tarkastellaan supistettua jäännössysteemiä modulo 5, joka on joukko {1,2,3,4}. Nyt

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

Siis luvut 1 ja 4 ovat neliönjäännöksiä modulo 5 ja luvut 2 ja 3 ovat neliönepäjäännöksiä modulo 5.

Seuraavan lauseen tulos voidaan huomata myös edellisestä esimerkistä.

Lause 3.12. *Olkoon p pariton alkuluku ja olkoon a sellainen kokonaisluku, että $p \nmid a$. Tällöin kongruenssiyhtälöllä*

$$x^2 \equiv a \pmod{p}$$

on joko tasan kaksi ratkaisua tai ei ratkaisuja ollenkaan.

Todistus. [16, s. 402]. Jos kongruenssilla

$$x^2 \equiv a \pmod{p}$$

on ratkaisu, merkitään $x = x_0$, niin voidaan helposti osoittaa, että $x = -x_0$ on toinen epäkongruentti ratkaisu. Koska

$$(-x_0)^2 = {x_0}^2 \equiv a \pmod{p},$$

nähdään, että $-x_0$ on ratkaisu. Nyt $x_0 \not\equiv -x_0 \pmod{p}$, sillä jos $x_0 \equiv -x_0 \pmod{p}$, niin saadaan $2x_0 \equiv 0 \pmod{p}$. Tämä on mahdotonta, koska p on pariton ja $p \nmid x_0$. Voidaan tarkentaa, että $p \nmid x_0$, koska ${x_0}^2 \equiv a \pmod{p}$ ja $p \nmid a$. Jotta osoitettaisiin, että ei ole enempää kuin kaksi ratkaisua, oletetaan, että $x = x_0$ ja $x = x_1$ ovat molemmat kongruenssin

$$x^2 \equiv a \pmod{p}$$

ratkaisuja. Tällöin saadaan ${x_0}^2 \equiv {x_1}^2 \equiv a \pmod{p}$, niin että ${x_0}^2 - {x_1}^2 = (x_0 + x_1)(x_0 - x_1) \equiv 0 \pmod{p}$. Tällöin $p|(x_0 + x_1)$ tai $p|(x_0 - x_1)$ niin, että $x_1 \equiv -x_0 \pmod{p}$ tai $x_1 \equiv x_0 \pmod{p}$. Tästä syystä kongruenssilla

$$x^2 \equiv a \pmod{p}$$

on tasan kaksi ratkaisua, jos sillä on ratkaisu. □

Lause 3.13. *Jos p on pariton alkuluku, on olemassa tasan $(p-1)/2$ neliönjäännöstä ja $(p-1)/2$ neliönepäjäännöstä modulo p lukujen $1, 2, \ldots, p-1$ joukossa.*

Todistus. Vrt. [16, s. 403]. Jotta löydettäisiin kaikki neliönjäännökset modulo p lukujen $1, 2, \ldots, p-1$ joukosta, tulee tarkastella näiden lukujen neliöiden pienimpiä positiivisia jäännöksiä modulo p. Koska neliöitä on $p-1$ kappaletta ja jokaisella muotoa $x^2 \equiv a \pmod{p}$ olevalla kongruenssilla on joko kaksi tai ei yhtään ratkaisua, täytyy tällöin olla tasan $\frac{(p-1)}{2}$ neliönjäännöstä modulo p lukujen $1, 2, \ldots, p-1$ joukossa. Jäljelle jääneet $(p-1) - \frac{(p-1)}{2} = \frac{(p-1)}{2}$ lukua p pienempää positiivista lukua ovat neliönepäjäännöksiä modulo p. □

3.4 Legendren symboli ja Eulerin kriteeri

Seuraavaksi esitellään Legendren symboli ja Eulerin kriteeri. Eulerin kriteeri, kuten neliönjäännösten resiprookkilakikin, perustuu Legendren symbolin ominaisuuteen.

Määritelmä 3.10. Olkoon p pariton alkuluku ja olkoon a sellainen kokonaisluku, että $p \nmid a$. Tällöin

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{jos } a \text{ on neliönjäännös modulo } p \\ -1, & \text{jos } a \text{ on neliönepäjäännös modulo } p. \end{cases}$$

Tätä kutsutaan *Legendren symboliksi.* [16, s. 404]

Esimerkki 3.17. Koska luvut 1,4 ovat neliönjäännöksiä ja luvut 2,3 neliönepäjäännöksiä modulo 5,

$$\left(\frac{1}{5}\right) = \left(\frac{4}{5}\right) = 1$$

ja

$$\left(\frac{2}{5}\right) = \left(\frac{3}{5}\right) = -1.$$

Lause 3.14 (Eulerin kriteeri)**.** *Olkoon p pariton alkuluku ja olkoon a sellainen kokonaisluku, että $(p, a) = 1$. Tällöin*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{(p-1)}{2}} \pmod{p}.$$

[16, s. 404]

Todistus. Vrt.[7, s. 24]. Todistetaan ensin lauseen ensimmäinen osa. Oletetaan, että a on neliönjäännös modulo p. Silloin kongruenssilla $x^2 \equiv a \pmod{p}$ on ratkaisu, jota merkitään x_1. Koska $(a, p) = 1$, niin myös $(x_1, p) = 1$. Täten Fermat'n pienen lauseen nojalla

$$a^{(p-1)/2} \equiv ({x_1}^2)^{(p-1)/2} = {x_1}^{p-1} \equiv 1 \pmod{p}.$$

Oletetaan sitten, että $a^{(p-1)/2} \equiv 1 \pmod{p}$. Olkoon r primitiivinen juuri modulo p. Koska $(a, p) = 1$, niin $a \equiv r^k \pmod{p}$ jollakin k, missä
$1 \leq k \leq \phi(p) = p - 1$. Siis

$$r^{k \cdot \frac{(p-1)}{2}} \equiv a^{\frac{(p-1)}{2}} \equiv 1 \pmod{p}.$$

Täten lauseen 3.11 nojalla

$$\mathrm{ord}_p r | k \cdot \frac{(p-1)}{2}$$

eli $(p-1) | k \cdot \frac{(p-1)}{2}$. Huomaa, että $k \cdot \frac{(p-1)}{2} = c \cdot (p-1)$, missä $c \in \mathbb{Z}_+$ eli $\frac{k}{2} = c$ eli k on parillinen.

Merkitään $k = 2j$. Nyt $(r^j)^2 = r^k \equiv a \pmod{p}$, joten r^j on kongruenssin $x^2 \equiv a \pmod{p}$ ratkaisu. Näin ollen a on neliönjäännös modulo p.

Todistetaan lauseen toinen osa. Fermat'n pienen lauseen nojalla

$$(a^{(p-1)/2} - 1)(a^{(p-1)/2} + 1) = a^{p-1} - 1 \equiv 0 \pmod{p}.$$

Siis $a^{(p-1)/2} - 1 \equiv 0 \pmod{p}$ tai $a^{(p-1)/2} + 1 \equiv 0 \pmod{p}$
eli $a^{(p-1)/2} \equiv 1 \pmod{p}$ tai $a^{(p-1)/2} \equiv -1 \pmod{p}$.
Siis $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$. □

Eulerin kriteeri voidaan todistaa myös Wilsonin lauseen (lause 3.9) avulla. Kts. esimerkiksi [17, s. 189].

Esimerkki 3.18. Olkoon $p = 7$. Silloin Eulerin kriteerin mukaan

$$4^{\frac{(7-1)}{2}} = 4^3 = 64 \equiv 1 \pmod{7}$$

ja

$$6^{\frac{(7-1)}{2}} = 6^3 = 216 \equiv -1 \pmod{7}.$$

Siis on 4 neliönjäännös ja 6 on neliönepäjäännös modulo 7.

Lause 3.15. *Seuraavat ominaisuudet pätevät Legendren symboleille:*

$$\left(\frac{1}{p}\right) = 1 \tag{3.1}$$

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right) \tag{3.2}$$

$$\left(\frac{a^2}{p}\right) = 1 \tag{3.3}$$

$$\left(\frac{-1}{p}\right) = \begin{cases} 1, & jos\ p \equiv 1 \pmod 4 \\ -1, & jos\ p \equiv -1 \pmod 4 \end{cases} \tag{3.4}$$

$$\sum_{a \in \mathbb{Z}_p} \left(\frac{a}{p}\right) = 0 \tag{3.5}$$

$$Jos\ a \equiv b \pmod p,\ niin\ \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right). \tag{3.6}$$

Todistus. Vrt. [5, s. 132] ja [16, s. 405]. Kohta (3.1) seuraa Legendren symbolin määritelmästä.
Kohta (3.2): Eulerin kriteerin perusteella tiedetään, että $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod p$, $\left(\frac{b}{p}\right) \equiv b^{(p-1)/2} \pmod p$ ja $\left(\frac{ab}{p}\right) \equiv (ab)^{(p-1)/2}$. Näin ollen

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \equiv a^{(p-1)/2}b^{(p-1)/2} = (ab)^{(p-1)/2} \equiv \left(\frac{ab}{p}\right) \pmod p.$$

Koska Legendren symboli voi saada vain arvot ± 1, voidaan päätellä, että

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right).$$

Kohta (3.3): koska $\left(\frac{a}{p}\right) = \pm 1$ kohdasta (3.2) seuraa, että

$$\left(\frac{a^2}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{p}\right) = 1.$$

Kohta (3.4): Eulerin kriteerin perusteella tiedetään, että $\left(\frac{-1}{p}\right) \equiv (-1)^{(p-1)/2} \pmod p$. Jos $p \equiv 1 \pmod 4$, niin $p = 4k+1$, jollakin kokonaisluvulla k. Näin ollen $(-1)^{(p-1)/2} = (-1)^{2k} = 1$. Siis $\left(\frac{-1}{p}\right) = 1$. Jos $p \equiv 3 \pmod 4$, niin $p = 4k+3$, jollakin kokonaisluvulla k. Näin ollen $(-1)^{(p-1)/2} = (-1)^{2k+1} = -1$. Siis $\left(\frac{-1}{p}\right) = -1$.
Kohta (3.5) seuraa siitä, että neliönjäännöksiä ja neliönepäjäännöksiä on yhtä paljon.

Kohta (3.6): jos $a \equiv b \pmod{p}$, niin kongruenssilla $x^2 \equiv a \pmod{p}$ on ratkaisu, jos ja vain jos kongruenssilla $x^2 \equiv b \pmod{p}$ on ratkaisu. Täten

$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right).$$

□

4 Neliönjäännösten resiprookkilain todistus

Olkoot p ja q erisuuria parittomia alkulukuja. Jos kongruenssi

$$x^2 \equiv p \pmod{q}$$

on ratkeava, merkitään $\left(\frac{p}{q}\right) = 1$. Jos kongruenssi ei ole ratkeava, merkitään $\left(\frac{p}{q}\right) = -1$. Vastaavasti kongruenssin ratkeavuuden perusteella merkitään $\left(\frac{q}{p}\right) = 1$ tai $\left(\frac{q}{p}\right) = -1$. Tällä tavoin määriteltyjen Legendren symbolien välillä on voimassa yhtälö, jota kutsutaan neliönjäännösten resiprookkilaiksi.

Lause 4.1 (Neliönjäännösten resiprookkilaki)**.** *Olkoot p ja q erisuuria parittomia alkulukuja. Tällöin*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

Neliönjäännösten resiprookkilaki siis väittää, että Legendren symbolit $\left(\frac{p}{q}\right)$ ja $\left(\frac{q}{p}\right)$ vastaavat toisiaan aina, kun kongruenssi $p \equiv q \equiv 3 \pmod{4}$ ei ole voimassa. Kun $p \equiv q \equiv 3 \pmod{4}$,

$$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right).$$

Koska Legendren symboli $\left(\frac{p}{q}\right) = \pm 1$, jos p ja q ovat parittomia alkulukuja ja $p \neq q$, saadaan, että $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = +1$. Tämä todistaa seuraavan korollaarin.

Korollaari 4.1. *Jos p ja q ovat erillisiä parittomia alkulukuja, niin*

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

[14, s. 162]

Ennen kuin voidaan todistaa neliönjäännösten resiprookkilaki johdannossa esitetyllä tavalla, tulee todistaa Gaussin lemma.

4.1 Gaussin lemma

Gaussin lemma tarjoaa tavan selvittää, onko alkuluvun p kanssa suhteellinen alkuluku a, $a \in \mathbb{Z}$, neliönjäännös vai neliönepäjäännös modulo p.

Lause 4.2 (Gaussin lemma)**.** *Olkoon p pariton alkuluku ja olkoon a sellainen kokonaisluku, että $(a, p) = 1$. Olkoon s joukon $X = \{a, 2a, 3a, \ldots, \frac{(p-1)}{2}a\}$ sellaisten alkioiden lukumäärä, joiden jakojäännös modulo p on suurempi kuin $\frac{p}{2}$. Silloin $\left(\frac{a}{p}\right) = (-1)^s$.[16, s. 407]*

Todistus. Vrt.[11, s. 140] ja [16, s. 407]. Joukon X alkiot ovat epäkongruentteja modulo p. Nimittäin koska $(a, p) = 1$, kongruenssilla

$$ha \equiv ka \pmod{p}$$

on ratkaisu ainoastaan, kun $h \equiv k \pmod{p}$. Muodostetaan joukot U ja V siten, että joukkoon U kuuluvat ne joukon X alkioiden jakojäännökset, jotka ovat pienempiä kuin $p/2$ ja joukkoon V kuuluvat ne joukon X alkioiden jakojäännökset, jotka ovat suurempia kuin $p/2$. Merkitään $U = \{u_1, u_2, \ldots, u_t\}$ ja $V = \{v_1, v_2, \ldots, v_s\}$. Tällöin $s+t = \frac{1}{2}(p-1)$. Luvut $p-v_1, p-v_2, \ldots, p-v_s$ ovat kaikki välillä $[0, \frac{1}{2}p]$. Yksikään näistä luvuista ei ole kongruentti joukon U alkion kanssa modulo p, sillä jos

$$p - v_i \equiv u_j \pmod{p}$$

ja

$$v_i \equiv ba \pmod{p}, u_j \equiv ca \pmod{p},$$

missä $i \in \{1, 2, \ldots, s\}, j \in \{1, 2, \ldots, t\}$ ja $b, c \in \{1, 2, \ldots, \frac{1}{2}(p-1)\}$, niin

$$b + c \equiv 0 \pmod{p}.$$

Tämä on mahdotonta, sillä $0 < b + c < p$, ehdon $b, c \in \{1, 2, \ldots, \frac{1}{2}(p-1)\}$ perusteella. Siis luvut

$$u_1, u_2, \ldots, u_t, p - v_1, p - v_2, \ldots, p - v_s$$

ovat kaikki pienempiä tai yhtäsuuria kuin luku $\frac{1}{2}(p-1)$ ja niitä on $\frac{1}{2}(p-1)$ kappaletta. Kertomalla nämä luvut keskenään, saadaan

$$u_1 u_2 \cdots u_t \cdot (p - v_1)(p - v_2) \cdots (p - v_s)$$

$$\equiv \left(\frac{p-1}{2}\right)! \equiv (-1)^s \cdot \left(\frac{p-1}{2}\right)! \cdot a^{\frac{1}{2}(p-1)} \pmod{p}.$$

Nyt Eulerin kriteerin perusteella seuraa, että

$$\left(\frac{a}{p}\right) = (-1)^s.$$

□

Esimerkki 4.1. Lasketaan $\left(\frac{7}{11}\right)$ Gaussin lemman avulla. Lukujen $7, 2 \cdot 7$, $3 \cdot 7, 4 \cdot 7, 5 \cdot 7$ jakojäännökset modulo 11 ovat $7, 3, 10, 6, 2$, joista kolme on suurempia kuin $\frac{11}{2}$. Näin ollen $\left(\frac{7}{11}\right) = (-1)^3 = -1$. Siis luku 7 on neliönepäjäännös modulo 11.

Koska tiedetään, että $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$, Legendren symbolin $\left(\frac{x}{p}\right)$ arvon laskemiseksi riittää laskea $\left(\frac{q}{p}\right)$ kaikilla alkuluvuilla q, joka jakaa luvun x.

Tarkastellaan ensin tapausta $q = 2$. Osoitetaan, että Legendren symbolin $\left(\frac{2}{p}\right)$ arvo riippuu ainoastaan kongruenssiluokasta p modulo 8.

Lause 4.3. *Olkoon p pariton alkuluku. Silloin $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$. Siis luku 2 on neliönjäännös alkuluvuille $p \equiv \pm 1 \pmod 8$ ja neliönepäjäännös alkuluvuille $p \equiv \pm 3 \pmod 8$.*

Todistus. Vrt.[16, s. 408]. Olkoon s kokonaislukujen

$$1 \cdot 2, 2 \cdot 2, \ldots, ((p-1)/2) \cdot 2$$

sellaisten pienimpien positiivisten jakojäännösten määrä, jotka ovat lukua $p/2$ suurempia. Silloin Gaussin lemman perusteella tiedetään, että

$$\left(\frac{2}{p}\right) = (-1)^s.$$

Koska kaikki yllämainitut kokonaissluvut ovat lukua p pienempiä, riittää laskea ainoastaan lukua $p/2$ suurempien määrä, jotta tiedettäisiin kuinka monen jakojäännös on suurempi kuin $p/2$. Kokonaisluku $2j$, missä $1 \leq j \leq (p-1)/2$, on pienempi kuin $p/2$, kun $j \leq p/4$. Näin ollen lukua $p/2$ pienempiä kokonaislukuja on $\lfloor p/4 \rfloor$ kappaletta. Täten lukua $p/2$ suurempia kokonaislukuja on $s = (p-1)/2 - \lfloor p/4 \rfloor$ kappaletta. Nyt Gaussin lemman perusteella nähdään, että

$$\left(\frac{2}{p}\right) = (-1)^{\frac{(p-1)}{2} - \lfloor p/4 \rfloor}.$$

Lauseen todistamiseksi riittää osoittaa, että kaikilla parittomilla kokonaisluvuilla p pätee

$$\frac{p-1}{2} - \lfloor p/4 \rfloor \equiv \frac{p^2-1}{8} \pmod 2. \tag{4.1}$$

Pitää huomata, että (4.1) pätee positiiviselle kokonaisluvulle p, jos ja vain jos se pätee luvulle $p+8$. Tämä seuraa siitä, että

$$\frac{(p+8)-1}{2} - \lfloor (p+8)/4 \rfloor = \left(\frac{p-1}{2} + 4\right) - (\lfloor p/4 \rfloor + 2) \equiv \frac{p-1}{2} - \lfloor p/4 \rfloor \pmod 2$$

ja

$$\frac{(p+8)^2-1}{8} = \frac{p^2-1}{8} + 2p + 8 \equiv \frac{p^2-1}{8} \pmod 2.$$

Koska jokainen pariton alkuluku p on kongruentti luvun $n = \pm 1$ tai $n = \pm 3$ kanssa modulo 8, voidaan päätellä, että 4.1 pätee jokaiselle parittomalle alkuluvulle p, jos se pätee luvuille $n = \pm 1$ ja $n = \pm 3$. Sillä, että luvut ± 1, -3 eivät ole alkulukuja, ei ole merkitystä kongruenssien käsittelyn kannalta. Tarkastellaan nämä tapaukset:

$$\begin{aligned}
n = 1 &: \frac{1-1}{2} - \lfloor 1/4 \rfloor = 0 \equiv 0 = \frac{1^2-1}{8} \pmod 2 \\
n = -1 &: \frac{-1-1}{2} - \lfloor -1/4 \rfloor = -2 \equiv 0 = \frac{(-1)^2-1}{8} \pmod 2 \\
n = 3 &: \frac{3-1}{2} - \lfloor 3/4 \rfloor = 1 \equiv 1 = \frac{3^2-1}{8} \pmod 2 \\
n = -3 &: \frac{-3-1}{2} - \lfloor -3/4 \rfloor = -3 \equiv 1 = \frac{(-3)^2-1}{8} \pmod 2.
\end{aligned}$$

Koska jokainen pariton alkuluku p on kongruentti luvun $n = \pm 1$ tai $n = \pm 3$ kanssa modulo 8, seuraa, että jokaiselle parittomalle alkuluvulle p pätee

$$\frac{p-1}{2} - \lfloor p/4 \rfloor \equiv \frac{p^2-1}{8} \pmod 2$$

ja edelleen

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

Kongruenssiluokassa $(p^2-1)/8 \pmod 2$ tehdyistä laskuista voidaan huomata, että

$$\left(\frac{2}{p}\right) = 1, \text{ jos } p \equiv \pm 1 \pmod 8$$

ja

$$\left(\frac{2}{p}\right) = -1, \text{ jos } p \equiv \pm 3 \pmod 8.$$

□

(Vaihtoehtoisia todistuksia esitetään muun muassa lähteissä [5, s. 137], [12, s. 105] ja [17, s. 192].)

Ericksonin mukaan [5, s. 138] Legendren symbolin $\left(\frac{3}{p}\right)$ arvon laskeminen kokonaislukua kolme suuremmalle alkuluvulle Gaussin lemmaa kayttäen on vaikeampaa. On kuitenkin olemassa tapa määrittää tämän Legendren symbolin arvo kongruenssiluokasta p modulo 12.

Legendren symboli $\left(\frac{3}{p}\right)$ voidaan liittää symboliin $\left(\frac{p}{3}\right)$. Koska $\left(\frac{p}{3}\right) = 1$, jos ja vain jos $p \equiv 1 \pmod 3$, saadaan ratkaistua alkuperäinen ongelma. Tätä suhdetta Legendren symbolien $\left(\frac{p}{3}\right)$ ja $\left(\frac{3}{p}\right)$ välillä kutsutaan siis neliönjäännösten resiprookkilaiksi.

4.2 Resiprookkilain todistus

Tässä luvussa esiteltävä todistus noudattaa tiukasti Rosenin esittämää todistusta [16, s. 420].Todistuksen pohjana käytetään Rosenin todistusta, koska se on yksi helpoimmista resiprookkilain todistuksista ymmärtää.

Neliönjäännösten resiprookkilaki on Rosenin [16] mielestä yksi kiehtovimmista ja haastavimmista lukuteorian tuloksista. Lause liittää siis toisiinsa Legendren symbolien arvot, kuten edellä ollaan todettu, kun p ja q ovat parittomia alkulukuja.

Ennen varsinaista lauseen todistusta Rosen [16, s. 418] esittelee resiprookkilauseesta muodon, joka osoittaa, että Legendren symbolin $\left(\frac{a}{p}\right)$ arvo riippuu ainoastaan jäännösluokasta p modulo $4a$ ja että Legendren symbolin $\left(\frac{a}{p}\right)$ arvo on sama kaikilla alkuluvuilla p, jonka jäännös on r tai $4a - r$ jaettaessa luvulla $4a$. Tämä muoto esitetään lauseessa 4.4.

Lause 4.4. *Olkoon p pariton alkuluku ja olkoon a kokonaisluku sekä $(a, p) = 1$. Jos q on alkuluku, jolle pätee $p \equiv \pm q \pmod{4a}$, niin $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$*
[16, s. 418]

Osoitamme luvussa 4.3, että edellä esitetyt kaksi resiprookkilain muotoa (lauseet 4.1 ja 4.4) ovat ekvivalentit.

Seuraava Eisensteinin lause mahdollistaa johdannossa mainitun Gaussin kolmannen resiprookkilaille esittämän todistuksen yksinkertaistuksen.

Lause 4.5. *Jos p on pariton alkuluku ja a on pariton kokonaisluku sekä $(a, p) = 1$, niin*

$$\left(\frac{a}{p}\right) = (-1)^{T(a,p)},$$

missä

$$T(a, p) = \sum_{i=1}^{(p-1)/2} \lfloor ja/p \rfloor.$$

Todistus. Vrt.[16, s. 421-422]. Tarkastellaan lukujen $a, 2a, \ldots, ((p-1)/2)a$ pienimpiä positiivisia jakojäännöksiä. Olkoot $u_1, u_2, \ldots, u_s$ niistä ne, jotka ovat lukua $p/2$ suurempia, ja $v_1, v_2, \ldots, v_t$ ne, jotka ovat lukua $p/2$ pienempiä. Jakoalgoritmista saadaan

$$ja = p\lfloor ja/p \rfloor + r_j,$$

missä jäännös r_j on muotoa u_j tai v_j. Kun lasketaan yhteen $\frac{(p-1)}{2}$ tällaista yhtälöä, saadaan

$$\sum_{j=1}^{(p-1)/2} ja = \sum_{j=1}^{(p-1)/2} p\lfloor ja/p \rfloor + \sum_{j=1}^{s} u_j + \sum_{j=1}^{t} v_j \tag{4.2}$$

Kuten Gaussin lemman todistuksessa osoitettiin, kokonaisluvut $p-v_1, \ldots, p-v_s, u_1, \ldots, u_t$ ovat kokonaisluvut $1, 2, \ldots, (p-1)/2$ jossakin järjestyksessä. Kun lasketaan yhteen nämä kokonaisluvut, saadaan

$$\sum_{j=1}^{(p-1)/2} j = \sum_{j=1}^{s}(p - v_j) + \sum_{j=1}^{t} u_j = ps - \sum_{j=1}^{s} v_j + \sum_{j=1}^{t} u_j \tag{4.3}$$

Kun vähennetään yhtälöstä (4.3) yhtälö (4.2) puolittain, nähdään, että

$$\sum_{j=1}^{(p-1)/2} ja - \sum_{j=1}^{(p-1)/2} j = \sum_{j=1}^{(p-1)/2} p\lfloor ja/p \rfloor - ps + 2\sum_{j=1}^{s} v_j.$$

Koska $T(a,p) = \sum_{j=1}^{(p-1)/2} \lfloor ja/p \rfloor$, niin saadaan edellinen lauseke seuraavaan ekvivalenttiin muotoon

$$(a-1)\sum_{j=1}^{(p-1)/2} j = pT(a,p) - ps + 2\sum_{j=1}^{s} v_j.$$

Kun supistetaan tätä viimeistä yhtälöä modulo 2, päästään muotoon

$$0 \equiv T(a,p) - s \pmod 2,$$

sillä a ja p ovat parittomia. Näin ollen

$$T(a,p) \equiv s \pmod 2.$$

Gaussin lemman perusteella

$$\left(\frac{a}{p}\right) = (-1)^s.$$

Näin ollen siitä, että $(-1)^s = (-1)^{T(a,p)}$, seuraa

$$\left(\frac{a}{p}\right) = (-1)^{T(a,p)}.$$

□

Esimerkki 4.2. Käytetään edellistä lausetta Legendren symbolin $\left(\frac{5}{13}\right)$ arvon selvittämiseksi. Arvioidaan siis summaa

$$\begin{aligned}\sum_{i=1}^{6}\lfloor 5i/13\rfloor &= \lfloor 5/13\rfloor + \lfloor 10/13\rfloor + \lfloor 15/13\rfloor + \lfloor 20/13\rfloor + \lfloor 25/13\rfloor + \lfloor 30/13\rfloor \\ &= 0+0+1+1+1+2 = 5.\end{aligned}$$

Siis $\left(\frac{5}{13}\right) = (-1)^5 = -1$.

Vastaavasti Legendren symbolin $\left(\frac{13}{5}\right)$ arvon selvittämiseksi arvioidaan summaa

$$\sum_{i=1}^{2}\lfloor 13i/5\rfloor = \lfloor 13/5\rfloor + \lfloor 26/5\rfloor = 2+5 = 7.$$

Siis $\left(\frac{13}{5}\right) = (-1)^7 = -1$.

Seuraava esimerkki esittelee resiprookkilain todistuksen kulkua. Kyseessä on siis yksi neliönjäännösten resiprookkilain esityistapaus.

Esimerkki 4.3. Olkoon $p = 5$ ja $q = 13$. Tarkastellaan kokonaislukupareja (x, y), missä

$$1 \leq x \leq \frac{(5-1)}{2} = 2$$

ja

$$1 \leq y \leq \frac{(13-1)}{2} = 6.$$

Tällaisia pareja on 12 kappaletta. Voidaan huomata, että mikään näistä pareista ei täytä ehtoa $13x = 5y$, koska silloin $13|5y$ ja näin ollen $13|5$, mikä on mahdotonta, tai $13|y$, mikä on mahdotonta, sillä $1 \leq y \leq 6$.

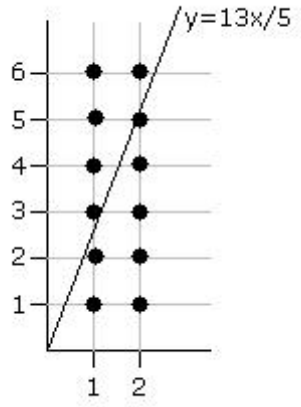
Nämä 12 paria jaetaan kahteen ryhmään kuvan 1 mukaisesti riippuen lukujen $13x$ ja $5y$ suhteellisesta koosta.

Ne kokonaislukuparit (x, y), missä

$$1 \leq x \leq 2, \quad 1 \leq y \leq 6 \quad \text{ja} \quad 13x > 5y$$

ovat täsmälleen ne samat parit, missä

$$1 \leq x \leq 2 \text{ ja } 1 \leq y \leq 13x/5.$$



Kuva 1. Kokonaislukupisteiden laskeminen tulon $\left(\frac{5}{13}\right)\left(\frac{13}{5}\right)$ selvittämiseksi.

Kiinnitetylle kokonaislukuarvolle x, $\quad 1 \leq x \leq 2$, on olemassa $\lfloor 13x/5 \rfloor$ mahdollista luvun y arvoa. Näin ollen niiden parien kokonaismäärä, jotka toteuttavat ehdot

$$1 \leq x \leq 2, \quad 1 \leq y \leq 6 \quad \text{ja} \quad 13x > 5y,$$

on

$$\sum_{i=1}^{2} \lfloor 13i/5 \rfloor = \lfloor 13/5 \rfloor + \lfloor 26/5 \rfloor = 2 + 5 = 7.$$

Nämä 7 paria ovat $(1,1), (1,2), (2,1), (2,2), (2,3), (2,4)$ ja $(2,5)$.

Ne kokonaislukuparit (x, y), missä

$$1 \leq x \leq 2 \text{ ja } 1 \leq y \leq 6 \quad \text{ja} \quad 13x < 5y,$$

ovat täsmälleen ne samat parit, missä

$$1 \leq y \leq 6 \text{ ja } 1 \leq x \leq 5y/13.$$

Kiinnitetylle kokonaislukuarvolle y, $\quad 1 \leq y \leq 6$, on olemassa $\lfloor 5y/13 \rfloor$ mahdollista luvun x arvoa. Näin ollen niiden parien kokonaismäärä, jotka toteuttavat ehdot

$$1 \leq x \leq 2, \quad 1 \leq y \leq 6 \quad \text{ja} \quad 13x < 5y,$$

on

$$\begin{aligned} \sum_{i=1}^{6} \lfloor 5i/13 \rfloor &= \lfloor 5/13 \rfloor + \lfloor 10/13 \rfloor + \lfloor 15/13 \rfloor + \lfloor 20/13 \rfloor + \lfloor 25/13 \rfloor + \lfloor 30/13 \rfloor \\ &= 0 + 0 + 1 + 1 + 1 + 2 = 5. \end{aligned}$$

Nämä 5 paria ovat $(1,3),(1,4),(1,5),(1,6)$ ja $(2,6)$.

Täten nähdään, että

$$\frac{13-1}{2}\cdot\frac{5-1}{2}=6\cdot 2=12=\sum_{i=1}^{2}\lfloor 13i/5\rfloor+\sum_{i=1}^{6}\lfloor 5i/13\rfloor=7+5.$$

Siis

$$(-1)^{\frac{13-1}{2}\cdot\frac{5-1}{2}}=(-1)^{\sum_{i=1}^{2}\lfloor 13i/5\rfloor+\sum_{i=1}^{6}\lfloor 5i/13\rfloor}=(-1)^{\sum_{i=1}^{2}\lfloor 13i/5\rfloor}\cdot(-1)^{\sum_{i=1}^{6}\lfloor 5i/13\rfloor}.$$

Koska lauseen 4.5 perusteella

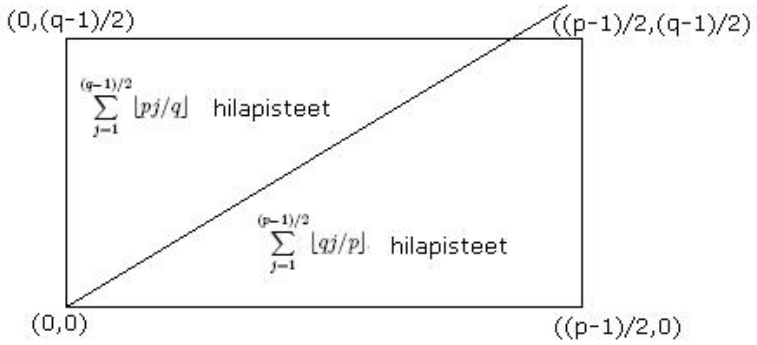
$$\left(\frac{13}{5}\right)=(-1)^{\sum_{i=1}^{2}\lfloor 13i/5\rfloor}\text{ ja }\left(\frac{5}{13}\right)=(-1)^{\sum_{i=1}^{6}\lfloor 5i/13\rfloor},$$

nähdään, että

$$\left(\frac{13}{5}\right)\left(\frac{5}{13}\right)=(-1)^{\frac{13-1}{2}\cdot\frac{5-1}{2}}.$$

Seuraavaksi esitetään todistus neliönjäännösten resiprookkilaille edellisen esimerkin tyyliä noudattaen.

Todistus. Vrt.[16, s. 420]. Tarkastellaan kokonaislukupareja (x,y), missä $1\le x\le(p-1)/2$ ja $1\le y\le(q-1)/2$. Tällaisia pareja on selvästi $\frac{p-1}{2}\cdot\frac{q-1}{2}$ kappaletta. Jaetaan parit kahteen ryhmään kuvan 2 mukaisesti riippuen lukujen qx ja py suhteellisesta koosta.



Kuva 2. Kokonaislukupisteiden laskeminen tulon $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)$ selvittämiseksi.

Ensiksi huomataan, että kaikille pareille pätee $qx\neq py$. Jos olisi $qx=py$, niin $q|py$, jolloin $q|p$ tai $q|y$. Kuitenkin, koska q ja p ovat erisuuria alkulukuja, tiedetään, että $q\not|p$, ja koska $1\le y\le(q-1)/2$, tiedetään, että $q\not|y$.

Jotta tiedettäisiin sellaisten kokonaislukuparien (x, y), missä

$$1 \leq x \leq (p-1)/2,$$

$$1 \leq y \leq (q-1)/2,$$

ja

$$qx > py,$$

määrä, pitää huomata, että kyseessä olevat parit ovat täsmälleen samat parit, missä

$$1 \leq x \leq (p-1)/2 \quad \text{ja} \quad 1 \leq y \leq qx/p.$$

Jokaiselle kiinnitetylle kokonaisluvulle x, $1 \leq x \leq (p-1)/2$, on olemassa $\lfloor qx/p \rfloor$ ehdon $1 \leq y \leq qx/p$ täyttävää y:n arvoa. Täten kokonaislukuparien (x, y), missä

$$1 \leq x \leq (p-1)/2,$$

$$1 \leq y \leq (q-1)/2$$

ja

$$qx > py,$$

kokonaismäärä on

$$\sum_{j=1}^{(p-1)/2} \lfloor qj/p \rfloor.$$

Tarkastellaan sitten kokonaislukupareja (x, y), missä

$$1 \leq x \leq (p-1)/2,$$

$$1 \leq y \leq (q-1)/2$$

ja

$$qx < py.$$

Nämä parit ovat täsmälleen samat, kuin ne parit (x, y), missä

$$1 \leq y \leq (q-1)/2 \quad \text{ja} \quad 1 \leq x \leq py/q,$$

kuten kuvasta 2 voidaan nähdä. Näin ollen jokaiselle kiinnitetylle kokonaisluvulle y, $1 \leq y \leq (q-1)/2$, on olemassa tasan $\lfloor py/q \rfloor$ kokonaislukua x, jolle pätee $1 \leq x \leq py/q$. Siis sellaisten kokonaislukuparien (x, y), missä

$$1 \leq x \leq (p-1)/2,$$

$$1 \leq y \leq (q-1)/2$$

ja

$$qx < py,$$

kokonaismäärä on

$$\sum_{j=1}^{(q-1)/2} \lfloor pj/q \rfloor.$$

Kun lasketaan yhteen näiden luokkien sisältämien parien kokonaismäärät ja muistetaan, että tällaisten parien kokonaismäärä on $\frac{p-1}{2} \cdot \frac{q-1}{2}$, nähdään, että

$$\sum_{j=1}^{(p-1)/2} \lfloor qj/p \rfloor + \sum_{j=1}^{(q-1)/2} \lfloor pj/q \rfloor = \frac{p-1}{2} \cdot \frac{q-1}{2},$$

sillä jokaisen parin on kuuluttava jompaan kumpaan luokkaan. Jos käytetään edellisen lauseen merkintöjä saadaan,

$$T(q,p) + T(p,q) = \frac{p-1}{2} \cdot \frac{q-1}{2}.$$

Näin ollen

$$(-1)^{T(q,p)+T(p,q)} = (-1)^{T(q,p)}(-1)^{T(p,q)} = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

Gaussin lemman ja lauseen 4.5 perusteella

$$(-1)^{T(q,p)} = \left(\frac{q}{p}\right) \quad ja \quad (-1)^{T(p,q)} = \left(\frac{p}{q}\right).$$

Näin ollen

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

□

4.3 Ekvivalenttisuustodistus

Tässä luvussa todistamme edellä esitetyt kaksi resiprookkilain muotoa ekvivalenteiksi.

Lause 4.6. *Olkoot p ja q erisuuria parittomia alkulukuja ja olkoon a positiivinen kokonaisluku. Tällöin neliönjäännösten resiprookkilain muoto*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$$

on ekvivalentti muodon

$$p \equiv \pm q \pmod{4a} \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$$

kanssa.

Todistus. Vrt.[15, s. 60-61]. Oletetaan, että p ja q ovat erisuuria parittomia alkulukuja ja a on positiivinen kokonaisluku. Lisäksi oletetaan, että

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

Nyt riittää todistaa, että

$$p \equiv \pm q \pmod{4a} \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{a}{q}\right),$$

kun a on pariton alkuluku($a \neq p, q$). Jos lause pätee tässä tapauksessa, yleinen tapaus seuraa tekijöihinjaon ja kongruenssin ominaisuuksien perusteella.

Tarkastellaan ensin tapausta, $p \equiv q \pmod{4a}$. Koska kongruenssin $p \equiv q \pmod{4a}$ mukaan on voimassa kongruenssi $p \equiv q \pmod{a}$. Tästä saadaan lauseen 3.15 perusteella, että $\left(\frac{p}{a}\right) = \left(\frac{q}{a}\right)$. Tämän tiedon ja resiprookkilain ensimmäisen muodon perusteella saadaan

$$\left(\frac{a}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{a-1}{2}}\left(\frac{q}{a}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{a-1}{2}}(-1)^{\frac{q-1}{2}\cdot\frac{a-1}{2}}\left(\frac{a}{q}\right) = (-1)^{\frac{a-1}{2}\cdot\frac{p+q-2}{2}}\left(\frac{a}{q}\right).$$

Nyt, kun $p = q+4at$, jollakin $t \in \mathbb{Z}$, saadaan $p+q-2 = 2(q-1+2at)$. Koska luku $q-1+2at$ on parillinen, niin $p+q-2 \equiv 0 \pmod{4}$. Siis $\frac{a-1}{2}\cdot\frac{p+q-2}{2}$ on parillinen ja täten $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$. Näin ollen resiprookkilain toinen muoto pätee tässä tapauksessa.

Vastaavasti käsitellään tapausta $p \equiv -q \pmod{4a}$. Nyt on voimassa kongruenssi $p \equiv -q \pmod{a}$. Tästä saadaan, että $\left(\frac{p}{a}\right) = \left(\frac{-q}{a}\right)$. Tämän tiedon ja resiprookkilain ensimmäisen muodon perusteella saadaan

$$\begin{aligned}\left(\frac{a}{p}\right) &= (-1)^{\frac{p-1}{2}\cdot\frac{a-1}{2}}\left(\frac{-q}{a}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{a-1}{2}}(-1)^{\frac{a-1}{2}}\left(\frac{q}{a}\right)\\ &= (-1)^{\frac{p-1}{2}\cdot\frac{a-1}{2}}(-1)^{\frac{a-1}{2}}(-1)^{\frac{q-1}{2}\cdot\frac{a-1}{2}}\left(\frac{a}{q}\right)\\ &= (-1)^{\frac{a-1}{2}\cdot\frac{p-1+2+q-1}{2}}\left(\frac{a}{q}\right) = (-1)^{\frac{a-1}{2}\cdot\frac{p+q}{2}} = \left(\frac{a}{q}\right)\end{aligned}$$

ja $p+q \equiv 0 \pmod{4}$. Siis $\frac{a-1}{2}\cdot\frac{p+q}{2}$ on parillinen, joten $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$.

Kääntäen oletetaan, että resiprookkilain toinen muoto pätee. Oletetaan lisäksi, että

$$p > q \quad ja \quad p \equiv q \pmod{4}.$$

Näin ollen $p = q + 4a$, jollekin $a \geq 1$. Nyt tätä toista muotoa ja lauseita 3.15 ja 4.3 käyttämällä saadaan

$$\begin{aligned}\left(\frac{p}{q}\right) &= \left(\frac{q+4a}{q}\right) = \left(\frac{4a}{q}\right) = \left(\frac{a}{q}\right) = \left(\frac{a}{p}\right) = \left(\frac{4a}{p}\right) \\ &= \left(\frac{p-q}{p}\right) = \left(\frac{-q}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{q}{p}\right).\end{aligned}$$

Täten, jos $p \equiv 1 \pmod 4$, niin $(p-1)/2$ on parillinen ja $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$. Koska $p \equiv q \pmod 4$, niin $\frac{q-1}{2}$ on parillinen ja siten $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

Jos $p \equiv 3 \pmod 4$, niin $(p-1)/2$ on pariton ja $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$. Tällöin myös $(q-1)/2$ on pariton ja siten $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$. Näin ollen resiprookkilaki pätee kummassakin tapauksessa.

Viimeiseksi oletetaan, että $p \equiv -q \pmod 4$. Tällöin $p+q = 4a$, jollekin $a \geq 1$. Tästä ja resiprookkilain toisesta muodosta sekä lauseesta 3.15 saadaan

$$\left(\frac{p}{q}\right) = \left(\frac{-q+4a}{q}\right) = \left(\frac{a}{q}\right) = \left(\frac{a}{p}\right) = \left(\frac{4a}{p}\right) = \left(\frac{p+q}{p}\right) = \left(\frac{q}{p}\right).$$

Nyt jos $p \equiv 1 \pmod 4$, niin $q \equiv 3 \pmod 4$ ja siten $(p-1)/2$ on parillinen ja $(q-1)/2$ on pariton. Näin ollen $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

Jos sitten $p \equiv 3 \pmod 4$, niin $q \equiv 1 \pmod 4$ ja siten $(p-1)/2$ on pariton ja $(q-1)/2$ on parillinen. Näin ollen $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

Täten resiprookkilain muodot ovat yhtäpitävät. □

Ericksonin mukaan [5, s. 138] Legendren symbolin $\left(\frac{3}{p}\right)$ arvon laskeminen kokonaislukua kolme suuremmalle alkuluvulle Gaussin lemmaa kayttäen on hankalaa. Seuraavassa esimerkissä huomataan, kuinka kätevästi se saadaan laskettua resiprookkilain avulla.

Esimerkki 4.4. Edellisen lauseen perusteella saadaan, että

$$\left(\frac{3}{p}\right) = 1, \text{ jos ja vain jos } p \equiv \pm 1 \pmod{12}.$$

Tätä tarkastellaan tarkemmin seuraavassa luvussa.

5 Resiprookkilain sovelluksia

Neliönjäännösten resiprookkilailla on sekä teoreettisia että käytännöllisiä sovelluksia. Sitä voidaan käyttää muun muassa laskuissa ja hyödyllisten tulosten todistamiseen. Tässä luvussa esitellään muutamia kiintoisia sovelluksia.

5.1 Legendren symbolin arvioiminen

Resiprookkilakia käytetään muun muassa Legendren symbolien arvioimiseen. Edellisessä kappaleessa voitiin huomata, että $(p-1)/2$ on parillinen, kun $p \equiv 1 \pmod 4$, ja pariton, kun $p \equiv 3 \pmod 4$. Edelleen voidaan huomata, että $\frac{(p-1)}{2} \cdot \frac{(q-1)}{2}$ on parillinen, kun $p \equiv 1 \pmod 4$ ja $q \equiv 1 \pmod 4$, ja $\frac{(p-1)}{2} \cdot \frac{(q-1)}{2}$ on pariton, jos $p \equiv q \equiv 3 \pmod 4$. Tällöin saadaan

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = \begin{cases} 1, & \text{jos } p \equiv 1 \pmod 4 \text{ tai } q \equiv 1 \pmod 4 \\ -1, & \text{jos } p \equiv q \equiv 3 \pmod 4. \end{cases}$$

(Pitää huomata, että yllä ei ole kyse poissulkevasta tai:sta.)
Koska ainoat mahdolliset arvot Legendren symboleille $\left(\frac{p}{q}\right)$ ja $\left(\frac{q}{p}\right)$ ovat ± 1, nähdään, että

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right), & \text{jos } p \equiv 1 \pmod 4 \text{ tai } q \equiv 1 \pmod 4 \\ -\left(\frac{q}{p}\right), & \text{jos } p \equiv q \equiv 3 \pmod 4. \end{cases}$$

Tämä tarkoittaa sitä, että jos p ja q ovat parittomia alkulukuja, niin $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ elleivät molemmat p ja q ole kongruentteja luvun 3 kanssa modulo 4. Jos molemmat p ja q ovat kongruentteja luvun 3 kanssa modulo 4, niin $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$.

Esimerkki 5.1. Olkoon $p = 17$ ja $q = 21$. Koska $17 \equiv 21 \equiv 1 \pmod 4$, neliönjäännösten resiprookkilain nojalla $\left(\frac{17}{21}\right) = \left(\frac{21}{17}\right)$. Nyt lauseen 3.15 kohdan (3.6) nojalla tiedetään, että $\left(\frac{21}{17}\right) = \left(\frac{4}{17}\right)$ ja saman lauseen kohdan (3.3) nojalla seuraa, että $\left(\frac{4}{17}\right) = \left(\frac{2^2}{17}\right) = 1$. Tästä saadaan, että $\left(\frac{17}{21}\right) = 1$.

5.1.1 Neliönjäännösten kaksi perusongelmaa ja muita laskuesimerkkejä

Seuraavat esimerkit osoittavat kuinka neliönjäännösten resiprookkilakia voidaan käyttää neliönjäännöksiin liittyvien perusongelmien ratkaisuissa. Esimerkit ovat lähteen [2, s. 186-187] mukaisia.

Esimerkki 5.2. Määritä, onko 219 neliönjäännös vai neliönepäjäännös modulo 383.

Ratkaisu. Arvioidaan Legendren symbolia $\left(\frac{219}{383}\right)$ käyttämällä Legedren symbolien multiplikatiivisuutta, resiprookkilakia, jaksollisuutta ja Legendren symbolien $\left(\frac{-1}{p}\right)$ ja $\left(\frac{2}{p}\right)$ arvoja, jotka on laskettu aiemmin.

Koska $219 = 3 \cdot 73$ Legendren symbolien ominaisuuksien perusteella saadaan

$$\left(\frac{219}{383}\right) = \left(\frac{3}{383}\right)\left(\frac{73}{383}\right).$$

Resiprookkilakia ja lausetta 3.15 sekä jaksollisuutta käyttämällä saadaan

$$\left(\frac{3}{383}\right) = \left(\frac{383}{3}\right)(-1)^{\frac{383-1}{2}\cdot\frac{3-1}{2}} = -\left(\frac{-1}{3}\right) = -(-1)^{\frac{3-1}{2}} = 1,$$

ja

$$\left(\frac{73}{383}\right) = \left(\frac{383}{73}\right)(-1)^{\frac{383-1}{2}\cdot\frac{73-1}{2}} = \left(\frac{18}{73}\right) = \left(\frac{2}{73}\right)\left(\frac{9}{73}\right) = (-1)^{\frac{(73)^2-1}{8}} = 1.$$

Näin ollen $\left(\frac{219}{383}\right) = 1$ ja 219 on siis neliönjäännös modulo 383.

Esimerkki 5.3. Määritä ne parittomat alkuluvut p, joille luku 3 on neliönjäännös, ja ne, joille se on neliönepäjäännös.

Ratkaisu. Resiprookkilain korollaarin 4.1 nojalla saadaan

$$\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)(-1)^{\frac{p-1}{2}\cdot\frac{3-1}{2}} = (-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right).$$

Jotta voitaisiin määrittää $\left(\frac{p}{3}\right)$, pitää tietää arvo $p \pmod 3$, ja jotta voitaisiin määrittää $(-1)^{\frac{p-1}{2}}$, pitää tietää arvo $\frac{p-1}{2} \pmod 2$ tai arvo $p \pmod 4$. Siksi tarkastellaan arvoa $p \pmod{12}$. Tarkasteltavana on vain neljä tapausta, $p \equiv 1, 5, 7$ tai $11 \pmod{12}$. Muut tapaukset tulevat poissuljetuksi, sillä p on pariton.

Tapaus 1. $p \equiv 1 \pmod{12}$. Tässä tapauksessa $p \equiv 1 \pmod 3$, joten $\left(\frac{p}{3}\right) = \left(\frac{1}{3}\right) = 1$. Lisäksi $p \equiv 1 \pmod 4$, joten $\frac{p-1}{2}$ on parillinen ja näin ollen $\left(\frac{3}{p}\right) = 1$.

Tapaus 2. $p \equiv 5 \pmod{12}$. Tässä tapauksessa $p \equiv 2 \pmod 3$, joten $\left(\frac{p}{3}\right) = \left(\frac{2}{3}\right) = (-1)^{\frac{3^2-1}{8}} = -1$. Jälleen $\frac{p-1}{2}$ on parillinen, sillä $p \equiv 1 \pmod 4$, joten $\left(\frac{3}{p}\right) = -1$.

Tapaus 3. $p \equiv 7 \pmod{12}$ eli $p \equiv -5 \pmod{12}$. Tässä tapauksessa $p \equiv 1 \pmod 3$, joten $\left(\frac{p}{3}\right) = \left(\frac{1}{3}\right) = 1$. Lisäksi $\frac{p-1}{2}$ on pariton, sillä $p \equiv 3 \pmod 4$. Näin ollen $\left(\frac{3}{p}\right) = -1$.

Tapaus 4. $p \equiv 11 \pmod{12}$ eli $p \equiv -1 \pmod{12}$. Tässä tapauksessa $p \equiv 2 \pmod 3$, joten $\left(\frac{p}{3}\right) = \left(\frac{2}{3}\right) = -1$. Jälleen $\frac{p-1}{2}$ on pariton, sillä $p \equiv 3 \pmod 4$. Näin ollen $\left(\frac{3}{p}\right) = 1$.

Yhteenvetona näistä neljästä tapauksesta nähdään, että luku 3 on neliönjäännös modulo p, jos $p \equiv \pm 1 \pmod{12}$, ja luku 3 on neliönepäjäännös modulo p, jos $p \equiv \pm 5 \pmod{12}$. Päättely voidaan tehdä myös kiinalaista jäännöslausetta 3.10 ja korollaaria 4.1 käyttäen, kts.[14, s. 163].

Seuraavaksi esitetään lisää laskuesimerkkejä. Esimerkit noudattavat lähteessä [14, s. 161-168] esitettyjä esimerkkejä.

Korollaaria 4.1 käytetään seuraavassa esimerkissä.

Esimerkki 5.4. Onko $x^2 \equiv -42 \pmod{61}$ ratkeava?

Ratkaisu. Kongruessi on ratkeava, joss $\left(\frac{-42}{61}\right) = +1$. Koska tiedetään, että $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$, saadaan

$$\left(\frac{-42}{61}\right) = \left(\frac{-2}{61}\right)\left(\frac{21}{61}\right) = \left(\frac{-1}{61}\right)\left(\frac{2}{61}\right)\left(\frac{3}{61}\right)\left(\frac{7}{61}\right).$$

Soveltaen tätä tulosta, lausetta 4.3 ja korollaaria 4.1 saadaan

$$\begin{aligned}
\left(\frac{-1}{61}\right) &= (-1)^{61-1/2} = (-1)^{30} = +1, \\
\left(\frac{2}{61}\right) &= (-1)^{61^2-1/8} = (-1)^{60\cdot 62/8} = (-1)^{15\cdot 31} = -1, \\
\left(\frac{3}{61}\right) &= \left(\frac{61}{3}\right)(-1)^{(3-1/2)(61-1/2)} = \left(\frac{1}{3}\right)(-1)^{30} = +1, \\
\left(\frac{7}{61}\right) &= \left(\frac{61}{7}\right)(-1)^{(7-1/2)(61-1/2)} = \left(\frac{5}{7}\right)(-1)^{90} \\
&= \left(\frac{5}{7}\right) = \left(\frac{7}{5}\right)(-1)^{(5-1/2)(7-1/2)} = \left(\frac{2}{5}\right)(-1)^6 \\
&= \left(\frac{2}{5}\right) = (-1)^{(5^2-1)/8} = (-1)^3 = -1.
\end{aligned}$$

Siis

$$\left(\frac{-42}{61}\right) = (+1)(-1)(+1)(-1) = +1,$$

ja yhtälö on ratkeava. Itse asiassa kokeilemalla löydettävät ratkaisut ovat $x \equiv 18$ ja $43 \pmod{61}$.

Annetaan resiprookkilailla sovellus Legendren symbolien laskemiseen. Tämä on Eulerin versio neliönjäännösten resiprookkilaista.

Lause 5.1. *Olkoon p pariton alkuluku. Jokaiselle alkuluvulle q, $q > p$, määritellään positiivinen kokonaisluku r seuraavasti:*

$$\textit{jos } p \equiv 1 \pmod 4, \textit{ niin } q = kp + r, 0 < r < p,$$

$$\textit{jos } p \equiv 3 \pmod 4, \textit{ niin } q = 4kp \pm r, 0 < r < 4p, r \equiv 1 \pmod 4.$$

Tällöin

$$\left(\frac{p}{q}\right) = \left(\frac{r}{p}\right).$$

Todistus. Vrt.[14, s. 164-165]. Jos $p \equiv 1 \pmod 4$, niin resiprookkilain ja lauseen 3.15 perusteella saadaan

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) = \left(\frac{kp+r}{p}\right) = \left(\frac{r}{p}\right).$$

Jos $p \equiv 3 \pmod 4$, näytetään ensin, että r on olemassa väitetyllä tavalla. Kirjoitetaan

$$q = 4kp + r_0, \quad 0 \leq r_0 \leq 4p.$$

Jos $r_0 \equiv 1 \pmod 4$, niin valitaan $r = r_0$, ja jos $r_0 \equiv 3 \pmod 4$, valitaan $r = 4p - r_0$. Näin ollen luvun r yksiselitteisyys on selvää.

Jos $q = 4kp + r$, niin $q \equiv r \equiv 1 \pmod 4$ ja saadaan jälleen

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) = \left(\frac{r}{p}\right).$$

Jos $q = 4kp - r$, niin $q \equiv -r \equiv 3 \pmod 4$. Resiprookkilain ja lauseen 3.15 perusteella saadaan

$$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right) = -\left(\frac{-r}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{r}{p}\right) = \left(\frac{r}{p}\right),$$

mikä todistaa tuloksen. □

Esimerkki 5.5. Etsi kaikki sellaiset alkuluvut, joille luku 19 on neliönjäännös.
Ratkaisu. Tämä joukko on helppo muodostaa huomautuksen 3.7 perusteella. Nyt luvun 19 neliönjäännösten $r, 0 < r < 76$ ja $r \equiv 1 \pmod 4$, joukko on

$$R = \{1, 9, 17, 25, 45, 49, 61, 73\}.$$

Näin ollen edellisen lauseen perusteella parittomat alkuluvut q, joille luku 19 on neliönjäännös, ovat muotoa

$$76k \pm r, r \in R.$$

5.2 Pepinin testi

Testi on kehitetty Fermat'n alkuluvuille. Fermat on esittänyt väitteen, jonka mukaan muotoa $2^{2^n} + 1, \text{kun} \quad n \in \mathbb{Z}_+$, olevat luvut ovat alkulukuja. Euler on todistanut vuonna 1732, että Fermat'n esittelemä sääntö alkuluvuille ei aina päde ja tämän lause kertoo, mitkä luvuista ovat oikeasti alkulukuja.

Lause 5.2. *Fermat'n alkuluku* $2^{2^n} + 1$ *on alkuluku, jos ja vain jos*

$$3^{(F_n-1)/2} \equiv -1 \pmod{F_n}.$$

Todistus. Vrt. [16, s. 425]. Osoitetaan ensin, että Fermat'n alkuluku F_n on alkuluku, jos väitteessä esitetty kongruenssi pitää paikkansa. Oletetaan, että

$$3^{(F_n-1)/2} \equiv -1 \pmod{F_n}.$$

Korottamalla puolittain toiseen potenssiin saadaan korollaarin 3.2 perusteella

$$3^{F_n-1} \equiv -1 \pmod{F_n}.$$

Tästä kongruenssista nähdään, että jos p on alkuluku, joka jakaa luvun F_n, niin

$$3^{F_n-1} \equiv -1 \pmod{p},$$

joten

$$\text{ord}_p 3 | (F_n - 1) = 2^{2^n}.$$

Näin ollen luvun $\text{ord}_p 3$ tulee olla luvun 2 potenssi. Kuitenkin

$$\text{ord}_p 3 \not| 2^{2^n-1} = (F_n - 1)/2,$$

koska $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$. Täten ainoa mahdollisuus on, että $\text{ord}_p 3 = 2^{2^n} = F_n - 1$. Koska $\text{ord}_p 3 = F_n - 1 \leq p - 1$ ja $p | F_n$, nähdään, että $p = F_n$ ja täten F_n on alkuluku.

Oletetaan sitten, että F_n on alkuluku, ja osoitetaan, että kongruenssi $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$ pitää paikkansa.

Jos $F_n = 2^{2^n} + 1$ on alkuluku, niin neliönjäännösten resiprookkilauseen perusteella

$$\left(\frac{3}{F_n}\right) = \left(\frac{F_n}{3}\right) = \left(\frac{2}{3}\right) = -1, \tag{5.1}$$

koska $F_n \equiv 1 \pmod 4$ ja $F_n \equiv 2 \pmod 3$. Nyt Eulerin kriteerin nojalla saadaan

$$\left(\frac{3}{F_n}\right) \equiv 3^{(F_n-1)/2} \pmod{F_n}. \tag{5.2}$$

Näiden kahden yhtälön (5.1) ja (5.2) perusteella voidaan päätellä, että

$$3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$$

□

Esimerkki 5.6. Olkoon $n = 1$. Nyt $F_1 = 2^{2^1} + 1 = 5$ ja

$$3^{(F_1-1)/2} = 3^2 = 9 \equiv -1 \pmod 5.$$

Pepinin testin perusteella $F_1 = 5$ on alkuluku.

Olkoon $n = 5$. Nyt $F_5 = 2^{2^5} + 1 = 2^{32} + 1 = 4294967297$ ja

$$3^{(F_5-1)/2} = 3^{2^{31}} = 3^{2146483648} \equiv 10324303 \not\equiv -1 \pmod{2^{32}+1}.$$

Pepinin testin perusteella $F_5 = 2^{32} + 1$ ei ole alkuluku.[16, s. 426]

5.3 Resiprookkilaki Jacobin symbolille

Jacobin symboli on yleistys Legendren symbolille. Jacobin symbolit ovat hyödyllisiä Legendren symbolien arvioimiseen ja pseudoalkulukujen määrittelyyn.

Määritelmä 5.1. Olkoon n pariton positiivinen alkuluku, jonka alkulukuesitys on $n = {p_1}^{t_1}{p_2}^{t_2}\cdots{p_m}^{t_m}$, ja olkoon a kokonaisluku, $(a, n) = 1$. Tällöin Jacobin symboli $\left(\frac{a}{n}\right)$ määritellään seuraavasti:

$$\left(\frac{a}{n}\right) = \left(\frac{a}{{p_1}^{t_1}{p_2}^{t_2}\cdots{p_m}^{t_m}}\right) = \left(\frac{a}{p_1}\right)^{t_1}\left(\frac{a}{p_2}\right)^{t_2}\cdots\left(\frac{a}{p_m}\right)^{t_m},$$

missä yhtäsuuruuden oikealla puolella olevat symbolit ovat Legendren symboleja [16, s. 430].

Esimerkki 5.7. Jacobin symbolin määritelmästä nähdään, että

$$\left(\frac{2}{49}\right) = \left(\frac{2}{3^2 \cdot 7}\right) = \left(\frac{2}{3}\right)^2 \left(\frac{2}{7}\right) = (-1)^2(1) = 1$$

ja

$$\begin{aligned}\left(\frac{109}{105}\right) &= \left(\frac{109}{3 \cdot 5 \cdot 7}\right) = \left(\frac{109}{3}\right)\left(\frac{109}{5}\right)\left(\frac{109}{7}\right) \\ &= \left(\frac{1}{3}\right)\left(\frac{4}{5}\right)\left(\frac{4}{7}\right) = \left(\frac{1}{3}\right)\left(\frac{2}{5}\right)^2\left(\frac{4}{7}\right)^2 \\ &= 1(-1)^2 1^2 = 1.\end{aligned}$$

Kun n on alkuluku, Jacobin symboli vastaa Legendren symbolia. Jos n ei ole alkuluku, Jacobin symbolin $\left(\frac{a}{n}\right)$ arvo ei kerro onko kongruenssilla $x^2 \equiv a \pmod{n}$ ratkaisua. Tiedetään kuitenkin, että jos kongruenssilla $x^2 \equiv a \pmod{n}$ on ratkaisu, niin $\left(\frac{a}{n}\right) = 1$. Nimittäin, jos p on luvun n alkulukutekijä ja kongruenssilla $x^2 \equiv a \pmod{n}$ on ratkaisu, niin kongruenssilla $x^2 \equiv a \pmod{p}$ on myös ratkaisu. Näin ollen $\left(\frac{a}{p}\right) = 1$. Täten $\left(\frac{a}{n}\right) = \prod_{j=1}^{m} \left(\frac{a}{p_j}\right)^{t_j} = 1$, missä luvun n alkulukuesitys on $n = {p_1}^{t_1}{p_2}^{t_2} \cdots {p_m}^{t_m}$. On mahdollista, että $\left(\frac{a}{n}\right) = 1$, vaikka kongruenssilla $x^2 \equiv a \pmod{n}$ ei olisikaan ratkaisua. Olkoon esimerkiksi $a = 2$ ja $n = 15$. Huomataan, että $\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)(-1) = 1$. Kuitenkaan kongruenssilla $x^2 \equiv 2 \pmod{15}$ ei ole ratkaisua, koska kongruensseilla $x^2 \equiv 2 \pmod{3}$ ja $x^2 \equiv 2 \pmod{5}$ ei ole ratkaisuja.

Jacobin symboleilla on joitakin samankaltaisia ominaisuuksia kuin Legendren symboleilla.

Lause 5.3. *Olkoon n positiivinen kokonaisluku, ja olkoot a ja b luvun n kanssa suhteellisia alkulukuja. Tällöin*

$$a \equiv b \pmod{n} \Rightarrow \left(\frac{a}{n}\right) = \left(\frac{b}{n}\right) \tag{5.3}$$

$$\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right) \tag{5.4}$$

$$\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2} \tag{5.5}$$

$$\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8}. \tag{5.6}$$

Todistus. Vrt. [16, s. 431]. Kohta 5.3: Oletetaan, että $a \equiv b \pmod{n}$. Jos p on alkuluku, joka jakaa kokonaisluvun n, niin $a \equiv b \pmod{p}$. Näin ollen lauseesta 3.15 saadaan, että $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$. Edelleen saadaan, että

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{t_1}\left(\frac{a}{p_2}\right)^{t_2}\cdots\left(\frac{a}{p_m}\right)^{t_m} = \left(\frac{b}{p_1}\right)^{t_1}\left(\frac{b}{p_2}\right)^{t_2}\cdots\left(\frac{b}{p_m}\right)^{t_m} = \left(\frac{b}{n}\right).$$

Kohta 5.4: Lauseen 3.15 perusteella tiedetään, että $\left(\frac{ab}{p_i}\right) = \left(\frac{a}{p_i}\right)\left(\frac{b}{p_i}\right)$ kaikilla $i = 1, 2, \ldots, m$. Näin ollen

$$\begin{aligned}\left(\frac{ab}{n}\right) &= \left(\frac{ab}{p_1}\right)^{t_1}\left(\frac{ab}{p_2}\right)^{t_2}\cdots\left(\frac{ab}{p_m}\right)^{t_m}\\ &= \left(\frac{a}{p_1}\right)^{t_1}\left(\frac{b}{p_1}\right)^{t_1}\left(\frac{a}{p_2}\right)^{t_2}\left(\frac{b}{p_2}\right)^{t_2}\cdots\left(\frac{a}{p_m}\right)^{t_m}\left(\frac{b}{p_m}\right)^{t_m}\\ &= \left(\frac{a}{n}\right)\left(\frac{b}{n}\right).\end{aligned}$$

Kohta 5.5: Lauseen 3.15 perusteella tiedetään myös, että jos p on alkuluku, niin $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$. Tästä seuraa, että

$$\begin{aligned}\left(\frac{-1}{n}\right) &= \left(\frac{-1}{p_1}\right)^{t_1}\left(\frac{-1}{p_2}\right)^{t_2}\cdots\left(\frac{-1}{p_m}\right)^{t_m}\\ &= (-1)^{(p_1-1)/2+(p_2-1)/2+\cdots+(p_m-1)/2}.\end{aligned}$$

Nyt pitää vielä osoittaa, että

$$(n-1)/2 \equiv t_1(p_1-1)/2 + t_2(p_2-1)/2 + \cdots + t_m(p_m-1)/2 \pmod{2}.$$

Kokonaisluvun n alkulukuesityksen perusteella saadaan

$$n = (1+(p_1-1))^{t_1}(1+(p_2-1))^{t_2}\cdots(1+(p_m-1))^{t_m}.$$

Koska luku $p_i - 1$ on parillinen, saadaan, että

$$(1+(p_i-1))^{t_i} \equiv (1+t_i(p_i-1)) \pmod{4}$$

ja

$$(1+t_i(p_i-1))(1+t_j(p_j-1)) \equiv 1 + t_i(p_i-1) + t_j(p_j-1) \pmod{4}.$$

Näin ollen

$$n \equiv 1 + t_1(p_1-1) + t_2(p_2-1) + \cdots + 1 + t_m(p_m-1) \pmod{4},$$

mistä seuraa, että

$$(n-1)/2 \equiv t_1(p_1-1)/2 + t_2(p_2-1)/2 + \cdots + t_m(p_m-1)/2 \pmod 2.$$

Yhdistämällä kongruenssi luvulle $(n-1)/2$ ja lauseke Jacobin symbolille $\left(\frac{-1}{n}\right)$ saadaan

$$\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}.$$

Kohta 5.6: Jos p on alkuluku, niin $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$. Näin ollen

$$\begin{aligned}\left(\frac{2}{n}\right) &= \left(\frac{2}{p_1}\right)^{t_1}\left(\frac{2}{p_2}\right)^{t_2}\cdots\left(\frac{2}{p_m}\right)^{t_m} \\ &= (-1)^{t_1(p_1^2-1)/8 + t_2(p_2^2-1)/8 + \cdots + t_m(p_m^2-1)/8}.\end{aligned}$$

Samoin kuten edellisen kohdan todistuksessa huomattiin

$$n^2 = (1+(p_1^2-1)/8)^{t_1}(1+(p_2^2-1)/8)^{t_2} + \cdots (1+(p_m^2-1)/8)^{t_m}.$$

Koska luku $p_i^2 - 1 \equiv 0 \pmod 8$ kaikilla $i = 1, 2, \ldots, m$, saadaan, että

$$(1+(p_i^2-1))^{t_i} \equiv 1 + t_i(p_i^2-1) \pmod{64}$$

ja

$$(1+t_i(p_i^2-1))(1+t_j(p_j^2-1)) \equiv 1 + t_i(p_i^2-1) + t_j(p_j^2-1) \pmod{64}.$$

Näin ollen

$$n^2 \equiv 1 + t_1(p_1^2-1) + t_2(p_2^2-1) + \cdots + t_m(p_m^2-1) \pmod{64},$$

mistä seuraa, että

$$(n^2-1)/8 = t_1(p_1^2-1)/8 + t_2(p_2^2-1)/8 + \cdots + t_m(p_m^2-1)/8.$$

Yhdistämällä kongruenssi luvulle $(n^2-1)/8$ ja lauseke Jacobin symbolille $\left(\frac{2}{n}\right)$ saadaan

$$\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8}.$$

□

Seuraavaksi osoitetaan, että resiprookkilaki pätee myös Jacobin symbolille.

Lause 5.4 (Resiprookkilaki Jacobin symbolille)**.** *Olkoot n ja m parittomia positiivisia kokonaislukuja ja keskenään suhteellisia alkulukuja. Tällöin*

$$\left(\frac{n}{m}\right)\left(\frac{m}{n}\right) = (-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}.$$

Todistus. Vrt.[16, s. 433]. Olkoot lukujen m ja n alkulukuesitykset seuraavat: $m = {p_1}^{a_1}{p_2}^{a_2}\cdots{p_s}^{a_s}$ ja $n = {q_1}^{b_1}{q_2}^{b_2}\cdots{q_r}^{b_r}$. Nähdään, että

$$\left(\frac{m}{n}\right) = \prod_{i=1}^{r}\left(\frac{m}{q_i}\right)^{b_i} = \prod_{i=1}^{r}\prod_{j=1}^{s}\left(\frac{p_j}{q_j}\right)^{b_i a_j}$$

ja

$$\left(\frac{n}{m}\right) = \prod_{j=1}^{s}\left(\frac{n}{p_j}\right)^{a_j} = \prod_{j=1}^{s}\prod_{i=1}^{r}\left(\frac{q_i}{p_j}\right)^{a_j b_i}.$$

Näin ollen

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = \Big[\prod_{i=1}^{r}\prod_{j=1}^{s}\left(\frac{p_j}{q_j}\right)^{b_i a_j}\Big]\Big[\prod_{j=1}^{s}\prod_{i=1}^{r}\left(\frac{q_i}{p_j}\right)^{a_j b_i}\Big] = \prod_{i=1}^{r}\prod_{j=1}^{s}\left[\left(\frac{p_j}{q_i}\right)\left(\frac{q_i}{p_j}\right)\right]^{a_j b_i}.$$

Neliönjäännösten resiprookkilain nojalla tiedetään, että

$$\left(\frac{p_j}{q_i}\right)\left(\frac{q_i}{p_j}\right) = (-1)^{\frac{(p_j-1)}{2}\cdot\frac{(q_i-1)}{2}},$$

joten

(5.7)

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = \prod_{i=1}^{r}\prod_{j=1}^{s}(-1)^{a_j\left(\frac{p_j-1}{2}\right)b_i\left(\frac{q_i-1}{2}\right)} = (-1)^{\sum_{i=1}^{r}\sum_{j=1}^{s}a_j\left(\frac{p_j-1}{2}\right)b_i\left(\frac{q_i-1}{2}\right)}.$$

Huomataan, että

$$\sum_{i=1}^{r}\sum_{j=1}^{s}a_j\Big(\frac{p_j-1}{2}\Big)b_i\Big(\frac{q_i-1}{2}\Big) = \sum_{j=1}^{s}a_j\Big(\frac{p_j-1}{2}\Big)\sum_{i=1}^{r}b_i\Big(\frac{q_i-1}{2}\Big).$$

Kuten edellisen lauseen kaavan (5.5) todistuksen perusteella voidaan huomata

$$\sum_{j=1}^{s}a_j\Big(\frac{p_j-1}{2}\Big) \equiv \frac{m-1}{2} \pmod 2$$

ja

$$\sum_{i=1}^{r}b_i\Big(\frac{q_i-1}{2}\Big) \equiv \frac{n-1}{2} \pmod 2.$$

Näin ollen

$$\sum_{i=1}^{r}\sum_{j=1}^{s}a_j\Big(\frac{p_j-1}{2}\Big)b_i\Big(\frac{q_i-1}{2}\Big) \equiv \frac{m-1}{2}\cdot\frac{n-1}{2} \pmod 2. \tag{5.8}$$

Nyt yhtälöiden (5.7) ja (5.8) nojalla voidaan päätellä, että

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}.$$

□

5.4 Ortogonaaliset yksikkömatriisit

Usein on tarpeen muodostaa matriiseja, joilla on tiettyjä erityisiä ominaisuuksia ja joiden alkioiden määrää on rajoitettu jollain tavalla. Lukuteorian ominaisuudet tulevat ajoittain avuksi. Tässä luvussa käsitellään yhtä tällaista matriisityyppiä[4]. Luvussa seurataan Andersonin ja Bellin [1, s. 239-250] teoksen lukua 3.11.

Aloitetaan aiheen käsittely kertaamalla muutama matriisien ominaisuus ja selventämällä termin *ortogonaalinen* käyttöä tässä yhteydessä.

Määritelmä 5.2. Olkoot V ja W rivi- tai sarakematriiseja, joissa on n alkiota. Merkitään

$$\begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix} \quad \text{tai} \quad \begin{bmatrix} v_1 & v_2 & \cdots & v_n \end{bmatrix}$$

ja

$$\begin{bmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{bmatrix} \quad \text{tai} \quad \begin{bmatrix} w_1 & w_2 & \cdots & w_n \end{bmatrix}.$$

Matsiisien V ja W ($\neq \bar{o}$) sanotaan olevan ortogonaalisia, jos niiden pistetulo on nolla eli jos

$$V \bullet W = v_1 w_1 + v_2 w_2 + \cdots + v_n w_n = 0.$$

[1, s. 239]

Esimerkki 5.8. Matriisit

$$A = \begin{bmatrix} 2 \\ 0 \\ -1 \\ 4 \end{bmatrix} \quad \text{ja} \quad B = \begin{bmatrix} 0 \\ 7 \\ 4 \\ 1 \end{bmatrix}$$

ovat ortogonaalisia, sillä

$$A \bullet B = 2 \cdot 0 + 0 \cdot 7 + (-1) \cdot 4 + 1 \cdot 4 = 0 + 0 - 4 + 4 = 0.$$

Määritelmä 5.3. Reaalinen $n \times n$ matriisi A on *ortogonaalinen*, jos $AA^t = A^tA = I_n$, missä I_n on $n \times n$ identiteettimatriisi ja A^t on matriisin A traspoosi. [1, s. 240]

[4]Toinen tällainen matriisityyppi on Hadamardin matriisit, joista tarkemmin esim. [5, s. 155-157]

Yhtälö $AA^t = I_n$ tarkoittaa siis sitä, että matriisin A i:nnen rivin ja matriisin A^t j:nnen sarakkeen pistetulo tuottaa luvun 1, kun $i = j$, ja luvun 0, kun $i \neq j$. Toisin sanoen matriisin A i:s rivi on ortogonaalinen matriisin A^t j:nen rivin kanssa, kun $i \neq j$, ja tulo saa arvon 1, kun $i = j$. Mikäli matriisin A rivit sisältävät samat alkiot kuin matriisin A^t sarakkeet, se, että matriisi A on ortogonaalinen, tarkoittaa matriisin A eri rivien olevan ortogonaalisia ja rivin pistetulo itsensä kanssa antaa arvon 1. Tällöin pitää huomata, että mikään matriisin A riveistä ei voi sisältää pelkästään nollaa alkioinaan, sillä rivien pistetulon itsensä kanssa pitää olla 1. Koska $A^tA = I_n$, väitteet voidaan todistaa myös matriisiin A sarakkeille.

Määritelmä 5.4. Reaalinen $n \times n$ matriisi $A = [a_{ij}]$ on *U-matriisi*, jos

$$a_{ij} = \pm 1 \text{ kaikilla } i, j = 1, 2, \ldots, n$$

ja

$$AA^t = A^tA = D = \begin{bmatrix} d_1 & 0 & 0 & \cdots & 0 \\ 0 & d_2 & 0 & \cdots & 0 \\ 0 & 0 & d_3 & \cdots & 0 \\ \vdots & & & & \vdots \\ 0 & 0 & 0 & \cdots & d_n \end{bmatrix},$$

missä $D = [d_{ij}]$ on diagonaalimatriisi, jolle $d_i \neq 0$ kaikilla $i = 1, 2, \ldots, n$. Koska ainoastaan diagonaalilla olevat alkiot matriisissa D saattavat olla nollasta poikkeavia, kirjoitetaan usein $d_i = d_{ii}$ ja $D = \{d_1, d_2, \ldots, d_n\}$. [1, s. 240]

Huomautus 5.1. Ainoa ero U-matriisin ja ortogonaalimatriisin välillä on se, että U-matriisin komponenttien vaaditaan olevan joko +1 tai -1 ja rivin tai sarakkeen pistetulo itsensä kanssa pitää olla nollasta poikkeava. Koska A on reaalilukumatriisi, $d_i > 0$ kaikilla $i = 1, 2, \ldots, n$.

Esimerkki 5.9. Tarkastellaan matriisia

$$A = \begin{bmatrix} 1 & 1 & -1 & 1 \\ -1 & 1 & -1 & 1 \\ 1 & 1 & 1 & 1 \\ -1 & 1 & 1 & 1 \end{bmatrix}.$$

Laskemalla on helppo osoittaa, että

$$A^tA = \begin{bmatrix} 1 & -1 & 1 & -1 \\ 1 & 1 & 1 & 1 \\ -1 & -1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 & -1 & 1 \\ -1 & 1 & -1 & 1 \\ 1 & 1 & 1 & 1 \\ -1 & 1 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 4 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 4 \end{bmatrix}$$

ja

$$AA^t = \begin{bmatrix} 1 & 1 & -1 & 1 \\ -1 & 1 & -1 & 1 \\ 1 & 1 & 1 & 1 \\ -1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & -1 & 1 & -1 \\ 1 & 1 & 1 & 1 \\ -1 & -1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 4 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 4 \end{bmatrix}.$$

Näin ollen A on U-matriisi. Matriisi A ei ole ortogonaalinen, sillä jokaisen rivin ja sarakkeen pistetulo itsensä kanssa ei ole 1 vaan se on 4.

Huomautus 5.2. U-matriisit n:n arvoilla $n = 1$ ja $n = 2$ ovat esimerkiksi

$$A_1 = [1] \quad A_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix},$$

sillä $A_1 A_1^t = [1][1] = [1]$ ja $A_2 A_2^t = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}$. [1, s. 241]

Esimerkki 5.10. Jos voidaan konstruoida U-matriisi, voidaan konstruoida myös ortogonaalinen matriisi, sillä jos A on $n \times n$ U-matriisi, niin

$$AA^t = A^t A = D = \begin{bmatrix} d_1 & 0 & 0 & \cdots & 0 \\ 0 & d_2 & 0 & \cdots & 0 \\ 0 & 0 & d_3 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & d_n \end{bmatrix},$$

missä $d_1 \neq 0$. Olkoon

$$E = \{\frac{1}{\sqrt{d_1}}, \frac{1}{\sqrt{d_2}}, \cdots, \frac{1}{\sqrt{d_n}}\}$$

ja olkoon $B = EA$. Kun A kerrotaan vasemmalta matriisilla E, matriisin A jokainen alkio k:nnessa rivissä kerrotaan luvulla $\frac{1}{\sqrt{d_k}}$. Olkoot B_j ja B_k matriiseja, jotka sisältävät matriisin B j:nnen ja k:nnen rivin. Samalla tavoin olkoot A_j ja A_k matriiseja, jotka sisältävät matriisin A j:nnen ja k:nnen rivin. Silloin näiden rivien pistetulo on

$$\begin{aligned} B_j \bullet B_k &= \left(\frac{1}{\sqrt{d_j}} A_j\right) \bullet \left(\frac{1}{\sqrt{d_k}} A_k\right) \\ &= \left(\frac{1}{\sqrt{d_j}} \frac{1}{\sqrt{d_k}}\right)(A_j \bullet A_k). \end{aligned}$$

Näin ollen saadaan

$$B_j \bullet B_k = \begin{cases} \left(\frac{1}{\sqrt{d_j}} \frac{1}{\sqrt{d_k}}\right) 0, & \text{jos } j \neq k \\ \left(\frac{1}{\sqrt{d_j}} \frac{1}{\sqrt{d_k}}\right) d_k, & \text{jos } j = k \end{cases}$$

eli $BB^t = I_n$. Samoin voidaan osoittaa matriisin B sarakkeita käyttäen, että $B^t B = I_n$. Näin ollen $B = EA$ on ortogonaalinen. [1, s. 241]

Seuraavaksi tarkastellaan, onko jokaisella positiivisella kokonaisluvulla n olemassa $n \times n$ U-matriisia, jonka rivit ja sarakkeet olisivat ortogonaalisia. Tarkastellaan myös sitä, että jos tämä on mahdollista jollakin positiivisella kokonaisluvulla n niin, miten sellainen matriisi A voidaan muodostaa. Seuraava lause antaa osittaisen vastauksen.

Lause 5.5. *Jos A on $n \times n$-matriisi ja U-matriisi, niin $n = 1, 2$ tai $n \equiv 0 \pmod 4$.*

Todistus. Vrt.[1, s. 242]. Tapaukset $n = 1, 2$ ovat selviä. Jos $n > 2$, niin matriisissa $A = [a_{ij}]$ on ainakin kolme riviä siten, että

$$\sum_{j=1}^{n}(a_{1j}+a_{2j})(a_{1j}+a_{3j}) = \sum_{j=1}^{n} a_{1j}^2+\sum_{j=1}^{n} a_{2j}a_{1j}+\sum_{j=1}^{n} a_{2j}a_{3j}+\sum_{j=1}^{n} a_{1j}a_{3j} = \sum_{j=1}^{n} a_{1j}^2 = n,$$

missä kolme näistä summista on tyhjiä, koska matriisin A rivit ovat ortogonaalisia, ja missä jäljelle jäävä summa on n, sillä $a_{ij} = \pm 1$.

Ensimmäisen summan tulo $(a_{1j} + a_{2j})(a_{1j} + a_{3j})$ voi olla ainoastaan 0 tai 4, sillä tapauksilla a_{1j}, a_{2j} ja a_{3j} on kahdeksan kombinaatiovaihtoehtoa taulukon 2 mukaisesti, joten

$$n = \sum_{j=i}^{n}(a_{1j} + a_{2j})(a_{1j} + a_{3j}) \equiv 0 \pmod 4.$$

a_{1j}	a_{2j}	a_{3j}	$(a_{1j} + a_{2j})(a_{1j} + a_{3j})$
1	1	1	4
1	−1	1	0
1	1	−1	0
1	−1	−1	0
−1	1	1	0
−1	−1	1	0
−1	1	−1	0
−1	−1	−1	4

Taulukko 2. Tulon $(a_{1j} + a_{2j})(a_{1j} + a_{3j})$ mahdolliset arvot.

□

U-matriisien konstruoimiseksi tarvitaan keinoja lukujen ± 1 tuottamiseksi. Tämän keinon tarjoaa Legendren symboli $\left(\frac{a}{p}\right)$, kts. 3.10. Sovitaan, että $\left(\frac{a}{p}\right) = 0$, jos $p|a$. Jatkossa tarvitaan lauseen 3.15 tuloksia.

Seuraavassa lauseessa käsitellään yhtä Legendren symbolin hyödyllistä ominaisuutta.

Lause 5.6. *Jos p on pariton alkuluku ja $0 \leq a, b \leq p-1, a \neq b$, niin*

$$\sum_{k=0}^{p-1} \left(\frac{k-a}{p}\right)\left(\frac{k-b}{p}\right) = -1.$$

[1, s. 243]

Todistus. Vrt. [13, s. 312]. Koska $\sum_{k=0}^{p-1} \left(\frac{k-a}{p}\right)\left(\frac{k-b}{p}\right) = \sum_{k=0}^{p-1} \left(\frac{(k-a)(k-b)}{p}\right)$ lauseen 3.15 perusteella, valitaan

$$u = k - \frac{a+b}{2} \quad \text{ja} \quad u_0 = \frac{a-b}{2}.$$

Nyt saadaan lauseke muotoon $\sum_{u=0}^{p-1} \left(\frac{u^2-u_0^2}{p}\right)$. Valitaan edelleen, että $u = u_0 v$ ($v \in \mathbb{Z}$). Edelleen lauseke saadaan muotoon

$$\begin{aligned}\sum_{v=0}^{p-1} \left(\frac{u_0^2(v^2-1)}{p}\right) &= \sum_{v=0}^{p-1} \left(\frac{u_0^2}{p}\right)\left(\frac{v^2-1}{p}\right) \\ &= \sum_{v=0}^{p-1} \left(\frac{v^2-1}{p}\right)\end{aligned}$$

lauseen 3.15 perusteella. Pitää huomata, että termillä $\left(\frac{u_0^2}{p}\right)$ ei ole vaikutusta summaan.

Todistuksen jatkon kannalta on tarpeen ottaa käyttöön merkinnät $x, y, w \in \mathbb{Z}$. Nyt, jos $v^2 - 1 = x^2$ eli $v^2 - x^2 = 1$, niin $(v-x)(v+x) = 1$. Jos $v + x = y$, niin $v - x = y^{-1}$. Tästä syystä

$$v = \frac{1}{2}(y + y^{-1}) \quad \text{ja} \quad x = \frac{1}{2}(y - y^{-1}).$$

Näin ollen niiden luvun v arvojen lukumäärä, joilla $\left(\frac{v^2-1}{p}\right) = +1$ tai $\left(\frac{v^2-1}{p}\right) = 0$, on niiden luvun v arvojen lukumäärä, joilla $v = \frac{1}{2}(y + y^{-1})$.

Nyt, jos $y + y^{-1} = w + w^{-}1$, niin $y^2 w + w = yw^2 + y$ ja edelleen $(y - w)(1 - yw) = 0$. Tästä syystä $w = y$ tai $w = y^{-1}$. Luvut y ja y^{-1} ovat erisuuria, ellei $y = \pm 1$ tai $v = \pm 1$. Jos $y = \pm 1$ tai $v = \pm 1$, niin

$$\left(\frac{v^2-1}{p}\right) = \left(\frac{0}{p}\right) = 0.$$

Näin ollen jokainen käänteislukupari (y, y^{-1}), joita on $\frac{1}{2}(p-1)$ kappaletta, vastaa tiettyä luvun v arvoa. Tässä kohtaa on hyvä muistaa, että lauseen 3.13 perusteella on olemassa $\frac{1}{2}(p-1)$ neliönjäännöstä ja $\frac{1}{2}(p-1)$ epäneliönjäännöstä. Täten on olemassa $\frac{1}{2}(p-3)$ mahdollista luvun v arvoa, missä $\left(\frac{v^2-1}{p}\right) = +1$, poislukien vaihtoehdot $v = \pm 1$. On kaksi mahdollista luvun v arvoa ($v = \pm 1$), missä $\left(\frac{v^2-1}{p}\right) = 0$. Näin ollen on olemassa $\frac{1}{2}(p-1)$ mahdollista luvun v arvoa, missä $\left(\frac{v^2-1}{p}\right) = -1$. Pitää kuitenkin huomioida, että kaikki nämä arvot eivät sisälly summausalueeseen luvusta 0 lukuun $p-1$.

Tästä syystä

$$\sum_{k=0}^{p-1}\left(\frac{k-a}{p}\right)\left(\frac{k-b}{p}\right) = \sum_{v=0}^{p-1}\left(\frac{v^2-1}{p}\right) = -1.$$

□

Jatkon kannalta on kätevää merkitä neliömatriisin $A = [a_{ij}]$ indeksit alkamaan nollasta eli $i = 0, 1, \ldots, n-1$ ja $j = 0, 1, \ldots, n-1$. Seuraavassa lauseessa esitetään keino U-matriisien generointiin.

Lause 5.7. *Olkoon p sellainen alkuluku, että $p \equiv 3 \pmod 4$ ja $n = p+1$. Määritellään $n \times n$-matriisi $A = [a_{ij}]$ seuraavasti:*

$$\begin{aligned} a_{ij} &= 1, \quad \textit{jos } i = 0 \textit{ tai } j = 0, \\ a_{ij} &= \left(\frac{j-i}{p}\right), \quad \textit{jos } 1 \leq i, j \leq p \textit{ ja } i \neq j, \\ a_{ii} &= -1, \quad \textit{jos } 1 \leq i \leq p. \end{aligned}$$

Nyt A on U-matriisi.

Todistus. Vrt.[1, s. 243]. Selvästi, $a_{ij} = \pm 1$ kaikilla i, j, joten matriisin A i:nnen rivin pistetulo itsensä kanssa antaa

$$\sum_{k=0}^{p} a_{ik}a_{ik} = \sum_{k=0}^{p} 1 = p+1.$$

Jos $i \neq 0$, niin

$$\begin{aligned} \sum_{k=0}^{p} a_{0k}a_{ik} = \sum_{k=0}^{p} a_{ik} &= a_{i0} + a_{ii} + \sum_{k=1, k\neq i}^{p} a_{ik} \\ &= \sum_{k=0}^{p}\left(\frac{k-i}{p}\right) \\ &= \sum_{j=0}^{p-1}\left(\frac{j}{p}\right), \end{aligned}$$

koska $a_{i0} = 1$, $a_{ii} = -1$, $\left(\frac{0}{p}\right) = 0$ ja
$\{[[k-i]]_p : 1 \leq k \leq p\} = \{[[j]]_p : 0 \leq j \leq p-1\}$, missä $[[k-i]]_p$ ja $[[j]]_p$ ovat jäännösluokkia. Näin ollen matriisin A rivi, jonka indeksi on nolla, on ortogonaalinen matriisin A kaikkien muiden rivien kanssa.

Jos $0 \neq i \neq j \neq 0$, niin

$$\sum_{k=0}^{p} a_{ik}a_{jk} = a_{ii}a_{ji} + a_{ij}a_{jj} + a_{i0}a_{j0} + \sum_{w=1}^{p} \Big(\frac{w-i}{p}\Big)\Big(\frac{w-j}{p}\Big),$$

koska $\left(\frac{w-i}{p}\right)\left(\frac{w-j}{p}\right) = 0$, kun $w = i$ ja $w = j$. Kuitenkin $a_{i0}a_{j0} = 1 \cdot 1 = 1$ ja

$$a_{ii}a_{ji} + a_{ij}a_{jj} = (-1)\Big(\frac{i-j}{p}\Big) + \Big(\frac{j-i}{p}\Big)(-1) = 0,$$

koska

$$\Big(\frac{i-j}{p}\Big) = \Big(\frac{-(j-i)}{p}\Big) = \Big(\frac{-1}{p}\Big)\Big(\frac{j-i}{p}\Big) = -\Big(\frac{j-i}{p}\Big),$$

missä viimeinen yhtäsuuruus pätee, koska $p \equiv 3 \pmod 4$. Näin ollen

$$\sum_{k=0}^{p} a_{ik}a_{jk} = 1 + \sum_{w=1}^{p} \Big(\frac{w-i}{p}\Big)\Big(\frac{w-j}{p}\Big) = 1 - 1 = 0,$$

koska $p \equiv 0 \pmod 4$ mahdollistaa summaamisen nollasta lukuun $p-1$ ja koska lause 5.6 pätee. Näin ollen mitkä tahansa matriisin A riviä, joista kummankaan indeksi ei ole nolla, ovat ortogonaaliset. Väite voidaan todistaa myös matriisin A sarakkeille. □

Esimerkki 5.11. Jos $p = 11 \equiv 3 \pmod 4$ ja $n = p + 1 = 12$, saadaan U-matriisi seuraavasti. Huomataan, että luvut 2, 6, 7, 8 ja 10 ovat luvun 11 neliönjäännöksiä ja luvut 1, 3, 4, 5 ja 9 ovat luvun 11 epäneliönjäännöksiä. Jotta tiedettäisiin kuudes ja yhdeksäs rivi matriisista $A = [a_{ij}]$ eli rivit, joille $i = 5$ ja $i = 8$, luodaan taulukko 3.

Koko 12×12-matriisi on

$$A = \begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & -1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 \\
1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 \\
1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 \\
1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 \\
1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 & -1 \\
1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 \\
1 & 1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 \\
1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\
1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 & -1 \\
1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & -1 & 1 \\
1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & 1 & -1 & -1
\end{bmatrix}.$$

Matriisin muut rivit voidaan ratkaista vastaavasti taulukon 3 osoittamalla tavalla. [1, s. 244]

j	$j-5$	$\left(\frac{j-5}{p}\right)$	$j-8$	$\left(\frac{j-8}{p}\right)$
0	$a_{50}=1$		$a_{80}=1$	
1	-4	-1	-7	1
2	-3	-1		1
3	-2	1		-1
4	-1	-1		-1
5	$a_{55}=-1$		-3	-1
6	1	1	-2	1
7	2	-1	-1	-1
8	3	1		$a_{88}=-1$
9	4	1	1	1
10	5	1	2	-1
11	6	-1	3	1

Taulukko 3. U-matriisin kuudennen ja yhdeksännen rivin selvittäminen, kun $p=11$.

Nyt tiedetään, että on olemassa asteen $n=1,2$ ja $p+1$ U-matriiseja, missä p on alkuluku ja $p \equiv 3 \pmod 4$. Seuraavaksi tarkastellaan taulukkoa 4, missä $n \equiv 0 \pmod 4$ ja $4 \leq n \leq 50$ sekä $n=k+1$. Näin tulee käsitellyksi kaikki lauseen 5.5 mukaiset tapaukset $4 \leq n \leq 50$.

$n=k+1$	k	k on alkuluku
4	3	kyllä
8	7	kyllä
12	11	kyllä
16*	15	ei
20	19	kyllä
24	23	kyllä
28*	27	ei
32	31	kyllä
36*	35	ei
40*	39	ei
44	43	kyllä
48	47	kyllä

Taulukko 4. Tutkitaan, voidaanko lauseen 5.5 tapauksiin soveltaa lausetta 5.7.

Ne n:n arvot, joita ei ole merkitty tähdellä, viittaavat $n \times n$-U-matriisiin, joka on lauseen 5.7 mukaan on olemassa. Ne n:n arvot, jotka on merkitty tähdellä, viittaavat tapauksiin, jossa lauseen 5.7 mukaan ei ole olemassa $n \times n$-U-matriisia. Tämä ei kuitenkaan tarkoita, etteikö tällaisia U-matriiseja olisi olemassa. Tällaisissa tapauksissa on muita keinoja U-matriisin konstruoimiseen.

Määritelmä 5.5. Olkoon $A = [a_{ij}]$ $n \times n$-matriisi ja $B = [b_{ij}]$ $m \times m$-matriisi. Määritellään, että tulo $A \otimes B$ on $nm \times nm$-matriisi

$$A \otimes B = \begin{bmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ a_{21}B & a_{22}B & \cdots & a_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1}B & a_{n2}B & \cdots & a_{nn}B \end{bmatrix}.$$

missä $a_{ij}B$ on $m \times m$-matriisi, joka saadaan, kun matriisi B kerrotaan skalaarilla a_{ij}. [1, s. 246]

Huomautus 5.3. $A \otimes B$ ei ole tavallinen matriisien kertolasku.

Lause 5.8. *Jos $n \times n$-matriisi A ja $m \times m$-matriisi B ovat U-matriiseja, niin $A \otimes B$ on myös U-matriisi. Edelleen, jos matriisien A ja B sekä ensimmäisten rivien että ensimmäisten sarakkeiden jokainen alkio on $+1$, niin myös matriisin $A \otimes B$ sekä ensimmäisen rivin että ensimmäisen sarakkeen jokainen alkio on $+1$. [1, s. 246]*

Todistus. Todistetaan ensin lauseen ensimmäinen osa. Oletetaan, että $n \times n$-matriisi A ja $m \times m$-matriisi B ovat U-matriiseja. Tällöin $a_{ij}, b_{ij} = \pm 1$ kaikilla $i, j = 1, 2, \ldots, n$ ja $AA^t = A^tA = D$, $BB^t = B^tB = D$, missä $d_{ij} \neq 0$ kaikilla $i, j = 1, 2, \ldots, n$.

Tarkastellaan sitten $nm \times nm$-matriisia $A \otimes B$. Nyt matriisin $A \otimes B$ jokainen alkio $(a \otimes b)_{ij} = \pm B$ kaikilla $i, j = 1, 2, \ldots, n$, sillä matriisin $A \otimes B$ alkiot muodostuvat matriisista B, joka on kerrottu skalaarilla a_{ij}. Koska matriisin B alkio $b_{ij} = \pm 1$ kaikilla $i, j = 1, 2, \ldots, n$ ja matriisin A alkio $a_{ij} = \pm 1$ kaikilla $i, j = 1, 2, \ldots, n$, myös matriisin $A \otimes B$ alkiomatriisien $(\pm B)$ alkiot $= \pm 1$ kaikilla $i, j = 1, 2, \ldots, n$.

Nyt pitää vielä osoittaa, että $(A \otimes B)(A \otimes B)^t = (A \otimes B)^t(A \otimes B) = D$, missä $d_{ij} \neq 0$ kaikilla $i, j = 1, 2, \ldots, n$.

$$
\begin{aligned}
(A \otimes B)(A \otimes B)^t &= \begin{bmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ a_{21}B & a_{22}B & \cdots & a_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1}B & a_{n2}B & \cdots & a_{nn}B \end{bmatrix} \begin{bmatrix} a_{11}B & a_{21}B & \cdots & a_{n1}B \\ a_{12}B & a_{22}B & \cdots & a_{n2}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{1n}B & a_{2n}B & \cdots & a_{nn}B \end{bmatrix} \\
&= \begin{bmatrix} nB^2 & 0 & \cdots & 0 \\ 0 & nB^2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & nB^2 \end{bmatrix} \\
&= \begin{bmatrix} a_{11}B & a_{21}B & \cdots & a_{n1}B \\ a_{12}B & a_{22}B & \cdots & a_{n2}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{1n}B & a_{2n}B & \cdots & a_{nn}B \end{bmatrix} \begin{bmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ a_{21}B & a_{22}B & \cdots & a_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1}B & a_{n2}B & \cdots & a_{nn}B \end{bmatrix} \\
&= (A \otimes B)^t (A \otimes B)
\end{aligned}
$$

Näin ollen matriisi $A \otimes B$ on U-matriisi.

Jatketaan sitten lauseen toiseen osaan. Oletetaan, että matriisien A ja B sekä ensimmäisten rivien että ensimmäisten sarakkeiden jokainen alkio on $+1$. Matriisin $A \otimes B$ ensimmäinen rivi on rivimatriisi $\begin{bmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \end{bmatrix}$ ja ensimmäinen sarake on sarakematriisi $\begin{bmatrix} a_{11}B \\ a_{21}B \\ \vdots \\ a_{n1}B \end{bmatrix}$.

Koska matriisin $A \otimes B$ alkiot ovat matriiseja, auki kirjoitettuna matriisin $A \otimes B$ ensimmäinen rivi on rivimatriisi

$$
\begin{bmatrix} a_{11}b_{11} & a_{11}b_{12} & \cdots & a_{11}b_{1n} & \cdots & a_{1n}b_{11} & a_{1n}b_{12} & \cdots & a_{1n}b_{1n} \end{bmatrix}
$$

ja ensimmäinen sarake on sarakematriisi

$$
\begin{bmatrix} a_{11}b_{11} \\ a_{11}b_{21} \\ \vdots \\ a_{11}b_{n1} \\ \vdots \\ a_{n1}b_{11} \\ a_{n1}b_{21} \\ \vdots \\ a_{n1}b_{n1} \end{bmatrix}.
$$

Nyt, koska matriisien A ja B sekä ensimmäisten rivien että ensimmäisten sarakkeiden jokainen alkio on $+1$, matriisin $A \otimes B$ sekä ensimmäisen rivin että ensimmäisen sarakkeen jokainen alkio on $+1$. □

Esimerkki 5.12. Kuten edellistä esimerkkiä seuranneesta taulukosta 4 huomattiin $n = 16$ ei täyttänyt lauseen 5.7 ehtoja. Kuitenkin tiedetään, että

$$A_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

on U-matriisi. Tällöin edellisen lauseen perusteella

$$A_4 = A_2 \otimes A_2 = \begin{bmatrix} A_2 & A_2 \\ A_2 & -A_2 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

ja

$$A_8 = A_2 \otimes A_4 = \begin{bmatrix} A_4 & A_4 \\ A_4 & -A_4 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{bmatrix}$$

ovat U-matriiseja. Tätä prosessia voidaan jatkaa ja saadaan

$$A_{16} = A_2 \otimes A_8 = \begin{bmatrix} A_8 & A_8 \\ A_8 & -A_8 \end{bmatrix}$$

Myös $A_4 \otimes A_4$ on 16×16-matriisi.
[1, s. 246]

Huomautus 5.4. Voidaan huomata, että esimerkissä 5.12 matriiseissa A_2, A_4 ja A_8 sekä ensimmäisen rivin että ensimmäisen sarakkeen alkiot ovat ykkösiä.

Aiheesta on mahdollista lukea lisää Andersonin ja Bellin teoksesta [1, s. 247-249]. Teoksessa on myös viitteitä useisiin teoksiin, jotka sisältävät lisätietoa.

Viitteet

[1] Anderson, James A. ja Bell, James M.:*Number theory with applications*. Prentice-Hall, Inc. New Jersey 1997.

[2] Apostol, Tom M.: *Introduction to analytic number theory*. Springer Verlag New York Inc 1995.

[3] Bressoud, David M. ja Wagon, Stan *A course in computational number theory*. Key College Publishing, 2000.

[4] Burton, David M.: *Elementary number theory*. McMGraw-Hill Boston 2005.

[5] Erickson, Martin J.: *Introduction to number theory*. Chapman & Hall/CRC Boca Raton 2008.

[6] Goldman, Jay R.: *The queen of mathematics : a historically motivated guide to number theory*. A.K. Peters Wellwsley, Massachusets 1998.

[7] Haukkanen, Pentti: *Lukuteoria*, luentomoniste http://mtl.uta.fi/Opiskelu/Algebra/Lukuteoria (16.3.2007).

[8] Haukkanen, Pentti: *Algebra 1*, luentomoniste http://mtl.uta.fi/Opiskelu/Algebra/ (16.3.2007).

[9] Ilmonen, Pauliina: Lukuteoria-kurssin luentomuistiinpanot syksy 2007

[10] Lemmermeyer, Franz: *Reciprocity laws I*. Springer Verlag Berlin 2000.

[11] Nagell, Trygve: *Introduction to number theory*. Chelsea Publishing company New York 1981.

[12] Nathanson, Melvyn B.: *Elementary methods in number theory*. Springer Verlag New York Inc 2000.

[13] Plackett, R. L. ja Burman, J. P.:*The design of optimum multifactorial experiments*. Biometrika, Vol. 33, No. 4 (1946), 305-325. http://www.jstor.org/stable/2332195

[14] Redmond, Don: *Number theory: an introduction*. Marcel Dekker, Inc. New York 1996.

[15] Rose, H.E.: *A course in number theory*. Clarendon Press Oxford 1988.

[16] Rosen, Kenneth H.: *Elementary number theory and its applications*. Pearson/Addison-Wesley Boston 2005.

[17] Tattersall, James J.:*Elementary number theory in nine chapters*. Cambridge University Press Cambridge 1999.

Liite

Seuraavat teokset ovat viitteiden lisäksi suositeltavaa luettavaa.

- Fine, Benjamin :*Number theory an introduction via the distribution of primes*. Birkhäuser Boston 2007.
- Long, Calvin T.: *Elementary number theory and its applications*. Waveland Press Illinois 1987.
- Stillwell, John: *Elements of number theory*. Springer Verlag New York Inc 2003.