Eisensteinin todistus neliönjäännösten resiprookkilaille

Iida Turpeinen

LuK-tutkielma
Tammikuu 2026

Tarkastaja:
Dos. Mika Hirvensalo

MATEMATIIKAN JA TILASTOTIETEEN LAITOS

TURUN YLIOPISTO
Matematiikan ja tilastotieteen laitos

Iida Turpeinen: Eisensteinin todistus neliönjäännösten resiprookkilaille
LuK-tutkielma, 10 s.
Matematiikka
Tammikuu 2026

Neliönjäännösten resiprookkilaki on keskeinen tulos lukuteoriassa. Se kertoo, millä ehdoin kaksi eri alkulukua ovat toistensa neliönjäännöksiä. Tutkielmassa on esitelty lakia ja erityisesti Gotthold Eisensteinin vuoden 1845 todistusta sille. Laki yksinkertaistaa Legendre-symbolien laskemista ja kongruenssien ratkaisemista.

Asiasanat: neliönjäännösten resiprookkilaki, Eisenstein.

Sisällys

1 Johdanto

Neliönjäännösten resiprookkilaki on klassinen ja keskeinen tulos lukuteoriassa. Se antaa ehdon sille, milloin kahden eri parittoman alkuluvun keskinäiset neliöjäännökset ovat ratkaistavissa. Kun tiedetään, onko q neliönjäännös modulo p, laki kertoo, onko p neliönjäännös modulo q. Laki on tärkeä, koska sen avulla voidaan tehokkaasti laskea Legendre-symbolien arvoja ja ratkaista kongruenssien $x^2 \equiv a \pmod{p}$ ratkeavuutta luvun a eri arvoilla.

Neliönjäännösten resiprookkilaki on lukuteorian resiprookkilakien yksinkertaisin ja vanhin muoto. Tähän viittaa David Hilbertin vuonna 1900 esittämä yhdeksäs ongelma, jossa kysymyksenä on, voidaanko neliönjäännösten resiprookkilakia vastaava rakenne yleistää lukukuntiin. Ongelma ratkesi 1920–1930 -luvuilla Artinin resiprookkilain myötä osittain. Nykyinen neliönjäännösten resiprookkilaki voidaan nähdä tämän yleisemmän teorian erikoistapauksena [1].

Ensimmäiset viitteet resiprookkilakiin löytyivät Leonhard Eulerilta, joka havaitsi lain kokeellisesti jo 1780-luvulla. Adrien-Marie Legendre esitti lain vuonna 1785 ottaen käyttöön nykyisin hänen nimeään kantavan Legendre-symbolin. Legendre ei kuitenkaan onnistunut esittämään täysin pätevää todistusta, ja lopulta Carl Friedrich Gauss esitti ensimmäisen aukottoman todistuksen teoksessaan Disquisitiones Arithmeticae (1801). Gauss arvosti tulosta niin suuresti, että hän julkaisi uransa aikana useita erilaisia todistuksia. Häntä onkin kutsuttu ”neliönjäännösten resiprookkilain isäksi”. Myöhempinä vuosikymmeninä lukuisat muutkin matemaatikot, kuten Augustin Cauchy, Richard Dedekind ja Ferdinand Gotthold Eisenstein, kehittivät omat todistuksensa resiprookkilaille [2]. Nykyisin tunnetaan satoja erilaisia todistuksia. Viimeisimpien laskelmien mukaan erilaisia julkaistuja todistuksia on yli 300 [3]. Tässä tutkielmassa esitetään Gotthold Eisensteinin vuoden 1845 todistus neliöjäännösten resiprookkilaille.

2 Käsitteitä

Resiprookkilain ja sen todistuksen ymmärtämiseksi tarvitaan seuraavia muutamia käsitteitä.

Määritelmä 1 (*Neliönjäännös ja -epäjäännös*)**.** Neliönjäännös modulo p tarkoittaa lukua a, jolle on olemassa jokin kokonaisluku x siten, että

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

Mikäli tällaista lukua x ei ole olemassa, a on neliönepäjäännös modulo p. Erityisesti, jos p on alkuluku ja a ei ole jaollinen luvulla p, niin a on neliönjäännös modulo p täsmälleen silloin, kun yhtälöllä

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

on ratkaisu.

Esimerkki 1. Tarkastellaan tilannetta modulo $p = 5$. Luvut 1 ja 4 ovat tällöin neliöjäännöksiä, koska ne voidaan esittää kokonaislukujen neliöinä modulo 5:

$$1^2 \equiv 1 \quad \text{ja} \quad 2^2 \equiv 4 \pmod 5.$$

Luvut 2 ja 3 taas ovat neliönepäjäännöksiä modulo 5, koska yhtälöille

$$x^2 \equiv 2 \quad \text{tai} \quad x^2 \equiv 3 \pmod 5$$

ei löydy yhtään ratkaisua $x \in \mathbb{Z}$.

Määritelmä 2 (*Legendre-symboli*)**.** Legendre-symboli on merkintä, joka tiivistää edellä mainitun neliönjäännöksen käsitteen. Määritelmän mukaan, jos p on pariton alkuluku ja a kokonaisluku, jolle $\gcd(a, p) = 1$, niin Legendre-symboli

$$\left(\frac{a}{p}\right)$$

määritellään seuraavasti:

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

Toisin sanoen $\left(\frac{a}{p}\right) = 1$ tarkoittaa, että kongruenssilla $x^2 \equiv a \pmod p$ on ratkaisu, ja $\left(\frac{a}{p}\right) = -1$ tarkoittaa, ettei ratkaisua ole. Legendre-symbolin arvon voi ymmärtää myös indeksin parillisuuden avulla. Oletetaan, että g on primitiivijuuri modulo p. Tällöin jokainen luku a, jolle pätee $p \nmid a$, voidaan esittää muodossa

$$a \equiv g^k \pmod p,$$

missä kokonaislukua k kutsutaan luvun a g-kantaiseksi indeksiksi (tai diskreetiksi logaritmiksi) modulo p.
Legendre-symboli voidaan tällöin ilmaista muodossa

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

Toisin sanoen Legendre-symbolin arvo määräytyy sen mukaan, onko indeksi k parillinen vai pariton:

- Jos k on parillinen, niin $\left(\frac{a}{p}\right) = 1$,
- Jos k on pariton, niin $\left(\frac{a}{p}\right) = -1$.

Esimerkki 2. Esimerkin 1 tulokset voidaan esittää Legendre-symbolien avulla:

$$\left(\frac{1}{5}\right) = \left(\frac{4}{5}\right) = 1 \quad \text{ja} \quad \left(\frac{2}{5}\right) = \left(\frac{3}{5}\right) = -1.$$

Legendre-symbolin avulla voidaan kätevällä tavalla esittää ja laskea neliönjäännöksisyyttä. On huomattava, että $\left(\frac{a}{p}\right)$ on määritelty vain tapauksessa $\gcd(a, p) = 1$. Jos p jakaa luvun a, ei symbolia aina määritellä tällä tavalla (yleensä kuitenkin määritellään $\left(\frac{a}{p}\right) = 0$ kun $p \mid a$ [4]).

Määritelmä 3 (*p-positiivinen ja p-negatiivinen luku*)**.** Olkoon p pariton alkuluku ja $m \in \mathbb{Z}$. Merkitään $r \equiv m \pmod{p}$, missä $r \in \{0, 1, \ldots, p-1\}$ on luvun m pienin ei-negatiivinen edustaja modulo p.

- Luku m on p-positiivinen, jos $1 \leq r \leq \frac{p-1}{2}$.
- Luku m on p-negatiivinen, jos $\frac{p+1}{2} \leq r \leq p-1$.

Jos $p \mid m$, eli $m \equiv 0 \pmod{p}$, niin luvun m p-positiivisuutta tai p-negatiivisuutta ei määritellä.

Esimerkki 3. Kun $p = 11$, luvun 5 pienin jäännös modulo 11 on 5. Tästä nähdään suoraan, että $5 \leq \frac{11-1}{2} = 5$, eli 5 on p-positiivinen. Vastaavasti luvun 7 pienin jäännös modulo 11 on 7, ja koska $7 > \frac{11-1}{2} = 5$, niin 7 on p-negatiivinen.

Lemma 1 (*Gaussin lemma* [5])**.** *Olkoon p pariton alkuluku ja a kokonaisluku, jota p ei jaa. Tarkastellaan lukuja*

$$a, 2a, 3a, \ldots, \frac{p-1}{2}a$$

ja niiden jakojäännöksiä modulo p välillä $1, 2, ..., p-1$. Merkitään luvulla r niiden jakojäännösten lukumäärää, jotka ovat suurempia kuin $\frac{p}{2}$. Tällöin pätee

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

Toisin sanoen, a on neliöjäännös modulo p jos ja vain jos tällaisten "yli $\frac{p}{2}$" olevien jakojäännösten määrä on parillinen, ja vastaavasti a on neliönepäjäännös modulo p jos ja vain jos näiden määrä on pariton.

Esimerkki 4. Olkoon $p = 7$ ja $a = 3$. Tarkastellaan lukuja

$$a, 2a, 3a = 3, 6, 9.$$

Määritetään lukujen ka $(1 \leq k \leq \frac{p-1}{2})$ jakojäännökset modulo p.

$$3 \equiv 3 \pmod{7}, \quad 6 \equiv 6 \pmod{7}, \quad 9 \equiv 2 \pmod{7}.$$

Saadaan siis jäännökset $3, 6, 2$. Näistä jäännöksistä suurempia kuin $\frac{p}{2} = \frac{7}{2} = 3.5$ on vain 6, eli yksi luku. Siis $r = 1$ on pariton, joten

$$\left(\frac{3}{7}\right) = (-1)^r = (-1)^1 = -1.$$

3 ei siis ole neliöjäännös modulo 7.

Määritelmä 4 (*Chebyshevin polynomit*)**.** Chebyshevin polynomit $T_n(Y)$, missä $n \in \mathbb{N}$, määritellään rekursiivisesti seuraavasti:

$$\begin{aligned} T_0(Y) &= 1, \\ T_1(Y) &= Y, \\ T_{n+1}(Y) &= 2YT_n(Y) - T_{n-1}(Y) \quad \text{kaikilla } n \geq 1. \end{aligned}$$

Vaihtoehtoisesti ne voidaan esittää trigonometrisessa muodossa

$$T_n(\cos x) = \cos(nx). \tag{1}$$

missä $x \in \mathbb{R}$.

Esimerkki 5. Kun $n = 1$ ja $n = 2$, saadaan:

$$\begin{aligned} &T_1(Y) = Y, \\ &T_2(Y) = 2Y^2 - 1 \quad (\text{koska } \cos(2x) = 2\cos^2 x - 1). \end{aligned}$$

3 Neliönjäännösten resiprookkilaki

Lause 1 (*Neliönjäännösten resiprookkilaki*)**.** *Neliönjäännösten resiprookkilain esitetään usein Legendre-symbolin avulla, jolloin lause saa seuraavanlaisen muodon:*

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

missä p ja q ovat parittomia alkulukuja.

Resiprookkilaki voidaan tulkita myös väittämänä siitä, ovatko lukujen p ja q indeksit parillisia vai parittomia, kun ne esitetään toistensa primitiivijuurten potensseina. Olkoon g primitiivijuuri modulo p. Tällöin mikä tahansa luku $a \in \mathbb{F}_p^*$ voidaan esittää muodossa:

$$a \equiv g^r \pmod{p},$$

missä $r = \mathrm{ind}_g(a)$ on luvun a indeksi eli diskreetti logaritmi kantaan g.
Toisin sanoen, a on neliöjäännös modulo p jos ja vain jos sen indeksi on parillinen [6].
Hieman erilainen, mutta myös yleinen muotoilu neliönjäännösten resiprookkilaista on

$$\left(\frac{p^*}{q}\right) = \left(\frac{q}{p}\right),$$

missä $p^* = (-1)^{\frac{p-1}{2}}p$. Jos siis joko p tai q on kongruentti 1 modulo 4, niin p on neliönjäännös modulo q täsmälleen silloin kun q on neliönjäännös modulo p. Jos taas molemmat p ja q ovat kongruentteja 3 modulo 4, niin p on neliönjäännös modulo q, jos ja vain jos q ei ole neliönjäännös modulo p. Huomaa, että eksponentti $\frac{p-1}{2} \cdot \frac{q-1}{2}$

on pariton vain jos molemmat kertoimet ovat parittomia, ja parillinen muutoin. Jos $\frac{p-1}{2} \cdot \frac{q-1}{2}$ on parillinen, niin

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

eli p ja q ovat molemmat joko neliönjäännöksiä toistensa suhteen, tai kumpikaan ei ole. Luku muotoa $(n-1)/2$ on parillinen täsmälleen silloin kun $n \equiv 1 \pmod 4$. Toisaalta, jos $\frac{p-1}{2} \cdot \frac{q-1}{2}$ on pariton, niin

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

eli vain toinen p ja q on neliönjäännös toisen suhteen. Luku muotoa $(n-1)/2$ on pariton täsmälleen silloin kun $n \equiv 3 \pmod 4$.

On olemassa myös erikoistapaukset $\left(\frac{-1}{p}\right)$ ja $\left(\frac{2}{p}\right)$. Näitä käsitellään täydentävien lakien avulla, jotka usein esitetään resiprookkilain yhteydessä. Täydentävät lait eivät ole tässä työssä keskeisessä osassa, mutta mainittakoon:

$$\left(\frac{-1}{p}\right) = 1 \iff p \equiv 1 \pmod 4,$$
$$\left(\frac{2}{p}\right) = 1 \iff p \equiv 1 \text{ tai } 7 \pmod 8.$$

Resiprookkilain kuvaama suhde $\left(\frac{p}{q}\right)$ ja $\left(\frac{q}{p}\right)$ välillä on yllättävä. Päällisin puolin ei ole lainkaan ilmeistä, että se, onko p neliönjäännös mod q, antaisi mitään tietoa siitä, onko q neliönjäännös mod p [5]. Joidenkin tulosten, kuten kiinalainen jäännöslauseen perusteella, voisikin olla syytä odottaa päinvastaista, (ks. alla oleva esimerkki 6 [7]).

Esimerkki 6. Kiinalaisen jäännöslauseen välitön seuraus on, että kun on annettu mitkä tahansa alkuluvut $p_1, p_2, \ldots, p_n$ ja kokonaisluvut $a_1, a_2, \ldots, a_n$, niin on olemassa kokonaisluku x, jolle pätee

$$\begin{aligned} x &\equiv a_1 \pmod{p_1} \\ x &\equiv a_2 \pmod{p_2} \\ &\vdots \\ x &\equiv a_n \pmod{p_n}. \end{aligned}$$

Olkoot $p_1 = 2$ ja $p_2 = 3$. Jos tiedetään, että x on pariton, eli $x \equiv 1 \pmod 2$, tämä ei kerro mitään siitä, mikä x on mod 3, sillä jäännöslauseen mukaan seuraavat kongruenssiparit

$$x \equiv 1 \pmod 2 \quad \text{ja} \quad x \equiv 0 \pmod 3$$
$$x \equiv 1 \pmod 2 \quad \text{ja} \quad x \equiv 1 \pmod 3$$
$$x \equiv 1 \pmod 2 \quad \text{ja} \quad x \equiv 2 \pmod 3$$

ovat kaikki mahdollisia ja niillä kaikilla on ratkaisu.

Toisin sanoen, aivan kuten kongruenssiyhtälöt $x \equiv q \pmod{p}$ ja $x \equiv p \pmod{q}$ ovat aina samanaikaisesti ratkaistavissa mille tahansa alkuluvuille p ja q, voisi olettaa, että myös yhtälöt $x^2 \equiv q \pmod{p}$ ja $x^2 \equiv p \pmod{q}$ olisivat aina samanaikaisesti ratkaistavissa, tai ainakin, ettei niiden ratkeavuuden välillä olisi mitään yhteyttä. Neliönjäännösten resiprookkilain perusteella näin ei kuitenkaan ole.

4 Todistus neliönjäännösten resiprookkilaille

Tässä luvussa esitetään Eisensteinin todistus neliönjäännösten resiprookkilaille mukaillen Chapmanin [8] esitystapaa.

Kuten edellä on esitetty, Gaussin lemman ytimessä on kokonaislukujen jako p-positiivisiin ja p-negatiivisiin. Palataan Gaussin lemmaan ja esitetään se trigonometrisesti. Tarkastellaan jokaiselle parittomalle alkuluvulle p trigonometrisesti määriteltyä funktiota

$$f_p(x) = \sin\left(\frac{2\pi x}{p}\right).$$

Funktiolla on jakso p:

$$f_p(x+p) = f_p(x).$$

Kun kokonaisluku a toteuttaa $0 < a < p/2$, on $f_p(a) > 0$, sillä silloin $0 < 2\pi a/p < \pi$. Vastaavasti, jos $0 > a > -p/2$, on $f_p(a) < 0$, koska $0 > 2\pi a/p > -\pi$. Jaksollisuuden vuoksi pätee

$$f_p(a) \begin{cases} > 0, & \text{kun } a \text{ on } p\text{-positiivinen}, \\ < 0, & \text{kun } a \text{ on } p\text{-negatiivinen}, \\ = 0, & \text{kun } p \mid a. \end{cases}$$

Kun $p \nmid a$, saadaan Gaussin lemman mukaisesti

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

missä r on niiden kokonaislukujen k lukumäärä, joille $0 < k < p/2$ ja $f_p(ak) < 0$. Toisin sanoen Legendre-symboli $\left(\frac{a}{p}\right)$ määräytyy tulon

$$\prod_{k=1}^{(p-1)/2} f_p(ak)$$

etumerkistä. Merkitään yleisesti luvun $x \neq 0$ etumerkkiä merkinnällä sgn(x). Tällöin

$$\left(\frac{a}{p}\right) = \operatorname{sgn}\left(\prod_{k=1}^{(p-1)/2} f_p(ak)\right) = \operatorname{sgn}\left(\prod_{k=1}^{(p-1)/2} \sin\left(\tfrac{2\pi ak}{p}\right)\right). \tag{2}$$

Sovellettaessa tätä resiprookkilakiin, asetetaan $a = q$, missä q on toinen pariton alkuluku. Tällöin funktio $\sin(qx)$ voidaan ilmaista funktion $\sin(x)$ avulla. Tähän

voidaan soveltaa Chebyshevin polynomeja. Polynomin $T_n(Y)$ korkeimman asteen termi on $2^{n-1}Y^n$.
Toistaiseksi oletetaan, että n on pariton. Tällöin $n = 2k + 1$ jollakin $k \in \mathbb{Z}_{\geq 0}$. Identiteetillä $\sin x = \cos\left(x - \frac{\pi}{2}\right)$ ja Chebyshevin polynomien määritelmällä (1), saadaan

$$\begin{aligned} T_n(\sin x) &= T_n\left(\cos\left(x - \frac{\pi}{2}\right)\right) \\ &= \cos\left(n\left(x - \frac{\pi}{2}\right)\right) \\ &= \cos\left(nx - \frac{n\pi}{2}\right). \end{aligned}$$

Kun $n = 2k + 1$, niin

$$\begin{aligned} \cos\left(nx - \frac{n\pi}{2}\right) &= \cos\left(nx - \frac{(2k+1)\pi}{2}\right) \\ &= \cos\left(nx - k\pi - \frac{\pi}{2}\right) \\ &= (-1)^k \cos\left(nx - \frac{\pi}{2}\right) \\ &= (-1)^k \sin(nx), \end{aligned}$$

mistä seuraa, että

$$\begin{aligned} T_n(\sin x) &= \cos\left(nx - \frac{n\pi}{2}\right) \\ &= (-1)^{\frac{n-1}{2}} \sin(nx). \end{aligned}$$

Määritellään

$$G_n(Y) = (-1)^{(n-1)/2} T_n(Y),$$

jolloin parittomille n pätee:

$$G_n(\sin x) = \sin(nx)$$

ja korkeimman asteen termi on

$$(-1)^{\frac{n-1}{2}} \cdot 2^{n-1} Y_n = (-4)^{\frac{n-1}{2}} Y_n.$$

Seuraavaksi voidaan määrittää polynomin G_n nollakohdat. Kokonaisluvuille j pätee:

$$G_n\left(\sin\left(\frac{2\pi j}{n}\right)\right) = \sin(2\pi j) = 0.$$

Siispä nollakohtia ovat luvut

$$\sin\left(\frac{2\pi j}{n}\right), j = 0, 1, \ldots, n-1.$$

Kun $-\frac{p-1}{2} \leq j \leq \frac{p-1}{2}$, juuret ovat erisuuria, joten ne ovat täsmälleen polynomin $G_n(Y)$ juuret. Siispä $G_n(Y)$ voidaan jakaa tekijöihin seuraavasti:

$$G_n(Y) = (-4)^{(n-1)/2} \prod_{j=-(n-1)/2}^{(n-1)/2} \left(Y - \sin(\tfrac{2\pi j}{n})\right).$$

Kun $0 < j < \frac{n-1}{2}$, niin $0 > -j > -\frac{n-1}{2}$, ja $\sin\left(\frac{2\pi(-j)}{n}\right) = -\sin\left(\frac{2\pi j}{n}\right)$. Jokainen positiivinen luku j voidaan laittaa vastalukunsa $-j$ kanssa pariksi, jolloin saadaan

$$\begin{aligned} G_n(Y) &= (-4)^{\frac{n-1}{2}} Y \prod_{j=1}^{(n-1)/2} \left(Y^2 - \sin^2\left(\tfrac{2\pi j}{n}\right)\right) \\ &= 2^{n-1} Y \prod_{j=1}^{(n-1)/2} \left(\sin^2\left(\tfrac{2\pi j}{n}\right) - Y^2\right). \end{aligned}$$

Siispä

$$\sin(nx) = 2^{n-1} \sin x \prod_{j=1}^{(n-1)/2} \left(\sin^2\left(\frac{2\pi j}{n}\right) - \sin^2 x\right). \tag{3}$$

Olkoot p ja q erisuuria parittomia alkulukuja. Tällöin kaava (2) saadaan muotoon

$$\frac{q}{p} = \operatorname{sgn}\left(\prod_{k=1}^{(p-1)/2} \sin\left(\tfrac{2\pi q k}{p}\right)\right).$$

Sovelletaan kaavaa (3), kun $n = q$ ja $x = \frac{2\pi k}{p}$. Tällöin

$$\begin{aligned} \left(\frac{q}{p}\right) &= \operatorname{sgn}\left(\prod_{k=1}^{(p-1)/2} 4^{(q-1)/2} \sin\left(\frac{2\pi k}{p}\right) \prod_{j=1}^{(q-1)/2} \left(\sin^2\left(\frac{2\pi j}{q}\right) - \sin^2\left(\frac{2\pi k}{p}\right)\right)\right) \\ &= \operatorname{sgn}\left(\prod_{k=1}^{(p-1)/2} \prod_{j=1}^{(q-1)/2} \left(\sin^2\left(\frac{2\pi j}{q}\right) - \sin^2\left(\frac{2\pi k}{p}\right)\right)\right). \end{aligned}$$

Koska lausekkeessa kerrotaan kaikkien mahdollisten indeksiparien yli, voidaan lukujen p ja q sekä indeksien j ja k paikat vaihtaa, jolloin saadaan

$$\left(\frac{p}{q}\right) = \operatorname{sgn}\left(\prod_{j=1}^{(q-1)/2} \prod_{k=1}^{(p-1)/2} \left(\sin^2\left(\frac{2\pi k}{p}\right) - \sin^2\left(\frac{2\pi j}{q}\right)\right)\right).$$

Kaavat luvuille $\left(\frac{q}{p}\right)$ ja $\left(\frac{p}{q}\right)$ ovat lähes identtiset. Molemmat esitetään etumerkkifunktiona tuloista, jossa termejä on yhteensä $\frac{(p-1)(q-1)}{4}$. Jälkimmäisen tulon termit ovat ensimmäisen tulon termien vastalukuja.

Tästä seuraa:

$$\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{q}{p}\right).$$

Ellei $p \equiv q \equiv 3 \pmod 4$, luku $\frac{(p-1)(q-1)}{4}$ on parillinen, jolloin

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

Jos taas $p \equiv q \equiv 3 \pmod 4$, luku $\frac{(p-1)(q-1)}{4}$ on pariton, ja pätee

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

□

Viitteet

[1] Hilbert, D. (1902) 'Mathematical Problems'. *Bulletin of the American Mathematical Society*, 8(10), 437–479. Saatavilla: https://people.reed.edu/~davidp/341/resources/hilbert.pdf.

[2] Frei, G. (1994) 'The Reciprocity Law from Euler to Eisenstein', *The Intersection of History and Mathematics*. Birkhäuser Basel, pp. 67–90 Saatavilla: https://doi.org/10.1007/978-3-0348-7521-9_6.

[3] Lemmermeyer, F. (2025) *Quadratic Reciprocity — Proofs*. Saatavilla: http://web.archive.org/web/20250106010310/https://www.mathi.uni-heidelberg.de/%7Eflemmermeyer/qrg_proofs.html.

[4] Biswas, G. (2014–2015) 'Computational Number Theory: CS60094, Lecture V'. [Luentomoniste], Computer Science & Engineering Department, IIT Kharagpur. Saatavilla: https://cse.iitkgp.ac.in/~goutam/cnt/lect/Lect5.pdf.

[5] Dummit, E. (2024) 'Number Theory (part 5): Squares and Quadratic Reciprocity' (v. 4.00). [Luentomoniste], MATH 3527: Number Theory 1, Northeastern University. Saatavilla: https://dummit.cos.northeastern.edu/teaching_sp24_3527/numthy_5_squares_and_quadratic_reciprocity_v4.00.pdf.

[6] Fischer, M. J. (2008) 'Indexing and Quadratic Reciprocity' [Luentomoniste], *CPSC 467a: Cryptography and Computer Security*. Yale University. Saatavilla: https://zoo.cs.yale.edu/classes/cs467/2008f/handouts/ho07.pdf.

[7] D'Alessandro, W. (2021) 'Proving quadratic reciprocity: explanation, disagreement, transparency and depth', *Synthese*, 198(9), 8621–8664. Saatavilla: https://doi.org/10.1007/s11229-020-02591-6.

[8] Chapman, R. (2013) 'Quadratic reciprocity: Eisenstein's proof'. Saatavilla: http://empslocal.ex.ac.uk/people/staff/rjchapma/courses/nt13/Eisenstein.pdf.