Johdatus neliönjäännöksiin

Pro gradu-tutkielma

Anna Kolehmainen

1730133

Matemaattisten tieteiden laitos

Oulun yliopisto

Syksy 2018

Sisältö

1 Johdanto **2**

2 Neliönjäännökset **4**

2.1 Neliökongruenssi 4

2.2 Neliöt ja epäneliöt 6

2.3 Eulerin kriteeri 11

2.4 Legendren symboli 12

2.5 Jacobin symboli 15

2.6 Resiprookkilaki 19

3 Neliönjäännösten sovelluksia **30**

3.1 Turnausten konstruointi 30

3.2 Hadamardin matriisit 37

3.3 Eulerin pseudoalkuluvut 40

3.4 Nollatietotodistukset 44

Luku 1

Johdanto

Tässä tutkielmassa perehdytään neliönjäännöksiin ja joihinkin niihin liittyviin sovelluksiin. Aluksi tarkastellaan yleistä toisen asteen kongruenssia ja sen ratkeavuutta, joka johdattelee tutkimaan neliönjäännöksiä ja epäneliönjäännöksiä modulo n. Neliönjäännösten teorian perusteet luotiin 1700- ja 1800-luvuilla matematiikan suurmiesten toimesta. Tässä tutkielmassa esiteltävät tärkeät tulokset ovat peräisin Leonhard Eulerin, Adrien-Marie Legendren ja Johan Carl Friedrich Gaussin kynistä. Lukijan oletetaan hallitsevan lukuteorian ja erityisesti kongruensseilla laskemisen perusteet.

Luvussa 2 käydään läpi neliönjäännösten perusteisiin liittyviä määritelmiä ja lauseita esimerkkien kera. Luku 2 perustuu lähes kokonaan Ericksonin ja Vazzanan teokseen *Introduction to Number Theory* [1]. Muut lähteet on mainittu niissä kohdissa, joissa niitä on käytetty. Luvussa 2 tutkitaan milloin kongruenssi $x^2 \equiv a \pmod{p}$ on ratkeava, eli milloin luku a on neliönjäännös modulo p. Osoitamme myös, että tällä kongruenssilla on joko kaksi ratkaisua, tai ei yhtään ratkaisua. Eulerin kriteerin, Legendren symbolin ja Gaussin lemman kautta päästään tutustumaan erääseen matematiikan merkittävimmistä ja eleganteimmista tuloksista, resiprookkilakiin. Sekä Euler,

että Legendre esittivät resiprookkilain konjektuurina epäonnistuttuaan lukuisissa yrityksissään todistaa se. Nuori 19-vuotias matemaatikko Gauss oli ensimmäinen, joka onnistui sen todistamaan.

Luvussa 3 tutustutaan neljään neliönjännöksiin liittyvään sovellukseen. Luvut 3.1 ja 3.2 perustuvat teokseen [1]. Ensimmäiseksi tarkastellaan graafiteorian erästä haaraa, jossa neliönjäännösten avulla konstruoidaan tietyn ominaisuuden omaavia turnauksia. Seuraavaksi esitellään lyhyesti Hadamardin matriisit ja näytetään miten neliönjäännöksiä voidaan käyttää tiettyjä kertalukuja olevien Hadamardin matriisien konstruointiin. Luvuissa 3.3. ja 3.4. lähteenä on käytetty Rosenin teosta *Elementary Number Theory and Its Applications* [3]. Kolmas sovellusalue koskee pseudoalkulukuja. Pseudoalkuluvut ovat yhdistettyjä lukuja, joilla on jokin alkuluvuille tyypillinen ominaisuus. Pseudoalkuluvut luokitellaan näiden ominaisuuksien mukaan ja niitä käytetään muun muassa salausmenetelmissä. Tässä tutkielmassa esitellään Eulerin pseudoalkuluvut. Tutkielman päätteeksi tutustutaan nollatietotodistuksiin. Nollatietotodistuksessa on kaksi osapuolta, joista ensimmäinen pyrkii vakuuttamaan toisen siitä, että hänellä on salaista tietoa, paljastamatta mitä tämä tieto on. Tämä tärkeä neliönjäännösten sovellus on käyttökelpoinen esimerkiksi identiteettivarmennuksissa tietoverkoissa, sekä korttivarmennuksissa kortin ja päätteen välillä.

Luku 2

Neliönjäännökset

2.1 Neliökongruenssi

Yleinen toisen asteen kongruenssi on muotoa

$$ax^2 + bx + c \equiv 0 \pmod{n}, \tag{2.1}$$

missä luku a ei ole kongruentti nollan kanssa modulo n, eli luku n ei jaa lukua a.

Muokataan kongruenssia 2.1 täydentämällä neliöksi. Kerrotaan ensin kongruenssi puolittain luvulla $4a$, jolloin saadaan

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

Lisätään sitten molemmille puolille b^2-4ac, jolloin kongruenssi tulee muotoon

$$\begin{aligned} 4a^2x^2 + 4abx + b^2 &\equiv b^2 - 4ac \pmod{n}, \quad \text{eli} \\ (2ax + b)^2 &\equiv b^2 - 4ac \pmod{n}. \end{aligned} \tag{2.2}$$

Tekemällä sijoitus $y \equiv 2ax+b \pmod{n}$ päädytään seuraavaan huomioon:

Huomautus 2.1.1. Kongruenssilla $ax^2 + bx + c \equiv 0 \pmod{n}$, missä n on pariton ja $\text{syt}(a, n) = 1$, on ratkaisu jos ja vain jos kongruenssilla $y^2 \equiv b^2 - 4ac \pmod{n}$ on ratkaisu.

Lukua $d = b^2 - 4ac$ kutsutaan diskriminantiksi. Tällä merkinnällä kongruenssi 2.1 on ratkeava täsmälleen silloin, kun kongruenssi

$$y^2 \equiv d \pmod{n} \tag{2.3}$$

on ratkeava.

Huomautus 2.1.2. Yleisen neliökongruenssin modulo n ratkaiseminen voidaan aina palauttaa muotoon, jossa tutkitaan ratkaisuja modulo alkuluku p, sillä jokainen yhdistetty luku n voidaan ilmoittaa alkulukujen potenssien tulona $n = p_1^{a_1} p_2^{a_2} \cdots p_i^{a_i}$. Näin ollen tässä tutkielmassa keskitytään kongruenssien modulo p, missä p on alkuluku, ominaisuuksiin.

Tutkitaan seuraavaksi milloin kongruenssi 2.3 on ratkeava.

1. Jos $d \equiv 0 \pmod{n}$, saadaan ratkaisu $y \equiv 0 \pmod{n}$.

2. Jos n on alkuluku eli $n = p$, ja $d \equiv -1 \pmod{p}$, niin kongruenssilla on ratkaisu, kun $p = 4k + 1$ ja sillä ei ole ratkaisua, kun $p = 4k + 3$. [1, s.81] Ratkeavaan tapaukseen $p = 4k + 1$ liittyy vielä täsmälleen kaksi ratkaisua, sillä jos $x^2 \equiv y^2 \pmod{p}$, niin $p|x^2 - y^2$, eli $p|(x+y)(x-y)$. Näin ollen $p|x-y$ tai $p|x+y$. Siispä jos $x \equiv y \pmod{p}$ on ratkaisu, niin myös $x \equiv -y \pmod{p}$ on ratkaisu.

Toisen asteen kongruenssien ratkaisemiseksi on tehtävä ero neliöiden ja epäneliöiden välille.

2.2 Neliöt ja epäneliöt

Parittoman alkuluvun p jäännösluokkarenkaan $\mathbb{Z}_p$ yksikköryhmään $\mathbb{Z}_p^*$ kuuluu $p-1$ alkiota, joista jokainen on joko neliönjäännös tai neliönepäjäännös.

Määritelmä 2.2.1. Olkoon $n \in \mathbb{Z}^+$. Sanomme kokonaislukua a *neliönjäännökseksi* $\pmod{n}$, jos $\text{syt}(a,n) = 1$ ja kongruenssilla $x^2 \equiv a \pmod{n}$ on ratkaisu. Jos kongruessilla $x^2 \equiv a \pmod{n}$ ei ole ratkaisua sanomme, että a on *neliönepäjäännös* $\pmod{n}$. [3, s.331]

Jatkossa käytämme neliönjäännösten modulo p joukolle merkintää

$$R = \{x^2 | x \in \mathbb{Z}_p^*\},$$

ja neliönepäjäännösten joukolle merkintää

$$N = \mathbb{Z}_p^* \setminus R.$$

[1, s.131]

Esimerkki 2.2.2. *Määritetään luvun* 10 *neliönjäännökset. Korotetaan jokainen joukon* $\mathbb{Z}_{10}^* = \{1,3,7,9\}$ *alkio vuorotellen toiseen potenssiin, jolloin saadaan*

$$1^2 \equiv 1 \pmod{10},$$

$$3^2 \equiv 9 \pmod{10},$$

$$7^2 \equiv 9 \pmod{10},$$

$$9^2 \equiv 1 \pmod{10}.$$

Huomataan, että luvun 10 *neliönjäännökset ovat* 1 *ja* 9. *Luvut* 3 *ja* 7 *ovat siis luvun* 10 *neliönepäjäännökset. Toisin sanoen* $R = \{1,9\}$ *ja* $N = \{3,7\}$.

Esimerkki 2.2.3. *Määritetään luvun* 7 *neliönjäännökset. Korotetaan jokainen joukon* $\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$ *alkio vuorotellen toiseen potenssiin, jolloin saadaan*

$$1^2 \equiv 1 \pmod 7,$$

$$2^2 \equiv 4 \pmod 7,$$

$$3^2 \equiv 2 \pmod 7,$$

$$4^2 \equiv 2 \pmod 7,$$

$$5^2 \equiv 4 \pmod 7,$$

$$6^2 \equiv 1 \pmod 7.$$

Huomataan, että luvun 7 *neliönjäännökset ovat* 1, 2 *ja* 4. *Luvut* 3, 5 *ja* 6 *ovat tällöin luvun* 7 *neliönepäjäännökset. Toisin sanoen* $R = \{1, 2, 4\}$ *ja* $N = \{3, 5, 6\}$.

Palataan hetkeksi tarkastelemaan täydellisen toisen asteen kongruenssin ratkaisua.

Esimerkki 2.2.4. *Ratkaistaan neliöksi täydentämällä seuraavat kongruenssit:*

(a) $2x^2 + 2x + 1 \equiv 0 \pmod 7$,

(b) $2x^2 + 3x + 1 \equiv 0 \pmod 7$.

(a) Ensimmäisessä vaiheessa on saatava toisen asteen termin kertoimeksi luku 1. *Esimerkin kongruenssissa toisen asteen termin kerroin on* 2, *joten on etsittävä sen käänteisalkio kertolaskun suhteen modulo* 7. *Koska* $2 \cdot 4 \equiv 1 \pmod 7$, *niin käänteisalkio on luku* 4. *Kerrotaan kongruenssin molemmat puolet siis luvulla* 4, *jolloin saadaan*

$$x^2 + 8x + 4 \equiv 0 \pmod 7.$$

Lisätään sitten luku 12 *molemmille puolille, jolloin kongruenssi tulee muotoon*

$$x^2 + 8x + 16 \equiv 12 \pmod 7.$$

Nyt konruenssin vasen puoli voidaan kirjoittaa binomin neliöksi

$$(x + 4)^2 \equiv 5 \pmod 7.$$

Esimerkissä 2.2.3 todettiin, että luku 5 *on luvun* 7 *neliönepäjäännös, joten kongruenssilla ei ole ratkaisua.*

Huomautuksen 2.1.1 nojalla diskriminantin avulla voidaan ensin tutkia onko ratkaisuja olemassa. Lasketaan siis

$$d = b^2 - 4ac = 2^2 - 4 \cdot 4 \cdot 1 \equiv 3 \pmod 7.$$

Esimerkistä 2.2.3 nähdään, että luku 3 *on luvun* 7 *neliönepäjäännös. Näin ollen kongruenssilla ei ole ratkaisua.*

(b) Tutkitaan nyt ensin diskriminantin avulla, onko kongruenssilla ratkaisuja. Lasketaan

$$d = b^2 - 4ac = 2^2 - 4 \cdot 2 \cdot 1 = 1.$$

Koska 1 *on luvun* 7 *neliönjäännös, kongruenssilla on ratkaisuja. Ratkaistaan kongruenssi neliöksi täydentämällä. Toisen asteen termin kerroin on sama kuin (a)-kohdassa, joten kerrotaan kongruenssi jälleen luvulla* 4, *jolloin saadaan*

$$x^2 + 12x + 4 \equiv 0 \pmod 7.$$

Koska $2 \cdot 6 = 12$, *halutaan vasemalle puolelle saada* $6^2 = 36$. *Lisätään siis luku* 32 *molemmille puolille kongruenssia, jolloin se tulee muotoon*

$$x^2 + 12x + 36 \equiv 32 \pmod 7.$$

Nyt vasen puoli voidaan taas kirjoittaa binomin neliöksi

$$(x+6)^2 \equiv 4 \pmod 7.$$

Esimerkistä 2.2.3 huomataan, että $2^2 \equiv 4 \pmod 7$ *ja* $5^2 \equiv 4 \pmod 7$. *Siis kongruenssin ratkaisut ovat muotoa*

$$x_1 + 6 = 2 \quad ja \quad x_2 + 6 = 5, \quad eli$$

$$x_1 = -4 \equiv 3 \pmod 7 \quad ja \quad x_2 = -1 \equiv 6 \pmod 7.$$

Lemma 2.2.5. *Olkoon p pariton alkuluku ja a kokonaisluku, joka ei ole jaollinen luvulla p. Tällöin kongruenssilla*

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

joko ei ole ratkaisuja, tai sillä on täsmälleen kaksi epäkongruenttia ratkaisua modulo p.

Todistus. [3, s.332] 1° Todistetaan ensin, että epäkongruentteja ratkaisuja on kaksi. Oletetaan, että kongruenssilla $x^2 \equiv a \pmod p$ on ratkaisu $x = x_0$. Tällöin toinen epäkongruentti ratkaisu on $x = -x_0$, sillä

$$(-x_0)^2 = x_0^2 \equiv a \pmod p.$$

Huomataan myös, että $x_0 \not\equiv -x_0 \pmod p$. Sillä jos olisi $x_0 \equiv -x_0 \pmod p$, niin se tarkoittaisi, että $2x_0 \equiv 0 \pmod p$. Tämä on ristiriita, sillä selvästikään p ei jaa lukua 2, koska p on pariton alkuluku ja siten suurempi kuin 2. Myöskään x_0 ei voi olla jaollinen luvulla p, sillä tällöin olisi $x_0 \equiv 0 \pmod p$, ja edelleen $x_0^2 \equiv 0 \pmod p$, mutta oletuksen mukaan $x_0^2 \equiv a \pmod p$ ja p ei jaa lukua a.

2° Todistaaksemme ettei epäkongruentteja ratkaisuja ole kahta enempää tehdään vastaoletus. Oletetaan siis, että sekä $x = x_0$, että $x = x_1$ ovat kongruenssin $x^2 \equiv a \pmod{p}$ ratkaisuja. Tällöin olisi

$$x_0^2 \equiv x_1^2 \equiv a \pmod{p},$$

mikä voidaan kirjoittaa yhtäpitävästi

$$x_0^2 - x_1^2 = (x_0 - x_1)(x_0 + x_1) \equiv 0 \pmod{p}.$$

Siispä

$$x_1 \equiv -x_0 \pmod{p} \quad \text{tai} \quad x_1 \equiv x_0 \pmod{p}.$$

Näin ollen kohtien 1° ja 2° nojalla kongruenssilla $x^2 \equiv a \pmod{p}$ on täsmälleen kaksi epäkongruenttia ratkaisua.

□

Lause 2.2.6. *Olkoon p pariton alkuluku, tällöin joukossa $\{1, 2, \ldots, p-1\}$ on täsmälleen $(p-1)/2$ neliönjäännöstä modulo p ja $(p-1)/2$ neliönepäjäännöstä modulo p. Siis $|R| = |N| = \frac{p-1}{2}$.*

Todistus. [3, s.332] Löytääksemme kaikki luvun p neliönjäännökset joukosta $1, 2, \ldots, p-1$ laskemme lukujen $1, 2, \ldots, p-1$ neliöiden pienimmät jäännökset modulo p.

Koska tutkittavia neliöitä on $p-1$ kappaletta ja koska jokaisella kongruenssilla $x^2 \equiv a \pmod{p}$ on joko 0 tai 2 ratkaisua lemman 2.2.5 nojalla, lukujen $1, 2, \ldots, p-1$ joukossa on oltava täsmälleen $\frac{p-1}{2}$ luvun p neliönjäännöstä. Jäljelle jäävät $p - 1 - \frac{p-1}{2} = \frac{p-1}{2}$ lukua ovat luvun p neliönepäjäännöksiä.

□

2.3 Eulerin kriteeri

Leonhard Euler (1707-1783) esitti ja todisti vuonna 1748 lauseen, jonka avulla voidaan tutkia toisen asteen kongruenssin ratkaisujen olemassaoloa. Lauseen avulla ei kuitenkaan voida päätellä sitä, mitä mahdolliset ratkaisut ovat.

Määritelmä 2.3.1. Olkoon p alkuluku ja a neliönjäännös modulo p. Luku g on primitiivijuuri, jos g generoi koko ryhmän $\mathbb{Z}_p^*$, eli jokaista lukua a kohti on olemassa sellainen luku n, että $a \equiv g^n \pmod{p}$.

Huomautus 2.3.2. Luvut $1, q^2, q^4, \ldots, g^{p-1}$ kuuluvat joukkoon R. Lauseen 2.2.6 nojalla $|R| = \frac{p-1}{2}$, joten nämä luvut muodostavat kaikki joukon R alkiot. Näin ollen neliönjäännökset ovat primitiivijuuren g parilliset potenssit. [1, s.131]

Lause 2.3.3 (Eulerin kriteeri)**.** *Olkoon p pariton alkuluku, joka ei ole luvun a tekijä. Kongruenssilla $x^2 \equiv a \pmod{p}$ on kaksi ratkaisua, jos $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. Jos $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$, kongruenssilla $x^2 \equiv a \pmod{p}$ ei ole yhtään ratkaisua.*

Todistus. [1, s.132] Olkoon nyt g primitiivijuuri modulo p. Huomautuksen 2.3.2 nojalla tiedetään, että a on neliönjäännös täsmälleen silloin, kun se on kongruentti luvun g parillisten potenssien kanssa. Tällöin on olemassa sellainen kokonaisluku k, että $a \equiv g^{2k} \pmod{p}$. Fermat'n pienen lauseen nojalla $a^{p-1} \equiv 1 \pmod{p}$, kun p ei jaa lukua a. Näiden tietojen avulla voidaan laskea

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

Toisaalta, jos a ei ole neliönjäännös modulo p, niin on olemassa sellainen kokonaisluku k, että $a \equiv g^{2k+1} \pmod{p}$. Koska Fermat'n pienen lauseen mukaan $a^{p-1} \equiv (a^{\frac{p-1}{2}})^2 \equiv 1 \pmod{p}$, myös $g^{\frac{p-1}{2}}$ täytyy olla kongruentti joko

1 tai -1 modulo p. Koska g on primitiivijuuri, pienin eksponentti jolla $g^k \equiv 1 \pmod{p}$ on $k = p - 1$. Tästä seuraa, että $g^{\frac{p-1}{2}}$ täytyy olla kongruentti -1 modulo p. Siis

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

□

Esimerkki 2.3.4. *Määritetään Eulerin kriteerin avulla kongruenssin* $x^2 \equiv 10 \pmod{101}$ *ratkaisujen lukumäärä. Lasketaan*

$$10^{\frac{101-1}{2}} = 10^{50} = (10^2)^{25} \equiv (-1)^{25} \equiv -1 \pmod{101}.$$

Eulerin kriteerin nojalla kongruenssilla ei ole ratkaisuja.

Esimerkki 2.3.5. *Tutkitaan sitten Eulerin kriteeriä käyttäen onko kongruenssilla* $x^2 \equiv 2 \pmod{17}$ *ratkaisuja. Lasketaan*

$$2^{\frac{17-1}{2}} = 2^8 = (2^4)^2 \equiv (-1)^2 \pmod{17} \equiv 1 \pmod{17}.$$

Eulerin kriteerin nojalla kongruenssilla on kaksi ratkaisua.

2.4 Legendren symboli

Yrittäessään todistaa seuraavassa luvussa esiteltävää resiprookkilakia Adrien-Marie Legendre (1752-1833) otti vuonna 1798 julkaistussa teoksessaan *Essai sur la Theorie des Nombres* käyttöön uuden käytännöllisen merkintätavan, joka kertoo, onko luku a neliönjäännös modulo p. [4, s.180]

Määritelmä 2.4.1. Olkoon p pariton alkuluku. *Legendren symboli* $\left(\frac{a}{p}\right)$ on lukujen a ja p funktio, joka määritellään asettamalla

$$\left(\frac{a}{p}\right) = \begin{cases} 0, \text{ jos } a \equiv 0 \pmod{p}, \\ 1, \text{ jos } a \in R, \\ -1, \text{ jos } a \in N. \end{cases}$$

Yhdistämällä Legendren symboli ja Eulerin kriteeri saadaan seuraava tulos:

Lause 2.4.2. *Kun p on pariton alkuluku, niin*

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

Todistus. Jos $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, niin Eulerin kriteerin nojalla kongruenssilla $x^2 \equiv a \pmod{p}$ on ratkaisuja, eli $a \in R$, jolloin Legendren symbolin määritelmän nojalla $\left(\frac{a}{p}\right) = 1$.

Jos $\left(\frac{a}{p}\right) = -1$, niin Legendren symbolin määritelmän nojalla $a \in N$, eli kongruenssilla $x^2 \equiv a \pmod{p}$ ei ole ratkaisuja. Tällöin Eulerin kriteerin nojalla $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.

Jos $a \equiv 0 \pmod{p}$, niin luku p jakaa luvun a, mikä on Eulerin kriteerin oletuksen vastainen tilanne. □

Esimerkki 2.4.3. *Aikaisemmin esimerkissä 2.2.3 määritimme luvun 7 neliönjäännökset ja -epäjäännökset. Koska luvut* 1, 2 *ja* 4 *ovat luvun* 7 *neliönjäännöksiä, voimme merkitä Legendren symbolit*

$$\left(\frac{1}{7}\right) = \left(\frac{2}{7}\right) = \left(\frac{4}{7}\right) = 1.$$

Koska luvut 3, 5 *ja* 6 *taas ovat luvun* 7 *neliönepäjäännöksiä, voimme merkitä vastaavat Legendren symbolit*

$$\left(\frac{3}{7}\right) = \left(\frac{5}{7}\right) = \left(\frac{6}{7}\right) = -1.$$

Legendren symbolilla on monia käytön kannalta hyödyllisiä ominaisuuksia.

Lemma 2.4.4 (Legendren symbolin ominaisuuksia)**.** *Kun p on pariton alkuluku, niin*

(i) $\left(\frac{0}{p}\right) = 0,$

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

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

(iv) $\left(\frac{-1}{p}\right) = \begin{cases} \quad 1, \ jos\ p = 4k+1 \\ -\quad 1, \ jos\ p = 4k+3, \end{cases}$

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

(vi) $\Sigma_{a \in \mathbb{Z}_p}\left(\frac{a}{p}\right) = 0.$

Todistus. (i) Ensimmäinen kohta seuraa suoraan määritelmästä, sillä $0 \equiv 0 \pmod{p}$.

(ii) Myös toinen kohta on helppo nähdä määritelmän avulla, sillä $1 \equiv 1 \pmod{p}$ aina.

(iii) Tutkitaan Legendren symbolia $\left(\frac{a^2}{p}\right)$ Eulerin kriteerin avulla. Nyt

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

Fermat'n pienen lauseen nojalla.

(iv) Tuloksen 2.4.2 mukaisesti $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$. Kaikki alkuluvut p ovat joko muotoa $p = 4k+1$, tai muotoa $p = 4k+3$. Jos $p = 4k+1$, niin

$$(-1)^{\frac{p-1}{2}} = (-1)^{\frac{4k+1-1}{2}} = (-1)^{\frac{4k}{2}} = (-1)^{2k} = 1.$$

Jos puolestaan $p = 4k+3$, niin

$$(-1)^{\frac{p-1}{2}} = (-1)^{\frac{4k+3-1}{2}} = (-1)^{\frac{4k+2}{2}} = (-1)^{2k+1} = -1.$$

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

(vi) Tämä kohta seuraa lauseesta 2.2.6, jonka mukaan $|R| = |N|$.

□

Esimerkki 2.4.5. *Määritetään Legendren symbolin* $\left(\frac{-46}{17}\right)$ *arvo.*

Käytetään hyväksi lemman 2.4.4 kohtia (v) ja (iv), joiden avulla saadaan

$$\left(\frac{-46}{17}\right) = \left(\frac{-1}{17}\right)\left(\frac{46}{17}\right) = \left(\frac{46}{17}\right).$$

Koska $46 \equiv 12 \pmod{17}$, *niin* $\left(\frac{46}{17}\right) = \left(\frac{12}{17}\right)$. *Tämän tiedon ja lemman 2.4.4 kohtien (v) ja (iii) avulla saadaan nyt laskettua*

$$\left(\frac{12}{17}\right) = \left(\frac{3 \cdot 2^2}{17}\right) = \left(\frac{3}{17}\right).$$

Lasketaan sitten Eulerin kriteeriä käyttäen

$$\left(\frac{3}{17}\right) \equiv 3^{\frac{17-1}{2}} \equiv 3^8 \equiv (81)^2 \equiv (-4)^2 \equiv -1 \pmod{17}.$$

Huomautus 2.4.6. Lemman 2.4.4 kohta (v) johtaa mielenkiintoiseen havaintoon. Kahden neliönjäännöksen tai -epäjäännöksen tulo on neliönjäännös, kun taas neliönjäännöksen ja -epäjäännöksen tulo on neliönepäjäännös.

2.5 Jacobin symboli

Jacobin symboli on Legendren symbolin yleistys, jonka esitteli Carl Jacobi (1804-1851) vuonna 1846. Laskujen helpottamiseksi Jacobi laajensi Legendren symbolin myös niihin tapauksiin, kun alempi luku ei ole alkuluku. Legendren symboli ei auta, jos halutaan tutkia esimerkiksi kongruenssin $x^2 \equiv 6 \pmod{35}$ ratkeavuutta.

Määritelmä 2.5.1. Olkoon a kokonaisluku ja n positiivinen pariton kokonaisluku, jonka alkulukukehitelmä on $n = p_1 p_2 \cdots p_t$. *Jacobin symboli* $\left(\frac{a}{n}\right)$ määritellään

$$\left(\frac{a}{n}\right) = \prod_{i=1}^{t} \left(\frac{a}{p_i}\right),$$

missä oikean puolen tekijät ovat Legendren symboleita.

Esimerkki 2.5.2. *Lasketaan Jacobin symboli* $\left(\frac{2}{585}\right)$. *Hajotetaan ensin alempi luku alkulukutekijöihin* $585 = 3 \cdot 3 \cdot 5 \cdot 13$. *Siispä*

$$\left(\frac{2}{585}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{3}\right)\left(\frac{2}{5}\right)\left(\frac{2}{13}\right) = (-1)(-1)(-1)(-1) = 1.$$

Suurin osa Legendren symbolin ominaisuuksista pätee myös Jacobin symbolille. Tärkeä eroavuus on se, että vaikka $\left(\frac{a}{n}\right)$ olisi 1, niin kongruenssi $x^2 \equiv a \pmod{n}$ ei välttämättä ole ratkeava. Jos kuitenkin $\left(\frac{a}{n}\right)$ on -1, niin tiedetään että kongruenssilla ei ole ratkaisuja.

Esimerkki 2.5.3. *[2, s.151] Tarkastellaan kogruenssia* $x^2 \equiv -1 \pmod{21}$. *Tällä kongruenssilla ei ole ratkaisuja, sillä kongruenssilla* $x^2 \equiv -1 \pmod{3}$ *ei ole ratkaisuja (Lause 2.4.4 kohta (iv)). Tästä huolimatta*

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

Lemma 2.5.4 (Jacobin symbolin ominaisuuksia)**.** *Kun n ja m ovat parittomia kokonaislukuja ja a ja b mitä tahansa kokonaislukuja, niin*

(i) $\left(\frac{a}{n}\right) = 0$ *jos ja vain jos* $\operatorname{syt}(a, n) \neq 1$,

(ii) $\left(\frac{1}{n}\right) = 1$,

(iii) $\left(\frac{a^2}{n}\right) = 1$,

(iv) $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$,

(v) $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$,

(vi) $\left(\frac{-1}{n}\right) = 1$ *jos ja vain jos* $n \equiv 1 \pmod{4}$,

(vii) $\left(\frac{2}{n}\right) = 1$ *jos ja vain jos* $n \equiv \pm 1 \pmod{8}$.

Todistus. (i) Koska $\left(\frac{a}{n}\right) = \prod_{i=1}^{t} \left(\frac{a}{p_i}\right)$, niin tulon nollasäännön nojalla $\left(\frac{a}{n}\right) = 0$, jos ja vain jos on olemassa sellainen indeksi i, että $\left(\frac{a}{p_i}\right) = 0$. Tämä tarkoittaa Legendren symbolin määritelmän nojalla sitä, että luku p_i jakaa luvun a. Koska p_i jakaa myös luvun n, niin $p_i > 1$ on lukujen a ja n yhteinen tekijä, eli $\text{syt}(a, n) \neq 1$.

(ii) Jacobin symbolin määritelmän mukaan $\left(\frac{1}{n}\right) = \prod_{i=1}^{t} \left(\frac{1}{p_i}\right)$. Legendren symbolin ominaisuuksien nojalla $\left(\frac{1}{p}\right) = 1$, eli

$$\prod_{i=1}^{t} \left(\frac{1}{p_i}\right) = 1^t = 1.$$

(iii) Tämäkin kohta seuraa suoraviivaisesti Jacobin symbolin määritelmästä ja Legendren symbolin ominaisuuksista. Koska $\left(\frac{a^2}{p}\right) = 1$, niin

$$\left(\frac{a^2}{n}\right) = \prod_{i=1}^{t} \left(\frac{a^2}{p_i}\right) = 1^t = 1.$$

(iv) Käytämme jälleen Jacobin symbolin määritelmää ja Legendren symbolin ominaisuuksia, jolloin

$$\left(\frac{ab}{n}\right) = \prod_{i=1}^{t} \left(\frac{ab}{p_i}\right) = \prod_{i=1}^{t} \left(\frac{a}{p_i}\right)\left(\frac{b}{p_i}\right) = \prod_{i=1}^{t} \left(\frac{a}{p_i}\right) \prod_{i=1}^{t} \left(\frac{b}{p_i}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right).$$

(v) Jacobin symbolin määritelmän nojalla

$$\left(\frac{a}{nm}\right) = \prod_{i=1}^{t} \left(\frac{a}{p_i m}\right) = \prod_{i=1}^{t} \prod_{j=1}^{s} \left(\frac{a}{p_i p_j}\right) = \prod_{i=1}^{t} \left(\frac{a}{p_i}\right) \prod_{j=1}^{s} \left(\frac{a}{p_j}\right) = \left(\frac{a}{n}\right)\left(\frac{a}{m}\right).$$

(vi) [5, s.72] Todetaan aluksi, että väite voidaan kirjoittaa yhtäpitävästi muodossa $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$. Jos nimittäin $n \equiv 1 \pmod 4$, niin $\frac{n-1}{2}$ on parillinen luku, mutta jos $n \equiv 3 \pmod 4$, niin $\frac{n-1}{2}$ on pariton luku. Kun luvut n ja m ovat parittomia, niin

$$(n-1)(m-1) \equiv 0 \pmod 4,$$

mistä kertomalla sulut auki saadaan

$$nm - n - m + 1 \equiv 0 \pmod 4.$$

Lisäämällä molemmille puolille luvut n ja m, sekä vähentämällä molemmilta puolilta luku 2 saadaan kongruenssi muotoon

$$nm - 1 \equiv (n-1) + (m-1) \pmod 4.$$

Jakamalla sitten kongruenssi luvulla 2 saadaan

$$\frac{nm-1}{2} = \frac{n-1}{2} + \frac{m-1}{2} \pmod 2.$$

Toistamalla edellä kuvattua menettelyä t kertaa saadaan

$$\sum_{i=1}^{t} \frac{p_i - 1}{2} \equiv \frac{1}{2}\Big(\prod_{i=1}^{t} p_i - 1\Big) \equiv \frac{n-1}{2} \pmod 2. \tag{2.4}$$

Koska Eulerin kriteeriä käyttämällä voidaan kirjoittaa

$$\Big(\frac{-1}{n}\Big) = \prod_{i=1}^{t}\Big(\frac{-1}{p_i}\Big) = \prod_{i=1}^{t}(-1)^{\frac{p_i-1}{2}} = (-1)^{\sum_{i=1}^{t}\frac{p_i-1}{2}},$$

niin kongruenssiyhtälön 2.4 avulla saadaan

$$\Big(\frac{-1}{n}\Big) = (-1)^{\frac{n-1}{2}}.$$

(vii) [5, s.72] Väite voidaan kirjoittaa yhtäpitävästi muodossa $\big(\frac{2}{n}\big) = (-1)^{\frac{n^2-1}{8}}$. Samoin kuin edellisessä kohdassa jos n ja m ovat parittomia lukuja, niin

$$\frac{n^2m^2-1}{8} - \Big(\frac{n^2-1}{8} - \frac{m^2-1}{8}\Big) = \frac{(n^2-1)(m^2-1)}{8} \equiv 0 \pmod 8,$$

joten

$$\frac{n^2-1}{8} - \frac{m^2-1}{8} \equiv \frac{n^2m^2-1}{8} \pmod 2,$$

ja edelleen

$$\sum_{i=1}^{t} \frac{p_i^2 - 1}{8} \equiv \frac{n^2 - 1}{8} \pmod 2.$$

Näin ollen

$$\left(\frac{2}{n}\right) = \prod_{i=1}^{t} \left(\frac{2}{p_i}\right) = (-1)^{\sum_{i=1}^{t} \frac{p_i^2 - 1}{8}} = (-1)^{\frac{n^2-1}{8}}.$$

□

2.6 Resiprookkilaki

Resiprookkilaki on yhdessä aiemmin esiteltyjen Legendren symbolin ominaisuuksien kanssa voimakas työkalu toisen asteen kongruenssien ratkaisujen olemassaolon tutkimiseen. Minkä tahansa kongruenssin $x^2 \equiv a \pmod p$ ratkeavuus voidaan selvittää niiden avulla. Erityisesti kohdasta $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$ seuraa, että minkä tahansa luvun x Legendren symboli $\left(\frac{x}{p}\right)$ voidaan laskea, kun lasketaan ensin Legendren symboli $\left(\frac{q}{p}\right)$ kaikille luvun x alkulukutekijöille q. Laskeminen käy kuitenkin työlääksi kun luvut ovat isoja, jolloin alkulukukehitelmän löytäminen voi olla suorastaan mahdotonta. Gauss kehitti Legendren symbolien laskemiseen monta erilaista tapaa.

Lemma 2.6.1 (Gaussin lemma)**.** *Olkoon p pariton alkuluku ja a kokonaisluku, joka ei ole jaollinen luvulla p. Olkoon S_a joukon*

$$S = \{a, 2a, 3a, \ldots, \left(\frac{p-1}{2}\right)a\}$$

alkioiden pienimpien positiivisten jakojäännösten modulo p muodostama joukko. Olkoon s niiden joukon S_a alkioiden lukumäärä, jotka ovat suurempia kuin $\frac{p}{2}$. Tällöin

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

Todistus. [1, s.136] [4, s.184]

Olkoot $b_1, b_2, \ldots, b_s$ ne joukon S_a alkiot, jotka ovat suurempia kuin $\frac{p}{2}$, ja $l_1, l_2, \ldots, l_t$ ne joukon S_a alkiot, jotka ovat pienempiä kuin $\frac{p}{2}$. Toisin sanoen $0 < l_i < \frac{p}{2}$ ja $\frac{p}{2} < b_i < p$. Kutsutaan alkioita b_i suuriksi jäännöksiksi ja alkioita l_i pieniksi jäännöksiksi. Koska $\text{syt}(a, p) = 1$, yksikään joukon S alkioista ei ole jaollinen luvulla p, ja mitkään kaksi joukon S alkiota eivät ole kongruentteja toistensa kanssa modulo p. Huomataan, että $s + t = \frac{p-1}{2}$ ja kaikki luvut $p - b_1, p - b_2, \ldots, p - b_s, l_1, l_2, \ldots, l_t$ ovat positiivisia ja pienempiä kuin $\frac{p}{2}$.

Todistetaan seuraavaksi, että kaikki nämä luvut ovat myös keskenään erisuuria. Jos olisi $p - b_i = l_j$ jollain indeksien i ja j arvoilla, niin olisi myös olemassa sellaiset positiiviset ja lukua $\frac{p-1}{2}$ pienemmät tai enintään yhtä suuret luvut m_i ja m_j, joille pätisi $p - m_i a = m_j a$. Tämä tarkoittaisi sitä, että $a(m_i + m_j) \equiv 0 \pmod{p}$, mikä edelleen tarkoittaisi sitä, että p jakaisi luvun $m_i + m_j$. Näin ei kuitenkaan voi olla, sillä oletuksen mukaan $0 < m_i, m_j < \frac{p}{2}$. Siispä $l_i \neq l_j$ ja $b_i \neq b_j$ kun $i \neq j$.

Voimme siis päätellä, että luvut $p - b_1, p - b_2, \ldots, p - b_s, l_1, l_2, \ldots, l_t$ uudelleen järjestämällä muodostavat lukujonon $1, 2, \ldots, \frac{p-1}{2}$. Näin ollen niiden tulo on $\left(\frac{p-1}{2}\right)!$. Tällöin

$$(p - b_1)(p - b_2) \cdots (p - b_s) l_1 l_2 \cdots l_t = \left(\frac{p-1}{2}\right)!,$$

ja edelleen

$$(-1)^s b_1 b_2 \cdots b_s l_1 l_2 \cdots l_t \equiv \left(\frac{p-1}{2}\right)! \pmod{p}.$$

Toisaalta myös luvut $b_1, b_2, \ldots, b_s, l_1, l_2, \ldots, l_t$ ovat kongruentteja lukujen $a, 2a, \ldots, \frac{p-1}{2}a$ kanssa. Näin ollen

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

Kun jaetaan puolittain luvulla $\left(\frac{p-1}{2}\right)!$ ja kerrotaan luvulla $(-1)^s$, saadaan

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

Eulerin kriteerin nojalla voidaan kirjoittaa

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

□

Esimerkki 2.6.2. *Lasketaan Gaussin lemman avulla* $\left(\frac{27}{17}\right)$.

Nyt $S = \{27, 54, 81, 108, 135, 162, 189, 216\}$,

ja $S_a = \{10, 3, 13, 6, 16, 9, 2, 12\}$.

Suuret jäännökset ovat suurempia kuin $\frac{p}{2} = \frac{17}{2}$, *eli* $\{9, 10, 12, 13, 16\}$.

Tällöin $s = 5$, *eli Gaussin lemman nojalla*

$$\left(\frac{27}{17}\right) = (-1)^5 = -1.$$

Lause 2.6.3. *Olkoon p pariton alkuluku ja a pariton kokonaisluku joka ei ole jaollinen luvulla p. Asetetaan*

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

Tällöin

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

Todistus. [1, s.138] Käytämme samaa merkintätapaa kuin Gaussin lemman todistuksessa. Osoitamme, että $v \equiv s \pmod 2$, jolloin lause pätee. Olkoon luku k luvun ma pienin positiivinen jäännös modulo p. Huomioidaan ensin, että kokonaisluku ma on luvun $\left\lfloor \frac{ma}{p} \right\rfloor p$ ja luvun k summa. Tästä seuraa, että

$$\sum_{m=1}^{(p-1)/2} ma = \sum_{m=1}^{(p-1)/2} \left\lfloor \frac{ma}{p} \right\rfloor p + \sum_{i=1}^{s} b_i + \sum_{j=1}^{t} l_j. \tag{2.5}$$

Ensimmäinen termi yhtälön 2.5 oikealla puolella voidaan kirjoittaa lyhyesti vp. Kuten edellä Gaussin lemman todistuksessa huomattiin, luvut $p-b_1, p-b_2, \ldots, p-b_s, l_1, l_2, \ldots, l_t$ voidaan järjestää siten, että ne muodostavat lukujonon $1, 2, \ldots, \frac{p-1}{2}$. Näin ollen yhtälö 2.5 voidaan kirjoittaa uudelleen muotoon

$$\sum_{m=1}^{(p-1)/2} ma = vp + \left(\sum_{m=1}^{(p-1)/2} m \right) + 2\left(\sum_{i=1}^{s} b_i \right) - sp.$$

Järjestelemällä yhtälöä uudelleen saadaan

$$(a-1) \sum_{m=1}^{(p-1)/2} m = p(v-s) + 2\left(\sum_{i=1}^{s} b_i \right).$$

Koska a on pariton, vasemmalle puolelle tulee parillinen kokonaisluku. Kun tutkitaan edellistä yhtälöä modulo 2 tietäen, että p on pariton, saadaan $0 \equiv v - s \pmod 2$. Siis $v \equiv s \pmod 2$.

□

Esimerkki 2.6.4. *Lasketaan taas* $\left(\frac{27}{17}\right)$ *käyttäen nyt lausetta 2.6.3.*
Koska $\frac{p-1}{2} = 8$, *täytyy laskea* $\left\lfloor \frac{ma}{p} \right\rfloor$ *kun* $m = 1, 2, \ldots, 8$.

$$\left\lfloor \frac{27}{17} \right\rfloor = 1, \qquad \left\lfloor \frac{54}{17} \right\rfloor = 3, \qquad \left\lfloor \frac{81}{17} \right\rfloor = 4, \qquad \left\lfloor \frac{108}{17} \right\rfloor = 6,$$
$$\left\lfloor \frac{135}{17} \right\rfloor = 7, \qquad \left\lfloor \frac{162}{17} \right\rfloor = 9, \qquad \left\lfloor \frac{189}{17} \right\rfloor = 11, \qquad \left\lfloor \frac{216}{17} \right\rfloor = 12.$$

Näiden summa on $v = \sum_{m=1}^{(p-1)/2} \left\lfloor \frac{ma}{p} \right\rfloor = 53$, *jolloin*

$$\left(\frac{a}{p}\right) = (-1)^v = (-1)^{53} = -1.$$

Gaussin lemmaa käyttämällä voidaan määrittää milloin luku 2 on neliö modulo p mille tahansa alkuluvulle p.

Lause 2.6.5. *Olkoon* p *pariton alkuluku. Tällöin* $\left(\frac{2}{p}\right) = 1$ *täsmälleen silloin, kun* $p \equiv \pm 1 \pmod 8$. *Yhtäpitävästi voidaan kirjoittaa* $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

Todistus. [1, s.137] Ensin on laskettava sellaisten lukujen s, joiden pienimmät positiiviset jäännökset ovat suurempia kuin $\frac{p}{2}$, määrä joukossa $\{2, 2 \cdot 2, \ldots, (\frac{p-1}{2})2\}$. Kaikki tämän joukon alkiot ovat pienempiä kuin p, joten on vain laskettava niiden alkioiden lukumäärä, jotka ovat suurempia kuin $\frac{p}{2}$. Nyt $2m > \frac{p}{2}$ jos ja vain jos $m > \frac{p}{4}$. Tästä seuraa, että

$$s = \frac{p-1}{2} - \left\lfloor \frac{p}{4} \right\rfloor. \tag{2.6}$$

Tutkitaan seuraavaksi, milloin luvut $\frac{p-1}{2}$ ja $\left\lfloor \frac{p}{4} \right\rfloor$ ovat parillisia. Huomataan, että luku $\frac{p-1}{2}$ on parillinen, jos ja vain jos luku $p-1$ on jaollinen luvulla 4. Näin ollen luku $\frac{p-1}{2}$ on parillinen täsmälleen silloin, kun $p \equiv 1 \pmod 4$. Mikä tahansa pariton alkuluku voidaan kirjoittaa muodossa $8k + r$, missä $r = 1, 3, 5,$ tai 7. Lasketaan

$$\left\lfloor \frac{p}{4} \right\rfloor = \left\lfloor \frac{8k+r}{4} \right\rfloor = 2k + \left\lfloor \frac{r}{4} \right\rfloor.$$

Koska $\left\lfloor \frac{r}{4} \right\rfloor = 0$ kun $r = 1$ tai 3, mutta $\left\lfloor \frac{r}{4} \right\rfloor = 1$ kun $r = 5$ tai 7, niin $\left\lfloor \frac{p}{4} \right\rfloor$ on parillinen täsmälleen silloin, kun $p \equiv 1$ tai $3 \pmod 8$. Havainnollistetaan löydöksiä taulukon muodossa.

$p \pmod 8$	$\frac{p-1}{2}$	$\left\lfloor \frac{p}{4} \right\rfloor$
1	parillinen	parillinen
3	pariton	parillinen
5	parillinen	pariton
7	pariton	pariton

Yhtälön 2.6 avulla nähdään, että s on parillinen jos ja vain jos $p \equiv 1$ tai 7 (mod 8).

Jos $p \equiv 1 \pmod 8$ tai $p \equiv 7 \pmod 8$, niin

$$\frac{p^2-1}{8} = \frac{(8k \pm 1)^2 - 1}{8} = \frac{64k^2 \pm 16k}{8} = 8k^2 \pm 2k$$

on parillinen kokonaisluku. Tällöin $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = 1$. Toisaalta jos $p \equiv 3 \pmod 8$ tai $p \equiv 5 \pmod 8$, niin

$$\frac{p^2-1}{8} = \frac{(8k \pm 3)^2 - 1}{8} = \frac{64k^2 \pm 48k + 8}{8} = 8k^2 \pm 6k + 1$$

on pariton kokonaisluku ja $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = -1$.

□

Legendren symbolin $\left(\frac{3}{p}\right)$ laskeminen kun p on lukua 3 suurempi alkuluku ei onnistu yhtä helposti Gaussin lemman avulla. Koska tiedetään, että $\left(\frac{p}{3}\right) = 1$ täsmälleen silloin, kun $p \equiv 1 \pmod 3$, ongelma on ratkaistu, jos löydämme yhteyden Legendren symbolien $\left(\frac{3}{p}\right)$ ja $\left(\frac{p}{3}\right)$ välillä. Resiprookkilaki tarjoaa meille tämän yhteyden. [1, s.138]

Euler esitti resiprookkilain konjektuurina vuonna 1783, ja kaksi vuotta myöhemmin Legendre esitti sen käyttäen omaa merkintätapaansa. Sekä Legendre, että Euler yrittivät todistaa lain monella eri tavalla, mutta epäonnistuivat toistuvasti.

Vuonna 1795 nuori Gauss ilmeisesti epätietoisena Eulerin ja Legendren töistä löysi resiprookkilain uudestaan, ja vuoden yritettyään onnistui todistamaan sen. Lause tunnetaankin yleisesti myös nimellä *Gaussin resiprookkilaki*. Gauss julkaisi resiprookkilain teoksessaan *Disquisitiones Arithmeticae* vuonna 1801 ja otti sen omakseen. Legendre ei ollut tyytyväinen Gaussin tekoon, mutta Gaussin näkemyksen mukaan kunnia lauseesta kuului sille, joka sen ensimmäisenä todisti. [4, s.191]

Gauss löysi resiprookkilaille vielä seitsemän eri todistusta, jonka jälkeen lukuisat matemaatikot ovat esittäneet omansa, niin että laille on olemassa

tiettävästi ainakin 152 todistusta. [3, s.348]

Lause 2.6.6 (Resiprookkilaki)**.** *Olkoon p ja q erisuuria parittomia alkulukuja. Tällöin*

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

Yhtäpitävästi voidaan kirjoittaa

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

Todistus. [1, s.139] Tavoitteenamme on osoittaa, että

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

Kun käytämme aiemmin todistamaamme lausetta 2.6.3, riittää osoittaa, että

$$\sum_{m=1}^{(p-1)/2} \left\lfloor \frac{mq}{p} \right\rfloor + \sum_{n=1}^{(q-1)/2} \left\lfloor \frac{np}{q} \right\rfloor = \frac{(p-1)(q-1)}{4}.$$

Laskemme tätä varten järjestettyjen parien määrän joukossa

$$S = \{(x, y) : 1 \leq x \leq \frac{p-1}{2}, 1 \leq y \leq \frac{q-1}{2}\}.$$

Jokaisen luvun x valintaan on $\frac{p-1}{2}$ vaihtoehtoa, ja jokaisen luvun x pariksi y voidaan valita $\frac{q-1}{2}$ eri tavalla. Näin ollen joukossa S on $\frac{p-1}{2} \cdot \frac{q-1}{2}$ alkiota. Olkoon joukko S erillisten joukkojen A ja B unioni, missä A sisältää järjestetyt parit (x, y), joille pätee $xq < yp$, ja B sisältää järjestetyt parit (x, y), joille pätee $xq > yp$. Huomataan myös, että järjestetyille pareille pätee aina $xq \neq yp$, sillä muuten luvun q olisi jaettava joko y tai p, mutta p ja q ovat erisuuria alkulukuja, eli luku q ei jaa lukua p. Luku q ei myökään jaa lukua y, sillä $y \leq \frac{q-1}{2}$.

Jokaisen joukon A järjestetyn parin (x, y) luku x voidaan valita $\frac{p-1}{2}$ eri tavalla. Jokaista lukua x kohti luvun y täytyy toteuttaa ehto $y > \frac{xq}{p}$. Kaikki luvut y toteuttavat tämän ehdon ja muodostavat joukon A alkiot, sillä

$$\frac{xq}{p} < \frac{(\frac{p}{2})q}{p} = \frac{q}{2}.$$

Näin ollen jokaista lukua x kohti on täsmälleen $\left\lfloor \frac{xq}{p} \right\rfloor$ vaihtoehtoa luvuksi y. Näin ollen joukossa A on kaiken kaikkiaan

$$\sum_{x=1}^{(p-1)/2} \left\lfloor \frac{xq}{p} \right\rfloor$$

alkiota.

Jokaisen joukon B järjestetyn parin (x, y) luku y voidaan valita $\frac{q-1}{2}$ eri tavalla. Jokaista lukua y kohti luvun x täytyy nyt toteuttaa ehto $x > \frac{yp}{q}$. Kaikki luvut x toteuttavat tämän ehdon ja muodostavat joukon B alkiot, sillä

$$\frac{yp}{q} < \frac{(\frac{q}{2})p}{q} = \frac{p}{2}.$$

Näin ollen jokaista lukua y kohti on täsmälleen $\left\lfloor \frac{yp}{q} \right\rfloor$ vaihtoehtoa luvuksi x. Näin ollen joukossa B on kaiken kaikkiaan

$$\sum_{y=1}^{(q-1)/2} \left\lfloor \frac{yp}{q} \right\rfloor$$

alkiota.

Kaiken kaikkiaan järjestettyjen parien kokonaismäärä on näiden kahden summan summa, eli $|A| + |B| = |S|$. Olemme siis osoittaneet, että

$$\sum_{x=1}^{(p-1)/2} \left\lfloor \frac{xq}{p} \right\rfloor + \sum_{y=1}^{(q-1)/2} \left\lfloor \frac{yp}{q} \right\rfloor = \frac{(p-1)(q-1)}{4}.$$

□

Huomautus 2.6.7. Koska $\frac{p-1}{2}$ on parillinen silloin kun $p \equiv 1 \pmod 4$, ja pariton silloin kun $p \equiv 3 \pmod 4$, niin $\frac{p-1}{2} \cdot \frac{q-1}{2}$ on parillinen, jos $p \equiv 1 \pmod 4$, tai $q \equiv 1 \pmod 4$. Jos taas $p \equiv q \equiv 3 \pmod 4$, niin $\frac{p-1}{2} \cdot \frac{q-1}{2}$ on pariton. Siis

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

eli

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

Esimerkki 2.6.8. *[1, s.140] Lasketaan resiprookkilakia käyttäen* $\left(\frac{561}{659}\right)$. *Luvun* 561 *alkulukukehitelmä on* $3 \cdot 11 \cdot 17$, *joten lauseen 2.4.4 kohdan (v) nojalla*

$$\left(\frac{561}{659}\right) = \left(\frac{3}{659}\right)\left(\frac{11}{659}\right)\left(\frac{17}{659}\right).$$

Resiprookkilakia käyttämällä yhtälön oikea puoli saadaan muotoon

$$\left(-\left(\frac{659}{3}\right)\right)\left(-\left(\frac{659}{11}\right)\right)\left(\frac{659}{17}\right).$$

Koska $659 \equiv 2 \pmod 3$, $659 \equiv 10 \pmod{11}$, *ja* $659 \equiv 13 \pmod{17}$, *niin*

$$\left(-\left(\frac{659}{3}\right)\right)\left(-\left(\frac{659}{11}\right)\right)\left(\frac{659}{17}\right) = \left(-\left(\frac{2}{3}\right)\right)\left(-\left(\frac{10}{11}\right)\right)\left(\frac{13}{17}\right).$$

Tiedämmme lauseen 2.6.5 nojalla, että $\left(\frac{2}{3}\right) = -1$. *koska* $11 \equiv 3 \pmod 4$, *niin* $\left(\frac{10}{11}\right) = \left(\frac{-1}{11}\right) = -1$. *Viimeisen Legendren symbolin laskemiseksi täytyy tehdä vähän enemmän töitä. Käyttämällä resiprookkilakia uudelleen saadaan*

$$\left(\frac{13}{17}\right) = \left(\frac{17}{13}\right) = \left(\frac{4}{13}\right) = \left(\frac{2}{13}\right)\left(\frac{2}{13}\right) = (-1)(-1) = 1.$$

Yhdistämällä nämä laskelmat saadaan

$$\left(\frac{561}{659}\right) = (-(-1))(-(-1))(1) = 1.$$

Resiprookkilaki tunnetaan myös yleistettynä muotona Jacobin symbolia käyttäen.

Lause 2.6.9. *Olkoon a ja b sellaiset positiiviset parittomat kokonaisluvut, joiden suurin yhteinen tekijä on* 1. *Tällöin*

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

Todistus. [1, s.145] Olkoon luvun a alkulukukehitelmä $a = p_1 p_2 \cdots p_t$ ja luvun b alkulukukehitelmä $b = q_1 q_2 \cdots q_s$. Jacobin symbolin määritelmän ja Legendren symbolin ominaisuuksien nojalla

$$\left(\frac{a}{b}\right) = \prod_{i=1}^{t}\prod_{j=1}^{s}\left(\frac{p_i}{q_j}\right).$$

Oikean puolen tulontekijöille voidaan nyt käyttää Legendren symbolien resiprookkilakia, jolloin saadaan

$$\left(\frac{a}{b}\right) = \prod_{i=1}^{t}\prod_{j=1}^{s}(-1)^{\frac{p_i-1}{2}\frac{q_j-1}{2}}\left(\frac{q_j}{p_i}\right) = (-1)^{\sum_{i=1}^{t}\sum_{j=1}^{s}(\frac{p_i-1}{2})(\frac{q_j-1}{2})}\left(\prod_{i=1}^{t}\prod_{j=1}^{s}\left(\frac{q_j}{p_i}\right)\right)$$

$$= (-1)^{\sum_{i=1}^{t}(\frac{p_i-1}{2})\sum_{j=1}^{s}(\frac{q_j-1}{2})}\left(\frac{b}{a}\right).$$

Koska $\sum_{i=1}^{t}\frac{p_i-1}{2} \equiv \frac{n-1}{2} \pmod 2$ [1, s.144], saadaan viimeinen lauseke muotoon $(-1)^{\frac{a-1}{2}\cdot\frac{b-1}{2}}\left(\frac{b}{a}\right)$, jolloin

$$\left(\frac{a}{b}\right) = (-1)^{\frac{a-1}{2}\cdot\frac{b-1}{2}}\left(\frac{b}{a}\right). \tag{2.7}$$

Koska $(\left(\frac{b}{a}\right))^2 = (\pm 1)^2 = 1$, kertomalla yhtälö 2.7 tekijällä $\left(\frac{b}{a}\right)$, saadaan väite

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

□

Esimerkki 2.6.10. *Lasketaan Jacobin symboli* $\left(\frac{481}{3977}\right)$. *Luvun* 3977 *alkulukukehitelmä on* $41 \cdot 97$. *Käyttämällä lauseen 2.5.4 kohtaa (v) voimme hajottaa "nimittäjän", siis*

$$\left(\frac{481}{3977}\right) = \left(\frac{481}{41}\right)\left(\frac{481}{97}\right).$$

"Osoittajia" voidaan myös pienentää, sillä $481 \equiv 93 \pmod{97}$ *ja* $481 \equiv 30 \pmod{41}$. *Saadaan siis*

$$\left(\frac{481}{41}\right)\left(\frac{481}{97}\right) = \left(\frac{30}{41}\right)\left(\frac{93}{97}\right).$$

Seuraavaksi voidaan käyttää lauseen 2.5.4 kohtaa (iv), jonka avulla

$$\left(\frac{30}{41}\right)\left(\frac{93}{97}\right) = \left(\frac{2}{41}\right)\left(\frac{3}{41}\right)\left(\frac{5}{41}\right)\left(\frac{3}{97}\right)\left(\frac{31}{97}\right).$$

Koska $41 \equiv 1 \pmod{8}$, *tiedämme lauseen 2.6.5 nojalla, että* $\left(\frac{2}{41}\right) = 1$. *Koska myös tiedämme, että* $41 \equiv 1 \pmod{4}$ *ja* $97 \equiv 1 \pmod{4}$, *voimme käyttää resiprookkilakia, jolloin*

$$\left(\frac{2}{41}\right)\left(\frac{3}{41}\right)\left(\frac{5}{41}\right)\left(\frac{3}{97}\right)\left(\frac{31}{97}\right) = (1)\left(\frac{41}{3}\right)\left(\frac{41}{5}\right)\left(\frac{97}{3}\right)\left(\frac{97}{31}\right).$$

"Osoittajat" voidaan taas pienentää, sillä $41 \equiv 2 \pmod{3}$, $41 \equiv 1 \pmod{5}$, $97 \equiv 1 \pmod{3}$ *ja* $97 \equiv 1 \pmod{5}$. *Näin saadaan*

$$\left(\frac{41}{3}\right)\left(\frac{41}{5}\right)\left(\frac{97}{3}\right)\left(\frac{97}{31}\right) = \left(\frac{2}{3}\right)\left(\frac{1}{5}\right)\left(\frac{1}{3}\right)\left(\frac{4}{31}\right).$$

Koska $3 \equiv 3 \pmod{8}$, *niin lauseen 2.6.5 nojalla tiedetään, että* $\left(\frac{2}{3}\right) = -1$. *Lauseen 2.4.4 kohdan (ii) nojalla* $\left(\frac{1}{3}\right) = 1$ *ja* $\left(\frac{1}{5}\right) = 1$. *Koska* $2^2 = 4$, *lauseen 2.4.4 kohdan (iii) nojalla* $\left(\frac{4}{31}\right) = 1$. *Näin saadaan*

$$\left(\frac{2}{3}\right)\left(\frac{1}{5}\right)\left(\frac{1}{3}\right)\left(\frac{4}{31}\right) = (-1)(1)(1)(1) = -1.$$

Luku 3

Neliönjäännösten sovelluksia

3.1 Turnausten konstruointi

[1, s.147-151]

Neliönjäännösten joukko R on rakenteeltaan pseudosatunnainen. Jos tarkastellaan esimerkiksi Jacobin symboleita $\left(\frac{x}{p}\right)$, missä p on alkuluku ja $x \in [1, p-1]$, saamme joukon, jossa esiintyy yhtä paljon lukuja 1 ja -1 satunnaiselta näyttävässä järjestyksessä. Todellisuudessa joukko ei kuitenkaan ole satunnainen, vaan siellä vallitsee tiettyjä sääntöjä. Esimerkiksi $\left(\frac{x}{p}\right) = \left(\frac{p-x}{p}\right)$, jos $p = 4k+1$, ja $\left(\frac{x}{p}\right) = -\left(\frac{p-x}{p}\right)$, jos $p = 4k+3$. [1, s.134]

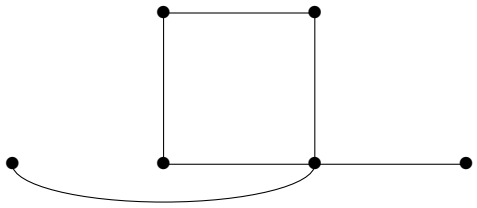
Tässä luvussa näytämme, kuinka tietyn ominaisuuden omaavan turnauksen kostruoinnissa käytetään hyväksi neliönjäännösten joukon pseudosatunnaista luonnetta. Turnausten konstruointi on eräs graafiteorian osa-alue. Graafiteorialla on valtavasti sovellusaloja, sillä se tutkii rakenteita, joita esiintyy kaikkialla sekä luonnossa, että ihmisen rakentamana. Graafiteorian sovellusaloja ovat muun muassa fysiikka, kemia, biologia, sosiologia, ja tietojenkäsittelytiede.

Määritelmä 3.1.1. *Graafi* on joukko *pisteitä*, ja joukko *viivoja*, jotka yh-

distävät graafin pistepareja.

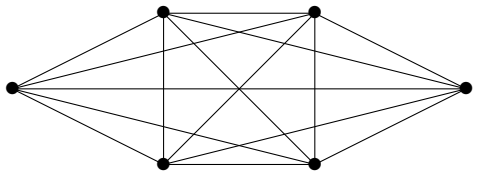
Graafin pisteet voivat sijaita missä tahansa, ja pisteitä yhdistävät viivat voivat olla kuinka tahansa pitkiä, minkä tahansa muotoisia, tai risteäviä. Oleellinen seikka graafissa on pisteiden ja viivojen välinen suhde, siis se liittyvätkö tietty viiva ja tietty piste toisiinsa. Ainoat rajoitukset ovat, että pisteestä lähtevä viiva ei saa muodostaa silmukkaa palaamalla takaisin samaan pisteeseen, ja kahden pisteen välillä ei sallita useita viivoja.

Kuva 3.1: Graafi



Määritelmä 3.1.2. *Täydellinen graafi* on sellainen, jonka jokainen pistepari on yhdistetty viivalla.

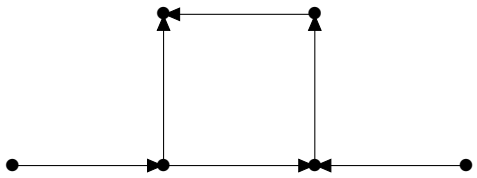
Kuva 3.2: Täydellinen graafi



Huomautus 3.1.3. Täydellisessä graafissa, jossa on n pistettä, on $\binom{n}{2}$ viivaa.

Määritelmä 3.1.4. *Suunnattu graafi* on sellainen, jossa jokainen viiva on korvattu nuolella.

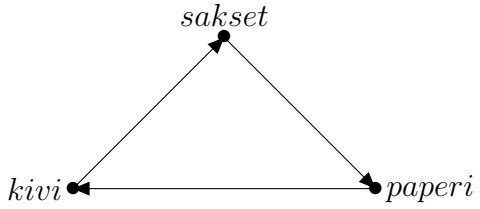
Kuva 3.3: Suunnattu graafi



Määritelmä 3.1.5. *Turnaus* on täydellinen suunnattu graafi. Jos turnauksessa on n pistettä, sanomme, että turnauksen *aste* on n.

Esimerkki 3.1.6. *Klassinen kivi-paperi-sakset -peli (Kuva 3.4) on eräs esimerkki turnauksesta. Turnauksessa on kolme pistettä, joista jokainen häviää yhdelle pisteelle ja voittaa yhden pisteen. Kivi voittaa sakset, joten nuoli on piirretty kiveä kuvaavasta pisteestä saksia kuvaavaan pisteeseen.*

Kuva 3.4: Turnaus



Yleistämme nyt esimerkin 3.1.6 tilanteen.

Määritelmä 3.1.7. Olkoon T_n turnaus, jossa on n pistettä. Sanomme, että turnauksella T_n on *ominaisuus* S_k, jos jokaista k pistettä sisältävää joukkoa $S \subseteq T_n$ kohti on olemassa sellainen piste $v \in T_n \setminus S$, että kaikki viivat pisteen v ja joukon S välillä on suunnattu pisteestä v joukkoon S.

Esimerkiksi kivi-paperi-sakset -pelillä on ominaisuus S_1, mutta sillä ei ole ominaisuutta S_2.

Seuraavaa lausetta kutsutaan Schütten lauseeksi, mutta sen on todistanut Erdös vuonna 1963.

Lause 3.1.8. *Olkoon k positiivinen kokonaisluku. Tällöin on olemassa sellainen kokonaisluku n, että turnauksella T_n on ominaisuus S_k.*

Todistus. [1, s.148] Olkoon k kiinnitetty ja n kokonaisluku joka määritetään myöhemmin. Koska n-asteisessa täydellisessä graafissa on $\binom{n}{2}$ viivaa, n pistettä sisältävästä joukosta voidaan muodostaa $2^{\binom{n}{2}}$ turnausta. Osoitamme, että kun n on riittävän suuri, suurimmalla osalla näistä turnauksista on ominaisuus S_k.

Olkoon t niiden n -asteisten turnausten lukumäärä, joilla ei ole ominaisuutta S_k. Olkoot joukoissa $S \subseteq T_n$ k pistettä, ja olkoon A_S jokaiselle joukolle S kokoelma sellaisia turnauksia, joissa yksikään nuoli ei ole suunnattu joukkoon S. Näillä turnauksilla ei ole siis ominaisuutta S_k, koska S on "huono" joukko. Tällöin $t = |\bigcup_S A_S|$, ja on voimassa epäyhtälö

$$t \leq \sum_S |A_S|. \tag{3.1}$$

Arvioidaan seuraavaksi epäyhtälön 3.1 oikean puolen summaa. Summassa on $\binom{n}{k}$ termiä. Kun jokin joukko S on valittu, tiedetään, että joukossa S on k pistettä ja joukon S komplementissa on $n-k$ pistettä. Näiden joukkojen pisteiden välisten nuolten suunnat voidaan valita vapaasti. Kaiken kaikkiaan mahdollisuuksia on $2^{\binom{n}{2}-k(n-k)}$ kappaletta. Jos jokin piste joukon S komplementissa on suunnattu kaikkiin pisteisiin joukossa S, niin S ei ole "huono" joukko, jolloin tällaisten nuolten suunnille on $2^k - 1$ vaihtoehtoa jokaisesta joukon S komplementin pisteestä, ja näin ollen kaiken kaikkiaan $(2^k-1)^{n-k}$ vaihtoehtoa. Näin ollen

$$\sum_S |A_S| = \binom{n}{k} 2^{\binom{n}{2}-k(n-k)} (2^k - 1)^{n-k}. \tag{3.2}$$

Yhdistämällä epäyhtälö 3.1 ja yhtälö 3.2, saadaan

$$t \leq \binom{n}{k}(1-2^{-k})^{n-k}2^{\binom{n}{2}}. \tag{3.3}$$

Kuten aiemmin on mainittu, joukossa jossa on n pistettä voidaan muodostaa $2^{\binom{n}{2}}$ turnausta. Tämä lauseke esiintyy myös oikealla puolella epäyhtälössä 3.3. Termi on kerrottu kahdella muulla lausekkeella, jotka ovat $\binom{n}{k}$ ja $(1-2^{-k})^{n-k}$. Koska k on vakio, termi $\binom{n}{k}$ on astetta k oleva muuttujan n polynomi. Termi $(1-2^{-k})^{n-k}$ puolestaan on muuttujan n eksponenttifunktio, jonka kantaluku on pienempi kuin 1. Kun n kasvaa rajatta, eksponenttifunktio lausekkeessa pienenee nopeammin kuin polynomifunktio kasvaa, jolloin niiden tulo lähestyy nollaa. Näin ollen epäyhtälön 3.3 yläraja lähenee mielivaltaisen pientä murto-osaa luvusta $2^{\binom{n}{2}} = 2^{\frac{n^2-n}{2}}$. Toisin sanoen, kun n kasvaa rajatta, niin melkein kaikilla n-asteisilla turnauksilla on ominaisuus S_k. Näin ollen, kun n on riittävän suuri, on olemassa turnaus jolla on ominaisuus S_k.

□

Seuraavaksi tutkimme miten voisimme konsturoida astetta n olevan turnauksen jolla on ominaisuus S_k. Lauseen 3.1.8 todistuksen perusteella voimme sanoa, että satunnaisella turnauksella on hyvin todennäköisesti ominaisuus S_k kun n on suuri. Satunnaisen turnauksen kontstruointiin käytämme neliönjäännöksiä.

Pohditaan ensin sellaisen turnauksen konstruointia, jolla on ominaisuus S_2. Kokeilemalla voidaan havaita, että sellaista turnausta ei voi muodostaa kuuden pisteen välille. Määritetään lauseen 3.1.8 todistuksen avulla funktio

$$f(n,k) = \binom{n}{k}(1-2^{-k})^{n-k},$$

jonka lauseke on sama kuin tekijän $2^{\binom{n}{2}}$ kerroin epäyhtälössä 3.3. Haluamme löytää sellaisen kokonaisluvun n, että $f(n,2) < 1$, sillä tällöin lauseen 3.1.8 todistuksessa käytetyn menetelmän mukaan täytyy olla olemassa astetta n oleva turnaus, jolla on ominaisuus S_2. Lasketaan

$$f(20,2) = \binom{20}{2}(1-2^{-2})^{20-2} =\approx 1,07116, \quad \text{ja}$$

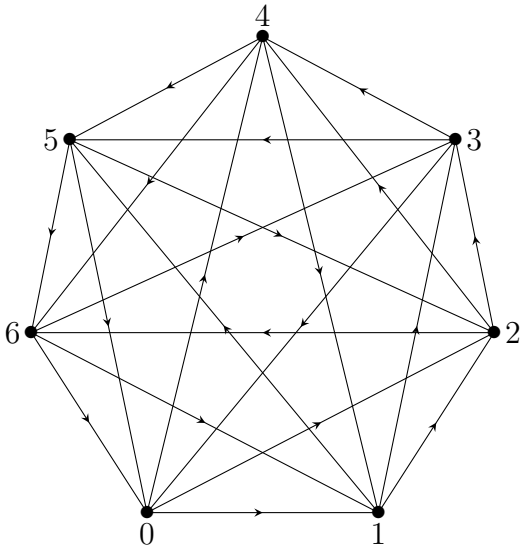
$$f(21,2) = \binom{21}{2}(1-2^{-2})^{21-2} =\approx 0,88794.$$

Näin ollen $n = 21$ toteuttaa vaatimuksen. Näin pienellä arvolla n todennäköisyys sille, että vaadittu turnaus muodostuu satunnaisesti ei kuitenkaan ole kovin suuri. Todennäköisyyden kasvattamiseksi pitäisi luku n valita suuremmaksi. Tämän jälkeen kolikkoa heittämällä jokaista nuolta varten voitaisiin turnaus satunnaistaa, jolloin turnauksella todennäköisesti olisi ominaisuus S_2. Konstruoinnin jälkeen pitäisi vielä huolellisesti tarkistaa, että turnauksella varmasti on ominaisuus S_2.

Itseasiassa ominaisuuden S_2 omaava astetta 7 oleva turnaus voidaan helposti muodostaa neliönjäännösten avulla, ja sen rakenteesta johtuen ominaisuuden S_2 olemassaolo on helppo todentaa. Seuraavaksi käydään läpi kuinka seitsemän pisteen turnaus, jolla on ominaisuus S_2, voidaan konsturuoida neliönjäännöksistä modulo 7.

Olkoot turnauksen pisteet $0, 1, 2, 3, 4, 5, 6$, ja 7. Olkoon R neliönjäännösten joukko modulo 7 ja N neliönepäjäännösten joukko modulo 7. Siis $R = \{1, 2, 4\}$ ja $N = \{3, 5, 6\}$ (Esimerkki 2.2.3). Asetetaan nuoli pisteestä i pisteeseen j, jos $j - 1$ kuuluu joukkoon R, ja nuoli pisteestä j pisteeseen i, jos $j - 1$ kuuluu joukkoon N. Tällaista turnausta kutsutaan *neliönjäännösturnaukseksi*. Huomioidaan myös, että nuolten suunnan valinta on hyvin määritelty, sillä $-1 \equiv 6$ on neliönepäjäännös. Turnaus on esitetty kuvassa 3.5.

Kuva 3.5: Turnaus jolla on ominaisuus S_2



Tarkistetaan vielä, että turnauksella on ominaisuus S_2. Otetaan tarkasteluun mitkä tahansa kaksi turnauksen pistettä. Koska turnauksella on syklinen symmetria, voimme valita pisteet niin, että yksi piste on 0 ja toinen piste on v. Seuraavaksi tarvitaan sellainen piste w, että w kuuluu joukkoon N ja $w - v$ kuuluu joukkoon N. Koska pisteiden määrä tässä turnauksessa on pieni, voimme esittää taulukossa jokaiselle pisteelle v vastaavan pisteen w.

v	1	2	3	4	5	6
w	6	5	6	3	3	5

Taulukko 3.1: Pisteet v ja w

Huomautus 3.1.9. Ominaisuuden S_2 omaavien neliönjäännösturnausten konstruoinnin tällä tavalla voi yleistää kaikille alkuluvuille, jotka ovat suurempia tai yhtä suuria kuin 7 ja kongruentteja luvun 3 kanssa modulo 4. Vuonna

1971 Joel Spencer ja Ronald Graham todistivat, että neliönjäännösturnauksella T_p on ominaisuus S_k, kun p on alkuluku, jolle pätee $p \equiv 3 \pmod 4$ ja $p > k^2 2^{2k-2}$.

3.2 Hadamardin matriisit

[1, s.155-157]

Vuonna 1893 Hadamard esitti kysymyksen, kuinka suuri voi olla sellaisen $n \times n$ matriisin determinantti, jonka alkiot a_{ij} ovat reaalilukuja väliltä $[-1, 1]$?

Neliömatriiseille pätee sääntö, jonka mukaan minkä tahansa $n \times n$ matriisin determinantti on merkkiä lukuunottamatta yhtä suuri kuin sellaisen suuntaissärmiön tilavuus, jonka sivut ovat kyseisen matriisin rivivektorit.

Olkoon A $n \times n$ matriisi, jonka alkiot ovat a_{ij}. Matriisin A rivivektorien pituus on korkeintaan $\sqrt{n}$. Näiden matriisien rivivektorien virittämän suuntaissärmiön tilavuus on korkeintaan sama kuin sellaisen suuntaissärmiön, jonka sivujen pituus on $\sqrt{n}$ ja jonka sivut ovat ortogonaaliset, eli kohtisuorassa toisiaan vastaan. Tilavuus on tällöin $(\sqrt{n})^n$.

Lause 3.2.1 (Hadamard)**.** *Olkoon A $n \times n$ matriisi, jonka alkioille a_{ij} pätee $-1 \leq a_{ij} \leq 1$. Tällöin $|\det A| \leq (\sqrt{n})^n$. Yhtäsuuruus on voimassa vain silloin, kun $a_{ij} = \pm 1$ kaikilla indeksien i ja j arvoilla, ja matriisin A rivivektorit ovat pareittain ortogonaalisia.*

Määritelmä 3.2.2. Astetta n oleva *Hadamardin matriisi* on $n \times n$ matriisi, jossa $a_{ij} = \pm 1$ kaikilla indeksien i ja j arvoilla, ja matriisin A rivivektorit ovat keskenään ortogonaalisia.

Esimerkki 3.2.3.

Kertalukua 2 oleva Hadamardin matriisi $\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$.

Kertalukua 4 oleva Hadamardin matriisi $\begin{pmatrix} 1 & 1 & 1 & 1 \\ -1 & 1 & -1 & 1 \\ -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$.

Tietyille kertaluvuille Hadamardin matriiseja voidaan konstruoida neliönjäännösten avulla.

Lause 3.2.4 (Payley)**.** *Olkoon p muotoa $4k+3$ oleva alkuluku, R neliönjäännösten joukko modulo p, ja N epäneliönjäännösten joukko modulo p. Olkoon $B = (b_{ij})$ sellainen $p \times p$ matriisi, että*

$$b_{ij} = \begin{cases} 1, \ jos\ j - i \in R, \\ -1, \ jos\ j - i \in N, ja \\ -1, \ jos\ i = j. \end{cases} \tag{3.4}$$

Olkoon A sellainen $(p+1) \times (p+1)$ matriisi, jonka ensimmäisen vaakarivin ja ensimmäinen pystyrivin alkiot ovat lukuja 1, ja jonka oikeassa alanurkassa on alimatriisina B. Tällöin A on Hadamardin matriisi.

Esimerkki 3.2.5. *Kostruoidaan kertalukua 8 oleva Hadamardin matriisi. Luku 7 on alkukuku, joka on muotoa $4k+3$. Nyt $R = \{1, 2, 4\}$ ja $N = \{3, 5, 6\}$. Muodostetaan alimatriisi B lauseen 3.2.4 antamalla säännöllä. Siis*

$$B = \begin{pmatrix} -1 & -1 & -1 & 1 & -1 & 1 & 1 \\ 1 & -1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & 1 & -1 \\ -1 & 1 & 1 & -1 & -1 & -1 & 1 \\ 1 & -1 & 1 & 1 & -1 & -1 & -1 \\ -1 & 1 & -1 & 1 & 1 & -1 & -1 \\ -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{pmatrix}.$$

Muodostetaan sitten Hadamardin matriisi lisäämällä ensimmäiseksi pysty- ja vaakariviksi luvuista 1 *muodostuvat rivit. Tällöin saadaan*

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

Payleyn lauseen mukaisen Hadamardin martiisin kertaluku on aina joko 1, 2, tai luvun 4 monikerta, sillä matriisin B kertaluku on muotoa $p = 4k+3$, ja matriisin A kertaluku on tällöin $p+1 = 4k+3+1$, joka on jaollinen luvulla 4. Sitä ei kuitenkaan tiedetä, onko jokaista kertalukua $4n$ kohti olemassa Hadamardin matriisi.

Konjektuuri 3.2.6. *Jokaista kertalukua* $4n$ *kohti on olemassa Hadamardin matriisi.*

Pienin kertaluku jota vastaavan Hadamardin matriisin olemassolosta ei ole varmuutta on 668.

3.3 Eulerin pseudoalkuluvut

[3, s.367-375] Olkoon p pariton alkuluku ja b sellainen kokonaisluku, joka ei ole jaollinen luvulla p. Tällöin Eulerin kriteerin nojalla

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

Jos siis halutaan selvittää, onko luku n alkuluku, voidaan valita sellainen kokonaisluku b, että $\text{syt}(b, n) = 1$, ja tutkia päteekö kongruenssi

$$b^{\frac{n-1}{2}} \equiv \left(\frac{b}{n}\right) \pmod{n}, \tag{3.5}$$

missä $\left(\frac{b}{n}\right)$ on Jacobin symboli. Jos kongruenssi 3.5 ei pidä paikkaansa, niin n on yhdistetty luku.

Esimerkki 3.3.1. *Olkoon $b = 2$ ja $n = 341$. Laskemalla huomataan, että $2^{170} \equiv 1 \pmod{341}$. Koska $341 \equiv -3 \pmod{8}$, niin lauseen 2.5.4 nojalla tiedetään, että $\left(\frac{2}{341}\right) = -1$. Tällöin*

$$2^{170} \not\equiv \left(\frac{2}{341}\right) \pmod{341}.$$

Näin ollen luku 341 ei ole alkuluku.

Pseudoalkuluvut ovat yhdistettyjä lukuja, joilla on tiettyjä alkuluvuille tyypillisiä ominaisuuksia. Pseudoalkulukuihin voi tarkemmin perehtyä teoksen [3] sivuilla 192-199. Määritellään ensin joitain käsitteitä, joita tarvitaan Eulerin pseudoalkulukujen tarkastelemisessa.

Määritelmä 3.3.2. Olkoon $b \geq 2$ positiivinen kokonaisluku. Jos n on yhdistetty luku ja $b^n \equiv b \pmod{n}$, niin n on *pseudoalkuluku kannan b suhteen.*

Määritelmä 3.3.3. Olkoon n sellainen positiivinen kokonaisluku, että $n - 1 = 2^s t$, missä s on ei-negatiivinen kokonaisluku ja t on pariton positiivinen kokonaisluku. Jos jompikumpi kongruensseista $b^t \equiv 1 \pmod{n}$ tai $b^{2^j t} \equiv -1 \pmod{n}$, kun $0 \leq j \leq s - 1$, totetuu, sanotaan, että n läpäisee *Millerin kokeen kannan b suhteen.*

Määritelmä 3.3.4. Jos n on yhdistetty luku, joka läpäisee Millerin kokeen kannan b suhteen, sanotaan, että n on *vahva pseudoalkuluku kannan b suhteen.*

Eräs Eulerin kriiteeriin perustuva pseudoalkulukujen tyyppi voidaan nyt määritellä.

Määritelmä 3.3.5. Paritonta yhdistettyä positiivista kokonaislukua n, joka toteuttaa kongruenssin

$$b^{\frac{n-1}{2}} \equiv \left(\frac{b}{n}\right) \pmod{n}, \tag{3.6}$$

missä b on positiivinen kokonaisluku, kutsutaan *Eulerin pseudoalkuvuksi kannan b suhteen.*

Eulerin pseudoalkuluvut kannan b suhteen ovat yhdistettyjä lukuja jotka toteuttamalla kongruenssin 3.6 käyttäytyvät kuten alkuluvut.

Esimerkki 3.3.6. *Olkoon $n = 1105$ ja $b = 2$. Laskemalla nähdään, että $2^{552} \equiv 1 \pmod{1105}$. Koska $1105 \equiv 1 \pmod{8}$, niin $\left(\frac{2}{1105}\right) = 1$. Näin ollen $2^{552} \equiv \left(\frac{2}{1105}\right) \pmod{1105}$. Koska 1105 on yhdistetty luku, se on Eulerin pseudoalkuluku kannan 2 suhteen.*

Lause 3.3.7. *Jos n on Eulerin pseudoalkuluku kannan b suhteen, niin n on pseudoalkuluku kannan b suhteen.*

Todistus. [3, s.368] Jos n on Eulerin pseudoalkuluku kannan b suhteen, niin

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

Korottamalla kongruenssin molemmat puolet toiseen potenssiin, saadaan

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

Koska $\left(\frac{b}{n}\right) = \pm 1$, niin kongruenssi saadaan muotoon

$$b^{n-1} \equiv 1 \pmod{n}.$$

Tällöin n on pseudoalkuluku kannan b suhteen. □

Jokainen pseudoalkuluku ei ole Eulerin pseudoalkuluku. Esimerkissä 3.3.1 osoitimme, että luku 341 ei ole Eulerin pseudoalkuluku kannan 2 suhteen, mutta se on kuitenkin pseudoalkuluku kannan 2 suhteen [3, s.193]. Jokainen Eulerin pseudoalkuluku on kuitenkin pseudoalkuluku.

Lause 3.3.8. *Jos n on vahva pseudoalkuluku kannan b suhteen, niin se on Eulerin pseudoalkuluku kannan b suhteen.*

Ohitamme tässä lauseen 3.3.8 todistuksen. Kiinnostunut lukija löytää sen teoksen [3] sivuilta 369-371.

Vaikka jokainen vahva pseudoalkuluku on Eulerin pseudoalkuluku saman kannan suhteen, jokainen Eulerin pseudoalkuluku ei kuitenkaan ole vahva alkuluku saman kannan suhteen.

Esimerkki 3.3.9. *Esimerkin 3.3.6 perusteella tiedämme, että* 1105 *on Eulerin pseudoalkuluku kannan* 2 *suhteen. Kokonaisluku* 1105 *ei kuitenkaan ole vahva pseudoalkuluku, sillä*

$$2^{\frac{1105-1}{2}} = 2^{552} \equiv 1 \pmod{1105}, \quad \textit{mutta}$$

$$2^{\frac{1105-1}{2^2}} = 2^{276} \equiv 781 \not\equiv \pm 1 \pmod{1105}.$$

Vaikka Eulerin pseudoalkuluku kannan b suhteen ei aina ole vahva alkuluku saman kannan suhteen, tietyillä lisäehdoilla Eulerin pseudoalkuluku kannan b suhteen itseasiassa on vahva alkuluku saman kannan suhteen.

Lause 3.3.10. *Jos $n \equiv 3 \pmod 4$ ja n on Eulerin pseudoalkuluku kannan b suhteen, niin n on vahva pseudoalkuluku kannan b suhteen.*

Todistus. Kongruenssista $n \equiv 3 \pmod 4$ seuraa, että $n - 1 = 2t$, missä $t = \frac{n-1}{2}$ on pariton. Koska n on Eulerin pseudoalkuluku kannan b suhteen, niin

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

Koska $\left(\frac{b}{n}\right) = \pm 1$, tiedetään, että joko $b^t \equiv 1 \pmod n$ tai $b^t \equiv -1 \pmod n$. Näin ollen toinen vahvan pseudoalkuluvun määritelmän kongruensseista toteutuu, joten n on vahva pseudoalkuluku kannan b suhteen.

□

Lause 3.3.11. *Jos n on Eulerin pseudoalkuluku kannan b suhteen, ja $\left(\frac{b}{n}\right) = -1$, niin n on vahva pseudoalkuluku kannan b suhteen.*

Todistus. Merkitään $n - 1 = 2^s t$, missä t on pariton ja s on positiivinen kokonaisluku. Koska n on Eulerin pseudoalkuluku kannan b suhteen, saadaan

$$b^{2^{s-1}t} = b^{\frac{n-1}{2}} \equiv \left(\frac{b}{n}\right) \pmod n.$$

Mutta koska $\left(\frac{b}{n}\right) = -1$, niin

$$b^{t2^{s-1}} \equiv -1 \pmod n.$$

Tämä on toinen vahvan pseudoalkuluvun määritelmässä esiintyvistä kongruensseista. Koska n on yhdistetty luku, se on vahva pseudoalkuluku kannan b suhteen. □

Eulerin pseudoalkulujen käsitettä käyttäen Solovay ja Strassen ovat kehittäneet todennäköisyyteen perustuvan alkulukutestin, johon voi tarkemmin perehtyä teoksen [3] sivuilla 372-375.

3.4 Nollatietotodistukset

[3, s.377-381] Oletetaan, että joku haluaa vakuuttaa jonkun toisen siitä, että hän tietää 200-numeroisen positiivisen kokonaisluvun alkulukukehitelmän paljastamatta kuitenkaan mitä nämä alkulukutekijät ovat. Menetelmä jonka avulla se onnistuu kehitettiin 1980-luvun puolivälissä.

Eräs nykyisessä tietoyhteiskunnassa erittäin tärkeä neliönjäännösten sovellus liittyy tietoturvallisuuteen ja on yleinen menetelmä esimerkiksi identiteetin todentamisessa. Nollatietotodistukseksi kutsutussa menetelmässä on kaksi osapuolta, *todistaja* ja *todentaja.* Todistajalla on hallussaan jotain salassa pidettävää tietoa ja hänen on vakuutettava todentaja siitä, että hänellä on tämä tieto, paljastamatta kuitenkaan mitä tämä tieto pitää sisällään. Todennäköisyys sille, että joku pystyisi huijaamaan todentajaa ja uskottelemaan tietävänsä salaisuuden vaikkei sitä itseasiassa tietäisi, on nollatietotodistusta käytettäessä häviävän pieni. Todentaja ei tämän menetelmän avulla saa selville lähes mitään siitä tiedosta jonka todistaja pitää hallussaan, ja mikä tärkeintä, todentaja ei saa selville mitään sellaista, jonka avulla hän voisi uskotella kolmannelle osapuolelle tietävänsä salaisuuden.

Seuraavissa esimerkeissä käytetään hyväksi sitä seikkaa, että neliöjuuren löytäminen modulo n, missä n on kahden alkuluvun tulo, on helppoa jos alkuluvut tiedetään, mutta hyvin vaikeaa jos niitä ei tiedetä.

Ensimmäisessä esimerkissä käydään läpi tilanne, jossa Paula (todistaja) haluaa vakuttaa Villen (todentaja) siitä, että hän tietää luvun n alkuluku-

kehitelmän. Oletetaan, että n on kahden alkuluvun p ja q tulo. Laskemisen helpottamiseksi oletetaan myös, että sekä p, että q ovat kongruentteja kolmen kanssa modulo 4. Paula siis haluaa vakuuttaa Villen siitä, että hän tietää mitä luvut p ja q ovat niin, ettei Ville saa niitä selville. Käytämme seuraavassa esimerkissä pieniä alkulukuja laskemisen helpottamiseksi, mutta todellisuudessa käytettävät luvut olisivat satojen numeroiden pituisia.

Esimerkki 3.4.1. *Oletetaan, että Paulan salainen tieto on luvun* $n = 103 \cdot 239 = 24617$ *alkulukukehitelmä. Ensimmäisessä vaiheessa Ville valitsee satunnaisen kokonaisluvun* $x = 9134$. *Hän laskee sitten luvun* y, *joka on luvun* x^4 *pienin positiivinen jäännös modulo* n, *ja lähettää sen Paulalle. Siis* $9134^4 \equiv 20682 \pmod{24617}$, *eli* $y = 20682$.

Saatuaan luvun y, *Paula laskee luvun* y *neliönjäännöksen modulo* n. *Tämä onnistuu Paulalta helposti, sillä hän tietää luvut* p *ja* q. *Tämä neliönjäännös on luvun* x^2 *pienin positiivinen jäännös modulo* n. *Paula laskee siis*

$$x^2 \equiv \pm 20682^{\frac{103+1}{4}} = \pm 20682^{26} \equiv \pm 59 \pmod{103}, \quad ja$$

$$x^2 \equiv \pm 20682^{\frac{239+1}{4}} = \pm 20682^{60} \equiv \pm 75 \pmod{239}.$$

Paula löytää siis neljä ratkaisua x^2 *modulo* 24617, *jotka ovat* $x^2 \equiv 2943 \pmod{24617}, x^2 \equiv 11786 \pmod{24617}, x^2 \equiv 12831 \pmod{24617}$, *ja* $x^2 \equiv 21674 \pmod{24617}$. *Näistä ratkaisuista vain* 2943 *on neliönjäännös modulo* 24617.

Paula päättelee siis, että $x^2 \equiv 2943 \pmod{24617}$ *ja lähettää Villelle luvun* 2943.

Ville tarkastaa Paulan vastauksen laskemalla luvun x^2 *jakojäännöksen kun se jaetaan luvulla* n. *Siis* $x^2 = 9134^2 \equiv 2943 \pmod{24617}$.

Nollatietotodistuksen tekniikkaan perustuu myös Shamirin vuonna 1985 kehittämä menetelmä, jolla pyritään varmentamaan todistajan henkilölli-

syys. Menetelmässä oletetaan jälleen, että $n = pq$, missä p ja q ovat kongruentteja 3 modulo 4. Olkoon nyt I jokin positiivinen kokonaisluku, joka edustaa jotain tiettyä informaatiota, kuten vaikkapa henkilötunnusta. Todistaja valitsee pienen luvun c, jolla on sellainen ominaisuus, että kun c liitetään luvun I perään, saatu luku v on neliönjäännös modulo n. Sopiva luku c löydetään kokeilemalla, todennäköisyys sille, että v on neliönjäännös on noin $\frac{1}{2}$. Todistajan on tällöin helppo laskea luku u, joka on luvun v neliöjuuri modulo n, eli $v \equiv u^2 \pmod{n}$.

Käydään seuraavaksi läpi, miten todistaja vakuuttaa todentajan siitä, että hän tietää luvut p ja q.

(i) Paula haluaa nyt todistaa identiteettinsä Villelle valitsemalla satunnaisen luvun r ja lähettämällä Villelle viestin, jossa on ilmoitettu 2 lukua. Ensimmäinen luku on sellainen x, missä $x \equiv r^2 \pmod{n}$, ja $0 \leq x < n$. Toinen luku on sellainen y, että $y \equiv v\bar{x} \pmod{n}$ ja $0 \leq y < n$. Luku $\bar{x}$ on luvun x käänteisalkio modulo n.

(ii) Laskemalla tulon $xy \equiv v \pmod{n}$ Ville saa selville luvun v ja valitsee satunnaisesti bitin $b \in \{0, 1\}$ jonka hän lähettää Paulalle.

(iii) Jos Villen lähettämä bitti on 0, Paula lähettää luvun r Villelle. Jos taas bitti on 1, Paula lähettää Villelle luvun $s \equiv u\bar{r}$ pienimmän positiivisen jäännöksen modulo n.

(iv) Ville laskee Paulan lähettämän luvun neliön. Jos Ville lähetti bitin 0, hän tarkistaa, että neliö on x, eli $r^2 \equiv x \pmod{n}$. Jos hänen lähettämänsä bitti oli 1, hän tarkistaa, että neliö on y, eli $s^2 \equiv y \pmod{n}$. Näin on oltava, sillä $s^2 \equiv u^2\bar{r}^2 \equiv v\bar{r}^2 \equiv xy\bar{r}^2 \equiv r^2y\bar{r}^2 \equiv y \pmod{n}$.

Tämäkin menetelmä perustuu siihen, että todistajan on suhteellisen helppoa laskea luku u, eli luvun v neliöjuuri modulo n, kun taas sellaisen ihmisen joka ei tiedä lukuja p ja q ei ole mahdollista laskea juuria modulo n järkevässä

ajassa.

Tarkastellaan vielä menetelmää esimerkin avulla. Esimerkissä käydään läpi yksi todennuskierros pienillä luvuilla. Todellisuudessa luvut ovat suuria, ja menetelmää toistetaan niin pitkään, että turvallisuudesta voidaan olla riittävän varmoja.

Esimerkki 3.4.2. *Oletetaan nyt, että Paula haluaa todistaa identiteettinsä Villelle osoittamalla, että hän tuntee luvun* $n = 31 \cdot 61 = 1891$ *alkulukutekijät. Hänen henkilökohtainen tunnistenumeronsa on* $I = 391$. *Huomataan, että* 391 *on luvun* 1891 *neliönjäännös, sillä se on sekä luvun* 31, *että luvun* 61 *neliönjäännös. Tällöin Paulan ei tarvitse liittää tunnistenumeroonsa lukua* c, *vaan hän voi suoraan valita luvun* $v = 391$. *Paula saa selville, että luku* $u = 239$ *on luvun* 391 *neliöjuuri modulo* 1891. *Paulan on helppo suorittaa tarvittavat laskut, sillä hän tuntee alkuluvut* 31 *ja* 61.

Ensin Paula valitsee satunnaisen luvun $r = 998$. *Seuraavaksi hän lähettää Villelle kaksi lukua,* $x \equiv r^2 \equiv 998^2 \equiv 1338 \pmod{1891}$ *ja* $y \equiv v\bar{x} \equiv 391 \cdot 1296 \equiv 1839 \pmod{1891}$.

Ville tarkistaa, että $xy \equiv 1338 \cdot 1839 \equiv 391 \pmod{1891}$ *ja lähettää Paulalle satunnaisen bitin, olkoon se nyt* $b = 1$.

Seuraavaksi Paula lähettää Villelle luvun $s \equiv u\bar{r} = 239 \cdot 1855 \equiv 851 \pmod{1891}$. *Lopuksi Ville tarkistaa, että* $s^2 \equiv 851^2 \equiv 1839 \equiv y \pmod{1891}$.

On huomattava, että jos todistaja lähettää todentajalle sekä luvut r, että s, niin todentaja saa selville salaisen tiedon $u = rs$. Tarpeeksi monta kierrosta läpäistyään todistaja on osoittanut, että hän voi pyydettäessä tarjota kumman tahansa luvuista r tai s. Tästä seuraa, että hänen on tunnettava luku u, sillä jokaisella kierroksella hän tuntee sekä luvun r, että luvun s. Todentajan lähettämän bitin satunnaisuus aiheuttaa sen, että kolmannen osapuolen on mahdotonta peukaloida todennusta käyttämällä lukuja, jotka

on ennalta ratkaistu läpäisemään testi. Joku voisi esimerkiksi laskea tunnetun luvun r neliön ja lähettää $x = r^2$, sen sijaan, että valitsisi satunnaisen luvun. Samoin joku voisi valita sellaisen luvun x, että $v\bar{x}$ on tunnettu neliö. Tuntematta lukua u on kuitenkin mahdotonta tehdä ennalta laskelmia siten, että sekä luku x, että luku y ovat tunnettujen lukujen neliöitä.

Koska todentaja valitsee bitin satunnaisesti, todennäköisyys sekä luvulle 0, että luvulle 1 on $\frac{1}{2}$. Jos osapuoli ei tunne lukua u, eli luvun v neliöjuurta, todennäköisyys sille, että hän läpäisee testin yhdellä iteraatiokierroksella on melkein täsmälleen $\frac{1}{2}$. Tästä seuraten todennäköisyys sille, että joku onnistuisi esittämään todistajaa 30 kierrosta, on noin $\frac{1}{2^{30}}$.

Eräs muunnelma tästä tekniikasta tunnetaan nimellä Fiat-Shamirin metodi, joka muodostaa pohjan verifikaatiomenetelmille joita muun muassa älykortit käyttävät henkilökohtaisten tunnistenumeroiden varmennukseen.

Seuraavaksi tarkastellaan miten nollatietotodistusta voidaan käyttää osoittamaan, että jollain on hallussaan tiettyä informaatiota. Oletetaan, että Paulalla on tietoa, jota edustaa lukujono $v_1, v_2, \ldots, v_m$, missä $1 \leq v_j < n$ kun $j = 1, 2, \ldots, m$. Kuten aiemmin n on nyt luku, joka on sellaisten alkulukujen p ja q tulo, jotka ovat kongruentteja kolmen kanssa modulo 4. Paula julkistaa kokonaislukujonon $s_1, s_2, \ldots, s_m$, missä $s_j \equiv \bar{v_j}^2 \pmod{n}$ ja $1 \leq s_j < n$. Paula haluaa vakuuttaa Villen siitä, että hänellä on tieto $v_1, v_2, \ldots, v_m$ paljastamatta tätä tietoa Villelle. Ville tietää vain hänen julkisen modulinsa n ja hänen julkistamansa tiedon $s_1, s_2, \ldots, s_m$.

Esimerkki 3.4.3. *Olkoon Paulalla nyt hallussaan salaisuus, jota edustavat luvut* $v_1 = 1144, v_2 = 877, v_3 = 2001, v_4 = 1221$, *ja* $v_5 = 101$. *Hänen salainen modulonsa on* $n = 47 \cdot 53 = 2491$. *Paulan julkinen tieto muodostuu kokonaisluvuista* s_j, *missä* $s_j \equiv \bar{v_j}^2 \pmod{2491}, 0 < s_j < 2491$ *ja* $j = 1, 2, 3, 4, 5$. *Tällöin hänen julkinen tietonsa koostuu luvuista* $s_1 = 197, s_2 = 2453, s_3 =$

$1553, s_4 = 941, s_5 = 494$.

Todistuksen yksi kierros sisältää neljä askelta, jotka käymme nyt läpi.

(i) Ensiksi Paula valitsee satunnaisen luvun r, olkoon se nyt $r = 1253$. Sitten hän laskee $x = r^2$ ja lähettää Villelle luvun r pienimmän positiivisen neliönjäännöksen x. Nyt $x = 1253^2 \equiv 679 \pmod{2491}$.

(ii) Seuraavaksi Ville valitsee joukosta $\{1, 2, \ldots, m\}$ alijoukon S, jonka hän lähettää Paulalle. Nyt joukko josta hänen on valittava on $\{1, 2, 3, 4, 5\}$. Oletetaan, että Ville valitsee alijoukon $S = \{1, 3, 4, 5\}$ ja lähettää sen Paulalle.

(iii) Sitten Paula laskee luvun y, joka on pienin postitiivinen jäännös modulo n luvun r ja sellaisten lukujen v_j tulosta, missä j kuuluu joukkoon S, eli $y \equiv r \prod_{j \in S} v_j \pmod{n}$, *missä* $0 \leq y < n$.

Nyt Paula laskee luvun

$$y \equiv r v_1 v_3 v_4 v_5 \equiv 1253 \cdot 1144 \cdot 2001 \cdot 1221 \cdot 101 \equiv 68 \pmod{2491},$$

jonka hän lähettää Villelle.

(iv) Viimeisessä vaiheessa Ville varmistaa, että $x \equiv y^2 z \pmod{n}$, *missä z on niiden lukujen s_j tulo, joiden indeksit kuuluvat joukkoon S, eli* $z \equiv \prod_{j \in S} s_j \pmod{n}$, *missä* $0 \leq z < n$.

Ville todentaa tuloksen laskemalla $x \equiv y^2 s_1 s_3 s_4 s_5 \equiv 68^2 \cdot 197 \cdot 1553 \cdot 941 \cdot 494 \equiv 679 \pmod{2491}$.

Ville voi pyytää Paulaa toistamaan tätä menettelyä niin kauan, että hänen mielestään huijauksen todennäköisyys on riittävän pieni.

Ainoa selvä tapa miten todistaja voi tätä menetelmää käytettäessä huijata, eli uskotella todentajalle omaavansa jotain tietoa mitä hänellä ei todellisuudessa ole, on joukon S arvaaminen ennalta. Koska joukosta $\{1, 2, \ldots, m\}$ voidaan muodostaa 2^m erilaista joukkoa, todennäköisyys sille, että todistaja

arvaa yhdellä kierroksella joukon S oikein on $\frac{1}{2^m}$. Kun kierroksia toistetaan T kertaa, todennäköisyys pienenee arvoon $\frac{1}{2^{mT}}$.

Kirjallisuutta

[1] Erickson M. ja Vazzana A.: Introduction to Number Theory (2008).

[2] Adler A. ja Coury, J.E.: The Theory of Numbers (1995).

[3] Rosen K.H.: Elementary Number Theory and Its Applications (1993).

[4] Burton, D.M.: Elementary Number Theory(1997).

[5] Niven I. ja Zuckerman H.S.: An Introduction to theTheory of Numbers(1960).