TAMPEREEN YLIOPISTO
Pro gradu -tutkielma

Piia Ryynänen

Epälineaarisia Diofantoksen yhtälöitä

Matematiikan ja tilastotieteen laitos
Matematiikka
Joulukuu 2010

Tampereen yliopisto
Matematiikan ja tilastotieteen laitos
RYYNÄNEN, PIIA: Epälineaarisia Diofantoksen yhtälöitä
Pro gradu -tutkielma, 30 s.
Matematiikka
Joulukuu 2010

Tiivistelmä

Tämän tutkielman tarkoituksena on perehdyttää lukija Diofantoksen yhtälöihin. Ne ovat kokonaislukukertoimisia yhtälöitä, joille etsitään kokonaislukuratkaisuja. Tutkielman aluksi esitellään muutamia määritelmiä ja lauseita, joita tarvitaan myöhemmin työssä, sekä perehdytään aiheen historiaan. Tämän jälkeen, luvussa 4, tarkastellaan kokonaislukujen esittämistä neliöiden summina. Luvussa 5 käsitellään neljänsien potenssien summia Waringin ongelman sekä Fermat'n suuren lauseen erikoistapauksen $n = 4$ avulla. Viimeisessä, luvussa 6, tarkastellaan Pellin yhtälöä ja siihen liittyen ketjumurtolukuja.

Sisältö

1 Johdanto **4**

2 Esitietoja **4**

3 Diofantoksen yhtälöiden historiaa **6**
3.1 Babylonialaisten algebra 6
3.2 Diofantos ja *Arithmetica* 7

4 Neliöiden summa **8**
4.1 Kahden neliön summa 8
4.2 Neljän neliön summa 11

5 Neljänsien potenssien summa **14**
5.1 Waringin ongelma 14
5.2 Fermat'n suuri lause 15

6 Pellin yhtälö **17**
6.1 Ketjumurtoluvuista 17
6.1.1 Äärelliset ketjumurtoluvut 17
6.1.2 Äärettömät ketjumurtoluvut 21
6.2 Pellin yhtälön ratkaiseminen 25

Viitteet **30**

1 Johdanto

Tämän tutkielman tarkoituksena on perehdyttää lukija Diofantoksen yhtälöihin. Diofantoksen yhtälöt ovat saaneet nimensä kreikkalaiselta matemaatikolta, Diofantos Aleksandrialaiselta. Hän oli kiinnostunut kokonaislukukertoimisista yhtälöistä ja yhtälöryhmistä, joille hän etsi rationaalisia ratkaisuja. Nykyään Diofantoksen yhtälöillä kuitenkin tarkoitetaan yhtälöitä tai yhtälöryhmiä, joille etsitään kokonaislukuratkaisuja.

Diofantoksen yhtälöt voidaan jakaa kahteen ryhmään: lineaarisiin ja epälineaarisiin yhtälöihin. Lineaariset 2. kertaluvun Diofantoksen yhtälöt ovat muotoa

$$ax + by = c,$$

missä $a, b, c \in \mathbb{Z}$. Intialainen matemaatikko Brahmagupta (598-670) oli ensimmäinen, joka esitti yllämainitun yhtälön yleisen ratkaisun. Sen sijaan kaikille epälineaarisille Diofantoksen yhtälöille ei ole olemassa yleistä ratkaisumallia. Tässä työssä tutustutaan muutamaan epälineaariseen Diofantoksen yhtälöön ja todistetaan niihin liittyviä tuloksia. Lukijan oletetaan tuntevan matematiikan yleiset merkintätavat ja hallitsevan algebran alkeet.

Luvussa 2 esitetään muutamia tutkielmassa myöhemmin tarvittavia määritelmiä ja lauseita. Tämän jälkeen, luvussa 3, perehdytään tarkemmin aiheen historiaan sekä Diofantoksen teokseen *Arithmetica*. Luvusta 4 lähtien tutkielmassa seurataan päälähteenä käytetyn Charles Vanden Eyndenin *Elementary Number Theory*-teoksen esitysjärjestystä ja -tapaa. Luvussa 4 tutustutaan kokonaislukujen esittämiseen kokonaislukuneliöiden summana ja todistetaan, että kaikki kokonaisluvut on mahdollista esittää neljän kokonaislukuneliön summana. Viidennessä luvussa perehdytään neljänsien potenssien summiin Waringin ongelman sekä Fermat'n suuren lauseen avulla. Luvussa todistetaan, että jokainen positiivinen kokonaisluku on mahdollista esittää 53 neljännen potenssin summana ja että yhtälöllä

$$x^n + y^n = z^n,$$

missä $x, y, z \in \mathbb{Z}$ ei ole epätriviaaleja ratkaisuja, kun $n = 4$. Itse asiassa yhtälö ei ole ratkeava millään $n > 2$, mutta sitä ei tässä työssä voida sen laajuuden ja syvällisyyden vuoksi todistaa. Tutkielman viimeisessä luvussa käsitellään Pellin yhtälöitä ja niihin liittyen ketjumurtolukuja.

2 Esitietoja

Tässä kappaleessa esitetään muutamia tutkielmassa myöhemmin tarvittavia määritelmiä, merkintätapoja sekä lauseita. Ensimmäisenä määritellään täydellinen jäännössysteemi.

Määritelmä 2.1. Kokonaislukujen joukko $a_1, a_2, ..., a_m$ on *täydellinen jäännössysteemi* modulo m, jos jokainen kokonaisluku on kogruentti täsmälleen yhden alkion a_i, $1 \leq i \leq m$, kanssa modulo m.

Määritellään seuraavaksi luvussa 4 tarvittavat neliönjäännös ja neliönepäjäännös.

Määritelmä 2.2. (Vrt.[2, s. 479]) Olkoon $m \geq 2$ positiivinen kokonaisluku ja a sellainen kokonaisluku, että $(a,\ m) = 1$. Tällöin a on *neliönjäännös modulo m*, jos kogruenssi $x^2 \equiv a \pmod{m}$ on ratkeava; muussa tapauksessa a on *neliönepäjäännös modulo m*.

Esimerkki 2.1. Etsitään kaikki neliönjäännökset modulo 17, kun $x = 1, 2, ..., 16$ seuraavan taulukon avulla

x		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
x^2	$\equiv$	1	4	9	16	8	2	15	13	13	15	2	8	16	9	4	1.

Taulukon toisesta rivistä löydetään ratkaisut: neliönjäännökset modulo 17 ovat 1, 2, 4, 8, 9, 13, 15 ja 16.

Esimerkistä 2.1 huomataan, että kunkin neliönjäännöksen kongruenssiluokka esiintyy jäännössysteemissä kahdesti, ensin jollakin k, $1 \leq k \leq (m-1)/2$ ja toisen kerran, kun $m - k$.

Määritellään seuraavaksi neliönjäännöksiin ja -epäjäännöksiin liittyvä Legendren symboli ja esitetään siihen liittyviä tuloksia.

Määritelmä 2.3. (Vrt.[2, s. 483]) Olkoon p pariton alkuluku ja a sellainen kokonaisluku, että $p \nmid a$. *Legendren symboli* $\left(\frac{a}{p}\right)$ määritellään kaavalla

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

Apulause 2.1. (Vrt. [3, s. 405]) *Olkoon p pariton alkuluku. Tällöin*

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

Apulause 2.2. (Vrt. [3, s. 406]) *Olkoon p pariton alkuluku. Tällöin*

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

Apulauseen 4.2 todistuksessa käytetään seuraavaksi esitettävää Dirichlet'n laatikkoperiaatetta.

Lause 2.1. (Vrt. [3, s. 9]) *Dirichlet'n laatikkoperiaate. Jos k+1 tai useampi esine laitetaan laatikoihin, joita on k kappaletta, vähintään yksi laatikko sisältää kaksi tai useamman esineen.*

Aliluvussa 5.2 tarvitaan Pythagoraan kolmikoita ja niihin liittyviä tuloksia, joita esitetään seuraavaksi.

Määritelmä 2.4. (Vrt. [4, s. 235]) Kokonaislukukolmikko $(x,\ y,\ z)$ on *Pythagoraan kolmikko*, jos se toteuttaa yhtälön $x^2 + y^2 = z^2$. Kolmikko on *primitiivinen Pythagoraan kolmikko*, mikäli lukujen x, y ja z suurin yhteinen tekijä on 1.

Apulause 2.3. (Vrt. [4, s. 237]) *Jos* (x, y, z) *on primitiivinen Pythagoraan kolmikko, niin* $(x, y) = (y, z) = (x, z) = 1$ *ja* x*:stä ja* y*:stä toinen on parillinen ja toinen pariton, ja* z *on pariton.*

Lause 2.2. (Vrt. [4, s. 238]) *Olkoon* (x, y, z) *primitiivinen Pythagoraan kolmikko, jossa* x *on parillinen sekä* y *ja* z *parittomia. Tällöin on olemassa sellaiset kokonaisluvut* u *ja* v*, että* $(u, v) = 1$*. Luvuista* u *ja* v *toinen on parillinen, toinen pariton ja* $u > v$*. Tällöin*

$$x = 2uv,\ y = u^2 - v^2 \text{ ja } z = u^2 + v^2.$$

Toisaalta, jos u *ja* v *ovat mielivaltainen kokonaislukupari, joka toteuttaa yllämainitut ehdot ja jos* x*,* y *ja* z *voidaan määrittää ylläolevilla yhtälöillä, niin silloin* (x, y, z) *on primitiivinen Pythagoraan kolmikko.*

Luvussa 6 esitellään aluksi ketjumurtoluvut, joita tarvitaan myöhemmin Pellin yhtälöihin liittyvissä todistuksissa. Äärettömien ketjumurtolukujen käsittelyssä tarvitaan reaaliluvun lattiafunktiota, joka määritellään seuraavasti.

Määritelmä 2.5. Reaaliluvun *lattia*, merkitään $\lfloor x \rfloor$, on suurin kokonaisluku, joka on pienempi tai yhtä suuri kuin x.

3 Diofantoksen yhtälöiden historiaa

3.1 Babylonialaisten algebra

Diofantoksen yhtälöiden tyyppisistä ongelmista ollaan oltu kiinnostuineita jo paljon ennen Diofantosta. Muinaisen Kaksoisvirranmaan alueelta on löydetty savitauluja ajalta 2000 - 600 eaa., joista selviää, että babylonialaisten algebrassa oli samoja piirteitä kuin noin 250 jaa. eläneen Diofantoksen *Arithmeticassa*. Babylonialaiset olivat kiinnostuineita yhtälöistä ja yhtälöryhmistä, ja he muun muassa tunsivat täydellisen kolmitermisen toisen asteen yhtälön ratkaisukaavan ja osasivat käyttää sitä. Säilyneistä savitauluista on myös selvinnyt, että he pystyivät ratkaisemaan joitain kolmannen asteen yhtälöitä. Selkein yhteys Diofantokseen on kuitenkin taulu, jonka taulukoita voisi helposti luulla kaupan tilikirjoiksi. Tarkempi tarkastelu on kuitenkin osoittanut,

että savitauluun on taulukoituna Pythagoraan kolmikoita vastaavia lukuja. Pythagoraan kolmikko on triadi, jonka suurimman luvun neliö on yhtä suuri kuin kahden pienemmän luvun neliöiden summa. Triadin lukuja voidaan käyttää kuvaamaan suorakulmaisen kolmion sivuja. Babylonialaiset siis mitä todennäköisimmin tunsivat ensimmäiset 38 Pythagoraan kolmikkoa. [1, s. 60-70]

Babylonialaisten matemaattisiksi heikkouksiksi todettakoon yleisien tapauksien puute, he käsittelivät aina erikoistapauksia. Babylonialaiset myös sekoittivat tarkat ja epätarkat arvot, esimerkiksi mittaustuloksien ja tarkkojen arvojen eroa ei huomioitu. [1, s. 75-77]

Babylonialaisten matematiikka, muun muassa heidän kehittämänsä lukujen paikkajärjestelmä, vaikutti epäilemättä seuraavien vuosisatojen matematiikkaan, vaikkakin helleeninen matematiikka oli geometriakeskeisempää kuin babylonialaisten käyttämä. Noin 250 jaa vaikuttanut Diofantos poikkesi aikalaisistaan ja hänen *Arithmetica*-teoksensa muistuttaa jonkin verran babylonialaista algebraa.

3.2 Diofantos ja *Arithmetica*

Diofantos Aleksandrialainen eli siis todennäköisesti vuoden 250 jaa tienoilla, mutta vuosisataa aikaisempia ja myöhempiäkin ajankohtia on esitetty. Hänen elämänsä yksityiskohdista ei tiedetä juuri mitään. 400- tai 500-luvulta peräisin olevassa ongelmakokoelmassa ”Kreikkalainen antologia” kerrotaan tarinan muodossa ongelma, josta selviää, että Diofantos olisi elänyt 84-vuotiaaksi. [1, s. 260-261]

Tunnetuista Diofantoksen töistä tärkein on *Arithmetica*, joka sisälsi alunperin kolmetoista kirjaa, mutta joista vain kuusi on säilynyt. *Arithmetica* on algebran soveltamiseen liittyvien ongelmien kokoelma. Teoksen kaikki ongelmat on ratkaistu numeeristen esimerkkien avulla, vaikka kirjoittaja ehkä pyrkikin metodin yleisyyteen. Se poikkesi aikansa kreikkalaisesta matematiikasta melkoisesti, ja muistuttaakin enemmän babylonialaista algebraa. Babylonialaiset kuitenkin keskittyivät määrättyjen yhtälöiden likimääräisiin ratkaisuihin, kun taas Diofantoksen *Arithmetica* on omistettu lähes kokonaan sekä yksikäsitteisen ratkaisun tuottavien yhtälöiden että sellaisten yhtälöiden, joiden ratkaisujoukko on ääretön, täsmällisille ratkaisuille. Näitä kahta yhtälötyyppiä ei teoksessa kuitenkaan selkeästi eroteta toisistaan, ja jälkimmäisillekin annetaan vain yksi ratkaisu. Postulaatteja teoksessa ei esitetä eikä ongelmien kaikkia mahdollisia ratkaisuja yritetä löytää. [1, s. 261-265]

Diofantosta kutsutaan usein algebran isäksi, vaikka valtaosa hänen tutkimuksista ei kuulu nykyisiin algebran alkeisiin vaan lukuteoriaan. Algebran isäksi kutsuminen perustuukin hänen käyttämiinsä merkintöihin. Nykyään algebra perustuu lähes yksinomaan symbolimuodossa esitettyihin väitteisiin, ei tavanomaiseen puhuttuun kieleen, jota varhaisempi kreikkalainen matematiikka ja kirjallisuus käyttivät. Diofantos oli tiettävästi ensimmäinen, joka

käytti teoksessaan systemaattisesti symboleita. [1, s. 264]

4 Neliöiden summa

Matemaatikot ovat vuosisatojen ajan pohtineet kokonaislukujen ominaisuuksia, muun muassa kokonaisluvun esittämistä neliöiden summana. Diofantos, Fermat, Euler ja Lagrange ovat matemaatikkoja, jotka ovat pohdinnoillaan edesauttaneet näiden ongelmien ratkaisemista. Tässä luvussa vastataan kahteen kiinnostavaan kysymykseen: Mitkä kokonaisluvut on mahdollista esittää kahden neliön summana? Ja mikä on pienin luonnollinen luku n, jolla kaikki positiiviset kokonaisluvut voidaan esittää n:n neliön summana?

4.1 Kahden neliön summa

Kaikkia kokonaislukuja ei voida esittää kahden kokonaislukuneliön summana, kuten esimerkistä 4.1 selviää.

Esimerkki 4.1. Tarkastellaan lukuja 1-10 ja niiden esittämistä kahden neliön summana. Nyt

$1 = 0^2 + 1^2$	6 ei ole kahden neliön summa
$2 = 1^2 + 1^2$	7 ei ole kahden neliön summa
3 ei ole kahden neliön summa	$8 = 2^2 + 2^2$
$4 = 0^2 + 2^2$	$9 = 0^2 + 3^3$
$5 = 1^2 + 2^2$	$10 = 1^2 + 3^2$.

Itse asiassa kokonaislukuja, joita ei voida esittää kahden neliön summana on ääretön määrä. Tämä todistetaan lauseessa 4.1.

Lause 4.1. *Olkoon k mielivaltainen kokonaisluku. Tällöin*

$$k^2 \equiv 0 \text{ } tai \text{ } 1 \pmod 4.$$

Todistus. Oletetaan ensin, että k on parillinen. Tällöin $k = 2l$, missä $l \in \mathbb{Z}$, ja $k^2 = (2l)^2 = 4l^2 \equiv 0 \pmod 4$. Oletetaan sitten, että k on pariton. Tällöin $k = 2l + 1$, missä $l \in \mathbb{Z}$, ja $k^2 = (2l + 1)^2 = 4l^2 + 4l + 1 = (4(l^2 + l) + 1) \equiv 1 \pmod 4$. □

Nyt lauseesta 4.1 nähdään, että $a^2 + b^2 \equiv 0$, 1 tai 2 (mod 4), joten kokonaislukuja, jotka ovat muotoa $4k+3$ ei voida esittää kahden kokonaislukuneliön summana. Tämä ei kuitenkaan ole vielä riittävä ehto sille, mitkä kokonaisluvut voidaan esittää kahden neliön summana, sillä kuten esimerkistä 4.1 selvisi, luku 6 ei ole kahden neliön summa, mutta sitä ei kuitenkaan voida ilmaista muodossa $4k+3$, kun $k \in \mathbb{Z}$. Pohditaan seuraavaksi, mitkä kokonaisluvut on sitten mahdollista esittää kahden neliön summana. Tätä pohdintaa varten tarvitaan apulauseiden 4.1 - 4.2 tuloksia.

Apulause 4.1. *Jos m ja n ovat kumpikin kahden neliön summia, niin myös mn on.*

Todistus. (Vrt.[3, s. 529]) Olkoon $m = a^2 + b^2$ ja $n = c^2 + d^2$. Tällöin

$$\begin{aligned} mn &= (a^2 + b^2)(c^2 + d^2) = a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 \\ &= a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 + 2abcd - 2abcd = (ac + bd)^2 + (ad - bc)^2. \end{aligned}$$

□

Esimerkki 4.2. Esimerkin 4.1 perusteella tiedetään, että luvut 5 ja 8 ovat kahden neliön summia. Nyt apulauseen 4.1 nojalla myös $5 \cdot 8 = 40$ on kahden neliön summa. Kun valitaan $a = 1$, $b = 2$, $c = 2$ ja $d = 2$, saadaan

$$40 = 5 \cdot 8 = (1^2 + 2^2)(2^2 + 2^2) = (2 + 4)^2 + (2 - 4)^2 = 6^2 + (-2)^2.$$

Apulauseesta 4.1 voidaan päätellä, että selvittääksemme, mitkä luvut ovat kahden neliön summia, on tarpeen selvittää, mitkä alkuluvut ovat kahden neliön summia. Apulause 4.2 vastaa tähän kysymykseen.

Apulause 4.2. *Alkuluku p on kahden neliön summa, jos ja vain jos $p = 2$ tai $p \equiv 1 \pmod 4$.*

Todistus. (Vrt.[4, s. 243]) Esimerkistä 4.1 nähdään, että $2 = 1^2 + 1^2$, ja lisäksi tiedetään, että mitään lukua, joka on kongruentti luvun 3 kanssa modulo 4, ei voida esittää kahden neliön summana. Tarvitsee siis vain osoittaa, että kaikki alkuluvut $p \equiv 1 \pmod 4$ ovat kahden neliön summia.

Nyt apulauseen 2.2 nojalla tiedetään, että $\left(\frac{-1}{p}\right) = 1$ eli on olemassa sellainen kokonaisluku x, että $x^2 \equiv -1 \pmod p$ tai $x^2 + 1 \equiv 0 \pmod p$.

Tutkitaan seuraavaksi kaikkia kokonaislukuja $rx+s$, missä $0 \leq r \leq \sqrt{p}$ ja $0 \leq s \leq \sqrt{p}$. Koska sekä r että s voivat saada myös arvon 0, mahdollisia luvun r arvoja on enemmän kuin $\sqrt{p}$ ja luvun s arvoja on enemmän kuin $\sqrt{p}$. Tästä johtuen pareja r, s on enemmän kuin $\sqrt{p}\sqrt{p} = p$. Nyt esitiedoissa esitetyn laatikkoperiaatteen mukaan ainakin kaksi lukua $rx+s$ on kongruentteja (mod p) seuraavasti:

$$r_1x + s_1 \equiv r_2x + s_2 \pmod p,$$

missä $r_1x + s_1 \neq r_2x + s_2$. Järjestetään alkiot ja kirjoitetaan

$$(r_1 - r_2)x \equiv s_2 - s_1 \pmod p.$$

Merkitään nyt $u = |r_1 - r_2|$ ja $v = |s_2 - s_1|$, jolloin edellinen yhtälö voidaan esittää muodossa

$$ux \equiv \pm v \pmod p.$$

Koska $r_1x + s_1 \neq r_2x + s_2$, niin u ja v eivät voi molemmat olla 0. Kun nyt $x^2 + 1 \equiv 0 \pmod p$ kerrotaan puolittain luvulla u^2 saadaan

$$0 \equiv u^2(x^2 + 1) \equiv (ux)^2 + u^2 \equiv v^2 + u^2 \pmod p.$$

Luku v^2+u^2 on siis jokin luvun p positiivinen moninkerta. Toisaalta $v^2+u^2 < (\sqrt{p})^2+(\sqrt{p})^2 = 2p$, joten täytyy olla $v^2+u^2 = p$. Tämä todistaa, että p on kahden neliön summa. □

Apulauseen 4.2 tulos on ratkaisevassa asemassa etsittäessä kaikkia kokonaislukuja, jotka voidaan esittää kahden neliön summana. Tuloksen esitti ensimmäisenä Albert Girard (1595-1632), ja Pierre de Fermat (1601-1665) väitti todistaneensa sen. Leonhard Euler (1707-1783) oli kuitenkin ensimmäinen, joka julkaisi todistuksen vuonna 1754. Todistetaan seuraavaksi lause, josta selviää mitkä kokonaisluvut on mahdollista esittää kahden kokonaislukuneliön summana.

Lause 4.2. *Positiivinen kokonaisluku n voidaan esittää kahden neliön summana, jos ja vain jos sen muotoa $4k+3$ oleva alkutekijä ei esiinny luvun n alkutekijähajoitelmassa paritonta kertaa.*

Todistus. (Vrt. [4, s. 244]) Oletetaan aluksi, että muotoa $4k+3$ olevat alkuluvut eivät esiinny paritonta kertaa alkutekijähajotelmassa. Tällöin voidaan kirjoittaa

$$n = hp_1p_2\cdots p_t,$$

missä h sisältää kaikki muotoa $4k+3$ olevat alkuluvut ja kukin alkuluvuista $p_1, p_2, ..., p_t$ on joko 2 tai muotoa $4k+1$ eli kongruentti yhden kanssa modulo 4. Oletuksen mukaan kaikki luvun h alkutekijät esiintyvät parillisina potensseina, joten $h = j^2$. Nyt haluttu tulos saadaan, kun käytetään apulauseen 4.1 tulosta ja huomataan, että $h = 0^2+j^2$ ja että $p_1, p_2, ..., p_t$ ovat apulauseen 4.2 nojalla kahden neliön summia.

Oletetaan sitten että $n = u^2+v^2$. Olkoon $d = (u,\ v)$, $U = \frac{u}{d}$, $V = \frac{v}{d}$ ja $N = \frac{n}{d^2}$. Nyt U, V ja N ovat kokonaislukuja, $(U,\ V) = 1$ ja $N = U^2+V^2$. Toisaalta oletetaan, että on olemassa alkuluku p, jolle $p \equiv 3 \pmod 4$ ja jolla on luvun n alkutekijähajotelmassa pariton, muotoa $(2i+1)$ oleva potenssi. Olkoon p^m luvun p suurin potenssi, joka jakaa luvun d. Tällöin N on jaollinen luvulla $p^{2i-2m+1}$ ja $2i-2m+1$ on vähintään 1, koska i ja m ovat positiivisia kokonaislukuja, joten $p|N$. Tiedetään, että p ei jaa lukua U, sillä silloin se jakaisi myös luvun V, mutta $(U,\ V) = 1$. On siis olemassa kokonaisluku x siten, että $xU \equiv 1 \pmod p$. Nyt kertomalla yhtälö $N = U^2+V^2$ puolittain luvulla x^2 ja käyttämällä tietoa $p|N$ saadaan

$$1 + (xV)^2 \equiv 0 \pmod p.$$

Yllä oleva voidaan kirjoittaa myös muodossa $(xV)^2 \equiv -1 \pmod p$. Tämä on kuitenkin ristiriidassa lauseen 2.2 kanssa, sillä -1 ei ole neliönjäännös, kun $p \equiv 3 \pmod 4$. Näin ollen, muotoa $p \equiv 3 \pmod 4$ oleva alkuluku p ei voi esiintyä n alkutekijähajotelmassa kuin parillisina potensseina. □

Nyt voidaan selittää, miksi esimerkin 4.1 luvut 3, 6 ja 7 eivät ole kahden neliön summia. Lukujen 3 ja 6 alkutekijähajotelmissa esiintyy luku 3

parittomana potenssina ja luvussa 7 luku 7. Tutkitaan asiaa vielä esimerkin avulla.

Esimerkki 4.3. Tutkitaan, onko luku 5445 kahden neliön summa, ja jos on, määritetään, minkä kahden neliön.

Hajotetaan aluksi luku 5445 alkulukutekijöihinsä eli $5445 = 5 \cdot 3^2 \cdot 11^2$. Luku $5 \equiv 1 \pmod 4$ ja luvut 3 ja 11 ovat kogruentteja luvun 3 kanssa (mod 4). Luvut 3 ja 11 kuitenkin esiintyvät parillisina potensseina alkutekijähajoitelmassa, joten luku 5445 on mahdollista esittää kahden neliön summana.

Koska $5 = 2^2 + 1^2$, saadaan

$$5445 = (11 \cdot 3)^2(2^2 + 1^2) = (11 \cdot 3 \cdot 2)^2 + (11 \cdot 3 \cdot 1)^2 = 66^2 + 33^2.$$

Seuraava kiinnostava kysymys on, että mikä on pienin luonnollinen luku n, jolla kaikki positiiviset kokonaisluvut voidaan esittää n:n neliön summana? Helposti huomataan, että lukua 7 ei voida esittää kolmen neliön summana, joten tarkastellaan seuraavaksi tapausta $n = 4$.

4.2 Neljän neliön summa

Tässä aliluvussa todistetaan, että kaikki kokonaisluvut voidaan esittää neljän neliön summana. On mahdollista, että jo Diofantos tunsi tämän tuloksen, vaikkei hän sitä selvästi tunnetuissa kirjoituksissaan ilmaisekaan. Fermat väitti todistaneensa tuloksen, mutta ei julkaissut mahdollista todistustaan. Eulerin oppilas Joseph Louis Lagrage (1736-1813) oli ensimmäinen, joka julkaisi todistuksen vuonna 1772. Hän käytti todistuksessaan monia Eulerin välituloksia. Yksi niistä on seuraavaksi esitettävä apulause 4.3. [4, s. 267]

Apulause 4.3. *Kahden neljän neliön summana esitettävän luvun tulo on myös neljän neliön summa.*

Todistus. (Vrt. [4, s. 247]) Olkoon $X = a^2 + b^2 + c^2 + d^2$ ja $Y = A^2 + B^2 + C^2 + D^2$. Nyt

$$\begin{aligned} XY &= (a^2 + b^2 + c^2 + d^2)(A^2 + B^2 + C^2 + D^2) \\ &= a^2A^2 + a^2B^2 + a^2C^2 + a^2D^2 + b^2A^2 + b^2B^2 + b^2C^2 + b^2D^2 \\ &+ c^2A^2 + c^2B^2 + c^2C^2 + c^2D^2 + d^2A^2 + d^2B^2 + d^2C^2 + d^2D^2 \\ &= (aA + bB + cC + dD)^2 + (aB - bA + cD - dC)^2 \\ &+ (aC - bD - cA + dB)^2 + (aD + bC - cB - dA)^2. \end{aligned}$$

□

Nyt apulauseen 4.3 nojalla riittää todistaa, että kaikki alkuluvut on mahdollista esittää neljän neliön summana. Lauseen 4.2 perusteella kuitenkin tiedetään, että vain alkulukuja, jotka ovat kongruentteja luvun 3 kanssa (mod

4) ei pystytä esittämään kahden neliön summana. Muut luvut on mahdollista esittää kahden ja siten myös neljän neliön summana. Riittää siis tarkastella vain muotoa $4k + 3$ olevia alkulukuja.

Apulause 4.4. *Olkoon p sellainen alkuluku, että $p \equiv 3$ (mod 4). Tällöin on olemassa kokonaisluku k, $0 < k < p$, niin, että kp on neljän neliön summa.*

Todistus. (Vrt. [4, s. 247]) Olkoon t pienin positiivinen kokonaisluku, joka on neliönepäjäännös modulo p. Selvästi nähdään, että $t > 1$. Nyt apulauseiden 2.1 ja 2.2 avulla saadaan

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

Eli $-t$ on neliönjäännös (mod p), joten on olemassa kokonaisluku x siten, että $x^2 \equiv -t \pmod{p}$. Kuten esimerkistä 2.1 huomattiin, kukin neliönjäännös esiintyy kogruenssiluokassa (mod p) kahdesti. Näin ollen x voidaan rajata välille $0 < x < \frac{p}{2}$.

Nyt, koska t on pienin positiivinen neliönepäjäännös modulo p, täytyy $t-1$ olla neliönjäännös modulo p. On siis olemassa kokonaisluku y siten, että $y^2 \equiv t - 1 \pmod{p}$ ja $0 < y < \frac{p}{2}$. Tällöin

$$x^2 + y^2 + 1 \equiv -t + (t-1) + 1 \equiv 0 \pmod{p},$$

joten $x^2 + y^2 + 1 = kp$, missä k on jokin positiivinen kokonaisluku. Mutta nyt

$$kp = x^2 + y^2 + 1 < \left(\frac{p}{2}\right)^2 + \left(\frac{p}{2}\right)^2 + 1 = \frac{p^2}{2} + 1 < \frac{p^2}{2} + \frac{p^2}{2} = p^2,$$

joten $k < p$. Nyt siis $kp = x^2 + y^2 + 1^2 + 0^2$. □

Seuraava esimerkki havainnollistaa apulauseen 4.4 tulosta.

Esimerkki 4.4. Olkoon $p = 11$. Nyt $1^2 = 1$, $2^2 = 4$, $3^2 = 9$, $4^2 \equiv 5 \pmod{11}$, $5^2 \equiv 3 \pmod{11}$ ja $6^2 \equiv 3 \pmod{11}$. Nähdään, että luku 2 on pienin positiivinen neliönepäjäännös modulo 11. Merkitään $t = 2$. Koska $-t = -2 \equiv 9 \equiv 3^2 \pmod{11}$, valitaan $x = 3$. Toisaalta $t - 1 = 1 \equiv 10^2 \pmod{11}$, joten $y = 10$. Tällöin $x^2 + y^2 + 1 = 3^2 + 10^2 + 1 = 110 = 10 \cdot 11$, joten $k = 10 < p$.

Lause 4.3. *Kaikki positiiviset kokonaisluvut voidaan esittää neljän neliön summana.*

Todistus. (Vrt. [4, s. 248]) Tiedetään, että riittää todistaa, että jokainen muotoa $4k+3$ oleva alkuluku voidaan esittää neljän neliön summana. Olkoon nyt p tällainen alkuluku. Apulauseen 4.4 perusteella tiedetään, että on olemassa positiivinen kokonaisluku $k < p$ siten, että kp on neljän neliön summa.

Valitaan nyt kaikista tällaisista kokonaisluvuista k pienin, ja merkitään sitä luvulla m. Nyt siis

$$mp = a^2 + b^2 + c^2 + d^2,$$

missä $0 < m < p$. Osoitetaan aluksi, että m on pariton. Jos m olisi parillinen, niin silloin kokonaisluvuista a, b, c ja d täsmälleen ei yhdenkään, kahden tai kaikkien tulisi olla parillisia. Jos kaksi luvuista, esimerkiksi a ja b ovat parillisia, niin silloin $a - b$, $a + b$, $c - d$ ja $c + d$ ovat kaikki parillisia. Mutta silloin

$$\left(\frac{a-b}{2}\right)^2 + \left(\frac{a+b}{2}\right)^2 + \left(\frac{c-d}{2}\right)^2 + \left(\frac{c+d}{2}\right)^2 = \frac{a^2+b^2+c^2+d^2}{2} = \frac{m}{2} \cdot p,$$

mikä on ristiriidassa luvun m määrittelyn kanssa.

Jos $m = 1$, p on neljän neliön summa. Tehdään siis oletus, että $m > 1$. Koska m peräkkäistä kokonaislukua

$$-\frac{m-1}{2}, -\frac{m-1}{2} + 1, ..., 0, 1, ..., \frac{m-1}{2}$$

muodostaa esitiedoissa määritellyn täydellisen jäännössysteemin modulo m, voidaan systeemistä valita luvut A, B, C ja D siten, että

$$A \equiv a, \quad B \equiv b, \quad C \equiv c \text{ ja } D \equiv d \pmod{m}.$$

Jokainen luvuista A, B, C ja D on pienempi kuin $\frac{m}{2}$. Tällöin

$$A^2 + B^2 + C^2 + D^2 \equiv a^2 + b^2 + c^2 + d^2 = mp \equiv 0 \pmod{m}.$$

Olkoon $A^2 + B^2 + C^2 + D^2 = rm$. Luku $r > 0$, sillä jos kaikki luvuista A, B, C ja D olisivat 0, m jakaisi kunkin luvuista a, b, c ja d. Mutta silloin m^2 jakaisi luvun $a^2 + b^2 + c^2 + d^2 = mp$, mikä on mahdotonta, sillä $1 < m < p$. Huomataan myös että

$$rm = A^2 + B^2 + C^2 + D^2 < 4\left(\frac{m}{2}\right)^2 = m^2,$$

joten $r < m$. Nyt kun kerrotaan mp ja rm keskenään ja käytetään apulauseen 4.3 tulosta, saadaan

$$(mp)(rm) = (a^2 + b^2 + c^2 + d^2)(A^2 + B^2 + C^2 + D^2) = w^2 + x^2 + y^2 + z^2,$$

missä

$$\begin{aligned}
w &= aA + bB + cC + dD \equiv a^2 + b^2 + c^2 + d^2 = mp \equiv 0 \pmod{m},\\
x &= aB - bA + cD - dC \equiv ab - ba + cd - dc \equiv 0 \pmod{m},\\
y &= aC - bD + cA - dB \equiv ac - bd - ca + db \equiv 0 \pmod{m},\\
z &= aD + bC - cB - dA \equiv ad + bc - cb - da \equiv 0 \pmod{m}.
\end{aligned}$$

Mutta nyt

$$rp = \left(\frac{w}{m}\right)^2 + \left(\frac{x}{m}\right)^2 + \left(\frac{y}{m}\right)^2 + \left(\frac{z}{m}\right)^2,$$

mikä on ristiriidassa luvun m valinnan kanssa, sillä $0 < r < m$. Näin ollen $m = 1$ ja lause todistettu. □

5 Neljänsien potenssien summa

5.1 Waringin ongelma

Englantilainen matemaatikko Edward Waring (1734-1793) julkaisi vuonna 1770 kirjan *Meditationes algebricae*, jossa hän esitti ongelman, joka tänä päivänä tunnetaan Waringin ongelmana tai probleemana. Sen mukaan jokainen positiivinen kokonaisluku on neljän neliön, yhdeksän kuution jne. summa. Toisin sanoen jokaista lukua $k > 1$ kohti on olemassa sellainen vakio $g(k)$, että jokainen luonnollinen luku voidaan esittää enintään $g(k)$:n luonnollisen luvun k:nnen potenssin summana. Tämän todisti vasta vuonna 1909 saksalainen David Hilbert. Hilbertin todistus on monimutkainen, eikä sitä tässä tutkielmassa esitetä, mutta todettakoon, että se ei anna $g(k)$:n lauseketta. Edellisessä luvussa, lauseessa 4.3 todistettiin tapaus $g(2) = 4$. Vuonna 1912 A. Wieferich ja A. J. Kempner osoittivat, että $g(3) = 9$. Seuraavan lauseen tuloksen, $g(4) \leq 53$, osoitti ensimmäisenä vuonna 1859 ranskalainen matemaatikko Joseph Liouville (1809-1882). [4, s. 251]

Lause 5.1. *Jokainen positiivinen kokonaisluku on mahdollista esittää 53 neljännen potenssin summana.*

Todistus. (Vrt. [4, s. 251]) Todistusta varten tarvitaan seuraavaa tietoa

$$\begin{aligned} 6(a^2+b^2+c^2+d^2)^2 &= 6(a^4+a^2b^2+a^2c^2+a^2d^2+a^2b^2+b^4+b^2c^2+b^2d^2 \\ &\quad + a^2c^2+b^2c^2+c^4+c^2d^2+a^2d^2+b^2d^2+c^2d^2+d^4) \\ &= 6(a^4+b^4+c^4+d^4) \\ &\quad + 12(a^2b^2+a^2c^2+a^2d^2+b^2c^2+b^2d^2+c^2d^2). \end{aligned}$$

Koska $(a \pm b)^4 = a^4 \pm 4a^3b + 6a^2b^2 \pm 4ab^3 + b^4$, voidaan ylläoleva esittää 12 neljännen potenssin summana seuraavasti

$$\begin{aligned} 6(a^2+b^2+c^2+d^2)^2 &= (a+b)^4 + (a-b)^4 + (a+c)^4 + (a-c)^4 + (a+d)^4 \\ &\quad + (a-d)^4 + (b+c)^4 + (b-c)^4 + (b+d)^4 + (b-d)^4 \\ &\quad + (c+d)^4 + (c-d)^4. \end{aligned}$$

Lauseen 4.3 perusteella tiedetään, että jokainen kokonaisluku on mahdollista esittää neljän neliön summana, merkitään $a^2+b^2+c^2+d^2$. Nyt todistuksen

alussa esitetyn yhtälön perusteella kaikki luvut, jotka ovat 6 kertaa neliö, voidaan esittää 12 neljännen potenssin summana.

Olkoon nyt n mielivaltainen kokonaisluku. Se voidaan esittää muodossa $n = 6q + r$, missä $0 \leq r < 6$. Koska q on kokonaisluku, se voidaan lauseen 4.3 perusteella kirjoittaa muotoon $w^2 + x^2 + y^2 + z^2$, jolloin saadaan

$$n = 6w^2 + 6x^2 + 6y^2 + 6z^2 + r.$$

Nyt neljä ensimmäistä termiä voidaan kirjoittaa 12 neljännen potenssin summana. Luku r, joka on korkeintaan 5, voidaan kirjoittaa viiden neljännen potenssin summana. Näin ollen n on $12 + 12 + 12 + 12 + 5 = 53$ neljännen potenssin summa. □

Liouvillen tulosta tarkensi vuonna 1974 H. E. Thomas, joka osoitti, että $g(4) \leq 22$. Vuonna 1986 R. Balasubramanian, J. Deshouillers ja F. Dress osoittivat, että $g(4) = 19$. Tiedetään myös, että $g(5) = 37$, $g(6) = 73$, $g(7) = 143$, $g(8) = 279$ ja $g(9) = 548$. [2, s. 565]

5.2 Fermat'n suuri lause

Pierre de Fermat (1601-1665) kuuluu matematiikan historian suuriin nimiin. Tämä perustuu hänen geometrian, analyysin sekä lukuteorian alalla saavuttamiinsa tuloksiin. Fermat oli toulouselainen juristi, joka tutki vapaa-aikanaan matematiikkaa. Fermat ei julkaissut suurinta osaa matemaattisista saavutuksistaan, vaan ne tulivat julki vasta hänen kuolemansa jälkeen. [5, s. 46]

Fermat muun muassa kehitti todistusmenetelmän, "äärettömän laskeutumisen", joka on eräänlainen takaperoinen induktio. Fermat todisti sen avulla muun muassa, että ei ole olemassa yhtälön $x^4 + y^4 = z^4$ toteuttavia positiivisia kokonaislukuja x, y ja z. Tässä tutkielmassa esitetään tuo tulos ja todistus lauseessa 5.2. Fermat ilmoitti Diofantoksen Arithmetican käännöksen marginaaliin tekemässään lisäyksessä osaavansa todistaa myös, että yhtälöllä $x^n + y^n = z^n$ ei ole ratkaisua, kun $n > 2$, mutta marginaalin tila ei riittänyt todistuksen esittämiseen. Tämä Fermat'n suuren lauseen nimellä tunnettu hypoteesi kiehtoi ammatti- ja amatöörimatemaatikkoja yli 300 vuoden ajan. Vuonna 1995 englantilainen matemaatikko Andrew Wiles (1953-) vihdoin todisti lauseen todeksi. Useimmat Fermat'n ilman todistusta ilmoittamista tuloksista ovat lopulta osoittautuneet oikeiksi. [5, s. 46-47]

Tarkastellaan siis tapausta $x^4 + y^4 = z^4$. Kun merkitään $z^2 = w$, saadaan yhtälö muotoon $x^4 + y^4 = w^2$.

Lause 5.2. *Yhtälöllä $x^4 + y^4 = w^2$ ei ole positiivisia kokonaislukuratkaisuja.*

Todistus. (Vrt. [4, s. 252]) Osoitetaan, että jos yhtälöllä $x^4 + y^4 = w^2$ on kokonaislukuratkaisut x, y ja w, niin tällöin on olemassa myös toiset ratkaisut X, Y ja W siten, että $W < w$.

1. Olkoon p alkuluku, joka jakaa luvut x, y ja w. Tällöin p^4 jakaa luvun $x^4 + y^4 = w^2$, joten p^2 jakaa luvun w. Niinpä

$$\left(\frac{x}{p}\right)^4 + \left(\frac{y}{p}\right)^4 = \left(\frac{w}{p^2}\right)^2,$$

joten $X = \frac{x}{p}$, $Y = \frac{y}{p}$, $W = \frac{w}{p^2}$ on myös ratkaisu ja $W < w$.

2. Oletetaan nyt, että yksikään alkuluku ei jaa kaikkia lukuja x, y ja w. Tällöin

$$(x^2)^2 + (y^2)^2 = w^2$$

ja x^2, y^2 ja w muodostavat esitiedoissa määritellyn primitiivisen Pythagoraan kolmikon. Apulauseen 2.3 perusteella tiedetään, että x^2, y^2 ja w, kuten myös x, y ja w ovat suhteellisia alkulukuja pareittain. Tiedetään myös, että toinen luvuista x^2 ja y^2 on parillinen, toinen pariton ja että w on pariton. Oletetaan, että x^2 on parillinen eli x on parillinen ja y on pariton. Nyt lauseesta 2.2 seuraa, että on olemassa positiiviset kokonaisluvut u ja v siten, että $(u, v) = 1$ ja

$$x^2 = 2uv, \quad y^2 = u^2 - v^2 \quad \text{ja} \quad w = u^2 + v^2.$$

Käytetään nyt uudestaan näitä esitiedoissa esitettyjä tuloksia yhtälöön $y^2+v^2 = u^2$. Huomataan, että y, v ja u muodostavat myös primitiivisen Pythagoraan kolmikon, ja koska y on pariton, täytyy luvun v olla parillinen ja u:n pariton. Tällöin on olemassa positiiviset kokonaisluvut r ja s siten, että $(r, s) = 1$ ja

$$v = 2rs, \quad y = r^2 - s^2 \quad \text{ja} \quad u = r^2 + s^2.$$

Koska v on parillinen, voidaan kirjoittaa $v = 2t$, jolloin $x^2 = 2uv = 4ut$. Kun jaetaan luvulla 4 ja sijoitetaan $t = \frac{v}{2}$ saadaan

$$\left(\frac{x}{2}\right)^2 = u\frac{v}{2}.$$

Nyt $(u, \frac{v}{2}) = 1$ ja tiedetään, että kahden suhteellisen alkuluvun tulo on neliö vain, jos molemmat tekijät ovat neliöitä. On siis olemassa positiiviset kokonaisluvut W ja Z siten, että $u = W^2$ ja $\frac{v}{2} = Z^2$. Kirjoitetaan nyt yhtälö $v = 2rs$ muotoon $rs = \frac{v}{2} = Z^2$. Koska $(r, s) = 1$, on olemassa positiiviset kokonaisluvut X ja Y siten, että $r = X^2$ ja $s = Y^2$.

Nyt yhtälö $r^2 + s^2 = u$ saadaan muotoon

$$X^4 + Y^4 = W^2,$$

joten yhtälölle $x^4 + y^4 = w^2$ löytyi toinen ratkaisu. Tutkitaan vielä, onko $W < w$. Yhtälö $w = u^2 + v^2$ voidaan esittää nyt muodossa

$$w = W^4 + v^2 > W^4 \geq W,$$

joten $W < w$.

Yllä osoitettiin, että jos yhtälöllä $x^4 + y^4 = w^2$ on kokonaislukuratkaisut x, y ja w, niin on olemassa toisetkin kokonaislukuratkaisut X, Y ja W, missä $W < w$. Ratkaisuista X, Y ja W voitaisiin johtaa seuraavat ratkaisut X', Y' ja W', missä $W' < W$. Näin jatkamalla saataisiin ääretön ketju $w > W > W' > W'' > ... > 0$. Tämä on selvästi mahdotonta, sillä lukua w pienempiä positiivisia kokonaislukuja on äärellinen määrä. Niinpä yhtälöllä $x^4+y^4 = w^2$ ei ole positiivisia kokonaislukuratkaisuja. □

6 Pellin yhtälö

Yhtälöä $x^2 - dy^2 = c$, missä d ja c ovat annettuja vakioita ja x ja y ovat tuntemattomia, kutsutaan Pellin yhtälöksi. Nimitys on kuitenkin harhaanjohtava, sillä englantilainen matemaatikko John Pell (1611-1685) ei tuonut yhtälöiden teoriaan tai ratkaisuun mitään uutta. Euler todennäköisesti kutsui ensimmäisenä yhtälöä $x^2 - dy^2 = c$ Pellin yhtälöksi, sillä hän oli lukenut Pellin teosta, jossa Pell tutki yhtälöä $x^2 - 12y^2 = n$. [3, s. 540]

Pellin yhtälöiden historia on pitkä, sillä jo Arkhimedes ja Diofantos pohtivat Pellin yhtälöiden erikoistapauksia. Kuitenkin vasta 1700-luvun loppupuolella todistettiin, kuinka yhtälöiden ratkaisut löydetään. Tässä tutkielmassa ratkaisujen löytämiseen käytetään ketjumurtolukuja, joihin perehdytään ensin tarkemmin.

6.1 Ketjumurtoluvuista

6.1.1 Äärelliset ketjumurtoluvut

Aloitetaan ketjumurtolukuihin perehtyminen Eukleideen algoritmista. Eukleideen algoritmilla kokonaisluvuille a ja b etsitään suurin yhteinen tekijä (a, b) ja löydetään kokonaisluvut x ja y siten, että $ax + by = (a, b)$. Esitetään seuraavassa Eukleideen algoritmi

$$\begin{aligned}
b &= aq_1 + r_1, & 0 < r_1 < a,\\
a &= r_1q_2 + r_2, & 0 < r_2 < r_1,\\
r_1 &= r_2q_3 + r_3, & 0 < r_3 < r_2,\\
&\vdots & \vdots\\
r_{i-2} &= r_{i-1}q_i + r_i, & 0 < r_i < r_{i-1}\\
&\vdots & \vdots
\end{aligned}$$

Käyttämällä ensimmäistä yhtälöä, r_1 voidaan kirjoittaa lukujen a ja b lineaarikombinaationa. Taas käyttämällä edellä saatua, voidaan r_2 kirjoittaa

a:n ja b:n lineaarikombinaationa. Jatkamalla näin saadaan

$$r_i = ax_i + by_i.$$

Esimerkiksi ensimmäisestä yhtälöstä saadaan $r_1 = a(-q_1)+b$, joten $x_1 = -q_1$ ja $y_1 = 1$. Toinen yhtälö saaadaan nyt muotoon

$$r_2 = a - r_1q_2 = a - (-aq_1 + b)q_2 = a(1 + q_1q_2) + b(-q_2),$$

joten $x_2 = 1 + q_1q_2$ ja $y_2 = -q_2$. Oletetaan nyt, että on löydetty x_k ja y_k, $k = 1,\ 2,\ ...,\ i-1$. Tällöin ylläolevan Euklideen algoritmin alimmalta riviltä saadaan

$$\begin{aligned} r_i &= r_{i-2} - r_{i-1}q_i \\ &= ax_{i-2} + by_{i-2} - (ax_{i-1} + by_{i-1})q_i \\ &= a(x_{i-2} - q_ix_{i-1}) + b(y_{i-2} - q_iy_{i-1}), \end{aligned}$$

joten saadaan, että $x_i = x_{i-2} - q_ix_{i-1}$ ja $y_i = y_{i-2} - q_iy_{i-1}$ Helpotetaan lukujen x_i ja y_i määrittelyä määrittelemällä arvot x_{-1}, x_0, y_{-1} ja y_0.

Lause 6.1. *(Vrt. [4, s. 204]) Eukleideen algoritmia on käytetty kokonaisluvuille a ja b, $a > 0$, jolloin on saatu osamäärät q_i ja jakojäännökset r_i. Määritellään kokonaisluvut x_i ja y_i seuraavasti*

$$\begin{aligned} &x_{-1} = 0, \quad x_0 = 1, \quad x_i = x_{i-2} - q_ix_{i-1},\ \text{kun } i \geq 1, \\ &y_{-1} = 1, \quad y_0 = 0, \quad y_i = y_{i-2} - q_iy_{i-1},\ \text{kun } i \geq 1. \end{aligned}$$

Tällöin $r_i = ax_i + by_i$, kun $i > 0$. Erityisesti, jos r_n on viimeinen nollasta eroava jakojäännös, niin $(a, b) = ax_n + by_n$.

Esimerkki 6.1. Olkoon $a = 165$ ja $b = 465$. Selvitetään Euklideen algoritmin avulla (a, b) ja lausetta 6.1 apuna käyttäen yhtälön $(a, b) = ax + by$ tuntemattomat x ja y. Nyt

$$\begin{aligned} 465 &= 165 \cdot 2 + 135 \\ 165 &= 135 \cdot 1 + 30 \\ 135 &= 30 \cdot 4 + 15 \\ 30 &= 15 \cdot 2 + 0. \end{aligned}$$

Kolmannelta riviltä nähdään, että $(165, 465) = 15$. Tutkitaan seuraavan

taulukon avulla lukujen x_i ja y_i arvoja:

i	q_i	$x_i = x_{i-2} - q_i x_{i-1}$	$y_i = y_{i-2} - q_i y_{i-1}$
-1		0	1
0		1	0
1	2	$0 - 2 \cdot 1 = -2$	$1 - 2 \cdot 0 = 1$
2	1	$1 - 1 \cdot (-2) = 3$	$0 - 1 \cdot 1 = -1$
3	4	$-2 - 4 \cdot 3 = -14$	$1 - 4 \cdot (-1) = 5$
4	2	$3 - 2 \cdot (-14) = 31$	$-1 - 2 \cdot 5 = -11.$

Riviltä $i = 3$ nähdään, että $165x + 465y = 15$, kun $x = -14$ ja $y = 5$. Riviltä $i = 4$ voidaan tarkistaa $165 \cdot 31 + 465 \cdot (-11) = 0$. Yleisesti, jos r_n on viimeinen nollasta eroava jakojäännös, niin $ax_{n+1} + by_{n+1} = 0$ ja $\frac{x_{n+1}}{y_{n+1}} = \frac{-b}{a}$.

Esimerkissä kerrointen x_i ja y_i merkit vuorottelivat, vaikka kaikki osamäärät q_i olivat positiivisia. Määritellään seuraavaksi muuttujat, jotka ovat aina positiivisia, kun osamäärät q_i ovat positiivisia. Olkoon

$$h_i = (-1)^i x_i \quad \text{ja} \quad k_i = (-1)^{i+1} y_i,$$

missä $i = -1, 0, 1, ...$ Nyt lauseen 6.1 avulla saadaan

$$\begin{aligned} h_i &= (-1)^i (x_{i-2} - q_i x_{i-1}) \\ &= (-1)^{i-2} x_{i-2} + q_i (-1)^{i-1} x_{i-1} \\ &= h_{i-2} + q_i h_{i-1} \end{aligned}$$

ja

$$\begin{aligned} k_i &= (-1)^{i+1} (y_{i-2} - q_i y_{i-1}) \\ &= (-1)^{i-1} y_{i-2} + q_i (-1)^i y_{i-1} \\ &= k_{i-2} + q_i k_{i-1}. \end{aligned}$$

Vaikka useimmiten luvut q_i ovat kokonaislukuja, luvut h_i ja k_i ovat määritelty mille tahansa päättyvälle reaaliselle lukujonolle $q_1, q_2, ..., q_{n+1}$.

Määritelmä 6.1. (Vrt. [4, s. 205]) Olkoot $q_1, q_2, ..., q_{n+1}$ reaalilukuja. Määritellään h_i ja k_i, $i = -1, 0, 1, ..., n + 1$ seuraavasti

$$\begin{aligned} &h_{-1} = 0, \quad h_0 = 1, \quad h_i = h_{i-2} - q_i h_{i-1}, \text{ kun } i \geq 1, \\ &k_{-1} = 1, \quad k_0 = 0, \quad k_i = k_{i-2} - q_i k_{i-1}, \text{ kun } i \geq 1. \end{aligned}$$

Tutkitaan seuraavaksi lukujen h_i ja k_i arvoja, kun $i = 1, 2, 3$. Saadaan

$$\begin{aligned}
h_1 &= h_{-1} + q_1 h_0 = 0 + q_1 \cdot 1 = q_1, \\
k_1 &= k_{-1} + q_1 k_0 = 1 + q_1 \cdot 0 = 1, \\
h_2 &= h_0 + q_2 h_1 = 1 + q_2 q_1, \\
k_2 &= k_0 + q_2 k_1 = 0 + q_2 \cdot 1 = q_2, \\
h_3 &= h_1 + q_3 h_2 = q_1 + q_3(1 + q_2 q_1), \\
k_3 &= k_1 + q_3 k_2 = 1 + q_3 q_2.
\end{aligned}$$

Lukujen h_i ja k_i suhteilla $\frac{h_i}{k_i}$ on kiinnostava ominaisuus, sillä

$$\begin{aligned}
\frac{h_1}{k_1} &= \frac{q_1}{1} = q_1, \\
\frac{h_2}{k_2} &= \frac{1 + q_2 q_1}{q_2} = q_1 + \frac{1}{q_2}, \\
\frac{h_3}{k_3} &= \frac{q_1 + q_3(1 + q_2 q_1)}{1 + q_3 q_2} = \frac{q_1 + q_3 + q_1 q_2 q_3}{1 + q_2 q_3} \\
&= \frac{q_1(1 + q_2 q_3) + q_3}{1 + q_2 q_3} = q_1 + \frac{q_3}{1 + q_2 q_3} = q_1 + \frac{1}{q_2 + \frac{1}{q_3}}.
\end{aligned}$$

Koska merkintätapa on hankala, määritellään käytännöllisempi muoto.

Määritelmä 6.2. (Vrt. [4, s. 206]) *Äärellisellä ketjumurtoluvulla* tarkoitetaan lauseketta

$$q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{\ddots + \frac{1}{q_r}}}},$$

missä q_1 on reaaliluku ja luvut q_2, ... , q_r positiivisia reaalilukuja. Merkitään tätä lyhyemmin $[q_1, q_2, ..., q_r]$. Jos kaikki luvut q_i ovat kokonaislukuja, kutsutaan ketjumurtolukua *yksinkertaiseksi*.

Tässä tutkielmassa käsitellään vain yksinkertaisia ketjumurtolukuja. Määritelmästä huomataan, että ketjumurtoluku ei ole yksikäsitteinen, sillä $[q_1, q_2, ..., q_r] = [q_1, q_2, ..., q_{r-1} + \frac{1}{q_r}]$. Nyt edellä kuvatut suhteet $\frac{h_i}{k_i}$ voidaan ilmaista kätevästi muodossa

$$\frac{h_1}{k_1} = [q_1], \qquad \frac{h_2}{k_2} = [q_1, q_2] \quad \text{ja} \quad \frac{h_3}{k_3} = [q_1, q_2, q_3].$$

Esitetään seuraavaksi kaksi päättyviin ketjumurtolukuihin liittyvää tulosta, joita ei tässä tutkielmassa kuitenkaan todisteta.

Lause 6.2. (Vrt. [4, s. 207]) *Olkoot $q_1, q_2, ..., q_r$ reaalilukuja, missä $q_i > 0$, kun $i > 1$, ja olkoot h_i ja k_i määritelty kuten yllä. Tällöin*

$$[q_1, q_2, ..., q_r] = \frac{h_r}{k_r}.$$

Lause 6.3. (Vrt. [4, s. 208]) *Jokainen yksinkertainen äärellinen ketjumurtoluku esittää rationaalilukua ja jokainen rationaaliluku voidaan esittää yksinkertaisena äärellisenä ketjumurtolukuna $[q_1, q_2, ..., q_{n+1}]$, missä $q_{n+1} > 1$.*

6.1.2 Äärettömät ketjumurtoluvut

Lauseen 6.3 mukaan kaikki äärelliset ketjumurtoluvut esittävät rationaalilukuja ja kaikki rationaaliluvut on mahdollista esittää äärellisinä ketjumurtolukuina. Tutkitaan seuraavaksi tilannetta $[q_1, q_2, ...]$, missä luvut q_i muodostavat äärettömän lukujonon. Äärettömät ketjumurtoluvut ja irrationaaliluvut vastaavat toisiaan kuten äärelliset ketjumurtoluvut rationaalilukuja, joten jaetaan tarkastelu kahteen osaan. Aluksi näytetään, että jokainen ääretön ketjumurtoluku esittää irrationaalilukua, ja toiseksi, että jokainen irrationaaliluku on ääretön ketjumurtoluku.

Ensimmäisenä tulisi mieleen määritellä $[q_1, q_2, ...]$ jonon $[q_1, q_2, ..., q_n]$ raja-arvoksi, kun $n \to \infty$, mutta ei ole selvää, onko raja-arvoa olemassa. Ratkaisevaksi tekijäksi tässä tarkastelussa nousee edellisessä pykälässä 6.1.1 esitetty tulos $[q_1, q_2, ..., q_n] = \frac{h_n}{k_n}$, jossa h_i ja k_i ovat määritelty kuten siellä. Oletetaan seuraavissa, että $q_1, q_2, ...$ on äärellinen tai ääretön kokonaislukujen jono, missä $q_i > 0$, kun $i > 1$.

Apulause 6.1. *Luvuille k_i pätee, että $1 = k_1 \leq k_2 < k_3 < ...$*

Todistus. (Vrt. [4, s. 211]) Pykälässä 6.1.1 laskettiin, että $k_1 = 1$ ja $k_2 = q_2$, joka on vähintään 1 q_i:n määrittelyn perusteella. Nyt yhtälöstä $k_i = k_{i-2} + q_i k_{i-1}$ nähdään, että $k_i \geq k_{i-2} + k_{i-1} > k_{i-1}$, kun $i > 2$. □

Tutkitaan seuraavaksi yhtälöitä

$$h_i = h_{i-2} + q_i h_{i-1},$$
$$k_i = k_{i-2} + q_i k_{i-1}.$$

Kerrotaan ylempi yhtälö puolittain luvulla k_{i-1} ja alempi puolittain luvulla h_{i-1} ja vähennetään alempi ylemmästä, jolloin saadaan

$$h_i k_{i-1} - k_i h_{i-1} = h_{i-2} k_{i-1} - k_{i-2} h_{i-1} = -(h_{i-1} k_{i-2} - k_{i-1} h_{i-2}).$$

Huomataan, että yhtälön oikea puoli on vasemman puolen vastaluku, jossa kuitenkin kaikki alaindeksit ovat yhden pienempiä. Koska $k_{-1} h_0 - h_{-1} k_0 = 1 \cdot 1 - 0 \cdot 0 = 1$, saadaan, että $k_0 h_1 - h_0 k_1 = -1$, $k_1 h_2 - h_1 k_2 = 1$ jne.

Apulause 6.2. (Vrt. [4, s. 212]) *Kun* $i = 0, 1, ...,$ *niin* $k_{i-1}h_i - h_{i-1}k_i = (-1)^i$. *Siis* h_i *ja* k_i *ovat suhteelliset alkuluvut.*

Nyt apulauseen 6.2 toisesta osasta seuraa, että osamäärä $\frac{h_i}{k_i}$ on supistumattomassa muodossa. Merkitään tätä suhdetta symbolilla R_i. Koska $k_0 = 0$, valitaan, että $i > 0$. Jaetaan nyt apulauseen 6.2 yhtälö puolittain luvulla $k_i k_{i-1}$, jolloin saadaan

$$R_i - R_{i-1} = \frac{(-1)^i}{k_i k_{i-1}}.$$

Pitää myös paikkansa, että

$$R_{i+1} - R_i = \frac{(-1)^{i+1}}{k_{i+1}k_i}$$

ja, kun kaksi edellistä yhtälöä lasketaan puolittain yhteen, saadaan

$$R_{i+1} - R_{i-1} = \frac{(-1)^i \left(\frac{1}{k_{i-1}} - \frac{1}{k_{i+1}}\right)}{k_i}.$$

Nyt apulauseen 6.1 perusteella tiedetään, että $k_{i+1} > k_{i-1}$, kun $i > 1$, joten $R_{i+1} - R_{i-1}$ on positiivinen tai negatiivinen riippuen siitä, onko i parillinen vai pariton. Kun $i = 2, 3, ...$ saadaan, että $R_3 - R_1 > 0$, $R_4 - R_2 < 0$, $R_5 - R_3 > 0$ jne. Tämä todistaa seuraavan apulauseen.

Apulause 6.3. (Vrt. [4, s. 212]) *Olkoon* R_i *määritelty kuten edellä. Tällöin*

$$R_1 < R_3 < R_5 < \cdots \quad \text{ja} \quad R_2 > R_4 > R_6 > \cdots .$$

Esitetään vielä ilman todistusta apulause 6.4, jonka tulosta tarvitaan lauseen 6.4 todistuksessa.

Apulause 6.4. (Vrt. [4, s. 213]) *Olkoot* i *ja* j *positiivisia kokonaislukuja, olkoon* i *parillinen ja* j *pariton. Tällöin* $R_i > R_j$.

Lause 6.4. *Olkoon* $q_1, q_2, ...$ *ääretön kokonaislukujono, jolle pätee* $q_i > 0$, *kun* $i > 1$. *Tällöin*

$$\lim_{r \to \infty} [q_1, q_2, ..., q_r]$$

on olemassa, ja se on irrationaaliluku.

Todistus. (Vrt. [4, s. 213]) Apulauseiden 6.3 ja 6.4 nojalla luvut $R_1, R_3, ...$ muodostavat kasvavan reaalilukujen jonon, jota rajoittaa ylhäältä R_2, joten sillä on raja-arvo. Toisaalta $R_2, R_4, ...$ on vähenevä jono, jota rajoittaa alhaalta R_1, joten silläkin on raja-arvo. Koska $R_i - R_{i-1} = \frac{(-1)^i}{k_i k_{i-1}}$ ja apulauseen 6.1 nojalla luvut k_i kasvavat kohti äärettömyyttä, niin näiden raja-arvojen täytyy olla samat, merkitään sitä reaaliluvulla R. Tämä todistaa lauseen ensimmäisen osan.

Todistetaan sitten, että R on irrationaalinen. Tehdään vastaoletus, että R on rationaalinen ja merkitään $R = \frac{b}{a}$, missä $a > 0$. Huomataan, että $R_1 < R_3 < \cdots < R < \cdots < R_4 < R_2$, joten $\frac{b}{a}$ on lukujen R_i ja R_{i-1} välissä eli

$$0 < \left| \frac{b}{a} - R_{i-1} \right| < |R_i - R_{i-1}| .$$

Tiedetään, että $|R_i - R_{i-1}| = \frac{1}{k_i k_{i-1}}$, $R_{i-1} = \frac{h_{i-1}}{k_{i-1}}$, ja kun kerrotaan epäyhtälö puolittain luvulla ak_{i-1} saadaan

$$0 < |bk_{i-1} - ah_{i-1}| < \frac{a}{k_i}.$$

Kun valitaan tarpeeksi suuri i, saadaan luku k_i suuremmaksi kuin a, jolloin oikea puoli on pienempi kuin 1. Itseisarvojen sisällä oleva luku on kokonaisluku. Nyt kokonaisluku $|bk_{i-1} - ah_{i-1}|$ on nollan ja yhden välissä, mikä on mahdotonta. Niinpä vastaoletus on väärä ja R on irrationaaliluku. □

Huomautus 6.1. Päälähdeteoksessa on todistuksessa kaksi painovirhettä. Siellä esiintyy virheellisesti $R_1 < R_3 < \cdots \underline{=} R \underline{=} \cdots < R_4 < R_2$ ja $1/k_i k_{i\underline{=}1}$

Määritelmä 6.3. Olkoot $q_1, q_2, ...$ ääretön jono kokonaislukuja, missä $q_i > 0$ ja $q_1 \geq 0$. Määritellään *ääretön ketjumurtoluku* seuraavasti

$$[q_1, q_2, ...] = \lim_{n \to \infty} [q_1, q_2, ..., q_n].$$

Lukuja $[q_1, q_2, ..., q_n] = R_n = \frac{h_n}{k_n}$, $n = 1, 2, ...$, kutsutaan äärettömän ketjumurtoluvun *konvergenteiksi.*

Annetusta jonosta $q_1, q_2, ...$ on mahdollista approksimoida vastaava irrationaaliluku $[q_1, q_2, ...]$ selvittämällä lukuja R_i.

Tutkitaan seuraavaksi käänteistä tapausta, jossa on annettu irrationaaliluku, S, jolle tulisi löytää vastaava ääretön ketjumurtoluku. Tarvitaan siis lukujono $q_1, q_2, ...$ siten, että $S = [q_1, q_2, ...]$.

Jos S olisi rationaalinen, merkitään $\frac{b}{a}$, osamäärät q_i saataisiin Eukleideen algoritmin avulla seuraavasti

$$\begin{aligned} b &= aq_1 + r_1, \quad && 0 < r_1 < a \\ a &= r_1 q_2 + r_2, \quad && 0 < r_2 < r_1, \end{aligned}$$

ja niin edelleen. Jos ensimmäinen yhtälö ja epäyhtälö jaetaan puolittain luvulla $a > 0$, saadaan

$$\frac{b}{a} = q_1 + \frac{r_1}{a}, \quad 0 < \frac{r_1}{a} < 1.$$

Huomataan, että luvun $\frac{b}{a}$ kokonaislukuosa on q_1 ja murto-osa $\frac{r_1}{a}$. Voidaan siis kirjoittaa esitiedoissa määritellyn lattiafunktion avulla

$$q_1 = \left\lfloor \frac{b}{a} \right\rfloor, \qquad \frac{r_1}{a} = \frac{b}{a} - \left\lfloor \frac{b}{a} \right\rfloor.$$

Samaan tapaan, toinen yhtälö ja epäyhtälö jaetaan puolittain luvulla r_1, jolloin saadaan

$$\frac{a}{r_1} = q_2 + \frac{r_2}{r_1}, \qquad 0 < \frac{r_2}{r_1} < 1.$$

Näin ollen

$$q_2 = \left\lfloor \frac{a}{r_1} \right\rfloor = \left\lfloor \frac{1}{\frac{r_1}{a}} \right\rfloor = \left\lfloor \frac{1}{\frac{b}{a} - \left\lfloor \frac{b}{a} \right\rfloor} \right\rfloor.$$

Yksinkertaistetaan seuraavaksi merkintöjä. Olkoon $S_1 = \frac{b}{a}$. Tällöin $q_1 = \lfloor S_1 \rfloor$. Määritellään sitten, että $S_2 = \frac{1}{S_1 - q_1}$, jolloin $q_2 = \lfloor S_2 \rfloor$.

Kun yleistetään edellä kuvattua prosessia, saadaan metodi, jolla löydetään irrationaaliluvun ketjumurtolukuesitys.

Lause 6.5. *Olkoon S reaaliluku. Olkoon $S_1 = S$ ja $q_1 = \lfloor S_1 \rfloor$. Oletetaan, että S_i ja q_i ovat määriteltyjä, kun $i = 1, 2, ..., r$. Jos S_i ei ole yhtä kuin q_i, niin määritellään S_{i+1} ja q_{i+1} seuraavasti*

$$S_{i+1} = \frac{1}{S_i - q_i}, \qquad q_{i+1} = \lfloor S_{i+1} \rfloor.$$

Jos S on rationaalinen, prosessi päättyy johonkin lukuun q_r, jolloin $S = [q_1, q_2, ..., q_r]$. Jos taas S on irrationaalinen, on olemassa ääretön jono $q_1, q_2, ...$ siten, että $S = [q_1, q_2, ...]$.

Todistus. (Vrt. [4, s. 216]) Jos S on rationaalinen, kokonaisluvut q_i ovat Eukleideen algoritmin osamäärät q_i, joten keskitytään tapaukseen S irrationaalinen.

Koska $S = S_1$ on irrationaalinen, se ei voi olla yhtä kuin kokonaisluku q_1, joten $S_2 = \frac{1}{S_1 - q_1}$ on määritelty. Myös S_2 on irrationaalinen, sillä muuten $S_1 = \frac{1}{S_2} + q_1$ olisi rationaalinen. Jatkamalla tätä päättelyä, nähdään, että luvut S_i ovat määriteltyjä ja irrationaalisia. Lukujono $q_1, q_2, ...$ on siis ääretön.

Koska $S_i - q_i$ on luvun S_i murto-osa, tiedetään, että $0 < S_i - q_i < 1$ ja siten $S_{i+1} = \frac{1}{S_i - q_i} > 1$. Niinpä $q_{i+1} = \lfloor S_{i+1} \rfloor \geq 1$, kun $i > 0$.

Nyt lauseen 6.4 nojalla tiedetään, että $[q_1, q_2, ...] = R$ jollekin irrationaaliluvulle R. Olkoot luvut h_i, k_i ja R_i määritelty kuten edellä ja R lukujen R_i raja-arvo. Aikaisemmin nähtiin, että

$$S_2 = \frac{1}{S_1 - q_1}, \text{ eli } S = S_1 = q_1 + \frac{1}{S_2},$$

ja yleisemmin

$$S_i = q_i + \frac{1}{s_{i+1}}.$$

Tällöin

$$S = S_1 = q_1 + \frac{1}{S_2} = q_1 + \frac{1}{q_2 + \frac{1}{S_3}} = \cdots = [q_1, q_2, ..., q_{n-1}, S_n].$$

Nyt lukujen h_i ja k_i määrittelyiden sekä lauseen 6.2 nojalla yllä oleva voidaan kirjoittaa muodossa

$$\frac{h_{n-2} + S_n h_{n-1}}{k_{n-2} + S_n k_{n-1}}.$$

Niinpä apulauseen 6.2 nojalla saadaan

$$\begin{aligned} S - R_{n-1} &= \frac{h_{n-2} + S_n h_{n-1}}{k_{n-2} + S_n k_{n-1}} - \frac{h_{n-1}}{k_{n-1}} \\ &= \frac{k_{n-1}(h_{n-2} + S_n h_{n-1}) - (k_{n-2} + S_n k_{n-1})h_{n-1}}{k_{n-1}(k_{n-2} + S_n k_{n-1})} \\ &= \frac{-(k_{n-2}h_{n-1} - h_{n-2}k_{n-1})}{k_{n-1}(k_{n-2} + S_n k_{n-1})} = \frac{(-1)^n}{k_{n-1}(k_{n-2} + S_n k_{n-1})}. \end{aligned}$$

Nyt k_i kasvaa äärettömyyteen ja $S_n > 0$, kun $n > 0$, joten viimeinen lauseke lähestyy lukua 0, kun n lähestyy ääretöntä. Niinpä

$$0 = \lim_{n \to \infty} (S - R_{n-1}) = S - R.$$

Siis $S = [q_1, q_2, ...]$. □

Luvut R_n ovat hyviä rationaaliapproksimaatioita irrationaaliluvuille S.

6.2 Pellin yhtälön ratkaiseminen

Palataan nyt luvun alussa esitettyyn yhtälöön $x^2 - dy^2 = c$. Jos $d < 0$, luvut x ja y eivät voi olla liian suuria, ja jos ratkaisuja on olemassa, niitä on äärellinen määrä, jotka voidaan löytää yrityksen ja erehdyksen kautta. Jos taas d on täydellinen neliö, merkitään $d = a^2$, yhtälö voidaan kirjoittaa muotoon

$$(x + ay)(x - ay) = c$$

ja ratkaisut löydetään luvun c tekijöstä.

Keskitytään tästä lähtien Pellin yhtälön tapaukseen, missä $d > 0$ ja d ei ole täydellinen neliö. Tällöin $\sqrt{d}$ on irrationaalinen. Riittää, kun etsitään positiivisia ratkaisuja, sillä muut ratkaisut on helppo löytää niiden avulla. Usein tarkastelussa on tapaukset, joissa c on pieni verrattuna lukuun d, ja tärkein tulos esitetään yhtälölle, missä $c = 1$. Tällöin luvun x^2 on oltava lähellä lukua dy^2, jotta x ja y ovat ratkaisut. Nyt jakamalla luvulla y^2 saadaan,

että luvun $\left(\frac{x}{y}\right)^2$ tulee olla lähellä lukua d eli rationaalisen $\frac{x}{y}$ tulee olla lähellä irrationaalista $\sqrt{d}$.

Aliluvun 6.1.2 lopussa todettiin, että irrationaaliluvun konvergentit ovat hyviä rationaaliapproksimaatioita luvulle. Tarkennetaan tätä ilmausta seuraavassa lauseessa.

Lause 6.6. *Olkoon d positiivinen kokonaisluku, joka ei ole täydellinen neliö, ja $[q_1, q_2, ...]$ luvun $\sqrt{d}$ ketjumurtolukuesitys. Olkoon $\frac{h_i}{k_i} = [q_1, q_2, ..., q_i]$ luvun $\sqrt{d}$ i. konvergentti ja kokonaisluvut h_i ja k_i määritelty kuten aliluvussa 6.1.2. Tällöin*

$$|h_i^2 - dk_i^2| < 2\sqrt{d} + 1$$

kaikille $i \geq 0$.

Todistus. (Vrt. [4, s. 256]) Kun $i = 0$, epäyhtälö pitää paikkansa, sillä $h_0 = 1$ ja $k_0 = 0$. Apulauseen 6.3 ja lauseiden 6.4 ja 6.5 perusteella saadaan, että

$$\frac{h_1}{k_1} < \frac{h_3}{k_3} < \cdots < \sqrt{d} < \cdots < \frac{h_4}{k_4} < \frac{h_2}{k_2}.$$

Näin ollen kaikille $i > 1$, voidaan kirjoittaa

$$\left|\frac{h_{i-1}}{k_{i-1}} - \sqrt{d}\right| < \left|\frac{h_{i-1}}{k_{i-1}} - \frac{h_i}{k_i}\right|.$$

Aliluvussa 6.1.2 nähtiin, että ylläolevan epäyhtälön oikea puoli on yhtä suuri kuin $\frac{1}{k_i k_{i-1}}$. Kerrotaan nyt epäyhtälön molemmat puolet luvulla k_{i-1}, jolloin saadaan $|h_{i-1} - k_{i-1}\sqrt{d}| < \frac{1}{k_1}$, ja tästä $h_{i-1} = k_{i-1}\sqrt{d} + E$, missä $|E| < \frac{1}{k_i}$. Näin ollen

$$h_{i-1}^2 = k_{i-1}^2 d + 2k_{i-1}\sqrt{d}E + E^2,$$

ja

$$\left|h_{i-1}^2 - k_{i-1}^2 d\right| = \left|2k_i\sqrt{d}E + E^2\right| < \frac{2k_{i-1}\sqrt{d}}{k_i} + \frac{1}{k_i^2} \leq 2\sqrt{d} + 1,$$

sillä luvut k_i muodostavat ei-vähenevän kokonaislukujen jonon, kun $i > 0$. □

Tarkastellaan seuraavaksi yhtälöä $x^2 - dy^2 = 1$, missä $d > 0$ ei ole täydellinen neliö. Selvästi nähdään, että x ei voi olla 0, ja jos $y = 0$, niin $x = \pm 1$. Keskitytään siis ratkaisuihin, missä sekä x että y ovat positiivisia.

Lause 6.7. *Jos positiivinen kokonaisluku d ei ole täydellinen neliö, niin yhtälöllä $x^2 - dy^2 = 1$ on positiiviset kokonaislukuratkaisut x ja y.*

Todistus. (Vrt. [4, s. 257]) Edellisen lauseen nojalla tiedetään, että on olemassa ääretön määrä kokonaislukupareja, joissa pari on keskenään suhteellisia alkulukuja, siten, että $|x^2 - dy^2| < 2\sqrt{d} + 1$. Nämä parit vastaavat siis lukuja h_i ja k_i luvun $\sqrt{d}$ ketjumurtolukuesityksestä. On olemassa kokonaisluku $t \neq 0$ siten, että $x^2 - dy^2 = t$. Luku t ei voi olla 0, sillä tällöin $\sqrt{d} = \frac{x}{y}$, joka ei ole mahdollista, sillä d irrationaalinen.

Jos r on x:n jakojäännös modulo $|t|$ ja s on y:n jakojäännös modulo $|t|$, niin pari (r, s) voi saada vain t^2 arvoa. Näin ollen on olemassa kaksi paria x, y ja X, Y siten, että

$$x^2 - dy^2 = t \quad \text{ja} \quad X^2 - dY^2 = t,$$

missä

$$x \equiv X \pmod{|t|} \quad \text{ja} \quad y \equiv Y \pmod{|t|}.$$

Huomataan, että

$$xX - yYd \equiv x^2 - y^2 d = t \equiv 0 \pmod{|t|},$$

ja

$$xY - Xy \equiv xy - xy = 0 \pmod{|t|},$$

joten on olemassa kokonaisluvut u ja v siten, että

$$xX - yYd = tu \quad \text{ja} \quad xY - Xy = tv.$$

Nyt

$$\begin{aligned} t^2 &= (x^2 - dy^2)(X^2 - dY^2) \\ &= (x - y\sqrt{d})(x + y\sqrt{d})(X - Y\sqrt{d})(X + Y\sqrt{d}) \\ &= (x - y\sqrt{d})(X + Y\sqrt{d})(x + y\sqrt{d})(X - Y\sqrt{d}) \\ &= (xX - yYd + (xY - Xy)\sqrt{d})(xX - yYd - (xY - Xy)\sqrt{d}) \\ &= (tu + tv\sqrt{d})(tu - tv\sqrt{d}) = t^2(u^2 - dv^2), \end{aligned}$$

joten $1 = u^2 - dv^2$. Haluttu ratkaisu on siis pari $|u|, |v|$. Osoitetaan vielä, että $v \neq 0$. Jos $v = 0$, niin $xY = Xy$ ja $\frac{x}{y} = \frac{X}{Y}$. Mutta tiedetään, että irrationaaliluvun konvergentit ovat erisuuria. □

Yhtälölle $x^2 - dy^2 = 1$ löydetään aina ratkaisu luvun $\sqrt{d}$ ketjumurtolukuesityksen konvergenttien joukosta. Tätä tulosta ei kuitenkaan tässä työssä todisteta, mutta seuraavassa lauseessa osoitetaan, kuinka yhtälön $x^2 - dy^2 = 1$ yhdestä ratkaisusta saadaan äärettömän monta ratkaisua. Lisäksi todistetaan, että yleisemmälle yhtälölle $x^2 - dy^2 = c$ on mahdollista löytää yhden annetun ratkaisun avulla äärettömän monta ratkaisua.

Lause 6.8. *Oletetaan, että kokonaisluku $d > 0$ ei ole täydellinen neliö.*

1. *Jos x, y on jokin yhtälön $x^2 - dy^2 = 1$ positiivinen ratkaisu ja jos $n > 0$, niin kokonaislukuparit x_n, y_n, joille pätee $x_n + y_n\sqrt{d} = (x + y\sqrt{d})^n$ ovat myös yhtälön $x^2 - dy^2 = 1$ positiivisia ratkaisuja. Parit (x_n, y_n) ovat erisuuria eri n:n arvoilla.*

2. *Jos u, v on jokin yhtälön $u^2 - dv^2 = c$ positiivinen ratkaisu ja jos x, y jokin yhtälön $x^2 - dy^2 = 1$ äärettömistä ratkaisuista, niin pari U, V, joka toteuttaa yhtälöt*

$$U = ux + vyd, \quad V = uy + vx,$$

on myös yhtälön $u^2 - dv^2 = c$ positiivinen ratkaisu. Parit U, V ovat erisuuria eri ratkaisuilla x, y.

Todistus. (Vrt. [4, s. 259])

1. Aloitetaan todistamalla, että kukin kokonaislukupari x_n, y_n on yksikäsitteisesti määritelty. Oletuksen perusteella lauseke $(x + y\sqrt{d})^n$ saadaan muotoon $X + Y\sqrt{d}$, missä X ja Y ovat positiivisia kokonaislukuja. Oletetaan, että $X + Y\sqrt{d} = U + V\sqrt{d}$ joillakin kokonaisluvuilla X, Y, U ja V. Nyt $(Y - V)\sqrt{d} = U - X$ ja jos $Y - V \neq 0$, niin tällöin $\sqrt{d}$ olisi rationaalinen. Täytyy siis olla $Y = V$ ja siten myös $U = X$, joten parit hyvin määriteltyjä.

   Huomataan, että jos käsitellään lauseketta $(x - y\sqrt{d})^n$, kaikkien luvun $\sqrt{d}$ parittomien potenssien eteen tulee mii-nusmerkki, joten saadaan, että $x_n - y_n\sqrt{d}$. Nyt

$$\begin{aligned} x_n^2 - dy_n^2 &= (x_n - y_n\sqrt{d})(x_n + y_n\sqrt{d}) \\ &= (x - y\sqrt{d})^n(x + y\sqrt{d})^n = (x^2 - dy^2)^n = 1^n = 1. \end{aligned}$$

   Pari x_n, y_n on siis ratkaisu kaikilla $n \in \mathbb{N}$.

   Koska $x + y\sqrt{d} > 1$, luvut $x_n + y_n\sqrt{d} = (x + y\sqrt{d})^n$ muodostavat aidosti kasvavan jonon. Niinpä parien x_n, y_n on oltava erisuuria. Koska $x_n^2 + y_n^2\sqrt{d} = 1$, niin molemmat jonot x_n ja y_n ovat kasvavia.

2. Tiedetään, että $x^2 - dy^2 = 1$ ja, että $u^2 - dv^2 = c$. Kun luvut U ja V ovat määritelty kuten edellä saadaan

$$\begin{aligned} U^2 - dV^2 &= u^2x^2 + 2uvxyd + v^2y^2d^2 - d(u^2y^2 + 2uvxy + v^2x^2) \\ &= u^2(x^2 - dy^2) - dv^2(x^2 - dy^2) = u^2 - dv^2 = c. \end{aligned}$$

   Jos x, y ja x', y' ovat yhtälön $x^2 - dy^2 = 1$ ratkaisuja ja $x > x'$, niin myös $y > y'$. Tällöin $U > U'$ ja $V > V'$, missä U' ja V' on määritelty lukujen x' ja y' avulla. Täten ratkaisut U ja V ovat erisuuria eri ratkaisuilla x, y.

□

Luku $c = 1$ on ainoa, jolle Pellin yhtälölle löydetään aina ratkaisu. Esitetään vielä Pellin yhtälön ratkaisuun liittyvä määritelmä.

Määritelmä 6.4. Olkoon $d > 0$ kokonaisluku, joka ei ole täydellinen neliö. Pellin yhtälön *perusratkaisulla* tarkoitetaan yhtälön $X^2 - dY^2 = c$ pienintä positiivista ratkaisua ts. sellaista positiivista ratkaisua x, y, että $x < x'$ ja $y < y'$ kaikilla muilla positiivisilla ratkaisuilla x', y'.

Jos x, y on yhtälön $X^2 - dY^2 = 1$ perusratkaisu, niin kaikki positiiviset ratkaisut saadaan lauseen 6.8 osasta 1.

Esitetään lopuksi esimerkki Pellin yhtälöistä.

Esimerkki 6.2. Olkoon Pellin yhtälö muotoa $x^2 - 23y^2 = 1$. Tiedetään, että $x = 24$, $y = 5$ on yhtälön ratkaisu. Etsitään nyt lauseen 6.8 ensimmäisen kohdan avulla kaksi seuraavaa ratkaisua.

Saadaan $(24 + 5\sqrt{23})^2 = 1151 + 240\sqrt{23}$, joten $x = 1151$ ja $y = 240$ on toinen ratkaisu. Kolmas saadaan, kun $(24 + 5\sqrt{23})^2 = (24 + 5\sqrt{23})(1151 + 240\sqrt{23}) = 55224 + 11515\sqrt{23}$.

Viitteet

[1] Boyer, C. *Tieteiden kuningatar, matematiikan historia. Osat I-II*. Toisen, uudistetun painoksen toimittanut U. Merzbach. Art House, 1994.

[2] Koshy, T. *Elementary number theory with applications*. Harcourt/Academic Press, 2002.

[3] Rosen K. *Elementary number theory and its applications*. 5th edition. Pearson Addison Wesley, 2005.

[4] Vanden Eynden C. *Elementary number theory*. 2nd edition. McGraw-Hill Higher Education, 2001.

[5] Lehtinen M. *Matematiikan historia*. Matematiikkalehti Solmu 9.9.2000, [Verkkodokumentti], [Viitattu 5.9.2010]
URL: http://solmu.math.helsinki.fi/2000/mathist/html/diffint/index.html