Neliönjäännökset

Riku Häkli

Pro gradu
Matemaattisten tieteiden laitos
Oulun yliopisto
Syksy 2017

Sisältö

Johdanto

Tutkielmassa perehdytään kongruenssin $x^2 \equiv a \pmod{c}$ ratkeavuuteen, kun luvut a ja c ovat keskenään jaottomia. Työssä tutustutaan muun muassa Legendren symboliin, jonka avulla edellä mainitun kongruenssin ratkeavuus voidaan päätellä.

Keskeisimpänä tuloksena voidaan pitää Neliönjäännösten resiprookkilakia, jonka ensimmäisenä esitteli Leonhard Euler jo vuonna 1775. Lauseen kuitenkin todisti ensimmäistä kertaa oikeaksi Carl Friedrich Gauss vasta yli kaksikymmentä vuotta myöhemmin. Tutkielmassa esitetty todistus perustuu kuitenkin Gotthold Eisensteinin laatimaan todistukseen.

Lopuksi tarkastellaan Jacobin symbolia, joka on eräänlainen yleistys Legendren symbolista, mutta ei aina tarjoa niin tarkkaa tietoa siihen liittyvän kongruenssin ratkeavuudesta kuin Legendren symboli.

Työssä on oletettu algebran sekä lukuteorian perusasiat tunnetuiksi, ja lähteenä on käytetty Michael Th. Rassias'n kirjaa *Problem-Solving and Selected Topics in Number Theory*.

1 Neliönjäännös

Määritelmä 1.1. Kokonaisluku a on *neliönjäännös modulo* c, jos $\text{syt}(a, c) = 1$ ja kongruenssilla $x^2 \equiv a \pmod{c}$ on ratkaisu. Jos kongruenssilla ei ole ratkaisua, niin a on *epäneliö modulo* c.

Esimerkki 1.2. Luku 1 on neliönjäännös modulo 4, koska

$$5^2 \equiv 1 \pmod{4}$$

ja luku 9 on neliönjäännös modulo 5, koska

$$7^2 \equiv 9 \pmod{5}.$$

Luku 2 on epäneliö modulo 3, koska

$$0^2 \not\equiv 2 \pmod{3}, \quad 1^2 \not\equiv 2 \pmod{3} \quad \text{ja} \quad 2^2 \not\equiv 2 \pmod{3}.$$

Seuraavaksi käsitellään muutamia lauseita liittyen neliönjäännöksiin.

Lause 1.3. *Olkoon p pariton alkuluku ja a sellainen kokonaisluku, että* $\text{syt}(a, p) = 1$. *Tällöin kongruenssilla*

$$x^2 \equiv a \pmod{p}, \tag{1}$$

on joko kaksi erisuurta ratkaisua mod p tai ei yhtään ratkaisua mod p.

Todistus. Oletetaan että x_0 on eräs kongruenssin (1) ratkaisu. Tällöin

$$x_0^2 \equiv a \pmod{p} \tag{2}$$

ja selvästi myös

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

eli myös $-x_0$ on myös kongruenssin (1) ratkaisu. Osoitetaan nyt, että $x_0 \not\equiv -x_0 \pmod{p}$.

Jos $x_0 \equiv -x_0 \pmod{p}$, saadaan $2x_0 \equiv 0 \pmod{p}$. Tästä seuraa, että $p \mid x_0$, sillä $p > 2$. Lauseen 1.3 oletuksen mukaan $p \mid (x_0^2 - a)$. Jos $p \mid x_0$, täytyy myös olla $p \mid a$. Tämä on kuitenkin ristiriita, sillä $\text{syt}(a, p) = 1$.

Jos siis kongruenssilla (1) on ratkaisu x_0 niin myös $-x_0$ on ratkaisu ja $x_0 \not\equiv -x_0 \bmod p$. Osoitetaan seuraavaksi, että kongruenssilla (1) ei ole muita ratkaisuja.

Olkoon x_0' eräs kongruenssin (1) ratkaisu eli $(x_0')^2 \equiv a \pmod{p}$. Puolittain vähentämällä kongruenssista (2) saadaan

$$x_0^2 - (x_0')^2 \equiv 0 \pmod{p}.$$

Edelleen

$$(x_0 - x_0')(x_0 + x_0') \equiv 0 \,(\mathrm{mod}\ p)$$

eli toisin sanoen

$$p \mid (x_0 - x_0') \quad \text{tai} \quad p \mid (x_0 + x_0').$$

Nyt siis

$$x_0 \equiv x_0' \,(\mathrm{mod}\ p) \quad \text{tai} \quad -x_0 \equiv x_0' \,(\mathrm{mod}\ p).$$

Näin ollen on oltava joko $x_0' \equiv x_0 \,(\mathrm{mod}\ p)$ tai $x_0' \equiv -x_0 \,(\mathrm{mod}\ p)$. Kongruenssilla (1) on siis joko täsmälleen kaksi ratkaisua mod p tai ei yhtään ratkaisua. □

Esimerkki 1.4. Tarkastellaan kongruenssia $x^2 \equiv 2 \,(\mathrm{mod}\ 7)$. Nyt

$$\begin{gathered} 7 \nmid 0^2 - 2, \\ 7 \nmid 1^2 - 2, \\ 7 \nmid 2^2 - 2, \\ 7 \mid 3^2 - 2, \\ 7 \mid 4^2 - 2, \\ 7 \nmid 5^2 - 2, \\ 7 \nmid 6^2 - 2. \end{gathered}$$

Tästä nähdään, että kongruenssilla $x^2 \equiv 2 \,(\mathrm{mod}\ 7)$ on täsmälleen kaksi ratkaisua mod 7.

Lause 1.5. *Jos p on pariton alkuluku, niin on olemassa täsmälleen $(p-1)/2$ neliönjäännöstä ja $(p-1)/2$ epäneliötä modulo p.*

Todistus. On selvää, että

$$\begin{gathered} p - 1 \equiv -1 \,(\mathrm{mod}\ p), \\ p - 2 \equiv -2 \,(\mathrm{mod}\ p), \\ \vdots \\ p - \frac{p-1}{2} \equiv -\frac{p-1}{2} \,(\mathrm{mod}\ p). \end{gathered}$$

Näin ollen

$$\begin{gathered} (p-1)^2 \equiv 1^2 \,(\mathrm{mod}\ p), \\ (p-2)^2 \equiv 2^2 \,(\mathrm{mod}\ p), \\ \vdots \\ \left(p - \frac{p-1}{2}\right)^2 \equiv \left(\frac{p-1}{2}\right)^2 \,(\mathrm{mod}\ p) \end{gathered}$$

eli jokainen kokonaisluvuista $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$ on neliönjäännös modulo p. Osoitetaan, että nämä luvut eivät ole keskenään kongruentteja modulo p.

Valitaan

$$x_1, x_2 \in \left\{1, 2, \ldots, \frac{p-1}{2}\right\}, \quad x_1 \neq x_2. \tag{3}$$

Oletetaan nyt että $x_1^2 \equiv x_2^2 \pmod{p}$, jolloin saadaan $p \mid (x_1 - x_2)(x_1 + x_2)$ eli $p \mid (x_1 - x_2)$ tai $p \mid (x_1 + x_2)$. Koska $1 < x_1 + x_2 < p$, niin $p \nmid (x_1 + x_2)$. On siis oltava $p \mid (x_1 - x_2)$. Toisaalta on oltava $p \nmid (x_1 - x_2)$, koska $|x_1 - x_2| < p$. Tämä on ristiriita, joten joukon (3) alkiot eivät ole keskenään kongruentteja modulo p.

Lauseen 1.3 mukaan jokaista neliönjäännöstä kohti on olemassa kaksi erisuurta ratkaisua mod p eli x ja $-x$. Näin ollen joukossa $\{1, 2, \ldots, p-1\}$ voi olla korkeintaan $(p-1)/2$ erisuurta neliönjäännöstä modulo p. Toisaalta neliönjäännöksiä on vähintään $(p-1)/2$ kappaletta, koska joukossa (3) on niin monta alkiota. Tästä seuraa, että on olemassa täsmälleen $(p-1)/2$ neliönjäännöstä ja $(p-1)/2$ epäneliötä modulo p. □

Esimerkki 1.6. Olkoon $p = 3$. Lauseen 1.5 nojalla on olemassa täsmälleen yksi neliönjäännös ja täsmälleen yksi epäneliö mod 3. Esimerkin (1.2) mukaan luku 2 on epäneliö mod 3, joten luvun 1 on siis oltava neliönjäännös mod 3. Näin onkin, sillä esimerkiksi $2^2 \equiv 1 \pmod{3}$.

Lause 1.7 (Dirichlet'n lause)**.** *Olkoon p alkuluku ja a sellainen kokonaisluku, että $1 \leqslant a \leqslant p-1$. Jos kongruenssilla $x^2 \equiv a \pmod{p}$ ei ole yhtään ratkaisua, niin*

$$p \mid (p-1)! - a^{(p-1/2)}.$$

Jos kongruenssilla $x^2 \equiv a \pmod{p}$ on ratkaisuja, niin

$$p \mid (p-1)! + a^{(p-1/2)}.$$

Todistus. Jos $p = 2$, niin $a = 1$ ja siten $x = 1$ on kongruenssiyhtälön ratkaisu. Selvästi myös $2 \mid 1! + 1^{1/2}$. Tutkitaan seuraavaksi tapaukset $p > 2$.

Tarkastellaan kongruenssia

$$a_1 x \equiv a \pmod{p}, \tag{4}$$

missä $1 \leqslant a_1 \leqslant p-1$. Koska $\mathrm{syt}(a_1, p) = 1$, niin yllä olevalla kongruenssilla on yksikäsitteinen ratkaisu mod p ja tämä ratkaisu kuuluu joukkoon

$$\{0, 1, \ldots, p-1\}$$

tai joukkoon

$$\left\{-\frac{p-1}{2}, \ldots, -2, -1, 0, 1, 2, \ldots, \frac{p-1}{2}\right\}.$$

Valitaan $x \in \{1, 2, \ldots, p-1\}$. Luku 0 jätetään pois, sillä $\text{syt}(0, p) \neq 1$.

Jos b on eräs kongruenssin (4) ratkaisu, niin

$$a_1 b \equiv a \pmod{p}. \tag{5}$$

Siis jos kongruenssilla

$$x^2 \equiv a \pmod{p} \tag{6}$$

ei ole ratkaisuja, niin $a_1 \neq b$. Kuitenkin koska $a_1, b \in \{1, 2, \ldots, p-1\}$, voimme muodostaa tästä joukosta $(p-1)/2$ kappaletta erillisiä pareja (a_1, b) siten, että ne toteuttavat ehdon (5) ja $a_1 \neq b$.

Lisäksi jos kerromme puolittain keskenään kaikki kongruenssit, jotka nämä parit muodostavat, saadaan

$$(p-1)! \equiv a^{(p-1)/2} \pmod{p}$$

eli

$$p \mid (p-1)! - a^{(p-1)/2},$$

kun kongruenssilla $x^2 \equiv a \pmod{p}$ ei ole ratkaisuja.

Jos kongruenssilla (6) on ratkaisuja, niitä on Lauseen 1.3 mukaan oltava täsmälleen kaksi. Oletetaan jälleen, että nämä ratkaisut kuuluvat joukkoon $\{1, 2, \ldots, (p-1)\}$.

Olkoon k toinen näistä ratkaisuista. Tällöin myös $p-k$ on kongruenssin (6) ratkaisu. Muita ratkaisuja mod p ei Lauseen 1.3 nojalla ole.

Poistetaan kokonaisluvut k ja $p-k$ joukosta $\{1, 2, \ldots, (p-1)\}$ ja muodostetaan jäljelle jääneistä luvuista $(p-3)/2$ kappaletta erillisiä pareja (a_1, b), joissa $a_1 \neq b$ ja jotka toteuttavat kongruenssin (5). Kertomalla näiden lukuparien muodostamat kongruenssit puolittain yhteen, saadaan

$$\frac{(p-1)!}{k \cdot (p-k)} \equiv a^{(p-3)/2} \pmod{p},$$

missä $(p-1)!/(k \cdot (p-k))$ on kokonaisluku, sillä tulo $(p-1)!$ sisältää sekä luvun $p-k$ että k.

Toisaalta

$$k \cdot (p-k) = kp - k^2 \equiv -a \pmod{p}$$

eli

$$\frac{(p-1)!}{k \cdot (p-k)} \cdot k \cdot (p-k) \equiv a^{(p-3)/2} \cdot (-a) \pmod{p}.$$

Edelleen

$$(p-1)! \equiv -a^{(p-1)/2} \pmod{p},$$

joten

$$p \mid (p-1)! + a^{(p-1)/2},$$

kun kongruenssilla $x^2 \equiv a \pmod{p}$ on ratkaisu. □

Esimerkki 1.8. Kongruenssilla $x^2 \equiv 2 \pmod 5$ ei ole yhtään ratkaisua. Nyt

$$(p-1)! - a^{(p-1)/2} = (5-1)! - 2^{(5-1)/2} = 20$$

on jaollinen luvulla 5. Kongruenssilla $x^2 \equiv 1 \pmod 5$ sen sijaan on ratkaisut ± 1 ja tällöin

$$(p-1)! + a^{(p-1)/2} = (5-1)! + 1^{(5-1)/2} = 25$$

on jaollinen luvulla 5.

Lause 1.9 (Lagrangen lause)**.** *Olkoon*

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

missä $a_0, a_1, \ldots, a_n \in \mathbb{Z}$ *ja* $a_n \neq 0$*. Jos* p *on alkuluku ja* $a_n \not\equiv 0 \pmod p$*, niin kongruenssilla*

$$f(x) \equiv 0 \pmod p$$

on korkeintaan n *ratkaisua mod* p*.*

Todistus. Kun $n = 1$, niin $f(x) = a_1 x + a_0$. Kongruenssilla

$$a_1 x + a_0 \equiv 0 \pmod p$$

on yksikäsitteinen ratkaisu, sillä $\operatorname{syt}(a_1, p) = 1$. Näin ollen lause pätee, kun $n = 1$.

Oletetaan nyt, että lause pätee myös polynomeille, joiden asteluku on korkeintaan $n-1$ ja että kongruenssilla

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \equiv 0 \pmod p$$

on vähintään $n+1$ ratkaisua mod p. Käytetään näille ratkaisuille merkintää

$$x_0, x_1, \ldots, x_n.$$

Tällöin saadaan

$$\begin{aligned}(a_n x_i^n + a_{n-1}x_i^{n-1} + \cdots + a_1 x_i + a_0) - (a_n x_0^n + a_{n-1}x_0^{n-1} + \cdots + a_1 x_0 + a_0)\\ = a_n(x_i^n - x_0^n) + a_{n-1}(x_i^{n-1} - x_0^{n-1}) + \cdots + a_1(x_i - x_0)\\ = (x_i - x_0)p(x_i), \quad i = 1, 2, \ldots, n,\end{aligned}$$

missä $p(x)$ on kokonaislukukertoiminen polynomi astetta $n-1$.

Koska

$$p \mid (a_n x_i^n + a_{n-1}x_i^{n-1} + \cdots + a_1 x_i + a_0)$$

ja

$$p \mid (a_n x_0^n + a_{n-1} x_0^{n-1} + \cdots + a_1 x_0 + a_0),$$

niin

$$p \mid (x_i - x_0) p(x_i), \quad i = 1, 2, \ldots, n.$$

Kokonaisluvut x_i ja x_0 ovat erisuuria ratkaisuja, joten

$$x_i \not\equiv x_0 \pmod{p}.$$

Näin ollen

$$p \mid p(x_i), \quad i = 1, 2, \ldots, n,$$

ja tästä seuraa, että kongruenssilla

$$p(x) \equiv 0 \pmod{p}$$

on n ratkaisua mod p. Tämä on kuitenkin mahdotonta, sillä polynomin $p(x)$ asteluku on vain $n-1$ ja oletuksen mukaan lause pätee polynomeille, joiden asteluku on korkeintaan $n-1$.

Induktioperiaatteen nojalla kongruenssilla

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \equiv 0 \pmod{p},$$

missä $a_n \not\equiv 0 \mod p$, on siis korkeintaan n ratkaisua mod p. □

Lause 1.10. *Olkoon*

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

missä $a_0, a_1, \ldots, a_n \in \mathbb{Z}$ *ja* $a_n \neq 0$. *Jos* p *on alkuluku ja kongruenssilla*

$$f(x) \equiv 0 \pmod{p}$$

on enemmän kuin n *ratkaisua mod* p, *niin* p *jakaa kaikki polynomin* $f(x)$ *kertoimet.*

Todistus. Koska kongruenssilla $f(x) \equiv 0 \pmod{p}$ on enemmän kuin n ratkaisua, niin $p \mid a_n$. Näin on oltava, sillä jos $a_n \not\equiv 0 \pmod{p}$, niin Lagrangen lauseen mukaan kongruenssilla $f(x) \equiv 0 \pmod{p}$ olisi enintään n ratkaisua. Näin ollen jokaisesta kongruenssin $f(x) \equiv 0 \pmod{p}$ ratkaisusta x_0 saadaan

$$p \mid a_{n-1} x^{n-1} + \cdots a_1 x + a_0.$$

Kongruenssilla

$$a_{n-1} x^{n-1} + \cdots a_1 x + a_0 \equiv 0 \pmod{p}$$

on siis enemmän kuin n ratkaisua. Tästä seuraa, että

$$p \mid a_{n-1}.$$

Nyt siis jokaista $v \leqslant n$ kohti kongruenssilla

$$a_v x^v + a_{v-1}x^{v-1} + \cdots a_1 x + a_0 \equiv 0 \,(\mathrm{mod}\ p)$$

on enemmän kuin v ratkaisua. Näin ollen $p \mid a_v$ kun $v = 1, 2, \ldots, n$. □

Lause 1.11 (Wilsonin lause)**.** *Luku p on alkuluku jos ja vain jos*

$$p \mid (p-1)! + 1.$$

Todistus 1. Osoitetaan ensin, että jos p on alkuluku, niin $p \mid (p-1)! + 1$. Tarkastellaan kongruenssia

$$x^2 \equiv 1 \,(\mathrm{mod}\ p),$$

jolla on ratkaisut $x = p - 1$ ja $x = -p + 1$. Dirichlet'n lauseen mukaan, kun $a = 1$,

$$p \mid (p-1)! + 1^{(p-1)/2}$$

eli

$$p \mid (p-1)! + 1, .$$

Oletetaan seuraavaksi että $p \mid (p-1)! + 1$ ja osoitetaan, että tällöin luvun p on oltava alkuluku.

On selvää, että $a \mid (p-1)!$ kaikilla $a \in \{2, 3, \ldots, p-1\}$. Tämän avulla nähdään helposti, että $a \nmid (p-1)! + 1$ aina, kun $a \in \{2, 3, \ldots, p-1\}$. Näin ollen ykköstä suurempi pienin positiivinen kokonaisluku, joka jakaa luvun $(p-1)!+1$ on p. Toisaalta jokaisen ykköstä suuremman kokonaisluvun pienin ei-triviaalinen jakaja on alkuluku. Siis p on alkuluku. □

Todistus 2. Tarkastellaan polynomia

$$f(x) = (x-1)(x-2)\cdots(x-(p-1)) - (x^{p-1} - 1),$$

missä $x = 1, 2, \ldots, p-1$ ja p on alkuluku.

Selvästi $\mathrm{syt}(x, p) = 1$ ja näin ollen Fermat'n pienen lauseen nojalla saadaan

$$x^{p-1} \equiv 1 \,(\mathrm{mod}\ p).$$

Lisäksi jonkun luvuista $x-1, x-2, \ldots, x-(p-1)$ on oltava nolla. Tästä seuraa, että

$$p \mid (x-1)(x-2)\cdots(x-(p-1)).$$

Näistä seuraa, että kongruenssilla

$$f(x) \equiv 0 \,(\mathrm{mod}\ p)$$

on $p-1$ ratkaisua. Koska polynomi $f(x)$ on astetta $p-2$, niin Lauseen 1.10 nojalla jos

$$f(x) = a_{p-2}x^{p-2} + \cdots + a_1 x + a_0,$$

niin

$$p \mid a_0, p \mid a_1, \ldots, p \mid a_{p-2}.$$

Nyt $a_0 = (p-1)! + 1$ eli

$$p \mid (p-1)! + 1.$$

Toinen suunta todistetaan vastaavasti kuin todistuksessa 1. □

Esimerkki 1.12. Luku 3 on alkuluku ja

$$3 \mid (3-1)! + 1.$$

Luku 4 sen sijaan ei ole alkuluku ja

$$4 \nmid (4-1)! + 1.$$

2 Legendren symboli

Määritelmä 2.1. Olkoon p pariton alkuluku ja a sellainen kokonaisluku, että $\mathrm{syt}(a,p) = 1$. Määritellään *Legendren symboli* $\left(\frac{a}{p}\right)$ siten, että

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

Jos a on sellainen kokonaisluku, että $p \mid a$, niin $\left(\frac{a}{p}\right) = 0$.

Esimerkki 2.2. Legendren symbolin määritelmän mukaan

$$\left(\frac{4}{7}\right) = 1, \left(\frac{2}{3}\right) = -1 \text{ ja } \left(\frac{22}{11}\right) = 0,$$

sillä $2^2 \equiv 4 \,(\mathrm{mod}\ 7)$, 2 on epäneliö modulo 3 (katso Esimerkki 1.2) ja $11 \mid 22$.

Seuraavaksi käsitellään ja osoitetaan muutamia Legendren symbolin ominaisuuksia ja niihin liittyviä lauseita.

Lause 2.3 (Eulerin kriteeri)**.** *Olkoon p pariton alkuluku ja a sellainen kokonaisluku, että* $\text{syt}(a,p) = 1$*. Tällöin*

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

Todistus. Oletuksen mukaan $p \nmid a$, eli

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

Käsitellään molemmat tapaukset erikseen.

Jos $\left(\frac{a}{p}\right) = 1$, niin a on neliönjäännös modulo p ja on olemassa sellainen kokonaisluku x_0, että $x_0^2 \equiv a \pmod{p}$. Näin ollen

$$(x_0^2)^{(p-1)/2} \equiv a^{(p-1)/2} \pmod{p}$$

eli

$$x_0^{p-1} \equiv a^{(p-1)/2} \pmod{p}. \tag{7}$$

Koska neliönjäännöksen määritelmän mukaan $p \mid (x_0^2 - a)$ ja $\text{syt}(a,p) = 1$, seurauksena on $\text{syt}(x_0, p) = 1$. Näin ollen Fermat'n pienen lauseen nojalla

$$x_0^{p-1} \equiv 1 \pmod{p}. \tag{8}$$

Kongruensseista (7) ja (8) seuraa

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

eli

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

Jos $\left(\frac{a}{p}\right) = -1$, niin a on epäneliö modulo p eikä kongruenssilla $x^2 \equiv a \pmod{p}$ ole yhtään ratkaisua. Dirichlet'n lauseen nojalla

$$p \mid (p-1)! - a^{(p-1)/2}$$

eli toisin sanoen

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

Wilsonin lauseen mukaan $(p-1)! \equiv -1 \pmod{p}$, joten saadaan

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

eli

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

□

Esimerkki 2.4. Valitaan $p = 7$ ja $a = 2$. Nyt $\text{syt}(2, 7) = 1$ ja $3^2 \equiv 2 \pmod 7$, joten luku 2 on neliönjäännös mod 7 eli $\left(\frac{2}{7}\right) = 1$. Luku $a^{(p-1)/2} = 2^{(7-1)/2} = 8$ on siis kongruentti luvun 1 kanssa mod 7.

Lause 2.5. *Olkoon p pariton alkuluku ja a sellainen kokonaisluku, että* $\text{syt}(a, p) = 1$. *Jos* $a \equiv b \pmod p$, *niin*

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

Todistus. Koska oletuksen mukaan $p \nmid a$, on oltava myös $p \nmid b$, sillä $a \equiv b \pmod p$. Näin ollen on selvää, että a on neliönjäännös/epäjäännös mod p jos ja vain jos b on neliönjäännös/epäjäännös mod p, joten Legendren symbolin määritelmän mukaan

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

□

Esimerkki 2.6. Valitaan $p = 11, a = 9$ ja $b = -2$. Luku 9 on neliönjäännös mod 11, koska $\text{syt}(9, 11) = 1$ ja $3^2 \equiv 9 \pmod{11}$. Luku 9 on kongruentti myös luvun -2 kanssa mod 11. Toisaalta $\text{syt}(-2, 11) = 1$ ja $3^2 \equiv -2 \pmod{11}$, joten

$$\left(\frac{9}{11}\right) = 1 = \left(\frac{-2}{11}\right).$$

Lause 2.7. *Olkoon p pariton alkuluku sekä a ja b sellaisia kokonaislukuja, että* $\text{syt}(ab, p) = 1$. *Tällöin*

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

Todistus. Eulerin kriteerin mukaan

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

eli

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

ja edelleen

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

Näin ollen

$$p \left| \left(\frac{ab}{p}\right) - \left(\frac{a}{p}\right)\left(\frac{b}{p}\right). \right. \tag{9}$$

Koska $\left(\frac{ab}{p}\right)$, $\left(\frac{a}{p}\right)$ ja $\left(\frac{b}{p}\right)$ saavat jokainen arvoksi joko -1 tai 1, on erotuksen

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

oltava $-2, 0$ tai 2. Lauseen oletuksen mukaan p on kuitenkin pariton ja koska sen tulee täyttää ehto (9), on erotuksen oltava 0. Siis

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

□

Esimerkki 2.8. Olkoon $p = 5, a = 4$ ja $b = 21$. Nyt $ab = 84 = 2^2 \cdot 3 \cdot 7$ eli $\text{syt}(ab, p) = 1$. Sekä a että b ovat neliönjäännöksia mod 5, sillä $2^2 \equiv 4 \pmod 5$ ja $1^2 \equiv 21 \pmod 5$. Näin ollen $\left(\frac{4}{5}\right) = \left(\frac{21}{5}\right) = 1$. Myös ab on neliönjäännös mod 5, sillä $2^2 \equiv 84 \pmod 5$ eli

$$\left(\frac{84}{5}\right) = 1 = \left(\frac{4}{5}\right)\left(\frac{21}{5}\right).$$

Lemma 2.9. *Olkoon p pariton alkuluku. Tällöin*

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

Todistus. Eulerin kriteerin mukaan

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

Nyt $\left(\frac{-1}{p}\right)$ ja $(-1)^{(p-1)/2}$ voivat saada vain arvot 1 tai -1. Lisäksi p on pariton alkuluku ja

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

joten

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

□

Esimerkki 2.10. Valitaan $p = 5$. Nyt -1 on neliönjäännös mod 5, sillä $2^2 \equiv -1 \pmod 5$. Näin ollen $\left(\frac{-1}{5}\right) = 1$. Myös $(-1)^{(5-1)/2} = 1$, joten

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

Lemma 2.11. *Olkoon p pariton alkuluku. Tällöin*

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

Todistus. Alkuluku p voi olla joko muotoa $4n+1$ tai $4n+3$, missä $n \in \mathbb{N}$.

Jos $p = 4n+1$, niin Lemman 2.9 nojalla

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

Jos $p = 4n+3$, niin Lemman 2.9 nojalla

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

□

Esimerkki 2.12. Jos $p = 17$, niin $p \equiv 1 \pmod 4$. Luku -1 on neliönjäännös mod 17, sillä $4^2 \equiv -1 \pmod{17}$ eli $\left(\frac{-1}{p}\right) = 1$.

Jos $p = 3$, niin $p \equiv 3 \pmod 4$. Luku -1 on epäneliö mod 3 eli myös $\left(\frac{-1}{p}\right) = -1$.

Lause 2.13. *Olkoon p pariton alkuluku. Tällöin*

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} 1, & jos\ p \equiv \pm 1 \pmod 8 \\ -1, & jos\ p \equiv \pm 3 \pmod 8). \end{cases}$$

Todistus. Tarkastellaan kongruensseja

$$\begin{aligned} p - 1 &\equiv 1 \cdot (-1)^1 \pmod p \\ 2 &\equiv 2 \cdot (-1)^2 \pmod p \\ p - 3 &\equiv 3 \cdot (-1)^3 \pmod p \\ 4 &\equiv 4 \cdot (-1)^4 \pmod p \\ &\vdots \\ k &\equiv \frac{p-1}{2} \cdot (-1)^{(p-1)/2} \pmod p, \end{aligned}$$

missä

$$k = \begin{cases} \frac{p-1}{2}, & \text{jos kokonaisluku } (p-1)/2 \text{ on pariton} \\ p - \frac{p-1}{2}, & \text{jos kokonaisluku } (p-1)/2 \text{ on parillinen.} \end{cases}$$

Kertomalla yllä olevat kongruenssit puolittain yhteen, saadaan

$$2 \cdot 4 \cdot 6 \cdots (p-1) \equiv \left(\frac{p-1}{2}\right)!(-1)^{(p^2-1)/8} \pmod{p},$$

missä $(p^2-1)/8$ saadaan, kun lasketaan

$$\sum_{n=1}^{(p-1)/2} n = \frac{\left(\frac{p-1}{2}\right)\left(\frac{p-1}{2}+1\right)}{2} = \frac{1}{2}\left(\frac{p^2-2p+1}{4} + \frac{2p-2}{4}\right) = \frac{p^2-1}{8}.$$

Nyt

$$\begin{aligned} 2 \cdot 4 \cdot 6 \cdots (p-1) &= (2 \cdot 1)(2 \cdot 2)(2 \cdot 3) \cdots \left(2 \cdot \frac{p-1}{2}\right) \\ &= 2^{(p-1)/2}\left(\frac{p-1}{2}\right)!, \end{aligned}$$

joten

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

Koska $p \nmid \left(\frac{p-1}{2}\right)!$, niin

$$2^{(p-1)/2} \equiv (-1)^{(p^2-1)/8} \pmod{p}$$

ja Eulerin kriteerin nojalla

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

Edellisten kongruenssien mukaan saadaan

$$\left(\frac{2}{p}\right) \equiv (-1)^{(p^2-1)/8} \pmod{p}. \tag{10}$$

Kongruenssissa (10) $\left(\frac{2}{p}\right)$ ja $(-1)^{(p^2-1)/8}$ voivat saada ainoastaan arvot ± 1. Näin ollen erotuksen

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

ainoat mahdolliset arvot ovat $-2, 0$ ja 2. Koska p on pariton, on erotuksen oltava 0, joten

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

Luku p voi olla joko muotoa $8n \pm 1$ tai $8n \pm 3$, missä $n \in \mathbb{N}$.

Jos $p = 8n \pm 1$, niin

$$\frac{p^2 - 1}{8} = 8n^2 \pm 2n,$$

joka on parillinen. Tässä tapauksessa siis $(-1)^{(p^2-1)/8} = 1$.

Jos $p = 8n \pm 3$, niin

$$\frac{p^2 - 1}{2} = 8n^2 \pm 6n + 1,$$

joka on pariton. Nyt $(-1)^{(p^2-1)/8} = -1$. Näin ollen

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} 1, & \text{jos } p \equiv \pm 1 \pmod 8 \\ -1, & \text{jos } p \equiv \pm 3 \pmod 8. \end{cases}$$

□

Esimerkki 2.14. Jos $p = 23$, niin $p \equiv -1 \pmod 8$. Luku 2 on neliönjäännös mod 23, sillä $5^2 \equiv 2 \pmod{23}$ eli $\left(\frac{2}{p}\right) = 1$. Lisäksi $(-1)^{(p^2-1)/8} = (-1)^{66} = 1$.

Jos $p = 5$, niin $p \equiv -3 \pmod 8$. Luku 2 on epäneliö mod 5 eli $\left(\frac{2}{p}\right) = -1$. Lisäksi $(-1)^{(p^2-1)/8} = (-1)^3 = -1$.

3 Neliönjäännösten resiprookkilaki

Lause 3.1 (Gaussin lemma)**.** *Olkoon p pariton alkuluku ja a sellainen kokonaisluku, että* $\text{syt}(a, p) = 1$. *Tarkastellaan kokonaislukujen*

$$a, 2a, 3a, \ldots, \frac{p-1}{2}a \tag{11}$$

pienimpiä positiivisia jakojäännöksiä mod p. Jos s on niiden jakojäännösten määrä, jotka ovat suurempia kuin $p/2$, niin

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

Todistus. Jokaisen kokonaisluvun ma, missä $m \in \{1, 2, \ldots, (p-1)/2\}$, jakojäännös luvulla p jaettaessa on nollasta poikkeava, koska $\text{syt}(a, p) = 1$ ja $\text{syt}(m, p) = 1$, kaikilla $m \in \{1, 2, \ldots, (p-1)/2\}$. Muodostetaan joukosta (11) kaksi erillistä joukkoa mod p. Olkoon siis

$$S_1 = \{r_1, r_2, \ldots, r_\lambda\}, \text{ jos } r_i < \frac{p}{2}, \text{ missä } i = 1, 2, \ldots, \lambda,$$

ja

$$S_2 = \{e_1, e_2, \ldots, e_s\}, \text{ jos } e_j > \frac{p}{2}, \text{ missä } j = 1, 2, \ldots, s.$$

On selvää, että $s + \lambda = (p-1)/2$, sillä $S_1 \cap S_2 = \emptyset$. Muodostetaan nyt sellainen joukko S_3, että

$$S_1 \cup S_3 = \{1, 2, \ldots, (p-1)/2\}.$$

Voidaan osoittaa, että jokainen joukon S_1 alkio r_i on eri kuin mikä tahansa $w_j = p - e_j$, missä $e_j \in S_2$. Toisin sanoen $r_i \neq w_j$, kaikilla $i \in \{1, 2, \ldots, \lambda\}$ ja $j \in \{1, 2, \ldots, s\}$. Jos olisi olemassa indeksipari (i, j) siten, että $w_j = r_i$, niin saataisiin $p = r_i + e_j$. Tämä ei kuitenkaan ole mahdollista, sillä jakojäännösten r_i ja e_j määritelmien mukaan voitaisiin kirjoittaa sekä

$$ka = k_i p + r_i, \text{ missä } 1 \leqslant k \leqslant \frac{p-1}{2} \text{ ja } i = 1, 2, \ldots, \lambda, \tag{12}$$

että

$$va = v_j p + e_j, \text{ missä } 1 \leqslant v \leqslant \frac{p-1}{2} \text{ ja } j = 1, 2, \ldots, s. \tag{13}$$

Näin ollen saataisiin

$$(k+v)a = (k_i + v_j)p + (r_i + e_j) = (k_i + v_j)p + p.$$

Nyt selvästi $p \mid (k_i + v_j)p + p$, joten luvun p tulisi jakaa myös $(k+v)a$. Näin ei kuitenkaan ole, sillä $\text{syt}(a, p) = 1$ ja $2 \leqslant k + v \leqslant p - 1$. Joukot S_1 ja $\{w_1, w_2, \ldots, w_s\}$ ovat siis erillisiä. Lisäksi $w_j \in \{1, 2, \ldots, \frac{p-1}{2}\}$, kaikilla $j = 1, 2, \ldots, s$, sillä

$$w_j = p - e_j \quad \text{ja} \quad \frac{p}{2} < e_j < p.$$

Myös $r_i \in \{1, 2, \ldots, \frac{p-1}{2}\}$, kaikilla $i = 1, 2, \ldots, \lambda$ ja lisäksi tiedetään, että $s + \lambda = (p-1)/2$. Näin ollen $S_3 = \{w_1, w_2, \ldots, w_s\}$ ja

$$S_1 \cup S_3 = \{r_1, r_2, \ldots, r_\lambda, w_1, w_2, \ldots, w_s\} = \{1, 2, \ldots, (p-1)/2\}.$$

Kertomalla kaikki joukon $S_1 \cup S_3$ alkiot keskenään, saadaan

$$r_1 r_2 \cdots r_\lambda w_1 w_2 \cdots w_s = 1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2}$$

eli

$$r_1 r_2 \cdots r_\lambda (p - e_1)(p - e_2) \cdots (p - e_s) = \left(\frac{p-1}{2}\right)!.$$

Kun yllä oleva kerrotaan auki, saadaan ainoastaan yksi termi, jossa p ei ole tekijänä. Tulo voidaan siis ilmaista kokonaisluvun c avulla muodossa

$$r_1 r_1 \cdots r_\lambda (p - e_1)(p - e_2) \cdots (p - e_s) = cp + r_1 r_2 \cdots r_\lambda (-1)^s e_1 e_2 \cdots e_s.$$

Nyt

$$p \left| cp + r_1 r_2 \cdots r_\lambda (-1)^s e_1 e_2 \cdots e_s - \left(\frac{p-1}{2} \right)! = 0 \right.$$

eli

$$p \left| (-1)^s r_1 r_2 \cdots r_\lambda e_1 e_2 \cdots e_s - \left(\frac{p-1}{2} \right)!. \right. \tag{14}$$

Yhtälöiden (12) ja (13) avulla saadaan

$$r_i = ka - k_i p, \text{ missä } 1 \leqslant k \leqslant \frac{p-1}{2} \text{ ja } i = 1, 2, \ldots, \lambda,$$

ja

$$e_j = va - v_j p, \text{ missä } 1 \leqslant v \leqslant \frac{p-1}{2} \text{ ja } j = 1, 2, \ldots, s.$$

Näin ollen

$$r_1 r_2 \cdots r_\lambda e_1 e_2 \cdots e_s \equiv a(2a)(3a) \cdots \left(\frac{p-1}{2} a \right) \pmod{p}.$$

Ehdon (14) ja yllä olevan kongruenssin nojalla

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

Eulerin kriteerin mukaan

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

Tästä seuraa, että

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

eli

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

ja edelleen

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

Koska $\left(\frac{a}{p}\right) - (-1)^s$ voi saada vain arvot $-2, 0$ tai 2 ja p on pariton, niin on oltava $\left(\frac{a}{p}\right) - (-1)^s = 0$ eli

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

□

Esimerkki 3.2. Olkoon $p = 13$ ja $a = 4$. Nyt

$$a, 2a, \ldots, \frac{p-1}{2}a = 4, 8, 12, 16, 20, 24$$

ja näitä lukuja vastaavat pienimmät positiiviset jakojäännökset mod p ovat

$$4, 8, 12, 3, 7 \text{ ja } 11.$$

Koska $(p-1)/2 = 6$, niin $s = 4$. Lisäksi $2^2 \equiv 4 \pmod{13}$, joten

$$\left(\frac{4}{13}\right) = 1 = (-1)^4.$$

Lause 3.3. *Olkoon p pariton alkuluku, a sellainen kokonaisluku, että $\text{syt}(a, p) = 1$ ja s Gaussin lemmassa määritelty jakojäännösten lukumäärä. Tällöin*

$$s \equiv (a-1)\frac{p^2-1}{8} + \sum_{m=1}^{(p-1)/2} \left\lfloor \frac{ma}{p} \right\rfloor \pmod{2},$$

missä $\lfloor x \rfloor$ on lattiafunktio, joka siis antaa reaaliluvun x kokonaisosan.

Todistus. Nyt

$$\begin{aligned} \sum_{m=1}^{(p-1)/2} m &= \sum_{i=1}^{\lambda} r_i + \sum_{j=1}^{s} w_j = \sum_{i=1}^{\lambda} r_i + \sum_{j=1}^{s} (p - e_j) \\ &= \sum_{i=1}^{\lambda} r_i + sp - \sum_{j=1}^{s} e_j. \end{aligned} \tag{15}$$

Lisäksi

$$\frac{ma}{p} = \left\lfloor \frac{ma}{p} \right\rfloor + v_m,$$

missä $0 < v_m < 1$. Edelleen

$$ma = \left\lfloor \frac{ma}{p} \right\rfloor p + v_m p. \tag{16}$$

Olkoon $h_m = v_m p$, jolloin on selvää, että $0 < h_m < p$ ja että h_m on pienin positiivinen jakojäännös kun ma jaetaan luvulla p. Näin ollen

$$\sum_{i=1}^{\lambda} r_i + \sum_{j=1}^{s} e_j = \sum_{m=1}^{(p-1)/2} h_m$$

ja yhtälön (16) avulla saadaan

$$a \sum_{m=1}^{(p-1)/2} m - p \sum_{m=1}^{(p-1)/2} \left\lfloor \frac{ma}{p} \right\rfloor = \sum_{i=1}^{\lambda} r_i + \sum_{j=1}^{s} e_j.$$

Kun lasketaan tämä yhtälö ja yhtälö (15) puolittain yhteen, saadaan

$$(a+1) \sum_{m=1}^{(p-1)/2} m - p \sum_{m=1}^{(p-1)/2} \left\lfloor \frac{ma}{p} \right\rfloor = 2 \sum_{i=1}^{\lambda} r_i + sp. \tag{17}$$

Koska $p \equiv 1 \pmod 2$, niin on selvää, että $sp \equiv s \pmod 2$ ja

$$p \sum_{m=1}^{(p-1)/2} \left\lfloor \frac{ma}{p} \right\rfloor \equiv \sum_{m=1}^{(p-2)/2} \left\lfloor \frac{ma}{p} \right\rfloor \pmod 2.$$

Lisäksi $a + 1 \equiv a - 1 \pmod 2$, joten

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

Lisäämällä äskeiset kongruenssit puolittain yhteen, saadaan

$$s + p \sum_{m=1}^{(p-1)/2} \left\lfloor \frac{ma}{p} \right\rfloor + (a+1) \sum_{m=1}^{(p-1)/2} m$$

$$\equiv sp + \sum_{m=1}^{(p-1)/2} \left\lfloor \frac{ma}{p} \right\rfloor + (a-1) \sum_{m=1}^{(p-1)/2} m \pmod 2$$

ja yhtälön (17) avulla edelleen saadaan

$$s + 2\sum_{i=1}^{\lambda} r_i + sp + 2p \sum_{m=1}^{(p-1)/2} \left\lfloor \frac{ma}{p} \right\rfloor \equiv sp + \sum_{m=1}^{(p-1)/2} \left\lfloor \frac{ma}{p} \right\rfloor + (a-1) \sum_{m=1}^{(p-1)/2} m \pmod 2.$$

Tästä saadaan

$$s \equiv \sum_{m=1}^{(p-1)/2} \left\lfloor \frac{ma}{p} \right\rfloor + (a-1) \sum_{m=1}^{(p-1)/2} m \pmod 2$$

eli

$$s \equiv \sum_{m=1}^{(p-1)/2} \left\lfloor \frac{ma}{p} \right\rfloor + (a-1)\frac{p^2-1}{8} \pmod 2.$$

□

Lause 3.4 (Neliönjäännösten resiprookkilaki)**.** *Jos p ja q ovat erisuuria parittomia kokonaislukuja, niin*

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

Todistus. Gaussin lemman nojalla

$$\left(\frac{p}{q}\right) = (-1)^{s_1} \quad \text{ja} \quad \left(\frac{q}{p}\right) = (-1)^{s_2},$$

missä s_1 on niiden positiivisten jakojäännösten määrä, jotka ovat suurempia kuin $\frac{q}{2}$. Nämä jakojäännökset saadaan kun jaetaan kokonaisluvut

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

alkuluvulla q. Lisäksi s_2 on niiden positiivisten jakojäännösten määrä, jotka ovat suurempia kuin $\frac{p}{2}$. Jakojäännökset saadaan jakamalla kokonaisluvut

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

alkuluvulla p. Näin ollen

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{s_1+s_2}.$$

Osoitetaan seuraavaksi, että

$$s_1 + s_2 \equiv \sum_{m_1=1}^{(q-1)/2} \left\lfloor \frac{m_1 p}{q} \right\rfloor + \sum_{m_2=1}^{(p-1)/2} \left\lfloor \frac{m_2 q}{p} \right\rfloor \pmod 2.$$

Lauseen 3.3 mukaan

$$s_1 \equiv \sum_{m_1=1}^{(q-1)/2} \left\lfloor \frac{m_1 p}{q} \right\rfloor + (p-1)\frac{(q-1)(q+1)}{8} \pmod 2.$$

Toinen luvuista $(q-1)$ ja $(q+1)$ on neljällä jaollinen, sillä $q > 2$. Tulo $(p-1)(q-1)(q+1)$ on siis jaollinen luvulla 16, joten $2 \mid (p-1)(q-1)(q+1)/8$. Näin ollen

$$s_1 \equiv \sum_{m_1=1}^{(q-1)/2} \left\lfloor \frac{m_1 p}{q} \right\rfloor \pmod 2.$$

Vastaavasti

$$s_2 \equiv \sum_{m_2=1}^{(p-1)/2} \left\lfloor \frac{m_2 q}{p} \right\rfloor \pmod 2,$$

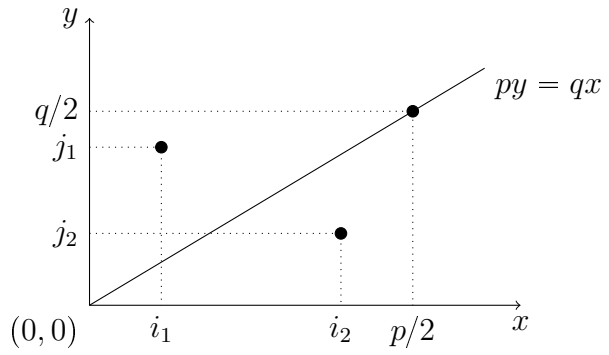
joten

$$s_1 + s_2 \equiv \sum_{m_1=1}^{(q-1)/2} \left\lfloor \frac{m_1 p}{q} \right\rfloor + \sum_{m_2=1}^{(p-1)/2} \left\lfloor \frac{m_2 q}{p} \right\rfloor \pmod 2. \tag{18}$$

Seuraavaksi todistetaan, että

$$\sum_{m_1=1}^{(q-1)/2} \left\lfloor \frac{m_1 p}{q} \right\rfloor + \sum_{m_2=1}^{(p-1)/2} \left\lfloor \frac{m_2 q}{p} \right\rfloor \equiv \frac{p-1}{2} \cdot \frac{q-1}{2} \pmod 2.$$

Tarkastellaan pisteitä (m_1, m_2) Kuvan 1 koordinaatistossa, kun $1 \leqslant m_1 \leqslant \frac{q-1}{2}$ ja $1 \leqslant m_2 \leqslant \frac{p-1}{2}$.



Kuva 1: Yhtälön $py = qx$ kuvaaja.

Yksikään näistä pisteistä ei ole suoralla $py = qx$. Näin täytyy olla, sillä jos olisi olemassa piste (m_1, m_2), jolle pätisi $pm_2 = qm_1$, niin $qm_1 \equiv 0 \pmod p$. Tämä on mahdotonta, sillä $\operatorname{syt}(q, p) = 1$ ja $1 \leqslant m_1 \leqslant \frac{q-1}{2}$. Näin ollen kaikki pisteet (m_1, m_2) sijaitsevat joko suoran $py = qx$ ylä- tai alapuolella.

Jos piste (m_1, m_2) sijaitsee suoran yläpuolella, niin

$$pm_1 > qm_2,$$

joten

$$m_2 < \frac{m_1 p}{q}.$$

Jokaista lukua m_1 kohti on siis $\left\lfloor \frac{m_1 p}{q} \right\rfloor$ kappaletta pisteitä, jotka sijoittuvat suoran $py = qx$ yläpuolelle. Näiden pisteiden yhteen laskettu määrä on

$$\sum_{m_1=1}^{(q-1)/2} \left\lfloor \frac{m_1 p}{q} \right\rfloor.$$

Jos piste (m_1, m_2) sijaitsee suoran $py = qx$ alapuolella, niin

$$pm_1 < qm_2$$

eli

$$m_1 < \frac{m_2 q}{p}.$$

Näin ollen suoran $py = qx$ alapuolelle jäävien pisteiden lukumäärä on yhteensä

$$\sum_{m_2=1}^{(p-1)/2} \left\lfloor \frac{m_2 q}{p} \right\rfloor.$$

Nyt siis suoran ylä- ja alapuolella on yhteensä

$$\sum_{m_1=1}^{(q-1)/2} \left\lfloor \frac{m_1 p}{q} \right\rfloor + \sum_{m_2=1}^{(p-1)/2} \left\lfloor \frac{m_2 q}{p} \right\rfloor$$

kappaletta pisteitä. Toisaalta pisteiden kokonaismäärä on

$$\frac{p-1}{2} \cdot \frac{q-1}{2},$$

sillä $1 \leqslant m_1 \leqslant \frac{q-1}{2}$ ja $1 \leqslant m_2 \leqslant \frac{p-1}{2}$, joten

$$\sum_{m_1=1}^{(q-1)/2} \left\lfloor \frac{m_1 p}{q} \right\rfloor + \sum_{m_2=1}^{(p-1)/2} \left\lfloor \frac{m_2 q}{p} \right\rfloor = \frac{p-1}{2} \cdot \frac{q-1}{2}.$$

Näin ollen äskeisen yhtälön ja kongruenssin (18) nojalla saadaan

$$s_1 + s_2 \equiv \frac{p-1}{2} \cdot \frac{q-1}{2} \pmod 2$$

eli

$$s_1 + s_2 - \frac{p-1}{2} \cdot \frac{q-1}{2} = 2k$$

jollakin kokonaisluvulla k. Tästä johtuen

$$\begin{aligned}\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) &= (-1)^{s_1+s_2} = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \cdot (-1)^{2k} \\ &= (-1)^{\frac{(p-1)(q-1)}{4}}.\end{aligned}$$

□

Huomautus 3.5. Neliönjäännösten resiprookkilaki antaa yhteyden kongruenssien

$$x^2 \equiv p \pmod{q} \tag{19}$$

ja

$$x^2 \equiv q \pmod{p} \tag{20}$$

ratkeavuuksien välille.

Jos $p \equiv 1 \pmod 4$ tai $q \equiv 1 \pmod 4$, niin p tai q on muotoa $4k+1$ ja toinen muotoa $2l+1$, joillakin $k, l \in \mathbb{N}$. Näin ollen

$$\frac{(p-1)(q-1)}{4} = \frac{(4k+1-1)(2l+1-1)}{4} = \frac{4k \cdot 2l}{4} = 2kl.$$

Luku on parillinen, joten

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

Kongruenssilla (19) on siis ratkaisu jos ja vain jos kongruenssilla (20) on ratkaisu, kun $p \equiv 1 \pmod 4$ tai $q \equiv 1 \pmod 4$.

Jos $p \equiv 3 \pmod 4$ ja $q \equiv 3 \pmod 4$, niin p on muotoa $4k+3$ ja q muotoa $4l+3$, joillakin $k, l \in \mathbb{N}$. Näin ollen

$$\frac{(p-1)(q-1)}{4} = \frac{(4k+3-1)(4l+1-1)}{4} = \frac{(4k+2)(4l+2)}{4} = \frac{16kl+8k+8l+4}{4} = 4kl+2k+2l$$

Luku on pariton, joten

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

Kongruenssilla (19) on siis ratkaisu jos ja vain jos kongruenssilla (20) ei ole ratkaisua, kun $p \equiv 3 \pmod 4$ ja $q \equiv 3 \pmod 4$.

Esimerkki 3.6. Olkoon $p = 11$ ja $q = 7$. Nyt $\frac{q-1}{2} = 3$ ja lukujen $p, 2p, 3p$ pienimmät positiiviset jakojäännökset luvulla q jaettaessa ovat $4, 1$ ja 5. Näin ollen $s_1 = 2$, sillä $\frac{q-i}{2} = 3$. Vastaavalla tavalla saadaan, että $s_2 = 3$, joten

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{s_1+s_2} = (-1)^5 = (-1)^{15} = (-1)^{\frac{(11-1)(7-1)}{4}}.$$

4 Jacobin symboli

Jacobin symboli on Legendren symbolin yleisempi muoto. Legendren symbolin avulla voidaan kertoa ratkeaako kongruenssi $x^2 \equiv a \pmod{p}$, missä p on pariton alkuluku ja $\text{syt}(a, p) = 1$. Jacobin symbolin avulla voidaan käsitellä kaikki parittomat positiiviset kokonaisluvut P, mutta se ei kuitenkaan aina anna tietoa siitä, ratkeaako kongruenssi $x^2 \equiv a \pmod{P}$, missä $\text{syt}(a, P) = 1$. Silloin kun P on alkuluku, niin Jacobin symboli antaa kuitenkin saman arvon kuin Legendren symboli.

Määritelmä 4.1. Olkoon P pariton, positiivinen kokonaisluku ja a sellainen kokonaisluku, että $\text{syt}(a, P) = 1$. Määritellään *Jacobin symboli* $\left(\frac{a}{P}\right)$ siten, että

$$\left(\frac{a}{P}\right) = \begin{cases} 1, & \text{jos } P = 1 \\ \left(\frac{a}{p_1}\right)^{m_1} \left(\frac{a}{p_2}\right)^{m_2} \cdots \left(\frac{a}{p_k}\right)^{m_k}, & \text{jos } P = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}, \end{cases}$$

missä $\left(\frac{a}{p_i}\right)$ on Legendren symboli ja $p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$ luvun P alkulukuesitys. Jacobin symboli on määritelty nollaksi niissä tapauksissa, kun $\text{syt}(a, P) > 1$.

Huomautus 4.2. Jacobin symboli ei välttämättä kerro kongruenssin $x^2 \equiv a \pmod{P}$ ratkeavuudesta mitään. Tämä voidaan nähdä olettamalla, että $P = p_1 p_2 \cdots p_k$, k on parillinen ja $\left(\frac{a}{p_i}\right) = -1$ kaikilla $i = 1, 2, \ldots, k$. Tällöin

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

Kongruenssilla

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

ei kuitenkaan ole ratkaisuja, sillä jos näin olisi, niin jokainen kongruensseista

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

ratkeaisi. Tällöin saataisiin

$$\left(\frac{a}{p_i}\right) = 1$$

kaikilla $i = 1, 2, \ldots, k$, mikä on ristiriidassa oletuksen mukaan.

Jos a on neliönjäännös mod P, niin

$$\left(\frac{a}{p_i}\right) = 1$$

kaikilla p_i. Näin ollen Jacobin symbolin arvo on tässä tapauksessa 1.

Jos $\left(\frac{a}{P}\right) = -1$, niin a on epäneliö mod P, sillä jos näin ei olisi, niin jokainen kongruensseista

$$x^2 \equiv a \,(\mathrm{mod}\ p_i)$$

ratkeaisi. Tästä seuraisi, että $\left(\frac{a}{P}\right) = 1$, mikä on ristiriita.

Näin ollen:

- Jos $\left(\frac{a}{P}\right) = 1$, niin ei voida tehdä päätelmiä siitä, onko a neliönjäännös vai epäneliö mod P.
- Jos $\left(\frac{a}{P}\right) = -1$, niin a on epäneliö mod P.
- Jos a on neliönjäännös mod P, niin $\left(\frac{a}{P}\right) = 1$.

Esimerkki 4.3. Jacobin symbolin määritelmän mukaan

$$\begin{aligned}
\left(\frac{15}{1}\right) &= 1, \\
\left(\frac{8}{15}\right) &= \left(\frac{8}{3}\right)\left(\frac{8}{5}\right) = (-1)\cdot(-1) = 1, \\
\left(\frac{2}{245}\right) &= \left(\frac{2}{5}\right)\left(\frac{2}{7}\right)^2 = (-1)\cdot 1^2 = -1 \text{ ja} \\
\left(\frac{12}{3}\right) &= 0.
\end{aligned}$$

Voimme lisäksi päätellä, että luku 2 on epäneliö mod 245.

Lause 4.4. *Olkoon P ja Q parittomia, positiivisia kokonaislukuja sekä a sellainen kokonaisluku, että* $\mathrm{syt}(a,P) = \mathrm{syt}(a,Q) = 1$. *Tällöin*

$$\left(\frac{a}{PQ}\right) = \left(\frac{a}{P}\right)\left(\frac{a}{Q}\right).$$

Todistus. Olkoon $P = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$ ja $Q = q_1^{n_1} q_2^{n_2} \cdots q_l^{n_l}$, missä $k, l \in \mathbb{N}$, lukujen P ja Q alkulukuesitykset. Tällöin Jacobin symbolin määritelmän mukaan saadaan

$$\begin{aligned}
\left(\frac{a}{PQ}\right) &= \left(\frac{a}{p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k} q_1^{n_1} q_2^{n_2} \cdots q_l^{n_l}}\right) \\
&= \left(\frac{a}{p_1}\right)^{m_1}\left(\frac{a}{p_2}\right)^{m_2} \cdots \left(\frac{a}{p_k}\right)^{m_k}\left(\frac{a}{q_1}\right)^{n_1}\left(\frac{a}{q_2}\right)^{n_2} \cdots \left(\frac{a}{q_l}\right)^{n_l} \\
&= \left(\frac{a}{P}\right)\left(\frac{a}{Q}\right).
\end{aligned}$$

□

Lause 4.5. *Olkoon P pariton ja positiivinen kokonaisluku sekä a ja b sellaisia kokonaislukuja, että* $\mathrm{syt}(a,P)=\mathrm{syt}(b,P)=1$. *Tällöin*

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

Todistus. Olkoon $P=p_1^{m_1}p_2^{m_2}\cdots p_k^{m_k}$, missä $k\in\mathbb{N}$, luvun P alkulukuesitys. Tällöin

$$\begin{aligned}\left(\frac{a}{P}\right)\left(\frac{b}{P}\right)&=\left(\frac{a}{p_1^{m_1}p_2^{m_2}\cdots p_k^{m_k}}\right)\left(\frac{b}{p_1^{m_1}p_2^{m_2}\cdots p_k^{m_k}}\right)\\&=\left(\frac{a}{p_1}\right)^{m_1}\left(\frac{a}{p_2}\right)^{m_2}\cdots\left(\frac{a}{p_k}\right)^{m_k}\left(\frac{b}{p_1}\right)^{m_1}\left(\frac{b}{p_2}\right)^{m_2}\cdots\left(\frac{b}{p_k}\right)^{m_k}\\&=\left[\left(\frac{a}{p_1}\right)\left(\frac{b}{p_1}\right)\right]^{m_1}\left[\left(\frac{a}{p_2}\right)\left(\frac{b}{p_2}\right)\right]^{m_2}\cdots\left[\left(\frac{a}{p_k}\right)\left(\frac{b}{p_k}\right)\right]^{m_k}.\end{aligned}$$

Lauseen 2.7 avulla saadaan

$$\left(\frac{a}{P}\right)\left(\frac{b}{P}\right)=\left(\frac{ab}{p_1}\right)^{m_1}\left(\frac{ab}{p_2}\right)^{m_2}\cdots\left(\frac{ab}{p_k}\right)^{m_k}=\left(\frac{ab}{P}\right).$$

□

Esimerkki 4.6. Nyt

$$\left(\frac{5}{39}\right)\left(\frac{4}{39}\right)=\left(\frac{5}{3}\right)\left(\frac{5}{13}\right)\left(\frac{4}{3}\right)\left(\frac{4}{13}\right)=(-1)\cdot(-1)\cdot1\cdot1=1.$$

Toisaalta

$$\left(\frac{20}{39}\right)=\left(\frac{20}{3}\right)\left(\frac{20}{13}\right)=(-1)\cdot(-1)=1$$

eli

$$\left(\frac{5}{39}\right)\left(\frac{4}{39}\right)=\left(\frac{20}{39}\right).$$

Seuraus 4.7. *Olkoon P pariton, positiivinen kokonaisluku ja a sellainen kokonaisluku, että* $\mathrm{syt}(a,P)=1$. *Tällöin*

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

Todistus. Lauseen 4.4 mukaan

$$\left(\frac{a}{P^2}\right) = \left(\frac{a}{P}\right)\left(\frac{a}{P}\right)$$

ja Lauseen 4.5 mukaan

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

On kuitenkin selvää, että

$$\left(\frac{a}{P}\right)\left(\frac{a}{P}\right) = 1,$$

joten

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

□

Lause 4.8. *Olkoon P pariton, positiivinen kokonaisluku sekä a ja b kokonaislukuja siten, että* $\text{syt}(a, P) = 1$. *Jos* $a \equiv b \pmod{P}$, *niin*

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

Todistus. Olkoon $P = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$, missä $k \in \mathbb{N}$, luvun P alkulukuesitys. Tällöin saadaan

$$a \equiv b \pmod{p_i},$$

kaikilla $i = 1, 2, \ldots, k$. Lauseen 2.5 nojalla

$$\left(\frac{a}{p_i}\right) = \left(\frac{b}{p_i}\right),$$

kaikilla $i = 1, 2, \ldots, k$. Näin ollen

$$\begin{aligned}\left(\frac{a}{P}\right) &= \left(\frac{a}{p_1}\right)^{m_1}\left(\frac{a}{p_2}\right)^{m_2}\cdots\left(\frac{a}{p_k}\right)^{m_k} \\ &= \left(\frac{b}{p_1}\right)^{m_1}\left(\frac{b}{p_2}\right)^{m_2}\cdots\left(\frac{b}{p_k}\right)^{m_k} \\ &= \left(\frac{b}{P}\right).\end{aligned}$$

□

Lause 4.9. *Olkoon P pariton, positiivinen kokonaisluku. Tällöin*

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

Todistus. Olkoon $P = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$, missä $k \in \mathbb{N}$, luvun P alkulukuesitys. Nyt Jacobin symbolin määritelmän mukaan

$$\left(\frac{-1}{P}\right) = \left(\frac{-1}{p_1}\right)^{m_1} \left(\frac{-1}{p_2}\right)^{m_2} \cdots \left(\frac{-1}{p_k}\right)^{m_k}.$$

Eulerin kriteerin nojalla saadaan

$$\left(\frac{-1}{p_i}\right) = (-1)^{(p_i-1)/2},$$

kaikilla $i = 1, 2, \ldots, k$, sillä jokainen p_i on pariton ja näin ollen suurempi kuin kaksi. Tästä seuraa, että

$$\left(\frac{-1}{P}\right) = (-1)^{\sum_{i=1}^{k} (p_i-1)m_i/2}.$$

Olkoon

$$p_i^{m_1} p_2^{m_2} \cdots p_k^{m_k} = q_1 q_2 \cdots q_l,$$

missä $l = m_1 + m_2 + \cdots + m_k$ ja $q_1, q_2, \ldots, q_l \in \{p_1, p_2, \ldots, p_k\}$. Nyt saadaan

$$\left(\frac{-1}{P}\right) = (-1)^{\sum_{j=1}^{l} (q_j-1)/2}. \tag{21}$$

Kokonaisluvulle P pätee

$$\begin{aligned} P &= \prod_{j=1}^{l} q_j = \prod_{j=1}^{l} [1 + (q_j - 1)] \\ &= [1 + (q_1 - 1)][1 + (q_2 - 1)] \cdots [1 + (q_l - 1)] \\ &= 1 + (q_1 - 1) + (q_2 - 1) + \cdots + (q_l - 1) + \sum_{j \neq k} (q_j - 1)(q_k - 1) + \cdots \\ &= 1 + \sum_{j=1}^{l} (q_j - 1) + 4r, \end{aligned}$$

jollakin kokonaisluvulla r, sillä jokainen $(q_j - 1)$ on parillinen. Jos $l = 1$, niin silloin $r = 0$. Näin ollen

$$(P-1)/2 = \frac{1}{2} \sum_{j=1}^{l} (q_j - 1) + 2r.$$

Sijoittamalla tämä yhtälöön (21), saadaan

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

□

Esimerkki 4.10. Olkoon $P = 95$. Tällöin

$$\left(\frac{-1}{95}\right) = \left(\frac{-1}{5}\right)\left(\frac{-1}{19}\right) = 1 \cdot (-1) = -1$$

ja toisaalta

$$(-1)^{(95-1)/2} = (-1)^{47} = -1.$$

Lause 4.11. *Olkoon P pariton, positiivinen kokonaisluku. Tällöin*

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

Todistus. Olkoon

$$P = p_i^{m_1} p_2^{m_2} \cdots p_k^{m_k} = q_1 q_2 \cdots q_l,$$

missä $l = m_1 + m_2 + \cdots + m_k$ ja $q_1, q_2, \ldots, q_l \in \{p_1, p_2, \ldots, p_k\}$. Nyt

$$\left(\frac{2}{P}\right) = \left(\frac{2}{q_1}\right)\left(\frac{2}{q_2}\right)\cdots\left(\frac{2}{q_l}\right)$$

ja Lauseen 2.13 nojalla

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

Näin ollen

$$\left(\frac{2}{P}\right) = (-1)^{\sum_{i=1}^{l}(q_i^2-1)/8}. \tag{22}$$

Lisäksi

$$\begin{aligned}\frac{P^2-1}{8} &= \frac{q_1^2 q_2^2 \cdots q_l^2 - 1}{8} \\ &= \frac{\left(1 + 8 \cdot \frac{q_1^2-1}{8}\right)\left(1 + 8 \cdot \frac{q_2^2-1}{8}\right)\cdots\left(1 + 8 \cdot \frac{q_l^2-1}{8}\right) - 1}{8}. \end{aligned} \tag{23}$$

Koska $q_i = 2s+1$, niin $(q_i^2-1) = (2s+1)^2 - 1 = 4s(s+1)$, jollakin kokonaisluvulla $s \geqslant 1$. Nähdään, että $q_i^2 - 1$ on jaollinen luvulla 8, joten

$$\begin{aligned}
&\left(1+8\cdot\frac{q_1^2-1}{8}\right)\left(1+8\cdot\frac{q_2^2-1}{8}\right)\cdots\left(1+8\cdot\frac{q_l^2-1}{8}\right)-1 \\
&= 1+\sum_{i=1}^{l}\frac{8(q_i^2-1)}{8}+\left(\sum_{i\neq j}\frac{8(q_i^2-1)}{8}\cdot\frac{8(q_j^2-1)}{8}\right. \\
&\quad \left.+\sum_{i\neq j\neq k}\frac{8(q_i^2-1)}{8}\frac{8(q_j^2-1)}{8}\frac{8(q_k^2-1)}{8}+\cdots\right)-1 \\
&= \sum_{i=1}^{l}(q_i^2-1)+\left(\sum_{i\neq j}8v_i\cdot 8v_j+\sum_{i\neq j\neq k}8v_i\cdot 8v_j\cdot 8v_k+\cdots\right),
\end{aligned}$$

missä $q_i^2 - 1 = 8v_i$, jollakin $v_i \in \mathbb{N}$. Yhtälö (23) saadaan siis muotoon

$$\frac{P^2-1}{8} = \frac{1}{8}\sum_{i=1}^{l}(q_i^2-1) + 2r,$$

jollakin $r \in \mathbb{N}$. Sijoittamalla yhtälöön (22) saadaan

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

□

Esimerkki 4.12. Nyt

$$\left(\frac{2}{525}\right) = \left(\frac{2}{3\cdot 5^2\cdot 7}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right)^2\left(\frac{2}{7}\right) = (-1)\cdot(-1)^2\cdot 1 = -1.$$

Edellisen Lauseen nojalla saadaan

$$(-1)^{(525^2-1)/8} = (-1)^{34453} = -1.$$

Lause 4.13. *Olkoon P ja Q parittomia, positiivisia ja keskenään jaottomia kokonaislukuja. Tällöin*

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{\frac{(P-1)(Q-1)}{4}}.$$

Todistus. Olkoon $P = p_1 p_2 \cdots p_k$ ja $Q = q_1 q_2 \cdots q_l$, joillakin $k, l \in \mathbb{N}$, luvun P ja Q alkulukuesitykset. Luvut $p_1, p_2, \ldots, p_k$ eivät välttämättä siis kaikki ole erisuuria keskenään. Sama pätee luvuille $q_1, q_2, \ldots, q_l$. Nyt

$$\left(\frac{P}{Q}\right) = \prod_{i=1}^{l} \left(\frac{P}{q_i}\right) = \prod_{i=1}^{l} \prod_{j=1}^{k} \left(\frac{p_j}{q_i}\right).$$

Vastaavasti

$$\left(\frac{Q}{P}\right) = \prod_{j=1}^{k} \prod_{i=1}^{l} \left(\frac{q_i}{p_j}\right),$$

joten

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = \prod_{j=1}^{k} \prod_{i=1}^{l} \left(\frac{p_j}{q_i}\right)\left(\frac{q_i}{p_j}\right).$$

Neliönjäännösten resiprookkilain nojalla

$$\left(\frac{p_j}{q_i}\right)\left(\frac{q_i}{p_j}\right) = (-1)^{\frac{(p_j-1)(q_i-1)}{4}}$$

eli

$$\begin{aligned}\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) &= (-1)^{\sum_{j=1}^{k}\sum_{i=1}^{l}\frac{1}{2}(p_j-1)\frac{1}{2}(q_i-1)} \\ &= (-1)^{\sum_{j=1}^{k}\frac{1}{2}(p_j-1)\sum_{i=1}^{l}\frac{1}{2}(q_i-1)}. \qquad (24)\end{aligned}$$

Lauseen 4.9 todistuksessa osoitettiin, että

$$(P-1)/2 = \frac{1}{2}\sum_{j=1}^{k}(p_j - 1) + 2r_1,$$

jollakin positiivisella kokonaisluvulla r_1. Vastaavasti

$$(Q-1)/2 = \frac{1}{2}\sum_{i=1}^{l}(q_i - 1) + 2r_2,$$

jollakin positiivisella kokonaisluvulla r_2, joten yhtälön (24) avulla

$$\begin{aligned}\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) &= (-1)^{-2r_1}(-1)^{-2r_2}(-1)^{\frac{1}{2}(P-1)\frac{1}{2}(Q-1)} \\ &= (-1)^{\frac{(P-1)(Q-1)}{4}}.\end{aligned}$$

□

Esimerkki 4.14. Valitaan $P = 21$ ja $Q = 55$. Nyt

$$\left(\frac{P}{Q}\right) = \left(\frac{21}{55}\right) = \left(\frac{3}{5}\right)\left(\frac{7}{5}\right)\left(\frac{3}{11}\right)\left(\frac{7}{11}\right) = (-1)\cdot(-1)\cdot 1\cdot(-1) = -1$$

ja

$$\left(\frac{Q}{P}\right) = \left(\frac{55}{21}\right) = \left(\frac{5}{3}\right)\left(\frac{11}{3}\right)\left(\frac{5}{7}\right)\left(\frac{11}{7}\right) = (-1)\cdot(-1)\cdot(-1)\cdot 1 = -1,$$

joten $\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = 1$. Toisaalta myös

$$(-1)^{\frac{(P-1)(Q-1)}{4}} = (-1)^{\frac{(21-1)(55-1)}{4}} = (-1)^{270} = 1.$$

Lähde

[1] Michael Th. Rassias: *Problem-Solving and Selected Topics in Number Theory*. Springer, New York, 2011.