TAMPEREEN YLIOPISTO

Pro gradu -tutkielma

Mikaela Hellstén

Pellin yhtälö

Luonnontieteiden tiedekunta

Matematiikka

Kesäkuu 2017

Tampereen yliopisto

Luonnontieteiden tiedekunta

HELLSTÉN, MIKAELA: Pellin yhtälö

Pro gradu -tutkielma, 47 s.

Matematiikka

Kesäkuu 2017

Tiivistelmä

Tässä tutkielmassa tarkastellaan Pellin yhtälöitä eli yhtälöitä, jotka ovat muotoa $x^2 - dy^2 = 1$, missä x ja y ovat kokonaislukumuuttujia ja d on positiivinen kokonaislukuvakio. Luvussa 2 esitetään ensin Pellin yhtälön määritelmä ja etsitään sen triviaalit ratkaisut. Tämän jälkeen näytetään, kuinka toistamalla tiettyjä vaiheita ennalta tunnettujen ratkaisujen avulla voidaan löytää ääretön määrä uusia ratkaisuja. Lopuksi tarkastellaan Pellin yhtälön yleistystä $x^2 - dy^2 = k$ ja osoitetaan, että jos tällä yhtälöllä on yksi ratkaisu, niin silloin sillä on äärettömän monta ratkaisua. Luvussa 3 esitellään ensin kolmio-, neliö- ja viisikulmiolukujen määritelmät ja näytetään sitten, kuinka nämä luvut voidaan ilmaista aritmeettisten sarjojen termien avulla. Tämän jälkeen määritellään kolmio-neliöluvut ja osoitetaan, että ne tuottavat Pellin yhtälön $x^2 - 2y^2 = 1$ ratkaisuja. Lopuksi esitetään neliö-viisikulmiolukujen määritelmä ja näytetään, että neliö-viisikulmioluvut tuottavat Pellin yhtälön $x^2 - 6y^2 = 1$ ratkaisuja. Luvussa 4 näytetään yksi esimerkki siitä, kuinka Pellin yhtälöitä voidaan hyödyntää toisten tulosten todistamiseksi. Ensin esitetään yleinen menetelmä yhtälön $Ax^2 - By^2 = C$ ratkaisujen löytämiseksi ja sitten näytetään kuinka tämän yhtälön ja Pellin yhtälöiden avulla voidaan muodostaa neljä positiivisten kokonaislukuratkaisujen perhettä yhtälölle $(x + y + z)^2 = xyz$.

Sisältö

1 Johdanto

Tämän tutkielman tarkoituksena on perehdyttää lukija Pellin yhtälöihin eli yhtälöihin, jotka ovat muotoa $x^2 - dy^2 = 1$, missä x ja y ovat kokonaislukumuuttujia ja d on positiivinen kokonaislukuvakio. Nimitys Pellin yhtälö on kuitenkin harhaanjohtava, sillä Pellillä itsellään ei ollut juurikaan tekemistä Pellin yhtälön kanssa. Nimitys sai alkunsa, kun Euler erehtyi luulemaan englantilaisen matemaatikon William Brounckerin keksimää yhtälön $x^2 - dy^2 = 1$ ratkaisumenetelmää Pellin laatimaksi. Virheellisestä alkuperästään huolimatta nimityksestä Pellin yhtälö tuli kuitenkin kirjallisuudessa niin yleisesti hyväksytty, että se jäi pysyväksi. [1, s. 175]

Luvussa 2 esitetään ensin Pellin yhtälön määritelmä ja etsitään sen triviaalit ratkaisut. Tämän jälkeen näytetään, kuinka toistamalla tiettyjä vaiheita ennalta tunnettujen ratkaisujen avulla voidaan löytää ääretön määrä uusia ratkaisuja. Lopuksi tarkastellaan Pellin yhtälön yleistystä $x^2 - dy^2 = k$ ja osoitetaan, että jos tällä yhtälöllä on yksi ratkaisu, niin silloin sillä on äärettömän monta ratkaisua.

Luvussa 3 esitellään ensin kolmio-, neliö- ja viisikulmiolukujen määritelmät ja näytetään sitten, kuinka nämä luvut voidaan ilmaista aritmeettisten sarjojen termien avulla. Tämän jälkeen määritellään kolmio-neliöluvut ja osoitetaan, että ne tuottavat Pellin yhtälön $x^2 - 2y^2 = 1$ ratkaisuja. Lopuksi esitetään neliö-viisikulmiolukujen määritelmä ja näytetään, että neliö-viisikulmioluvut tuottavat Pellin yhtälön $x^2 - 6y^2 = 1$ ratkaisuja.

Luvussa 4 näytetään yksi esimerkki siitä, kuinka Pellin yhtälöitä voidaan hyödyntää toisten tulosten todistamiseksi. Ensin esitetään yleinen menetelmä yhtälön $Ax^2 - By^2 = C$ ratkaisujen löytämiseksi ja sitten näytetään, kuinka tämän yhtälön ja Pellin yhtälöiden avulla voidaan muodostaa neljä positiivisten kokonaislukuratkaisujen perhettä yhtälölle $(x + y + z)^2 = xyz$.

Tutkielman luvussa 2 on käytetty päälähteenä William W. Adamsin ja Larry Joel Goldsteinin kirjaa Introduction to Number Theory. Kolmio-, neliö- ja viisikulmiolukujen tarkastelu pohjautuu Keith Conradin verkkodokumenttiin Pell's Equation, I. Luku 4 perustuu Titu Andreescun artikkeliin A note on the equation $(x+y+z)^2 = xyz$. Lukijan oletetaan tuntevan lukuteorian alkeet, kuten kongruenssin perusominaisuudet ja aritmetiikan peruslause.

2 Pellin yhtälö

2.1 Määritelmä ja triviaalit ratkaisut

Määritelmä 2.1 (vrt. [1, s. 174])**.** Yhtälöä $x^2 - dy^2 = 1$, missä x ja y ovat kokonaislukumuuttujia ja d positiivinen kokonaislukuvakio, kutsutaan *Pellin yhtälöksi*.

Huomautus (vrt. [1, s. 174–175])**.** Pellin yhtälöllä on yksi triviaali tapaus. Oletetaan, että $d = a^2$, missä $a \in \mathbb{Z}$ ja $a \neq 0$. Sijoittamalla $d = a^2$ Pellin yhtälöön $x^2 - dy^2 = 1$ saadaan

$$\begin{aligned} 1 &= x^2 - dy^2 \\ &= x^2 - a^2y^2 \\ &= (x - ay)(x + ay). \end{aligned}$$

Nyt koska

$$1 = (x - ay)(x + ay),$$

niin on oltava

$$x - ay = x + ay = 1 \quad \text{tai} \quad x - ay = x + ay = -1.$$

Ratkaisemalla edellä esitetyistä yhtälöistä muodostuvat yhtälöparit saadaan

$$\begin{array}{r} + \begin{cases} x - ay = 1 \\ x + ay = 1 \end{cases} \\ \hline 2x = 2 \\ x = 1 \end{array} \qquad\qquad \begin{array}{r} + \begin{cases} x - ay = -1 \\ x + ay = -1 \end{cases} \\ \hline 2x = -2 \\ x = -1 \end{array}$$

ja edelleen koska oletuksen nojalla $a \neq 0$, niin sijoittamalla arvot $x = 1$ ja $x = -1$ saadaan

$$\begin{aligned} 1 - ay &= 1 \\ -ay &= 0 \\ y &= 0 \end{aligned} \qquad\qquad \begin{aligned} -1 - ay &= -1 \\ -ay &= 0 \\ y &= 0. \end{aligned}$$

Tällöin saadaan ratkaisut $x = 1, y = 0$ ja $x = -1, y = 0$. Siis jos $d = a^2$, missä $a \in \mathbb{Z}$ ja $a \neq 0$, eli jos d on nollasta eroava neliöluku, niin Pellin yhtälöllä $x^2 - dy^2 = 1$ on vain kaksi ratkaisua $x = 1, y = 0$ ja $x = -1, y = 0$.

Koska Pellin yhtälön triviaalilla tapauksella on ainoastaan kaksi ratkaisua ja se ei näin ollen ole kovin mielenkiintoinen, niin tarkastelu rajataan jatkossa Pellin yhtälöön $x^2 - dy^2 = 1$, missä $d \in \mathbb{Z}_+$ ja d ei ole neliöluku. Täten keskitytään siis tarkastelemaan Pellin yhtälöitä, joilla on ääretön määrä ratkaisuja.

2.2 Uusien ratkaisujen generoiminen tunnetuista ratkaisuista

Tässä luvussa esitellään tapoja generoida Pellin yhtälön tunnettujen ratkaisujen avulla äärettömästi lisää ratkaisuja. Seuraavassa esimerkissä näytetään, miten yhden löydetyn ratkaisun avulla ja tiettyjä vaiheita toistamalla voidaan löytää ääretön määrä ratkaisuja Pellin yhtälölle.

Esimerkki 2.1. Tarkastellaan Pellin yhtälöä $x^2 - 3y^2 = 1$. Nyt koska $2^2 - 3 \cdot 1^2 = 1$, niin $x = 2, y = 1$ on yksi yhtälön ratkaisuista. Näin ollen yhtälöllä $x^2 - 3y^2 = 1$ on olemassa triviaaleista ratkaisuista $x = 1, y = 0$ ja $x = -1, y = 0$ eroava ratkaisu.

Olkoon (x_0, y_0) jokin yhtälön $x^2 - 3y^2 = 1$ ratkaisu. Osoitetaan, että myös

$$x = 2x_0 + 3y_0, \quad y = x_0 + 2y_0$$

on ratkaisu. Sijoittamalla saadaan

$$\begin{aligned} x^2 - 3y^2 &= (2x_0 + 3y_0)^2 - 3(x_0 + 2y_0)^2 \\ &= (4x_0^2 + 12x_0y_0 + 9y_0^2) - 3(x_0^2 + 4x_0y_0 + 4y_0^2) \\ &= 4x_0^2 + 12x_0y_0 + 9y_0^2 - 3x_0^2 - 12x_0y_0 - 12y_0^2 \\ &= x_0^2 - 3y_0^2. \end{aligned}$$

Nyt koska

$$x^2 - 3y^2 = x_0^2 - 3y_0^2 \quad \text{ja} \quad x^2 - 3y^2 = 1,$$

niin myös $x_0^2 - 3y_0^2 = 1$. Siis

$$x = 2x_0 + 3y_0, \quad y = x_0 + 2y_0$$

on yhtälön $x^2 - 3y^2 = 1$ ratkaisu.

Jos esimerkiksi $x_0 = 2$ ja $y_0 = 1$, niin sijoittamalla saadaan

$$\begin{aligned} x &= 2x_0 + 3y_0 \\ &= 2 \cdot 2 + 3 \cdot 1 \\ &= 7 \end{aligned} \qquad\qquad \begin{aligned} y &= x_0 + 2y_0 \\ &= 2 + 2 \cdot 1 \\ &= 4. \end{aligned}$$

Täten yhtälölle $x^2 - 3y^2 = 1$ on löydetty ratkaisu $x = 7, y = 4$. Jos edelleen valitaan $x_0 = 7$ ja $y_0 = 4$, niin sijoittamalla saadaan

$$\begin{aligned} x &= 2x_0 + 3y_0 \\ &= 2 \cdot 7 + 3 \cdot 4 \\ &= 26 \end{aligned} \qquad\qquad \begin{aligned} y &= x_0 + 2y_0 \\ &= 7 + 2 \cdot 4 \\ &= 15. \end{aligned}$$

Näin ollen yhtälölle $x^2 - 3y^2 = 1$ on edelleen löydetty ratkaisu $x = 26, y = 15$. Valitsemalla sitten $x_0 = 26$, $y_0 = 15$ ja sijoittamalla nämä arvot kaavoihin

$$x = 2x_0 + 3y_0 \quad \text{ja} \quad y = x_0 + 2y_0$$

saadaan jälleen uusi ratkaisu yhtälölle $x^2 - 3y^2 = 1$. Edelleen soveltamalla edellisiä vaiheita saatuun uuteen ratkaisuun saadaan ääretön määrä lukupareja, jotka toteuttavat yhtälön $x^2 - 3y^2 = 1$. Näin saadut ratkaisut ovat erisuuria, koska muuttujan y arvot muodostavat aidosti kasvavan jonon. Oikeastaan myös muuttujan x arvot muodostavat aidosti kasvavan jonon.

Seuraavaksi näytetään, kuinka kahden tunnetun ratkaisun avulla voidaan löytää kolmas ratkaisu Pellin yhtälölle $x^2 - dy^2 = 1$. Ennen tätä osoitetaan kuitenkin todeksi kolmannen ratkaisun löytämiseksi tarvittava identtinen yhtälö.

Apulause 2.1 (vrt. [1, s. 176])**.** Yhtälö

$$(x_1^2 - dy_1^2)(x_2^2 - dy_2^2) = (x_1x_2 - dy_1y_2)^2 - d(x_1y_2 - y_1x_2)^2$$

on tosi kaikilla muuttujien x_1, x_2, y_1, y_2 ja vakion d arvoilla.

Todistus. Koska

$$\begin{aligned} (x_1^2 - dy_1^2)(x_2^2 - dy_2^2) &= x_1^2x_2^2 - dx_1^2y_2^2 - dy_1^2x_2^2 + d^2y_1^2y_2^2 \\ &= x_1^2x_2^2 - d(x_1^2y_2^2 + y_1^2x_2^2) + d^2y_1^2y_2^2 \end{aligned}$$

ja

$$
\begin{aligned}
(x_1x_2 - dy_1y_2)^2 - d(x_1y_2 - y_1x_2)^2 &= x_1^2x_2^2 - 2dx_1y_1x_2y_2 + d^2y_1^2y_2^2 \\
&\quad - dx_1^2y_2^2 + 2dx_1y_1x_2y_2 - dy_1^2x_2^2 \\
&= x_1^2x_2^2 + d^2y_1^2y_2^2 - dx_1^2y_2^2 - dy_1^2x_2^2 \\
&= x_1^2x_2^2 - d(x_1^2y_2^2 + y_1^2x_2^2) + d^2y_1^2y_2^2,
\end{aligned}
$$

niin yhtälö on identtisesti tosi. □

Lause 2.1 (vrt. [1, s. 176])**.** *Jos* (x_1, y_1) *ja* (x_2, y_2) *ovat Pellin yhtälön* $x^2 - dy^2 = 1$ *ratkaisuja, niin myös* (x_3, y_3)*, missä*

$$x_3 = x_1x_2 - dy_1y_2 \quad \textit{ja} \quad y_3 = x_1y_2 - y_1x_2,$$

on ratkaisu.

Todistus. Olkoot (x_1, y_1) ja (x_2, y_2) Pellin yhtälön $x^2 - dy^2 = 1$ ratkaisuja. Tällöin

$$x_1^2 - dy_1^2 = 1 \quad \text{ja} \quad x_2^2 - dy_2^2 = 1$$

ja näin ollen

$$(x_1^2 - dy_1^2)(x_2^2 - dy_2^2) = 1 \cdot 1 = 1.$$

Nyt koska apulauseen 2.1 nojalla

$$(x_1^2 - dy_1^2)(x_2^2 - dy_2^2) = (x_1x_2 - dy_1y_2)^2 - d(x_1y_2 - y_1x_2)^2,$$

niin

$$(x_1x_2 - dy_1y_2)^2 - d(x_1y_2 - y_1x_2)^2 = 1.$$

Pellin yhtälölle $x^2 - dy^2 = 1$ on siis löydetty uusi ratkaisu (x_3, y_3), joka voidaan esittää muodossa

$$x_3 = x_1x_2 - dy_1y_2, \qquad y_3 = x_1y_2 - y_1x_2.$$

□

Näin ollen edellä apulauseessa 2.1 esitetty identtinen yhtälö sallii uusien ratkaisujen generoimisen tiedetyistä ratkaisuista.

Esimerkki 2.2. Tarkastellaan lukuja $d = 3$, $x_1 = 2$, $y_1 = 1$, $x_2 = 26$ ja $y_2 = 15$. Järjestetty kokonaislukupari $(x_1, y_1) = (2, 1)$ on Pellin yhtälön $x^2 - 3y^2 = 1$ ratkaisu, sillä

$$2^2 - 3 \cdot 1^2 = 4 - 3 = 1.$$

Vastaavasti järjestetty kokonaislukupari $(x_2, y_2) = (26, 15)$ on yhtälön $x^2 - 3y^2 = 1$ ratkaisu, sillä

$$26^2 - 3 \cdot 15^2 = 676 - 3 \cdot 225 = 676 - 675 = 1.$$

Nyt koska $(2, 1)$ ja $(26, 15)$ ovat ratkaisuja, niin lauseen 2.1 nojalla yhtälöllä on kolmas ratkaisu (x_3, y_3), missä

$$x_3 = x_1x_2 - dy_1y_2 \quad \text{ja} \quad y_3 = x_1y_2 - y_1x_2.$$

Sijoittamalla saadaan

$$\begin{aligned} x_3 &= x_1x_2 - dy_1y_2 & \qquad y_3 &= x_1y_2 - y_1x_2 \\ &= 2 \cdot 26 - 3 \cdot 1 \cdot 15 & &= 2 \cdot 15 - 1 \cdot 26 \\ &= 52 - 45 & &= 30 - 26 \\ &= 7 & &= 4. \end{aligned}$$

Täten kahden tunnetun ratkaisun avulla on löydetty yhtälölle $x^2 - 3y^2 = 1$ kolmas ratkaisu $(x_3, y_3) = (7, 4)$.

Huomautus. Jos yhtälön $x^2 - dy^2 = 1$ kolmannen ratkaisun (x_3, y_3) muodostamiseen käytettävistä ratkaisuista (x_1, y_1) ja (x_2, y_2) johdetut luvut $x_1 + \sqrt{d}y_1$ ja $x_2 + \sqrt{d}y_2$ ovat Pellin yhtälön $x^2 - dy^2 = 1$ ratkaisuista (x_n, y_n) johdetuista luvuista $x_n + \sqrt{d}y_n$ pienimmät, niin kaavoilla

$$x_3 = x_1x_2 - dy_1y_2 \quad \text{ja} \quad y_3 = x_1y_2 - y_1x_2$$

saatava kolmas ratkaisu ei poikkea aiemmista ratkaisuista, vaan $(x_3, y_3) = (x_1, y_1)$ tai $(x_3, y_3) = (x_2, y_2)$. Jotta edellä esitettyjen kaavojen avulla voitaisiin siis löytää jokin uusi ratkaisu, niin yhtälölle on oltava olemassa ratkaisu (x_3, y_3) niin, että $x_3 + \sqrt{d}y_3 < x_1 + \sqrt{d}y_1$ tai $x_3 + \sqrt{d}y_3 < x_2 + \sqrt{d}y_2$.

Esimerkki 2.3. Tarkastellaan lukuja $d = 3$, $x_1 = 2$, $y_1 = 1$, $x_2 = 7$ ja $y_2 = 4$. Järjestetty kokonaislukupari $(x_1, y_1) = (2, 1)$ on Pellin yhtälön $x^2 - 3y^2 = 1$ ratkaisu, sillä

$$2^2 - 3 \cdot 1^2 = 4 - 3 = 1.$$

Vastaavasti järjestetty kokonaislukupari $(x_2, y_2) = (7, 4)$ on yhtälön $x^2 - 3y^2 = 1$ ratkaisu, sillä

$$7^2 - 3 \cdot 4^2 = 49 - 3 \cdot 16 = 49 - 48 = 1.$$

Sijoittamalla saadaan

$$\begin{aligned} x_3 &= x_1x_2 - dy_1y_2 & \qquad y_3 &= x_1y_2 - y_1x_2 \\ &= 2 \cdot 7 - 3 \cdot 1 \cdot 4 & &= 2 \cdot 4 - 1 \cdot 7 \\ &= 14 - 12 & &= 8 - 7 \\ &= 2 & &= 1. \end{aligned}$$

Näin ollen kahden tunnetun ratkaisun avulla ei siis löydetty uutta ratkaisua, vaan kolmas ratkaisu $(x_3, y_3) = (x_1, y_1)$.

Esitetään seuraavaksi apulause, jota tarvitaan apulauseen 2.3 todistuksessa.

Apulause 2.2. Jokaista ei-neliölukua $d \in \mathbb{Z}_+$ kohden on olemassa äärettömän monta sellaista positiivista kokonaislukua x ja y, että $|x - y\sqrt{d}| < \frac{1}{y}$.

Todistus (vrt. [4, s. 1–2]). Olkoon $d \in \mathbb{Z}_+$ ei-neliöluku. Tarkastellaan $m + 1$ lukua

$$0,\ \sqrt{d},\ 2\sqrt{d}, \ldots,\ m\sqrt{d},$$

kun $m \geq 2$. Näiden lukujen murto-osat ovat lukuvälillä $[0, 1[$, missä lukuväliä $[0, 1[$ voidaan ajatella luvun m osoittamana lukumääränä puoliavoimia lukuvälejä $[0, 1/m[$, $[1/m, 2/m[, \ldots, [(m-1)/m, 1[$. Kyyhkyslakkaperiaatteen nojalla kahden luvun $m + 1$ luvusta $0, \sqrt{d}, 2\sqrt{d}, \ldots, m\sqrt{d}$, sanotaan lukujen $a\sqrt{d}$ ja $b\sqrt{d}$, kun $a < b$, murto-osat ovat samalla lukuvälillä. Näin ollen $a\sqrt{d} = A + \varepsilon$, $b\sqrt{d} = B + \delta$, missä $A, B \in \mathbb{Z}$ ja ε ja δ kuuluvat samaan väliin $[i/m, (i + 1)/m[$. Täten

$$|\varepsilon - \delta| < \frac{1}{m}.$$

Tämä epäyhtälö on aito, koska käytetyt välit ovat puoliavoimia. Käyttämällä yhtälöitä

$$a\sqrt{d} = A + \varepsilon \;\Leftrightarrow\; a\sqrt{d} - A = \varepsilon \quad \text{ja}$$
$$b\sqrt{d} = B + \delta \;\Leftrightarrow\; b\sqrt{d} - B = \delta$$

saadaan

$$\begin{aligned} |\varepsilon - \delta| < \frac{1}{m} &\Leftrightarrow |(a\sqrt{d} - A) - (b\sqrt{d} - B)| < \frac{1}{m} \\ &\Leftrightarrow |a\sqrt{d} - A - b\sqrt{d} + B| < \frac{1}{m} \\ &\Leftrightarrow |B - A - b\sqrt{d} + a\sqrt{d}| < \frac{1}{m} \\ &\Leftrightarrow |(B - A) - (b - a)\sqrt{d}| < \frac{1}{m}. \end{aligned}$$

Asetetaan $x = B - A$ ja $y = b - a$. Nyt koska $A, B \in \mathbb{Z}$, $a, b \in \mathbb{Z}_+$ ja aiemman oletuksen nojalla $a < b$, niin x ja y ovat kokonaislukuja, joille $0 < y \leq m$. Näin ollen

$$|x - y\sqrt{d}| < \frac{1}{m} \leq \frac{1}{y}.$$

Täten luvun x etäisyys luvusta $y\sqrt{d}$ on pienempi kuin 1. Koska lisäksi $d \in \mathbb{Z}_+$ on ei-neliöluku, niin

$$x > y\sqrt{d} - 1 \geq \sqrt{d} - 1 > 0.$$

Näin ollen siis x on nollaa suurempi kokonaisluku, joten $x \geq 1$.

Kun on löydetty yksi sellainen positiivinen kokonaislukupari (x, y), että $|x - y\sqrt{d}| < 1/y$, niin toisen samalla ominaisuudella varustetun positiivisen kokonaislukuparin löytämiseksi valitaan $m' \in \mathbb{Z}_+$ niin, että $1/m' < |x - y\sqrt{d}|$. (Tällainen m' on olemassa, koska $x - y\sqrt{d} \neq 0$, kun $\sqrt{d}$ on irrationaalinen.) Toistamalla edellä esitetyt vaiheet siten, että luku m korvataan luvulla m' löydetään positiiviset kokonaisluvut x' ja y', joille $|x' - y'\sqrt{d}| < 1/m'$, missä $y' \leq m'$. Tällöin $|x' - y'\sqrt{d}| \leq 1/y'$. Nyt koska

$$|x' - y'\sqrt{d}| < \frac{1}{m'} < |x - y\sqrt{d}|,$$

niin positiivinen kokonaislukupari (x, y) ei ole selvästikään sama kuin positiivinen kokonaislukupari (x', y'). Edelleen toistamalla edelliset vaiheet pienemmälle luvulle $|x'' - y''\sqrt{d}|$ saadaan jälleen aiempien positiivisten kokonaislukuparien kanssa erisuuri pari (x'', y''), jolle $|x'' - y''\sqrt{d}| < 1/y''$. Edellä esitettyjä vaiheita toistamalla voidaan siis löytää ääretön määrä sellaisia positiivisia kokonaislukuja, että $|x - y\sqrt{d}| < 1/y$. □

Esimerkki 2.4. Olkoon $d = 5$. Etsitään kaksi ratkaisua epäyhtälölle $|x-y\sqrt{5}| < 1/y$. Valitaan $m = 10$, jolloin luvun $k\sqrt{5}$, missä $0 \leq k \leq 10$, murto-osien joukossa on olemassa kaksi kokonaislukuparia (a, b), missä $a < b$ ja luvuilla $a\sqrt{5}$ ja $b\sqrt{5}$ on sama ensimmäinen desimaalinumero ja näin ollen niiden välinen etäisyys on pienempi kuin $1/10$. Nämä kaksi kokonaislukuparia ovat $(a, b) = (2, 6)$ ja $(a, b) = (5, 9)$.

k	0	1	2	3	4	5	6	7	8	9	10
luvun $k\sqrt{5}$ murto-osat	0	0,23	0,47	0,70	0,94	0,18	0,41	0,65	0,88	0,12	0,36

Taulukko 2.1: Luvun $k\sqrt{5}$, missä $0 \leq k \leq 10$, murto-osat kahteen desimaalipaikkaan annettuna.

Valitaan $a = 2$ ja $b = 6$. Nyt koska $a\sqrt{5} = 2\sqrt{5} = 4,47\ldots$ ja $b\sqrt{5} = 6\sqrt{5} = 13,41\ldots$, niin

$$\begin{aligned} & |(2\sqrt{5} - 4) - (6\sqrt{5} - 13)| < \frac{1}{10} \\ \Leftrightarrow\quad & |2\sqrt{5} - 6\sqrt{5} - 4 + 13| < \frac{1}{10} \\ \Leftrightarrow\quad & |-4\sqrt{5} + 9| < \frac{1}{10} \\ \Leftrightarrow\quad & |9 - 4\sqrt{5}| < \frac{1}{10} < \frac{1}{4}, \end{aligned}$$

joten saadaan $(x, y) = (9, 4)$.

Jos alussa olisi valittu kokonaislukuparin $(2, 6)$ sijaan pari $(5, 9)$, niin luvuille x ja y olisi saatu samat arvot kuin toisellakin parilla. Nimittäin, koska $a\sqrt{5} = 5\sqrt{5} = 11,18\ldots$ ja $b\sqrt{5} = 9\sqrt{5} = 20,12\ldots$, niin

$$\begin{aligned} & |(5\sqrt{5} - 11) - (9\sqrt{5} - 20)| < \frac{1}{10} \\ \Leftrightarrow\quad & |5\sqrt{5} - 9\sqrt{5} - 11 + 20| < \frac{1}{10} \\ \Leftrightarrow\quad & |-4\sqrt{5} + 9| < \frac{1}{10} \\ \Leftrightarrow\quad & |9 - 4\sqrt{5}| < \frac{1}{10} < \frac{1}{4}, \end{aligned}$$

joten saadaan $(x, y) = (9, 4)$. Ei siis ole väliä, mikä löydetyistä kokonaislukupareista valitaan.

Koska $|9 - 4\sqrt{5}| \approx 0,0557 > 1/20$, niin toisen sellaisen kokonaislukuparin (x', y'), että $|x' - y'\sqrt{5}| < 1/y'$, löytämiseksi tarkastellaan luvun $k\sqrt{5}$, missä $0 \leq k \leq 20$, murto-osia. Pyrkimyksenä on löytää kaksi murto-osaa, jotka kuuluvat jollekin lukuvälille $[i/20, (i + 1)/20[$. Tällaiset murto-osat löytyvät, kun $k = 2$ ja $k = 19$. Tällöin

$$2\sqrt{5} = 4,472\ldots \quad \text{ja} \quad 19\sqrt{5} = 42,485\ldots,$$

joten

$$|(2\sqrt{5} - 4) - (19\sqrt{5} - 42)| \approx 0,01 < \frac{1}{20} \Leftrightarrow |38 - 17\sqrt{5}| < \frac{1}{20} < \frac{1}{14}.$$

Siis saadaan $(x', y') = (38, 17)$.

Siirrytään seuraavaksi tarkastelemaan sitä, miten Pellin yhtälölle $x^2 - dy^2 = 1$, missä d ei ole neliöluku, voidaan löytää ainakin yksi yhtälön triviaaliratkaisuista $x = 1$, $y = 0$ ja $x = -1$, $y = 0$ eroava ratkaisu.

Apulause 2.3. Olkoon $B = 2\sqrt{d}+1$. Tällöin on olemassa äärettömän monta erisuurta kokonaislukuparia (x, y), joille

$$|x^2 - dy^2| < B.$$

Todistus (vrt. [4, s. 2–3]). Oletetaan, että $B = 2\sqrt{d} + 1$. Apulauseen 2.2 nojalla äärettömän monelle positiiviselle kokonaisluvulle x ja y pätee $|x - y\sqrt{d}| < 1/y$. Osoitetaan, että sellaisille luvuille x ja y pätee

$$|x^2 - dy^2| < 2\sqrt{d} + 1.$$

Keskeisenä kohtana tässä todistuksessa on, että yläraja ei sisällä lukuja x ja y. Koska apulauseen 2.2 nojalla $|x - y\sqrt{d}| < 1/y$, niin rajoittamalla ensin luku x yläpuolelta luvun y avulla saadaan

$$x = x - y\sqrt{d} + y\sqrt{d} \leq |x - y\sqrt{d}| + y\sqrt{d} < \frac{1}{y} + y\sqrt{d} \leq 1 + y\sqrt{d}.$$

Tällöin

$$\begin{aligned}
|x^2 - dy^2| &= |x + y\sqrt{d}| \cdot |x - y\sqrt{d}| \\
&= (x + y\sqrt{d}) \cdot |x - y\sqrt{d}| \\
&< (x + y\sqrt{d})\frac{1}{y} \\
&< (1 + y\sqrt{d} + y\sqrt{d})\frac{1}{y} \\
&= \frac{1}{y} + 2\sqrt{d} \\
&\leq 1 + 2\sqrt{d}.
\end{aligned}$$

Siis $|x^2 - dy^2| < 2\sqrt{d} + 1$ äärettömän monelle positiiviselle kokonaislukuparille (x, y). □

Esimerkki 2.5. Tarkastellaan Pellin yhtälöä $x^2 - 3y^2 = 1$. Nyt koska $d = 3$, niin $B = 2\sqrt{3} + 1$. Koska

$$\begin{aligned}
& 4 \cdot 3 < 16 \\
\Leftrightarrow \quad & 2\sqrt{3} < 4 \\
\Leftrightarrow \quad & 2\sqrt{3} + 1 < 5,
\end{aligned}$$

niin $B \leq 5$. Tällöin apulauseen 2.3 nojalla on olemassa äärettömän monta kokonaislukuparia (x, y), joille

$$|x^2 - 3y^2| < 5.$$

Seuraavaksi osoitetaan, että yhtälöllä $x^2 - dy^2 = 1$ on äärettömän monta ratkaisua. Tämän tuloksen todistaminen vähentää selvästi apulauseen 2.3 mielenkiintoa itsessään, sillä apulause 2.3 on tämän uuden tuloksen seuraus. Kuitenkin apulauseen 2.3 tulos on tarpeellinen yleisemmän tuloksen osoittamiseksi.

Lause 2.2. *Olkoon $d \in \mathbb{Z}_+$ ei-neliöluku. Tällöin Pellin yhtälöllä $x^2 - dy^2 = 1$ on ääretön määrä erisuuria kokonaislukuratkaisuja (x, y).*

Todistus (vrt. [1, s. 177]). Olkoon $d \in \mathbb{Z}_+$ ei-neliöluku. Apulauseen 2.3 nojalla on olemassa äärettömän monta kokonaislukuparia (x, y), joille $|x^2 - dy^2| < B$, missä $B = 2\sqrt{d} + 1$. Koska on olemassa vain äärellinen määrä kokonaislukuja k, joille $|k| < B$, ja koska jokainen luku $x^2 - dy^2$ on kokonaisluku, niin on olemassa sellainen kokonaisluku k, että on olemassa äärettömän monta kokonaislukuparia (x, y), joille $x^2 - dy^2 = k$.

Jos $k = 0$ ja $y \neq 0$, niin

$$\begin{aligned} & x^2 - dy^2 = 0 \\ \Leftrightarrow \quad & dy^2 = x^2 \\ \Leftrightarrow \quad & d = \frac{x^2}{y^2} \\ \Leftrightarrow \quad & d = \left(\frac{x}{y}\right)^2. \end{aligned}$$

Koska $d \in \mathbb{Z}_+$ ja $d = x^2/y^2$, niin $y^2 | x^2$. Tällöin aritmetiikan peruslauseen nojalla saadaan, että $y | x$. Näin ollen x/y on kokonaisluku, joten $d = (x/y)^2$ on neliöluku, mikä on ristiriidassa oletuksen kanssa, että d ei ole neliöluku. Siis on oltava $k \neq 0$.

Tarkastellaan sitten yhtälön $x^2 - dy^2 = k$ kokonaislukuratkaisuja (x, y) modulo $|k|$. Kaikille kokonaisluvuille x ja y on olemassa kokonaisluvut a ja b, joille $0 \leq a, b < |k|$ ja joille $x \equiv a \pmod{|k|}$, $y \equiv b \pmod{|k|}$. Kokonaislukuparille (a, b) on olemassa vain k^2 eri vaihtoehtoa. Täten, koska yhtälöllä $x^2 - dy^2 = k$ on äärettömän monta ratkaisua, niin voidaan löytää sellaiset kokonaisluvut a ja b, että äärettömän monta yhtälön $x^2 - dy^2 = k$ ratkaisua (x, y) toteuttaa kongruenssit $x \equiv a \pmod{|k|}$, $y \equiv b \pmod{|k|}$. Näistä ratkaisuista jokaiselle kokonaislukuparille (x_1, y_1) ja (x_2, y_2) pätee

$$x_1^2 - dy_1^2 = k, \qquad x_2^2 - dy_2^2 = k$$

ja

$$x_1 \equiv a \equiv x_2 \pmod{|k|}, \qquad y_1 \equiv b \equiv y_2 \pmod{|k|}.$$

Nyt koska

$$x_1^2 - dy_1^2 = k, \qquad x_2^2 - dy_2^2 = k,$$

niin

$$(x_1^2 - dy_1^2)(x_2^2 - dy_2^2) = k \cdot k = k^2.$$

Toisaalta apulauseen 2.1 nojalla

$$(x_1^2 - dy_1^2)(x_2^2 - dy_2^2) = (x_1x_2 - dy_1y_2)^2 - d(x_1y_2 - y_1x_2)^2,$$

joten saadaan

$$\begin{aligned} k^2 &= (x_1x_2 - dy_1y_2)^2 - d(x_1y_2 - y_1x_2)^2 \\ \Leftrightarrow \quad 1 &= \frac{(x_1x_2 - dy_1y_2)^2}{k^2} - d \cdot \frac{(x_1y_2 - y_1x_2)^2}{k^2} \\ \Leftrightarrow \quad 1 &= \left(\frac{x_1x_2 - dy_1y_2}{k}\right)^2 - d\left(\frac{x_1y_2 - y_1x_2}{k}\right)^2. \end{aligned}$$

Nyt koska

$$x_1 \equiv a \equiv x_2 \pmod{|k|} \quad \text{ja} \quad y_1 \equiv b \equiv y_2 \pmod{|k|},$$

niin

$$x_1x_2 - dy_1y_2 \equiv x_1x_1 - dy_1y_1 \equiv x_1^2 - dy_1^2 \pmod{|k|}.$$

Edelleen koska $x_1^2 - dy_1^2 = k$, niin saadaan

$$x_1x_2 - dy_1y_2 \equiv x_1^2 - dy_1^2 \equiv 0 \pmod{|k|}.$$

Vastaavasti, koska

$$x_1 \equiv a \equiv x_2 \pmod{|k|} \quad \text{ja} \quad y_1 \equiv b \equiv y_2 \pmod{|k|},$$

niin

$$x_1y_2 - y_1x_2 \equiv x_1y_1 - y_1x_1 \pmod{|k|}.$$

Edelleen, koska $x_1y_1 - y_1x_1 = 0$, niin

$$x_1y_2 - y_1x_2 \equiv x_1y_1 - y_1x_1 \equiv 0 \pmod{|k|}.$$

Näin ollen $x_1x_2 - dy_1y_2$ ja $x_1y_2 - y_1x_2$ ovat siis jaollisia luvulla k, joten yhtälöstä

$$1 = \left(\frac{x_1x_2 - dy_1y_2}{k}\right)^2 - d\left(\frac{x_1y_2 - y_1x_2}{k}\right)^2$$

saadaan Pellin yhtälölle $x^2 - dy^2 = 1$ kokonaislukuratkaisu (x, y), missä

$$x = \frac{x_1x_2 - dy_1y_2}{k}, \qquad y = \frac{x_1y_2 - y_1x_2}{k}.$$

Kiinnitetään yksi yhtälön $x^2 - dy^2 = k$ ja kongruenssien $x_1 \equiv a \equiv x_2 \pmod{|k|}$ ja $y_1 \equiv b \equiv y_2 \pmod{|k|}$ ratkaisu (x_1, y_1). Koska $k \neq 0$, niin vähintään toinen luvuista x_1 ja y_1 on nollasta eroava. Käyköön kokonaislukupari (x_2, y_2) läpi äärettömän joukon ratkaisuja yhtälöön $x^2 - dy^2 = k$ ja kongruensseihin $x_1 \equiv a \equiv x_2 \pmod{|k|}$ ja $y_1 \equiv b \equiv y_2 \pmod{|k|}$. Tällöin joko x_2 tai y_2 saa äärettömän monta arvoa, jolloin joko x tai y saa äärettömän monta arvoa. Näin ollen (x, y) käy läpi äärettömän monta ratkaisua yhtälöön $x^2 - dy^2 = 1$. □

Seuraavaksi näytetään, miten yhtälölle $x^2 - dy^2 = 1$ voidaan generoida äärettömän monta ratkaisua. Ensin kuitenkin osoitetaan todeksi kaksi yhtälöä, joita tarvitaan näiden ratkaisujen generoimiseksi.

Apulause 2.4 (vrt. [1, s. 178])**.** Yhtälöt

$$\begin{aligned}(x_1 + \sqrt{d}y_1)(x_2 + \sqrt{d}y_2) &= (x_1x_2 + dy_1y_2) + \sqrt{d}(x_1y_2 + y_1x_2)\\(x_1 - \sqrt{d}y_1)(x_2 - \sqrt{d}y_2) &= (x_1x_2 + dy_1y_2) - \sqrt{d}(x_1y_2 + y_1x_2)\end{aligned}$$

ovat tosia kaikilla muuttujien x_1, x_2, y_1, y_2 ja vakion d arvoilla.

Todistus. Koska

$$\begin{aligned}(x_1 + \sqrt{d}y_1)(x_2 + \sqrt{d}y_2) &= x_1x_2 + \sqrt{d}x_1y_2 + \sqrt{d}y_1x_2 + dy_1y_2\\&= (x_1x_2 + dy_1y_2) + \sqrt{d}(x_1y_2 + y_1x_2)\end{aligned}$$

ja

$$\begin{aligned}(x_1 - \sqrt{d}y_1)(x_2 - \sqrt{d}y_2) &= x_1x_2 - \sqrt{d}x_1y_2 - \sqrt{d}y_1x_2 + dy_1y_2\\&= (x_1x_2 + dy_1y_2) - \sqrt{d}(x_1y_2 + y_1x_2),\end{aligned}$$

niin yhtälöt ovat identtisisesti tosia. □

On siis osoitettu, että kahden muotoa $x + \sqrt{d}y$ olevan luvun tulo on myös muotoa $x + \sqrt{d}y$ oleva luku. Vastaavasti kahden muotoa $x - \sqrt{d}y$ olevan luvun tulo on muotoa $x - \sqrt{d}y$.

Seuraavaksi osoitetaan induktion avulla, että suuruusjärjestykseen järjestetyistä positiivisista kokonaislukupareista muodostuvan jonon, missä $(x_m, y_m) < (x_n, y_n)$, jos $x_m + \sqrt{d}y_m < x_n + \sqrt{d}y_n$, n. jäsen (x_n, y_n) voidaan määrittää tämän jonon ensimmäisen jäsenen (x_1, y_1) avulla.

Lause 2.3 (vrt. [1, s. 178])**.** *Olkoot x_1 ja y_1 kokonaislukuja ja olkoon d positiivinen kokonaisluku. Tällöin*

$$\begin{aligned}(x_1 + \sqrt{d}y_1)^n &= x_n + \sqrt{d}y_n \quad \text{ja}\\(x_1 - \sqrt{d}y_1)^n &= x_n - \sqrt{d}y_n,\end{aligned}$$

missä n on posiitivinen kokonaisluku ja x_n ja y_n ovat kokonaislukuja.

Todistus. Osoitetaan induktiolla, että kaikilla luonnollisilla luvuilla $n \geq 1$ pätee

$$(x_1 + \sqrt{d}y_1)^n = x_n + \sqrt{d}y_n,$$

missä x_n ja y_n ovat kokonaislukuja. Kaava pätee, kun $n = 1$, sillä

$$(x_1 + \sqrt{d}y_1)^1 = x_1 + \sqrt{d}y_1.$$

Oletetaan, että kaava pätee, kun $n = k$. Tällöin

$$(x_1 + \sqrt{d}y_1)^k = x_k + \sqrt{d}y_k.$$

Osoitetaan sitten, että kaava pätee, kun $n = k + 1$. Koska

$$\begin{aligned}(x_1 + \sqrt{d}y_1)^{k+1} &= (x_1 + \sqrt{d}y_1)(x_1 + \sqrt{d}y_1)^k \\ &\overset{I.O.}{=} (x_1 + \sqrt{d}y_1)(x_k + \sqrt{d}y_k) \\ &= x_1x_k + \sqrt{d}x_1y_k + \sqrt{d}y_1x_k + dy_1y_k \\ &= (x_1x_k + dy_1y_k) + \sqrt{d}(x_1y_k + y_1x_k) \\ &= x_{k+1} + \sqrt{d}y_{k+1},\end{aligned}$$

niin kaava pätee, kun $n = k + 1$. Näin ollen iduktioperiaatteen nojalla kaava pätee kaikilla $n \geq 1$.

Vastaavasti induktion avulla voidaan osoittaa, että kaikilla luonnollisilla luvuilla $n \geq 1$ pätee

$$(x_1 - \sqrt{d}y_1)^n = x_n - \sqrt{d}y_n,$$

missä x_n ja y_n ovat kokonaislukuja. Kaava pätee, kun $n = 1$, sillä

$$(x_1 - \sqrt{d}y_1)^1 = x_1 - \sqrt{d}y_1.$$

Oletetaan, että kaava pätee, kun $n = k$. Tällöin

$$(x_1 - \sqrt{d}y_1)^k = x_k - \sqrt{d}y_k.$$

Osoitetaan sitten, että kaava pätee, kun $n = k + 1$. Koska

$$\begin{aligned}(x_1 - \sqrt{d}y_1)^{k+1} &= (x_1 - \sqrt{d}y_1)(x_1 - \sqrt{d}y_1)^k \\ &\overset{I.O.}{=} (x_1 - \sqrt{d}y_1)(x_k - \sqrt{d}y_k) \\ &= x_1x_k - \sqrt{d}x_1y_k - \sqrt{d}y_1x_k + dy_1y_k \\ &= (x_1x_k + dy_1y_k) - \sqrt{d}(x_1y_k + y_1x_k) \\ &= x_{k+1} - \sqrt{d}y_{k+1},\end{aligned}$$

niin kaava pätee, kun $n = k + 1$. Näin ollen iduktioperiaatteen nojalla kaava pätee kaikilla $n \geq 1$. $\square$

Seuraus 2.1. *Olkoon* (x_1, y_1) *suuruusjärjestykseen järjestetyistä positiivisista kokonaislukupareista muodostuvan jonon, missä* $(x_m, y_m) < (x_n, y_n)$*, jos* $x_m + \sqrt{d}y_m < x_n + \sqrt{d}y_n$*, ensimmäinen jäsen ja olkoon* d *positiivinen kokonaisluku. Tällöin jonon* n*. jäsen* (x_n, y_n) *saadaan kaavoilla*

$$x_n = x_1x_{n-1} + dy_1y_{n-1}, \qquad y_n = x_1y_{n-1} + y_1x_{n-1}.$$

Todistus (vrt. [1, s. 178]). Lauseen 2.3 nojalla tiedetään, että kun $n \geq 2$, niin

$$\begin{aligned}(x_1 + \sqrt{d}y_1)^n &= (x_1 + \sqrt{d}y_1)(x_1 + \sqrt{d}y_1)^{n-1} \\ &= (x_1 + \sqrt{d}y_1)(x_{n-1} + \sqrt{d}y_{n-1}).\end{aligned}$$

Nyt apulauseen 2.4 nojalla

$$(x_1 + \sqrt{d}y_1)(x_{n-1} + \sqrt{d}y_{n-1}) = (x_1x_{n-1} + dy_1y_{n-1}) + \sqrt{d}(x_1y_{n-1} + y_1x_{n-1}),$$

jolloin voidaan merkitä

$$x_n = x_1x_{n-1} + dy_1y_{n-1}, \qquad y_n = x_1y_{n-1} + y_1x_{n-1}.$$

Vastaavasti lauseen 2.3 nojalla tiedetään, että kun $n \geq 2$, niin

$$\begin{aligned}(x_1 - \sqrt{d}y_1)^n &= (x_1 - \sqrt{d}y_1)(x_1 - \sqrt{d}y_1)^{n-1} \\ &= (x_1 - \sqrt{d}y_1)(x_{n-1} - \sqrt{d}y_{n-1}).\end{aligned}$$

Edelleen apulauseen 2.4 nojalla

$$(x_1 - \sqrt{d}y_1)(x_{n-1} - \sqrt{d}y_{n-1}) = (x_1x_{n-1} + dy_1y_{n-1}) - \sqrt{d}(x_1y_{n-1} + y_1x_{n-1}),$$

jolloin voidaan merkitä

$$x_n = x_1x_{n-1} + dy_1y_{n-1}, \qquad y_n = x_1y_{n-1} + y_1x_{n-1}.$$

$\square$

Huomautus. Esimerkissä 2.1 käytetyt kaavat

$$x_n = 2x_{n-1} + 3y_{n-1} \quad \text{ja} \quad y_n = 2y_{n-1} + x_{n-1}.$$

ovat seurauksessa 2.1 olleet relaatiot

$$x_n = x_1 x_{n-1} + d y_1 y_{n-1} \quad \text{ja} \quad y_n = x_1 y_{n-1} + y_1 x_{n-1}$$

luvulle $n \geq 2$. Kun $n = 2$, niin (x_2, y_2), missä

$$x_2 = 2x_1 + 3y_1 \quad \text{ja} \quad y_2 = 2y_1 + x_1,$$

on Pellin yhtälön $x^2 - dy^2 = 1$ ratkaisu.

Seuraavaksi esitetään, kuinka yksittäisen tunnetun ratkaisun avulla voidaan generoida uusi ratkaisu.

Lause 2.4. *Oletetaan, että $n \in \mathbb{Z}_+$ ja että (x_1, y_1) on Pellin yhtälön $x^2 - dy^2 = 1$ ratkaisu. Olkoot luvut x_n ja y_n määritelty ehdolla*

$$(x_1 + \sqrt{d} y_1)^n = x_n + \sqrt{d} y_n.$$

Tällöin (x_n, y_n) on yhtälön $x^2 - dy^2 = 1$ ratkaisu.

Todistus (vrt. [1, s. 178]). Lauseen 2.3 nojalla $(x_1 - \sqrt{d} y_1)^n = x_n - \sqrt{d} y_n$, joten

$$\begin{aligned} x_n^2 - dy_n^2 &= (x_n + \sqrt{d} y_n)(x_n - \sqrt{d} y_n) \\ &= (x_1 + \sqrt{d} y_1)^n (x_1 - \sqrt{d} y_1)^n \\ &= ((x_1 + \sqrt{d} y_1)(x_1 - \sqrt{d} y_1))^n \\ &= (x_1^2 - dy_1^2)^n. \end{aligned}$$

Koska (x_1, y_1) on yhtälön $x^2 - dy^2 = 1$ ratkaisu, niin $x_1^2 - dy_1^2 = 1$. Lisäksi koska

$$x_n^2 - dy_n^2 = (x_1^2 - dy_1^2)^n,$$

niin

$$x_n^2 - dy_n^2 = 1^n = 1.$$

Siis (x_n, y_n) on yhtälön $x^2 - dy^2 = 1$ ratkaisu. □

Esimerkki 2.6. Tarkastellaan yhtälöä $x^2 - 3y^2 = 1$. Valitaan $x_1 = 2$ ja $y_1 = 1$. Määritellään luvut x_n ja y_n siten, että

$$\begin{aligned} & x_n + \sqrt{3} y_n = (2 + \sqrt{3} \cdot 1)^n \\ \Leftrightarrow \quad & x_n + \sqrt{3} y_n = (2 + \sqrt{3})^n. \end{aligned}$$

Tällöin

$$
\begin{aligned}
(2+\sqrt{3})^2 &= 4+4\sqrt{3}+3 = 7+4\sqrt{3} \\
(2+\sqrt{3})^3 &= (2+\sqrt{3})^2(2+\sqrt{3}) \\
&= (7+4\sqrt{3})(2+\sqrt{3}) \\
&= 14+7\sqrt{3}+8\sqrt{3}+12 \\
&= 26+15\sqrt{3},
\end{aligned}
$$

mistä saadaan yhtälölle $x^2 - dy^2 = 1$ esimerkissä 2.1 esitetyt ratkaisut $(7, 4)$ ja $(26, 15)$.

2.3 Kaikkien ratkaisujen löytäminen

Tässä luvussa näytetään, kuinka yhden tunnetun ratkaisun avulla voidaan löytää kaikki yhtälön $x^2 - dy^2 = 1$ ratkaisut. Ensin huomataan, että jos (x, y) on ratkaisu, niin myös $(\pm x, \pm y)$ on ratkaisu millä tahansa lukujen x ja y etumerkkien yhdistelmällä. Näin ollen riittää, että määritetään kaikki ratkaisut, joille $x \geq 0$ ja $y \geq 0$. Lisäksi triviaalisti voidaan havaita, että ainoat ratkaisut, joille $x = 0$ tai $y = 0$, ovat $(\pm 1, 0)$. Täten riittää määrittää kaikki ratkaisut, joille $x > 0$ ja $y > 0$. Tällaisia ratkaisuja kutsutaan positiivisiksi ratkaisuiksi. Seuraavaksi esitetään yksinkertainen tapa määrittää, onko ratkaisu positiivinen vai ei.

Apulause 2.5. Oletetaan, että (x, y) on jokin yhtälön $x^2 - dy^2 = 1$ ratkaisu. Tällöin (x, y) on positiivinen ratkaisu, jos ja vain jos $x + \sqrt{d}y > 1$.

Todistus (vrt. [1, s. 179]). Oletetaan, että (x, y) on yhtälön $x^2 - dy^2 = 1$ positiivinen ratkaisu eli $x > 0$ ja $y > 0$. Koska x ja y ovat kokonaislukuja, niin $x \geq 1$ ja $y \geq 1$. Tällöin

$$x + \sqrt{d}y \geq 1 + \sqrt{d} \cdot 1 \geq 2 > 1.$$

Kääntäen oletetaan, että $x + \sqrt{d}y > 1$. Jos $x = 0$ tai $y = 0$, niin $(x, y) = (\pm 1, 0)$, jolloin $x + \sqrt{d}y \not> 1$. Oletetaan siis, että $x \neq 0$ ja $y \neq 0$.

Tarkastellaan neljää eri tapausta lukujen x ja y suhteen.

Tapaus 1: Olkoot $x < 0$ ja $y < 0$. Tällöin $x + \sqrt{d}y < 0$, joten $x + \sqrt{d}y \not> 1$.

Tapaus 2: Olkoot $x > 0$ ja $y < 0$. Tällöin

$$x - \sqrt{d}y \geq 1 + \sqrt{d} \cdot 1 \geq 2 > 1.$$

Nyt koska oletuksen nojalla $x + \sqrt{d}y > 1$ ja lisäksi $x^2 - dy^2 = 1$, niin

$$1 = x^2 - dy^2 = (x - \sqrt{d}y)(x + \sqrt{d}y) > 1 \cdot 1 = 1,$$

mikä on mahdotonta.

Tapaus 3: Olkoot $x < 0$ ja $y > 0$. Tällöin

$$-x + \sqrt{d}y \geq 1 + \sqrt{d} \cdot 1 \geq 2 > 1.$$

Nyt koska oletuksen nojalla $x + \sqrt{d}y > 1$ ja lisäksi

$$x^2 - dy^2 = 1 \;\Leftrightarrow\; -x^2 + dy^2 = -1,$$

niin

$$-1 = -x^2 + dy^2 = (-x + \sqrt{d}y)(x + \sqrt{d}y) > 1 \cdot 1 = 1,$$

mikä on mahdotonta.

Tapaus 4: Olkoot $x > 0$ ja $y > 0$. Koska tapaukset 1–3 ovat mahdottomia, niin on oltava $x > 0$ ja $y > 0$. □

Lauseen 2.2 nojalla tiedetään, että yhtälöllä $x^2 - dy^2 = 1$ on ainakin yksi kokonaislukuratkaisu (x_0, y_0), kun $x_0 \neq 0$ ja $y_0 \neq 0$. Lisäksi koska $(\pm x_0, \pm y_0)$ on myös ratkaisu millä tahansa etumerkkiyhdistelmällä, niin havaitaan, että on olemassa ainakin yksi positiivinen ratkaisu. Olkoon se (x_0', y_0'). Asetetaan $M = x_0' + \sqrt{d}y_0'$. Jos (x_1, y_1) on mikä tahansa yhtälön $x^2 - dy^2 = 1$ positiivinen ratkaisu, niin ehto $x_1 + \sqrt{d}y_1 \leq M$ implikoi, että $x_1 \leq M$ ja $y_1 \leq M$. [1, s. 180]

Täten erityisesti, on olemassa vain äärellinen määrä vaihtoehtoja luvuille x_1 ja y_1. Valitaan positiivinen ratkaisu (x_1, y_1), jolle $x_1 + \sqrt{d}y_1$ on pienin. Tämä on mahdollista, sillä yhtälöllä $x^2 - dy^2 = 1$ on äärellinen määrä positiivisia ratkaisuja niin, että $x_1 \leq \sqrt{d}$ ja $y_1 \leq M$. Kutsutaan ratkaisua (x_1, y_1) Pellin yhtälön fundamentaaliseksi ratkaisuksi. [1, s. 180]

Osoitetaan seuraavaksi aputulos, jota tarvitaan Pellin yhtälöihin liittyvän päätuloksen todistamiseen.

Apulause 2.6 (vrt. [1, s. 180]). Olkoot x_1 ja y_1 positiivisia kokonaislukuja. Tällöin myös x_n ja y_n ovat positiivisia kokonaislukuja, kun ne on määritelty ehdolla $x_n + \sqrt{d}y_n = (x_1 + \sqrt{d}y_1)^n$, missä $n \in \mathbb{Z}_+$.

Todistus. Oletetaan, että $x_1 > 0$ ja $y_1 > 0$. Osoitetaan induktion avulla, että kaikilla luonnollisilla luvuilla $n \geq 1$ pätee $x_n > 0$ ja $y_n > 0$. Koska (x_1, y_1) ovat positiivisista kokonaislukupareista muodostuvan jonon ensimmäinen jäsen, niin seurauksen 2.1 nojalla

$$x_n = x_1 x_{n-1} + d y_1 y_{n-1} \quad \text{ja} \quad y_n = x_1 y_{n-1} + y_1 x_{n-1}.$$

Näin ollen kun $n = 2$, niin

$$\begin{aligned} x_2 &= x_1 x_{2-1} + d y_1 y_{2-1} & \qquad y_2 &= x_1 y_{2-1} + y_1 x_{2-1} \\ &= x_1 x_1 + d y_1 y_1 & &= x_1 y_1 + y_1 x_1. \end{aligned}$$

Nyt koska $x_1 > 0$, $y_1 > 0$ ja $d > 0$, niin myös $x_2 > 0$ ja $y_2 > 0$. Oletetaan, että $x_k > 0$ ja $y_k > 0$. Osoitetaan sitten, että $x_{k+1} > 0$ ja $y_{k+1} > 0$. Koska $d > 0$,

$$\begin{aligned} x_{k+1} &= x_1 x_{k+1-1} + d y_1 y_{k+1-1} & \qquad y_{k+1} &= x_1 y_{k+1-1} + y_1 x_{k+1-1} \\ &= x_1 x_k + d y_1 y_k & &= x_1 y_k + y_1 x_k \end{aligned}$$

ja induktio-oletuksen nojalla $x_k > 0$ ja $y_k > 0$, niin $x_{k+1} > 0$ ja $y_{k+1} > 0$. Näin ollen induktioperiaatteen nojalla $x_n > 0$ ja $y_n > 0$ kaikilla luvun $n \in \mathbb{Z}_+$ arvoilla. □

Lause 2.5. *Olkoon* (x_1, y_1) *Pellin yhtälön* $x^2 - dy^2 = 1$ *positiivinen ratkaisu, jolle* $x_1 + \sqrt{d} y_1$ *on pienin. Jokaiselle positiiviselle kokonaisluvulle* n *määritellään* x_n *ja* y_n *yhtälöllä*

$$x_n + \sqrt{d} y_n = (x_1 + \sqrt{d} y_1)^n.$$

Tällöin Pellin yhtälön $x^2 - dy^2 = 1$ *kaikki ratkaisut saadaan ehdoista*

$$(x, y) = (\pm 1, 0) \quad \textit{ja} \quad (x, y) = (\pm x_n, \pm y_n),$$

missä kaikki etumerkkien yhdistelmävaihtoehdot sallitaan. Lisäksi nämä kaikki ratkaisut ovat erisuuria.

Todistus (vrt. [1, s. 180–181]). Lauseen 2.4 perusteella tiedetään, että kaikki yhtälön $(x_1 + \sqrt{d} y_1)^n = x_n + \sqrt{d} y_n$ ratkaisut (x_n, y_n) ovat itse asiassa yhtälön $x^2 - dy^2 = 1$ ratkaisuja.

Osoitetaan seuraavaksi, että kaikki ehdoista

$$(x, y) = (\pm 1, 0) \quad \text{ja} \quad (x, y) = (\pm x_n, \pm y_n),$$

missä kaikki etumerkkien yhdistelmävaihtoehdot sallitaan, saatavat ratkaisut (x, y) ovat erisuuria. Koska (x_1, y_1) on positiivisista kokonaislukupareista muodostuvan jonon, missä $(x_m, y_m) < (x_n, y_n)$, jos $x_m + \sqrt{d}y_m < x_n + \sqrt{d}y_n$, ensimmäinen jäsen, niin seurauksen 2.1 nojalla

$$x_n = x_1x_{n-1} + dy_1y_{n-1} \quad \text{ja} \quad y_n = x_1y_{n-1} + y_1x_{n-1},$$

ja koska oletuksen nojalla $x_1 > 0$ ja $y_1 > 0$, niin apulauseen 2.6 nojalla $x_n > 0$, $y_n > 0$ kaikilla luvun n arvoilla. Täten mikään ratkaisuista $(\pm x_n, \pm y_n)$ ei voi olla yhtä suuri kuin $(\pm 1, 0)$.

Osoitetaan sitten, että kaikki ratkaisut $(\pm x_n, \pm y_n)$ ovat erisuuria. Koska $x_n > 0$ ja $y_n > 0$, niin selvästi riittää osoittaa, että kaikki positiiviset ratkaisut (x_n, y_n) ovat erisuuria. Tehdään vastaoletus, että kaikki ratkaisut (x_n, y_n) eivät ole erisuuria. Tällöin on olemassa positiivinen kokonaisluku m, jolle $(x_n, y_n) = (x_m, y_m)$, kun $n < m$. (Yhtä hyvin ilman yleistettävyyden menetystä olisi voitu olettaa, että $m < n$.) Nyt lauseen 2.3 ja oletuksen nojalla saadaan

$$(x_1 + \sqrt{d}y_1)^n = x_n + \sqrt{d}y_n = x_m + \sqrt{d}y_m = (x_1 + \sqrt{d}y_1)^m,$$

joten

$$\frac{(x_1 + \sqrt{d}y_1)^m}{(x_1 + \sqrt{d}y_1)^n} = 1$$
$$(x_1 + \sqrt{d}y_1)^{m-n} = 1.$$

Kuitenkin koska (x_1, y_1) on positiivinen ratkaisu, niin apulauseen 2.5 nojalla saadaan $x_1 + \sqrt{d}y_1 > 1$. Tällöin koska oletuksen nojalla $m > n$, niin $(x_1 + \sqrt{d}y_1)^{m-n} > 1$. Siis on mahdotonta, että $(x_1 + \sqrt{d}y_1)^{m-n} = 1$. Täten kaikki kaavoilla

$$x_n = x_1x_{n-1} + dy_1y_{n-1} \quad \text{ja} \quad y_n = x_1y_{n-1} + y_1x_{n-1}$$

saatavat ratkaisut (x, y) ovat erisuuria.

Olkoon (u, v) mikä tahansa yhtälön $x^2 - dy^2 = 1$ ratkaisu. Koska

1. $(1, 0)$ ja $(-1, 0)$ ovat ainoat ratkaisut, joissa $x = 0$ tai $y = 0$, ja koska

2. jos (x, y) on ratkaisu, niin sitten myös $(\pm x, \pm y)$ on ratkaisu millä tahansa etumerkkien yhdistelmällä,

niin ilman yleistettävyyden menetystä voidaan olettaa, että $u > 0, v > 0$. Osoitetaan, että $(u, v) = (x_n, y_n)$ jollakin $n \geq 1$.

Koska oletuksen nojalla (x_1, y_1) on yhtälön $x^2 - dy^2 = 1$ positiivinen ratkaisu, jolle $x_1 + \sqrt{d}y_1$ on pienin, niin

$$x_1 + \sqrt{d}y_1 \leq u + \sqrt{d}v.$$

Väitetään, että on olemassa sellainen positiivinen kokonaisluku n, että

$$(x_1 + \sqrt{d}y_1)^n \leq u + \sqrt{d}v < (x_1 + \sqrt{d}y_1)^{n+1}.$$

Tiedetään, että $x_1 + \sqrt{d}y_1 > 1$, jolloin luvun $x_1 + \sqrt{d}y_1$ potensseista tulee mielivaltaisen suuria. Täten on olemassa luvun n suurin arvo, jolle

$$(x_1 + \sqrt{d}y_1)^n \leq u + \sqrt{d}v.$$

Epäyhtälön $x_1 + \sqrt{d}y_1 \leq u + \sqrt{d}v$ nojalla tämä suurin arvo luvulle n on vähintään 1. Lisäksi on selvää, että luvun n suurimmasta arvosta seuraa, että epäyhtälö

$$(x_1 + \sqrt{d}y_1)^n \leq u + \sqrt{d}v < (x_1 + \sqrt{d}y_1)^{n+1}$$

on tosi. Kerrotaan sitten epäyhtälö

$$(x_1 + \sqrt{d}y_1)^n \leq u + \sqrt{d}v < (x_1 + \sqrt{d}y_1)^{n+1}$$

puolittain luvulla $(x_1 - \sqrt{d}y_1)^n$. Tämä luku on positiivinen, koska $x_1 + \sqrt{d}y_1 > 0$ ja koska

$$1 = x_1^2 - dy_1^2 = (x_1 + \sqrt{d}y_1)(x_1 - \sqrt{d}y_1).$$

Tällöin lauseen 2.3 avulla saadaan

$$\begin{aligned}
& (x_1 + \sqrt{d}y_1)^n(x_1 - \sqrt{d}y_1)^n \leq (u + \sqrt{d}v)(x_1 - \sqrt{d}y_1)^n \\
& \qquad\qquad < (x_1 + \sqrt{d}y_1)^{n+1}(x_1 - \sqrt{d}y_1)^n \\
\Leftrightarrow\quad & (x_n + \sqrt{d}y_n)(x_n - \sqrt{d}y_n) \leq (u + \sqrt{d}v)(x_1 - \sqrt{d}y_1)^n \\
& \qquad\qquad < (x_1 + \sqrt{d}y_1)(x_n + \sqrt{d}y_n)(x_n - \sqrt{d}y_n) \\
\Leftrightarrow\quad & x_n^2 - dy_n^2 \leq (u + \sqrt{d}v)(x_1 - \sqrt{d}y_1)^n < (x_1 + \sqrt{d}y_1)(x_n^2 - dy_n^2) \\
\Leftrightarrow\quad & 1 \leq (u + \sqrt{d}v)(x_1 - \sqrt{d}y_1)^n < (x_1 + \sqrt{d}y_1) \cdot 1 \\
\Leftrightarrow\quad & 1 \leq (u + \sqrt{d}v)(x_1 - \sqrt{d}y_1)^n < x_1 + \sqrt{d}y_1.
\end{aligned}$$

Asetetaan

$$u_1 = ux_n - dvy_n, \quad v_1 = vx_n - y_nu.$$

Tällöin

$$\begin{aligned}(u+\sqrt{d}v)(x_1-\sqrt{d}y_1)^n &= (u+\sqrt{d}v)(x_n-\sqrt{d}y_n)\\ &= ux_n - \sqrt{d}y_nu + \sqrt{d}vx_n - dvy_n\\ &= (ux_n - dvy_n) + \sqrt{d}(vx_n - y_nu)\\ &= u_1 + \sqrt{d}v_1.\end{aligned}$$

Lisäksi sijoittamalla saadaan

$$\begin{aligned}u_1^2 - dv_1^2 &= (ux_n - dvy_n)^2 - d(vx_n - y_nu)^2\\ &= u^2x_n^2 - 2dux_nvy_n + d^2v^2y_n^2 - d(v^2x_n^2 - 2vx_ny_nu + y_n^2u^2)\\ &= u^2x_n^2 - 2dux_nvy_n + d^2v^2y_n^2 - dv^2x_n^2 + 2dvx_ny_nu - dy_n^2u^2\\ &= u^2x_n^2 + d^2v^2y_n^2 - dv^2x_n^2 - dy_n^2u^2\\ &= (u^2-dv^2)(x_n^2-dy_n^2).\end{aligned}$$

Nyt koska (u, v) ja (x_n, y_n) ovat yhtälön $x^2 - dy^2 = 1$ ratkaisuja, niin

$$(u^2 - dv^2)(x_n^2 - dy_n^2) = 1 \cdot 1 = 1.$$

Näin ollen myös $u_1^2 - dv_1^2 = 1$, joten (u_1, v_1) on yhtälön $x^2 - dy^2 = 1$ ratkaisu. Lisäksi koska edellä on osoitettu, että

$$1 \leq (u+\sqrt{d}v)(x_1-\sqrt{d}y_1)^n < x_1 + \sqrt{d}y_1$$

ja

$$(u+\sqrt{d}v)(x_1-\sqrt{d}y_1)^n = u_1 + \sqrt{d}v_1, \tag{2.1}$$

niin

$$1 \leq u_1 + \sqrt{d}v_1 < x_1 + \sqrt{d}y_1.$$

Jos $u_1 + \sqrt{d}v_1 > 1$, niin apulauseen 2.5 nojalla (u_1, v_1) on yhtälön $x^2 - dy^2 = 1$ positiivinen ratkaisu. Kuitenkin, jos asia on tällä tavoin, niin

$$1 \leq u_1 + \sqrt{d}v_1 < x_1 + \sqrt{d}y_1$$

mikä on ristiriidassa lauseen oletuksen kanssa, että (x_1, y_1) on Pellin yhtälön $x^2 - dy^2 = 1$ pienin ratkaisu. Näin ollen täytyy olla $u_1 + \sqrt{d}v_1 \leq 1$. Kuitenkin koska toisaalta

$$1 \leq u_1 + \sqrt{d}v_1 < x_1 + \sqrt{d}y_1,$$

niin on oltava $u_1 + \sqrt{d}v_1 = 1$. Tällöin yhtälön (2.1) perusteella myös

$$(u + \sqrt{d}v)(x_1 - \sqrt{d}y_1)^n = 1.$$

Edelleen kertomalla tämän yhtälön molemmat puolet luvulla $(x_1 + \sqrt{d}y_1)^n$ saadaan

$$\begin{aligned}
& (u + \sqrt{d}v)(x_1 - \sqrt{d}y_1)^n(x_1 + \sqrt{d}y_1)^n = (x_1 + \sqrt{d}y_1)^n \\
\Leftrightarrow \quad & (u + \sqrt{d}v)(x_n - \sqrt{d}y_n)(x_n + \sqrt{d}y_n) = x_n + \sqrt{d}y_n \\
\Leftrightarrow \quad & (u + \sqrt{d}v)(x_n^2 - dy_n^2) = x_n + \sqrt{d}y_n \\
\Leftrightarrow \quad & (u + \sqrt{d}v) \cdot 1 = x_n + \sqrt{d}y_n \\
\Leftrightarrow \quad & u + \sqrt{d}v = x_n + \sqrt{d}y_n.
\end{aligned}$$

Täten $u - x_n = \sqrt{d}(y_n - v)$. Jos $y_n - v \neq 0$, saadaan

$$\sqrt{d} = \left(\frac{u - x_n}{y_n - v}\right),$$

jolloin

$$d = \left(\frac{u - x_n}{y_n - v}\right)^2 \quad \Leftrightarrow \quad d = \frac{(u - x_n)^2}{(y_n - v)^2}.$$

Koska $d \in \mathbb{Z}_+$, niin $(y_n - v)^2 | (u - x_n)^2$. Tällöin aritmetiikan peruslauseen nojalla saadaan, että $(y_n - v) | (u - x_n)$. Näin ollen $(u - x_n)/(y_n - v)$ on kokonaisluku, joten d on neliöluku, mikä on ristiiidassa oletuksen kanssa, että d ei ole täydellinen neliö. Täten ristiriita on saavutettu ja $y_n - v = 0$ eli $y_n = v$. Koska edellä on osoitettu, että

$$u + \sqrt{d}v = (x_1 + \sqrt{d}y_1)^n$$

ja lauseen oletuksen nojalla tiedetään, että

$$(x_1 + \sqrt{d}y_1)^n = x_n + \sqrt{d}y_n,$$

niin

$$u + \sqrt{d}v = x_n + \sqrt{d}y_n.$$

Näin ollen saadaan $u = x_n$, joten olemme osoittaneet, että $(u, v) = (x_n, y_n)$. □

Esimerkki 2.7. Tarkastellaan yhtälöä $x^2 - 3y^2 = 1$. Aiemmin olemme todenneet, että $x = 2, y = 1$ on tämän yhtälön yksi ratkaisu. Tällöin pienimmän ratkaisun täytyy toteuttaa epäyhtälö

$$x_1 + \sqrt{3}y_1 \leq 2 + \sqrt{3} \cdot 1 < 4$$

ja täten $x_1 < 4$ ja $y_1 < 4$. Koska x_1 ja y_1 ovat positiivisia kokonaislukuja, niin $x_1 \leq 3$ ja $y_1 \leq 3$. Voidaan helposti huomata, että ainoa lukupari (x, y), joka on yhtälön $x^2 - 3y^2 = 1$ ratkaisu ja toteuttaa ehdot $0 < x \leq 3$ ja $0 < y \leq 3$, on nimenomaan $x = 2$ ja $y = 1$. Näin ollen $x_1 = 2$ ja $y_1 = 1$, ja triviaaliratkaisuja $x = \pm 1, y = 0$ lukuun ottamatta kaikki yhtälön $x^2 - 3y^2 = 1$ ratkaisut saadaan, kun $x = \pm x_n, y = \pm y_n$, missä

$$x_n + \sqrt{3}y_n = (2 + \sqrt{3} \cdot 1)^n.$$

Suorittamalla potenssiinkorotus $(2 + \sqrt{3} \cdot 1)^n$ eri arvoilla $n \in \mathbb{Z}_+$ ja tarkastelemalla näin saatuja lukuja voidaan havaita, että x_n ja y_n saadaan rekursiivisesti luvuista x_{n-1} ja y_{n-1} helpommin kaavojen

$$x_n = x_1 x_{n-1} + d y_1 y_{n-1} \quad \text{ja} \quad y_n = x_1 y_{n-1} + y_1 x_{n-1}$$

avulla, kun määritellään

$$x_n = 2x_{n-1} + 3y_{n-1}, \quad y_n = 2y_{n-1} + x_{n-1}.$$

Lause 2.5 antaa kaikki ratkaisut Pellin yhtälölle $x^2 - dy^2 = 1$, kun tiedetään pienin ratkaisu. Jos on löydetty mikä tahansa yhtälön $x^2 - dy^2 = 1$ ratkaisu, jolle $y \neq 0$, niin pienimmän ratkaisun määrittäminen on yksinkertaista. Kuitenkin käytännössä yhtälön $x^2 - dy^2 = 1$ ratkaisun määrittäminen voi olla haastava tehtävä, koska jopa pienillä muuttujan d arvoilla muuttujien x_1, y_1 pienimmät arvot voivat olla hyvin suuria. Esimerkiksi kun $d = 29$, niin $x_1 = 9801, y_1 = 1820$. Kaikkien ratkaisujen löytämiseksi on olemassa menetelmä, jota kutsutaan ketjumurtolukumenetelmäksi. Aihe on kuitenkin niin laaja, että se on suljettu tästä tutkielmasta sen vuoksi pois. Aihetta on käsitelty muun muassa Rosenin kirjassa [5].

2.4 Yksi yleistys

Tässä luvussa käsitellään tässä tutkielmassa pääasiallisesti käsiteltyä yhtälöä $x^2 - dy^2 = 1$ yleisempää yhtälöä $x^2 - dy^2 = k$, missä k on jokin kiinnitetty kokonaisluku. Osoitetaan seuraavaksi tätä yleisempää yhtälöä koskeva yksinkertainen tulos.

Yhtälöllä $x^2 - dy^2 = k$ ei välttämättä ole lainkaan ratkaisuja. Yleisenä esimerkkinä, jos $d = p$ on alkuluku, $p \nmid k$ ja k on neliönepäjäännös modulo p, niin yhtälöllä $x^2 - dy^2 = k$ ei voi olla ratkaisuja, sillä yhtälön $x^2 - dy^2 = k$ ratkaisu antaisi ratkaisun kongruenssille $x^2 \equiv k \pmod{p}$, mikä olisi ristiriidassa oletuksen k on neliönepäjäännös modulo p kanssa. [1, s. 182]

Lause 2.6. *Jos yhtälöllä $x^2 - dy^2 = k$ on yksi ratkaisu, niin sillä on äärettömän monta ratkaisua.*

Todistus (vrt. [1, s. 182]). Oletetaan, että (x_1, y_1) on yhtälön $x^2 - dy^2 = k$ ratkaisu ja (x_2, y_2) on yhtälön $x^2 - dy^2 = 1$ ratkaisu. Tällöin

$$x = x_1x_2 + dy_1y_2, \quad y = x_1y_2 + y_1x_2$$

on yhtälön $x^2 - dy^2 = k$ ratkaisu. Kun (x_2, y_2) käy läpi kaikki yhtälön $x^2 - dy^2 = 1$ ratkaisut huomataan, että saadaan ääretön määrä yhtälön $x^2 - dy^2 = k$ ratkaisuja. Tällaisia ratkaisuja, joilla $x_2 > 0, y_2 > 0$, on ääretön määrä. □

Esimerkki 2.8. Koska $9^2 - 3 \cdot 5^2 = 6$, määritellään x_n, y_n $(n \geq 0)$ ehdolla

$$x_n + \sqrt{3}y_n = (2 + \sqrt{3} \cdot 1)^n(9 + \sqrt{3} \cdot 5).$$

Tällöin $x_n^2 - 3y_n^2 = 6$, kun $n \geq 0$. Esimerkiksi jos $n = 1$, niin

$$\begin{aligned} x_1 &= 2 \cdot 9 + 3 \cdot 1 \cdot 5 = 18 + 15 = 33, \\ y_1 &= 2 \cdot 5 + 1 \cdot 9 = 10 + 9 = 19 \end{aligned}$$

ja

$$33^2 - 3 \cdot 19^2 = 1089 - 3 \cdot 361 = 1089 - 1083 = 6.$$

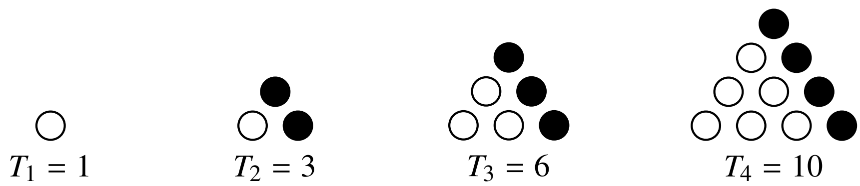
3 Kolmio-, neliö- ja viisikulmioluvut

Tässä luvussa tarkastellaan positiivisia kokonaislukuja, joiden osoittama määrä pisteitä voidaan järjestää jonkin säännöllisen monikulmion muotoiseksi kuvioksi. Tarkastelu rajataan positiivisiin kokonaislukuihin, joista voidaan tällä tavoin muodostaa tasasivuisia kolmioita, neliöitä tai säännöllisiä viisikulmioita. Erityisen mielenkiintoisia ovat luvut, joiden osoittamasta määrästä pisteitä voidaan muodostaa sekä kolmion että neliön muotoinen kuvio tai neliön ja viisikulmion muotoinen kuvio. Tällaiset luvut nimittäin tuottavat tiettyjen Pellin yhtälöiden ratkaisuja.

3.1 Määritelmät ja yleiset kaavat

Määritelmä 3.1 (vrt. [3, s. 2])**.** Positiivista kokonaislukua n sanotaan *kolmioluvuksi*, jos n pistettä voidaan järjestää siten, että ne muodostavat tasasivuisen kolmion muotoisen kuvion.

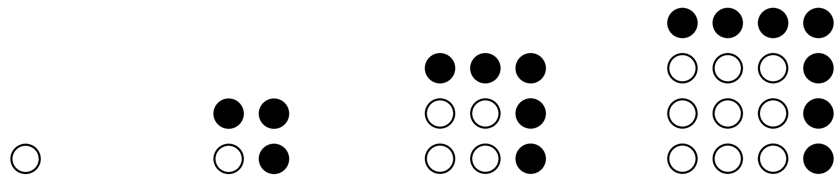
Esimerkki 3.1 (vrt. [3, s. 2])**.** Ensimmäiset neljä kolmiolukua ovat $1, 3, 6$ ja 10. Alla olevasta kuvasta 3.1 näkyy, miten kukin kolmioluku muodostaa tasasivuisen kolmion. Lisäksi alla olevassa kuvassa 3.1 tummennetut ympyrät näyttävät, miten seuraava kolmioluku on saatu edellisestä kolmioluvusta lisäämällä uusi sivu.



Kuva 3.1: Ensimmäiset neljä kolmiolukua.

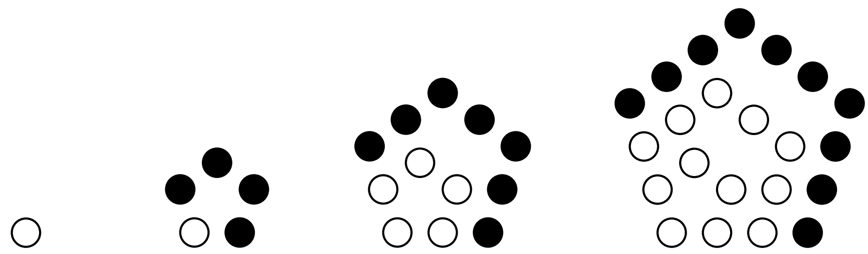
Määritelmä 3.2 (vrt. [3, s. 2])**.** Positiivista kokonaislukua n sanotaan *k-kulmioluvuksi*, jos n pistettä voidaan järjestää siten, että ne muodostavat säännöllisen k-kulmion.

Esimerkki 3.2 (vrt. [3, s. 2–3])**.** Edellä esimerkissä 3.1 näytettiin ensimmäiset neljä kolmiolukua, jotka vastaavat tapausta $k = 3$. Tapaukset $k = 4$ ja $k = 5$ puolestaan vastaavat neliö- ja viisikulmiolukuja. Näistä luvuista ensimmäiset neljä esitetään alla olevissa kuvissa 3.2 ja 3.3. Neliö- ja viisikulmiolukujen jono, kuten myös kolmiolukujen jono, alkaa erikoistapauksella, luvulla 1.



$S_1 = 1$ $S_2 = 4$ $S_3 = 9$ $S_4 = 16$

Kuva 3.2: Ensimmäiset neljä neliölukua.



$P_1 = 1$ $P_2 = 5$ $P_3 = 12$ $P_4 = 22$

Kuva 3.3: Ensimmäiset neljä viisikulmiolukua.

Kaava n. neliöluvulle S_n on selvästi $S_n = n^2$. Esimerkeissä 3.1 ja 3.2 esitetyistä ensimmäisistä neljästä kolmio- ja viisikulmioluvusta saadaan apua kolmio- ja viisikulmiolukujen, T_n ja P_n, kaavojen muodostamiseen. Näitä esimerkkitapauksia ja erityisesti tietoa siitä, miten edellisestä k-kulmioluvusta saadaan seuraava, hyödyntäen kolmio- ja viisikulmioluvut voidaan kirjoittaa aritmeettisen sarjan termien avulla. Tällöin

$$T_n = 1 + 2 + \cdots + n = \sum_{k=1}^{n} k,$$

$$P_n = 1 + 4 + \cdots + (3n - 2) = \sum_{k=1}^{n} (3k - 2).$$

Myös neliöluvut voidaan ilmaista summana $S_n = 1 + 3 + \cdots + (2n - 1) = \sum_{k=1}^{n} (2k - 1) = n^2$. Aritmeettisen sarjan A_n ensimmäisen n termin summa saadaan kaavalla

$$A_n = a_1 + a_2 + \cdots + a_n = \frac{n(a_1 + a_n)}{2} = \frac{n(2a_1 + (n-1)d)}{2},$$

joten kolmio- ja viisikulmioluvuille saadaan kaavat

$$T_n = \frac{n(2 \cdot 1 + (n-1) \cdot 1)}{2} = \frac{n(2 + n - 1)}{2} = \frac{n(n+1)}{2}$$

ja

$$P_n = \frac{n(2 \cdot 1 + (n-1) \cdot 3)}{2} = \frac{n(2 + 3n - 3)}{2} = \frac{n(3n-1)}{2}.$$

Käyttämällä näitä kaavoja saadaan selville ensimmäiset kymmenen kolmio-, neliö- ja viisikulmiolukua. Nämä luvut on esitetty alla taulukossa 3.1. [3, s. 3]

n	1	2	3	4	5	6	7	8	9	10
T_n	1	3	6	10	15	21	28	36	45	55
S_n	1	4	9	16	25	36	49	64	81	100
P_n	1	5	12	22	35	51	70	92	117	145

Taulukko 3.1: Ensimmäiset kymmenen kolmio-, neliö- ja viisikulmiolukua.

3.2 Kolmio-neliöluvut

Määritelmä 3.3 (vrt. [3, s. 3])**.** Positiivista kokonaislukua k sanotaan *kolmio-neliöluvuksi*, jos $k = T_m$ jollakin $m \in \mathbb{Z}_+$ ja $k = S_n$ jollakin $n \in \mathbb{Z}_+$.

Esimerkki 3.3 (vrt. [3, s. 3])**.** Taulukosta 3.1 nähdään, että luvun 1 ohella luku 36 on sekä kolmioluku että neliöluku, $36 = T_8 = S_6$. Näin ollen luvut 1 ja 36 ovat siis kolmio-neliölukuja.

Esimerkki 3.4. Koska $S_{35} = 35^2 = 1225$ ja

$$T_{49} = \frac{49(49+1)}{2} = \frac{49 \cdot 50}{2} = \frac{2450}{2} = 1225,$$

niin 1225 on kolmio-neliöluku.

Osoitetaan seuraavaksi, että kolmio-neliöluvut tuottavat tietyn Pellin yhtälön ratkaisuja. Siis kolmio-neliölukujen avulla voidaan löytää ratkaisuja tiettyyn Pellin yhtälöön ja vastaavasti tuon Pellin yhtälön ratkaisujen avulla voidaan löytää kolmio-neliölukuja.

Lause 3.1. *Kolmio-neliöluvut tuottavat yhtälön $x^2 - 2y^2 = 1$, missä x ja y ovat positiivisia kokonaislukuja, ratkaisuja, ja käänteisesti yhtälön $x^2 - 2y^2 = 1$ positiiviset kokonaislukuratkaisut tuottavat kolmio-neliölukuja.*

Todistus (vrt. [3, s. 3–4]). Oletetaan, että k on kolmio-neliöluku. Tällöin kolmio-neliölukujen määritelmän nojalla on olemassa sellaiset positiiviset kokonaisluvut m ja n, että $k = T_m = S_n$. Käyttämällä kolmiolukujen T_m ja neliölukujen S_n kaavoja saadaan

$$\begin{aligned}
T_m = S_n \quad &\Leftrightarrow \quad \frac{m(m+1)}{2} = n^2 \\
&\Leftrightarrow \quad m^2 + m = 2n^2 \\
&\Leftrightarrow \quad m^2 + m + \frac{1}{4} - \frac{1}{4} = 2n^2 \qquad || \cdot 4 \\
&\Leftrightarrow \quad 4m^2 + 4m + 1 - 1 = 2 \cdot 4n^2 \\
&\Leftrightarrow \quad (2m+1)^2 - 1 = 2(2n)^2 \\
&\Leftrightarrow \quad (2m+1)^2 - 2(2n)^2 = 1.
\end{aligned}$$

Siis $x = 2m + 1$, $y = 2n$ on yhtälön $x^2 - 2y^2 = 1$ ratkaisu.

Oletetaan kääntäen, että x, y on yhtälön $x^2 - 2y^2 = 1$ ratkaisu. Pellin yhtälöstä $x^2 - 2y^2 = 1$ eli $x^2 = 2y^2 + 1$ nähdään, että x^2 on pariton, joten myös x on pariton. Tällöin $x = 2m + 1$ jollakin kokonaisluvulla m. Sijoittamalla $x = 2m + 1$ Pellin yhtälöön $x^2 - 2y^2 = 1$ saadaan

$$\begin{aligned}
&(2m+1)^2 - 2y^2 = 1 \\
\Leftrightarrow \quad &4m^2 + 4m + 1 - 2y^2 = 1 \\
\Leftrightarrow \quad &-2y^2 = -4m^2 - 4m \quad ||: (-2) \\
\Leftrightarrow \quad &y^2 = 2m^2 + 2m.
\end{aligned}$$

Täten y^2 on parillinen, joten myös y on parillinen. Näin ollen $y = 2n$ jollakin kokonaisluvulla n. Nyt koska $x = 2m + 1, y = 2n$ on yhtälön $x^2 - 2y^2 = 1$ ratkaisu, niin edellä esitetyn ekvivalenssiketjun nojalla

$$(2m+1)^2 - 2(2n)^2 = 1 \quad \Leftrightarrow \quad T_m = S_n.$$

Merkitään $k = T_m = S_n$, jolloin k on kolmio-neliöluku. □

Esimerkki 3.5 (vrt. [3, s. 4])**.** Yhtälön $x^2 - 2y^2 = 1$ ratkaisuista $(x, y) = (3, 2)$ ja $(17, 12)$ saadaan kolmio-neliöluvut kirjoittamalla $x = 2m + 1$ ja $y = 2n$ kussakin tapauksessa lukujen m ja n löytämiseksi. Kun $(x, y) = (17, 12)$, niin

$$\begin{aligned}
&2m + 1 = x \;\Leftrightarrow\; 2m + 1 = 17 \;\Leftrightarrow\; 2m = 16 \;\Leftrightarrow\; m = 8 \quad \text{ja} \\
&2n = y \;\Leftrightarrow\; 2n = 12 \;\Leftrightarrow n = 6,
\end{aligned}$$

joten $T_8 = S_6$. Nyt kolmiolukujen tai neliölukujen kaavan avulla voidaan selvittää mistä kolmio-neliöluvusta on kyse. Kun $n = 6$, neliölukujen kaavasta saadaan $n^2 = 6^2 = 36$. Kolmiolukujen kaavasta saadaan

$$T_8 = \frac{n(n+1)}{2} = \frac{8(8+1)}{2} = \frac{8 \cdot 9}{2} = \frac{72}{2} = 36.$$

Tapaus $(x, y) = (3, 2)$ voidaan selvittää vastaavalla tavalla. Tällöin saadaan $T_1 = S_1 = 1$.

3.3 Neliö-viisikulmioluvut

Määritelmä 3.4 (vrt. [3, s. 4])**.** Positiivista kokonaislukua k sanotaan *neliö-viisikulmioluvuksi*, jos $k = S_m$ jollakin $m \in \mathbb{Z}_+$ ja $k = P_n$ jollakin $n \in \mathbb{Z}_+$.

Esimerkki 3.6. Tarkastellaan lukua 9801. Koska $m^2 = 9801 \Leftrightarrow m = 99$ tai $m = -99$ ja

$$\begin{aligned}
&\frac{n(3n-1)}{2} = 9801 \\
\Leftrightarrow\quad & 3n^2 - n = 19602 \\
\Leftrightarrow\quad & 3n^2 - n - 19602 = 0 \\
\Leftrightarrow\quad & n = 81 \quad \text{tai} \quad n = -\frac{242}{3},
\end{aligned}$$

niin on olemassa sellaiset positiiviset kokonaisluvut m ja n, että $S_m = P_n = 9801$. Siis $S_{99} = P_{81} = 9801$, joten luku 9801 on neliö-viisikulmioluku.

Osoitetaan seuraavaksi, että neliö-viisikulmioluvut tuottavat tietyn Pellin yhtälön ratkaisuja.

Lause 3.2 (vrt. [3, s. 4])**.** *Neliö-viisikulmioluvut tuottavat yhtälön $x^2 - 6y^2 = 1$, missä $x, y \in \mathbb{Z}_+$, ratkaisuja.*

Todistus. Olkoon k neliö-viisikulmioluku. Tällöin neliö-viisikulmiolukujen määritelmän nojalla on olemassa positiiviset kokonaisluvut m ja n niin, että $k = P_n = S_m$.

Hyödyntämällä neliölukujen S_m ja viisikulmiolukujen P_n kaavoja saadaan

$$\begin{aligned}
P_n = S_m \quad &\Leftrightarrow \quad \frac{n(3n-1)}{2} = m^2 \\
&\Leftrightarrow \quad 3n^2 - n = 2m^2 \quad \|\cdot 12 \\
&\Leftrightarrow \quad 36n^2 - 12n = 6 \cdot 2 \cdot 2m^2 \\
&\Leftrightarrow \quad 36n^2 - 12n + 1 - 1 = 6(2m)^2 \\
&\Leftrightarrow \quad (6n-1)^2 - 1 = 6(2m)^2 \\
&\Leftrightarrow \quad (6n-1)^2 - 6(2m)^2 = 1.
\end{aligned}$$

Siis $x = 6n - 1$, $y = 2m$ on yhtälön $x^2 - 6y^2 = 1$ ratkaisu. □

Esimerkki 3.7. Yhtälön $x^2 - 6y^2 = 1$ ratkaisut $(x, y) = (5, 2)$ ja $(485, 198)$ tuottavat neliö-viisikulmiolukuja. Sijoittamalla $x = 485$ ja $y = 198$ yhtälöihin $x = 6n - 1$ ja $y = 2m$ saadaan

$$\begin{aligned}
&x = 6n - 1 \ \Leftrightarrow \ 485 = 6n - 1 \ \Leftrightarrow \ 486 = 6n \ \Leftrightarrow \ n = 81, \\
&y = 2m \ \Leftrightarrow \ 198 = 2m \ \Leftrightarrow \ m = 99.
\end{aligned}$$

Siis Pellin yhtälön $x^2 - 6y^2 = 1$ ratkaisu $(485, 198)$ tuottaa neliö-viisikulmioluvun $S_{99} = P_{81} = 9801$. Vastaavasti toistamalla edellä esitetyt vaiheet ratkaisulle $(5, 2)$ saadaan $S_1 = P_1 = 1$.

Huomautus (vrt. [3, s. 4]). Vaikka kaikki neliö-viisikulmioluvut tuottavat Pellin yhtälön $x^2 - 6y^2 = 1$ ratkaisuja, niin päinvastainen ei pidä paikkaansa. Siis Pellin yhtälön $x^2 - 6y^2 = 1$ kaikki ratkaisut eivät tuota neliö-viisikulmiolukuja. Esimerkiksi $(49, 20)$ on yhtälön $x^2 - 6y^2 = 1$ ratkaisu mutta se ei tuota neliö-viisikulmiolukua, sillä

$$\begin{aligned}
&x = 6n - 1 \ \Leftrightarrow \ 49 = 6n - 1 \ \Leftrightarrow \ 50 = 6n \ \Leftrightarrow \ n = \frac{25}{3} \neq \mathbb{Z}_+, \\
&y = 2m \ \Leftrightarrow \ 20 = 2m \ \Leftrightarrow \ m = 10.
\end{aligned}$$

4 Pellin yhtälön yksi sovellus

Tässä luvussa konstruoidaan yhtälön $(x + y + z)^2 = xyz$ neljä positiivisten kokonaislukuratkaisujen perhettä. Näiden ratkaisuperheiden konstruoinnissa käytetään apuna yleistettyä Pellin yhtälöä $Ax^2 - By^2 = C$, sen Pellin resolventtia $r^2 - ABs^2 = 1$, näiden yhtälöiden fundamentaalisia ratkaisuja sekä lausetta 2.5. Tässä luvussa on käytetty lähteenä artikkelia [2] ja luvussa on noudatettu lähteen esitysjärjestystä.

4.1 Yleistetty Pellin yhtälö

Tässä alaluvussa tarkastellaan yleistettyä Pellin yhtälöä $Ax^2 - By^2 = C$ ja esitetään yleinen menetelmä sen ratkaisemiseksi.

Lause 4.1. *Olkoot A ja B sellaisia positiivisia kokonaislukuja, että AB ei ole täydellinen neliö, ja olkoon C nollasta eroava kokonaisluku. Jos yhtälöt $u^2 - ABv^2 = C$ ja $Aq^2 - Bt^2 = 1$ ovat ratkeavia, niin myös yhtälö*

$$Ax^2 - By^2 = C$$

on ratkeava ja sen kaikki ratkaisut (x, y) saadaan kaavoilla

$$x = q_0u + Bt_0v, \quad y = t_0u + Aq_0v,$$

missä (u, v) on mikä tahansa yleisen Pellin yhtälön $u^2 - ABv^2 = C$ ratkaisu ja (q_0, t_0) on yhtälön $Aq^2 - Bt^2 = 1$ pienin ratkaisu.

Todistus. Oletetaan, että (u, v) on yhtälön $u^2 - ABv^2 = C$ ratkaisu ja että (q_0, t_0) on yhtälön $Aq^2 - Bt^2 = 1$ pienin ratkaisu. Sijoittamalla $x = q_0u + Bt_0v$ ja $y = t_0u + Aq_0v$

saadaan

$$\begin{aligned}
Ax^2 - By^2 &= A(q_0u + Bt_0v)^2 - B(t_0u + Aq_0v)^2 \\
&= A(q_0^2u^2 + 2q_0uBt_0v + B^2t_0^2v^2) - B(t_0^2u^2 + 2t_0uAq_0v + A^2q_0^2v^2) \\
&= Aq_0^2u^2 + 2ABq_0t_0uv + AB^2t_0^2v^2 - Bt_0^2u^2 - 2ABq_0t_0uv - A^2Bq_0^2v^2 \\
&= Aq_0^2u^2 + AB^2t_0^2v^2 - Bt_0^2u^2 - A^2Bq_0^2v^2 \\
&= Aq_0^2u^2 - A^2Bq_0^2v^2 + AB^2t_0^2v^2 - Bt_0^2u^2 \\
&= Aq_0^2(u^2 - ABv^2) + Bt_0^2(ABv^2 - u^2) \\
&= Aq_0^2(u^2 - ABv^2) - Bt_0^2(u^2 - ABv^2) \\
&= (Aq_0^2 - Bt_0^2)(u^2 - ABv^2).
\end{aligned}$$

Nyt koska

$$Aq^2 - Bt^2 = 1 \quad \text{ja} \quad u^2 - ABv^2 = C,$$

niin

$$(Aq_0^2 - Bt_0^2)(u^2 - ABv^2) = 1 \cdot C = C.$$

Näin ollen (x, y), missä

$$x = q_0u + Bt_0v \quad \text{ja} \quad y = t_0u + Aq_0v,$$

on yhtälön $Ax^2 - By^2 = C$ ratkaisu.

Kääntäen oletetaan, että (x, y) on yhtälön $Ax^2 - By^2 = C$ ratkaisu ja että (q_0, t_0) on yhtälön $Aq^2 - Bt^2 = 1$ pienin ratkaisu. Olkoot $u = Aq_0x - Bt_0y$ ja $v = -t_0x + q_0y$. Tällöin

$$\begin{aligned}
u^2 - ABv^2 &= (Aq_0x + Bt_0y)^2 - AB(-t_0x + q_0y)^2 \\
&= A^2q_0^2x^2 - 2ABq_0t_0xy + B^2t_0^2y^2 - AB(t_0^2x^2 - 2q_0t_0xy + q_0^2y^2) \\
&= A^2q_0^2x^2 - 2ABq_0t_0xy + B^2t_0^2y^2 - ABt_0^2x^2 + 2ABq_0t_0xy - ABq_0^2y^2 \\
&= A^2q_0^2x^2 + B^2t_0^2y^2 - ABt_0^2x^2 - ABq_0^2y^2 \\
&= A^2q_0^2x^2 - ABq_0^2y^2 + B^2t_0^2y^2 - ABt_0^2x^2 \\
&= Aq_0^2(Ax^2 - By^2) + Bt_0^2(By^2 - Ax^2) \\
&= Aq_0^2(Ax^2 - By^2) - Bt_0^2(Ax^2 - By^2) \\
&= (Aq_0^2 - Bt_0^2)(Ax^2 - By^2) \\
&= 1 \cdot C = C.
\end{aligned}$$

Siis (u, v), missä

$$u = Aq_0x - Bt_0y \quad \text{ja} \quad v = -t_0x + q_0y,$$

on yleisen Pellin yhtälön $u^2 - ABv^2 = C$ ratkaisu. Muodostetaan yllä esitetyistä yhtälöistä yhtälöpari ja ratkaistaan se muuttujien x ja y suhteen. Tällöin saadaan

$$\begin{cases} Aq_0x - Bt_0y = u & \| \cdot q_0 \\ -t_0x + q_0y = v & \| \cdot Bt_0 \end{cases} \qquad \begin{cases} Aq_0x - Bt_0y = u & \| \cdot t_0 \\ -t_0x + q_0y = v & \| \cdot Aq_0 \end{cases}$$

$$+\begin{cases} Aq_0^2x - Bq_0t_0y = q_0u \\ -Bt_0^2x + Bq_0t_0y = Bt_0v \end{cases} \qquad +\begin{cases} Aq_0t_0x - Bt_0^2y = t_0u \\ -Aq_0t_0x + Aq_0^2y = Aq_0v \end{cases}$$

$$\begin{aligned} Aq_0^2x - Bt_0^2x &= q_0u + Bt_0v & \qquad Aq_0^2y - Bt_0^2y &= t_0u + Aq_0v \\ x(Aq_0^2 - Bt_0^2) &= q_0u + Bt_0v & y(Aq_0^2 - Bt_0^2) &= t_0u + Aq_0v \\ x \cdot 1 &= q_0u + Bt_0v & y \cdot 1 &= t_0u + Aq_0v \\ x &= q_0u + Bt_0v & y &= t_0u + Aq_0v. \end{aligned}$$

Näin ollen siis yhtälön $Ax^2 - By^2 = C$ ratkaisu (x, y) on muotoa $x = q_0u + Bt_0v$ ja $y = t_0u + Aq_0v$. □

Huomautus. Lähteessä on lauseessa 4.1 ja sen todistuksessa kolme painovirhettä. Lauseessa esiintyy virheellisesti (s_0, t_0) ja todistuksessa $(Aq_0^2 - Bt_0)^2(u^2 - ABv^2)$ ja $u = Ax_0x - Bt_0y$.

Lause 4.2. *Tarkastellaan kolmea lauseessa 4.1 esitettyä Diofantoksen yhtälöä*

(I) $Ax^2 - By^2 = C$

(II) $u^2 - ABv^2 = C$

(III) $Aq^2 - Bt^2 = 1.$

Seuraavat implikaatiot ovat tosia.

1. *Jos (II) ja (III) ovat ratkeavia, niin (I) on ratkeava.*
2. *Jos (I) ja (III) ovat ratkeavia, niin (II) on ratkeava.*
3. *Jos (I) ja (II) ovat ratkeavia ja on olemassa sellaiset ratkaisut (x, y) ja (u, v), että*

$$\frac{ux - Bvy}{C} \quad \textit{ja} \quad \frac{-Avx + uy}{C}$$

ovat molemmat kokonaislukuja, niin (III) on ratkeava.

Todistus. Ensimmäinen implikaatio osoitettiin todeksi lauseessa 4.1.

Osoitetaan sitten todeksi toinen implikaatio. Oletetaan, että (x, y) on yhtälön (I) $Ax^2 - By^2 = C$ ratkaisu ja että (q, t) on yhtälön (III) $Aq^2 - Bt^2 = 1$ ratkaisu. Olkoot $u = Aqx - Bty$ ja $v = -tx + qy$. Tällöin

$$\begin{aligned}
u^2 - ABv^2 &= (Aqx - Bty)^2 - AB(-tx + qy)^2 \\
&= (A^2q^2x^2 - 2ABqtxy + B^2t^2y^2) - AB(t^2x^2 - 2qtxy + q^2y^2) \\
&= A^2q^2x^2 - 2ABqtxy + B^2t^2y^2 - ABt^2x^2 + 2ABqtxy - ABq^2y^2 \\
&= A^2q^2x^2 + B^2t^2y^2 - ABt^2x^2 - ABq^2y^2 \\
&= A^2q^2x^2 - ABq^2y^2 + B^2t^2y^2 - ABt^2x^2 \\
&= Aq^2(Ax^2 - By^2) + Bt^2(By^2 - Ax^2) \\
&= Aq^2(Ax^2 - By^2) - Bt^2(Ax^2 - By^2) \\
&= (Aq^2 - Bt^2)(Ax^2 - By^2) \\
&= 1 \cdot C = C.
\end{aligned}$$

Näin ollen yhtälö (II) $u^2 - ABv^2 = C$ on ratkeva.

Kolmannen implikaation todistamiseksi olkoon (x, y) yhtälön (I) $Ax^2 - By^2 = C$ ratkaisu ja olkoon (u, v) yhtälön (II) $u^2 - ABv^2 = C$ ratkaisu. Olkoot

$$q = \frac{ux - Bvy}{C} \in \mathbb{Z} \quad \text{ja} \quad t = \frac{-Avx + uy}{C} \in \mathbb{Z}.$$

Nyt

$$\begin{aligned}
Aq^2 - Bt^2 &= A\left(\frac{ux - Bvy}{C}\right)^2 - B\left(\frac{-Avx + uy}{C}\right)^2 \\
&= A\left(\frac{u^2x^2 - 2Buvxy + B^2v^2y^2}{C^2}\right) - B\left(\frac{A^2v^2x^2 - 2Auvxy + u^2y^2}{C^2}\right) \\
&= \frac{Au^2x^2 - 2ABuvxy + AB^2v^2y^2}{C^2} + \frac{-A^2Bv^2x^2 + 2ABuvxy - Bu^2y^2}{C^2} \\
&= \frac{Au^2x^2 + AB^2v^2y^2 - A^2Bv^2x^2 - Bu^2y^2}{C^2} \\
&= \frac{Au^2x^2 - A^2Bv^2x^2 - Bu^2y^2 + AB^2v^2y^2}{C^2} \\
&= \frac{Ax^2(u^2 - ABv^2) - By^2(u^2 - ABv^2)}{C^2} \\
&= \frac{(Ax^2 - By^2)(u^2 - ABv^2)}{C^2} \\
&= \frac{C \cdot C}{C^2} = \frac{C^2}{C^2} = 1.
\end{aligned}$$

Siis yhtälö (III) $Aq^2 - Bt^2 = 1$ on ratkeava. $\square$

Huomautus. Lähteessä lauseen 4.2 todistuksessa on neljä painovirhettä. Siellä mainitaan kahteen kertaan virheellisesti (q, t) yhtälön (II) ratkaisuna. Lisäksi todistuksessa esiintyy virheellisesti $u = Aqx - Bt$ ja $(ux - Bvy)/c$.

Jatkossa tarkoituksena ei ole löytää yhtälön $Ax^2 - By^2 = C$ kaikkia ratkaisuja vaan ideana on löytää ratkaisuperhe. Tällainen ratkaisuperhe voidaan generoida seuraavalla tavalla. Oletetaan, että (x_0, y_0) on yhtälön $Ax^2 - By^2 = C$ ratkaisu ja että (r_m, s_m), kun $m \geq 1$, on yleinen ratkaisu yhtälön $Ax^2 - By^2 = C$ *Pellin resolventille* $r^2 - ABs^2 = 1$. Olkoot

$$x_m = x_0 r_m + B y_0 s_m \quad \text{ja} \quad y_m = y_0 r_m + A x_0 s_m.$$

Tällöin

$$\begin{aligned}
Ax_m^2 - By_m^2 =& A(x_0 r_m + B y_0 s_m)^2 - B(y_0 r_m + A x_0 s_m)^2 \\
=& A(x_0^2 r_m^2 + 2B x_0 y_0 r_m s_m + B^2 y_0^2 s_m^2) \\
&- B(y_0^2 r_m^2 + 2A x_0 y_0 r_m s_m + A^2 x_0^2 s_m^2) \\
=& A x_0^2 r_m^2 + 2AB x_0 y_0 r_m s_m + AB^2 y_0^2 s_m^2 \\
&- B y_0^2 r_m^2 - 2AB x_0 y_0 r_m s_m - A^2 B x_0^2 s_m^2 \\
=& A x_0^2 r_m^2 + AB^2 y_0^2 s_m^2 - B y_0^2 r_m^2 - A^2 B x_0^2 s_m^2 \\
=& A x_0^2 r_m^2 - B y_0^2 r_m^2 + AB^2 y_0^2 s_m^2 - A^2 B x_0^2 s_m^2 \\
=& r_m^2 (A x_0^2 - B y_0^2) + AB s_m^2 (B y_0^2 - A x_0^2) \\
=& r_m^2 (A x_0^2 - B y_0^2) - AB s_m^2 (A x_0^2 - B y_0^2) \\
=& (r_m^2 - AB s_m^2)(A x_0^2 - B y_0^2) \\
=& 1 \cdot C = C,
\end{aligned}$$

joten (x_m, y_m), missä $m \geq 1$, on myös yhtälön $Ax^2 - By^2 = C$ ratkaisu.

Huomautus. Lähteessä on yllä olevassa tekstissä kaksi painovirhettä. Lukujen x_m ja y_m kaavoissa esiintyy virheellisesti $x_m = x_0 u_m$ ja $y_m = y_0 u_m + A x_0 v_m$.

4.2 Neljä ratkaisuperhettä

Tässä alaluvussa konstruoidaan yhtälön $(x + y + z)^2 = xyz$ neljä positiivisten kokonaislukuratkaisujen perhettä. Tämä ratkaisuperheiden muodostaminen aloitetaan näyttämällä, kuinka suorittamalla tiettyjä muunnoksia ja muokkaamalla yhtälöä $(x+y+z)^2 = xyz$ saadaan yleistetty Pellin yhtälö $(b-4)u^2-bv^2 = 4((2a+b)^2-a^2b)$. Tämän jälkeen esitetään, miten edelleen sijoittamalla yleistettyyn Pellin yhtälöön neljän erisuuren positiivisen kokonaislukuparin (a, b) arvot saadaan vastaavasti neljä yleistettyä Pellin yhtälöä. Lopuksi näytetään, kuinka näiden yhtälöiden, niiden Pellin resolventtien $r^2 - ABs^2 = 1$ sekä näiden kaikkien yhtälöiden fundamentaalisten ratkaisujen avulla voidaan konstruoida yhtälön $(x + y + z)^2 = xyz$ neljä positiivisten kokonaislukuratkaisujen perhettä. Tässä ratkaisuperheiden konstruoinnissa hyödynnetään lausetta 2.5, jonka perusteella, jos $d \in \mathbb{Z}_+$ ei ole täydellinen neliö, niin Pellin yhtälö $r^2 - ds^2 = 1$ on ratkeava ja sen kaikki ratkaisut saadaan kaavalla

$$r_m + s_m\sqrt{d} = (r_1 + s_1\sqrt{d})^m, \text{ kun } m \geq 1,$$

missä (r_1, s_1) on yhtälön $r^2 - ds^2 = 1$ pienin ei-triviaalinen ratkaisu.

Aloitetaan suorittamalla muunnokset

$$x = \frac{u+v}{2} + a, \quad y = \frac{u-v}{2} + a, \quad z = b,$$

missä a ja b ovat nollasta eroavia kokonaislukuparametreja, jotka määritetään sopivalla tavalla. Sijoittamalla saadaan

$$\begin{aligned}
&(x + y + z)^2 = xyz \\
\Leftrightarrow\ &\left(\left(\frac{u+v}{2} + a\right) + \left(\frac{u-v}{2} + a\right) + b\right)^2 = \left(\frac{u+v}{2} + a\right)\left(\frac{u-v}{2} + a\right) \cdot b \\
\Leftrightarrow\ &\left(\left(\frac{u+v}{2} + \frac{a}{2}\right) + \left(\frac{u-v}{2} + \frac{a}{2}\right) + \frac{b}{2}\right)^2 = \left(\frac{u^2-v^2}{4} + \frac{a(u+v)}{2} + \frac{a(u-v)}{2} + a^2\right) \cdot b \\
\Leftrightarrow\ &\left(\frac{2u}{2} + \frac{2a}{2} + \frac{2b}{2}\right)^2 = \left(\frac{u^2-v^2}{4} + \frac{2a(u+v) + 2a(u-v)}{4} + \frac{4a^2}{4}\right) \cdot b \\
\Leftrightarrow\ &\left(\frac{2(u+2a+b)}{2}\right)^2 = \left(\frac{u^2 - v^2 + 2au + 2av + 2au - 2av + 4a^2}{4}\right) \cdot b \\
\Leftrightarrow\ &(u + 2a + b)^2 = \left(\frac{u^2 - v^2 + 4au + 4a^2}{4}\right) \cdot b \\
\Leftrightarrow\ &(u + 2a + b)^2 = \left(\frac{u^2 - v^2}{4} + \frac{4(au + a^2)}{4}\right) \cdot b
\end{aligned}$$

$$\Leftrightarrow (u+2a+b)^2 = \frac{b}{4}(u^2-v^2) + abu + a^2b.$$

Edelleen soveltamalla ehtoja $2(2a+b) = ab$ ja $b(b-4) > 0$ edellä saatuun yhtälöön saadaan

$$\begin{aligned}
& (u+2a+b)^2 = \frac{b}{4}(u^2-v^2) + abu + a^2b \\
\Leftrightarrow\quad & u^2 + 2au + bu + 2au + 4a^2 + 2ab + bu + 2ab + b^2 = \frac{b}{4}(u^2-v^2) + abu + a^2b \\
\Leftrightarrow\quad & u^2 + 4au + 2bu + 4a^2 + 4ab + b^2 = \frac{b}{4}(u^2-v^2) + abu + a^2b \\
\Leftrightarrow\quad & u^2 + 4a^2 + 4ab + b^2 + u(4a+2b) = \frac{b}{4}(u^2-v^2) + abu + a^2b \\
\Leftrightarrow\quad & u^2 + 4a^2 + 4ab + b^2 + uab = \frac{b}{4}(u^2-v^2) + abu + a^2b \\
\Leftrightarrow\quad & u^2 + (2a+b)^2 = \frac{b}{4}(u^2-v^2) + a^2b \\
\Leftrightarrow\quad & 4u^2 + 4(2a+b)^2 = bu^2 - bv^2 + 4a^2b \\
\Leftrightarrow\quad & 4u^2 - bu^2 + bv^2 = -4(2a+b) + 4a^2b \\
\Leftrightarrow\quad & -4u^2 + bu^2 - bv^2 = 4(2a+b) - 4a^2b \\
\Leftrightarrow\quad & (b-4)u^2 - bv^2 = 4\big((2a+b)^2 - a^2b\big).
\end{aligned}$$

Muokkaamalla edellä sovellettuja ehtoja saadaan

$$\begin{aligned}
& 2(2a+b) = ab \\
\Leftrightarrow\quad & ab - 4a - 2b = 0 \\
\Leftrightarrow\quad & ab - 4a - 2b + 8 = 8 \\
\Leftrightarrow\quad & (a-2)(b-4) = 8
\end{aligned}$$

ja

$$b(b-4) > 0 \quad \Leftrightarrow \quad (b < 0 \ \text{ tai } \ b > 4).$$

Alla olevassa taulukossa 4.1 on esitetty ainoat positiiviset kokonaislukuparit, jotka toteuttavat nämä ehdot.

(a,b)	$(a-2)(b-4)=8$
$(3,12)$	$(3-2)(12-4)=1\cdot 8=8$
$(4,8)$	$(4-2)(8-4)=2\cdot 4=8$
$(6,6)$	$(6-2)(6-4)=4\cdot 2=8$
$(10,5)$	$(10-2)(5-4)=8\cdot 1=8$

Taulukko 4.1: Positiiviset kokonaislukuparit, joille $(a-2)(b-4)=8$ ja ($b<0$ tai $b>4$).

Sijoittamalla $a=3$ ja $b=12$ yhtälöön $(b-4)u^2-bv^2=4((2a+b)^2-a^2b)$ saadaan

$$\begin{aligned} & (12-4)u^2-12v^2=4((2\cdot 3+12)-3^2\cdot 12) \\ \Leftrightarrow\quad & 8u^2-12v^2=4(18^2-9\cdot 12) \qquad \|:4 \\ \Leftrightarrow\quad & 2u^2-3v^2=324-108 \\ \Leftrightarrow\quad & 2u^2-3v^2=216. \end{aligned}$$

(Kuten edellä esitetystä ekvivalenssiketjusta voidaan huomata, niin yleistetyn Pellin yhtälön kertoimet voivat muuttua, kun kertoimia supistetaan.) Nyt koska

$$2u^2-3v^2=216 \quad\Leftrightarrow\quad 2u^2=3v^2+216 \quad\Leftrightarrow\quad u^2=\frac{3v^2+216}{2},$$

niin yhtälön $2u^2-3v^2=216$ fundamentaalinen ratkaisu voidaan löytää etsimällä positiivinen kokonaisluku v, jolla $(3v^2+216)/2$ on neliö, ja sitten ratkaisemalla luku u edellisestä yhtälöstä. Kokeilemalla havaitaan, että pienin tällainen positiivinen kokonaisluku on $v=12$. Tällöin

$$\frac{3v^2+216}{2}=\frac{3\cdot 12^2+216}{2}=\frac{3\cdot 144+216}{2}=\frac{432+216}{2}=\frac{648}{2}=324,$$

joten $u^2=324$ eli $u=18$ tai $u=-18$. Tarkoituksena on löytää positiivinen kokonaislukuratkaisu, joten yhtälön $2u^2-3v^2=216$ fundamentaaliseksi ratkaisuksi saadaan $(18,12)$.

Yleisesti yhtälön $Au^2-Bv^2=C$ Pellin resolventti on muotoa $r^2-ABs^2=1$. Näin ollen yhtälön $2u^2-3v^2=216$ Pellin resolventti on $r^2-2\cdot 3s^2=1$ eli $r^2-6s^2=1$. Tämän Pellin resolventin fundamentaalinen ratkaisu saadaan selville samaan tapaan kuin yhtälön $2u^2-3v^2=216$ fundamentaalinen ratkaisu. Kirjoitetaan $r^2-6s^2=1$

eli $r^2 = 6s^2 + 1$. Nyt koska

$$5^2 = 25 = 24 + 1 = 6 \cdot 4 + 1 = 6 \cdot 2^2 + 1,$$

niin yhtälön $r^2 - 6s^2 = 1$ fundamentaalinen ratkaisu on $(5, 2)$. Täten on siis saatu selville yleistetty Pellin yhtälö $(b-4)u^2 - bv^2 = 4((2a+b)^2 - a^2b)$, kun $(a, b) = (3, 12)$, tämän yhtälön Pellin resolventti sekä näiden kummankin yhtälön fundamentaalinen ratkaisu. Vastaavat tiedot tapauksissa $(a, b) = (4, 8)$, $(6, 6)$ ja $(10, 5)$ saadaan selville samalla tavoin kuin edellä tapauksessa $(a, b) = (3, 12)$. Nämä tiedot on esitetty taulukossa 4.2.

(a,b)	Yleistetty Pellin yhtälö $(b-4)u^2 - bv^2 = 4((2a+b)^2 - a^2b)$ ja sen fundamentaalinen ratkaisu	Pellin resolventti ja sen fundamentaalinen ratkaisu
$(3, 12)$	$2u^2 - 3v^2 = 216, (18, 12)$	$r^2 - 6s^2 = 1, (5, 2)$
$(4, 8)$	$u^2 - 2v^2 = 128, (16, 8)$	$r^2 - 2s^2 = 1, (3, 2)$
$(6, 6)$	$u^2 - 3v^2 = 216, (18, 6)$	$r^2 - 3s^2 = 1, (2, 1)$
$(10, 5)$	$u^2 - 5v^2 = 500, (25, 5)$	$r^2 - 5s^2 = 1, (9, 4)$

Taulukko 4.2: Yleistetyt Pellin yhtälöt eri kokonaislukupareilla (a, b), näiden yhtälöiden Pellin resolventit sekä kaikkien yhtälöiden fundamentaaliset ratkaisut.

Käyttämällä tämän tutkielman sivulla 41 muodostettuja kaavoja $u_m = u_0r_m + Bv_0s_m$, $v_m = v_0r_m + Au_0s_m$ ja yhtälön $2u^2 - 3v^2 = 216$ fundamentaalista ratkaisua $(18, 12)$ saadaan

$$\begin{aligned} u_m^{(1)} &= 18r_m^{(1)} + 3 \cdot 12s_m^{(1)} = 18r_m^{(1)} + 36s_m^{(1)}, \\ v_m^{(1)} &= 12r_m^{(1)} + 2 \cdot 18s_m^{(1)} = 12r_m^{(1)} + 36s_m^{(1)}. \end{aligned}$$

Lauseen 2.5 perusteella Pellin yhtälön $r^2 - ds^2 = 1$, missä $d \in \mathbb{Z}_+$, kaikki ratkaisut (r_m, s_m) saadaan kaavalla

$$r_m + s_m\sqrt{d} = (r_1 + s_1\sqrt{d})^m, \text{ kun } m \geq 1,$$

missä (r_1, s_1) on yhtälön $r^2 - ds^2 = 1$ pienin ei-triviaalinen ratkaisu. Näin ollen yhtälön $2u^2 - 3v^2 = 216$ Pellin resolventin $r^2 - 6s^2 = 1$ ja tämän resolventin fundamentaalisen ratkaisun $(5, 2)$ avulla saadaan ratkaisut $(r_m^{(1)}, s_m^{(1)})$ kaavalla

$$r_m^{(1)} + s_m^{(1)}\sqrt{6} = (5 + 2\sqrt{6})^m, \text{kun } m \geq 1.$$

Kun tapauksille $(a, b) = (4, 8)$, $(6, 6)$ ja $(10, 5)$ toistetaan samat vaiheet kuin edellä tapaukselle $(a, b) = (3, 12)$, niin yhtälöihin $(b-4)u^2 - bv^2 = 4\big((2a+b)^2 - a^2 b\big)$ saadaan seuraavat ratkaisujen jonot

$$u_m^{(1)} = 18r_m^{(1)} + 36s_m^{(1)}, \quad v_m^{(1)} = 12r_m^{(1)} + 36s_m^{(1)},$$

missä $r_m^{(1)} + s_m^{(1)}\sqrt{6} = (5 + 2\sqrt{6})^m$, kun $m \geq 1$,

$$u_m^{(2)} = 16r_m^{(2)} + 16s_m^{(2)}, \quad v_m^{(2)} = 8r_m^{(2)} + 16s_m^{(2)},$$

missä $r_m^{(2)} + s_m^{(2)}\sqrt{2} = (3 + 2\sqrt{2})^m$, kun $m \geq 1$,

$$u_m^{(3)} = 18r_m^{(3)} + 18s_m^{(3)}, \quad v_m^{(3)} = 6r_m^{(3)} + 18s_m^{(3)},$$

missä $r_m^{(3)} + s_m^{(3)}\sqrt{3} = (2 + \sqrt{3})^m$, kun $m \geq 1$,

$$u_m^{(4)} = 25r_m^{(4)} + 25s_m^{(4)}, \quad v_m^{(4)} = 5r_m^{(4)} + 25s_m^{(4)},$$

missä $r_m^{(4)} + s_m^{(4)}\sqrt{5} = (9 + 4\sqrt{5})^m$, kun $m \geq 1$.

Soveltamalla sitten kaavoja

$$x = \frac{u + v}{2} + a, \quad y = \frac{u - v}{2} + a, \quad z = b$$

edellä esitettyihin ratkaisujen jonoihin saadaan neljä perhettä nollasta eroavia kokonaislukuratkaisuja yhtälöön $Ax^2 - By^2 = C$. Ensimmäisessä ratkaisujen jonossa

$$u_m^{(1)} = 18r_m^{(1)} + 36s_m^{(1)}, \quad v_m^{(1)} = 12r_m^{(1)} + 36s_m^{(1)},$$

joten

$$\begin{aligned}
x_m^{(1)} &= \frac{(18r_m^{(1)} + 36s_m^{(1)}) + (12r_m^{(1)} + 36s_m^{(1)})}{2} + 3 \\
&= \frac{30r_m^{(1)} + 72s_m^{(1)}}{2} + 3 \\
&= 15r_m^{(1)} + 36s_m^{(1)} + 3, \\
y_m^{(1)} &= \frac{(18r_m^{(1)} + 36s_m^{(1)}) - (12r_m^{(1)} + 36s_m^{(1)})}{2} + 3 \\
&= \frac{6r_m^{(1)}}{2} + 3 \\
&= 3r_m^{(1)} + 3, \\
z_m^{(1)} &= 12.
\end{aligned}$$

Soveltamalla edelleen edellä esitettyjä kaavoja luvuille x, y ja z tapauksissa $(a, b) = (4, 8), (6, 6)$ ja $(10, 5)$ saadaan yhteensä neljä ratkaisuperhettä yhtälöön $(x+y+z)^2 = xyz$. Nämä positiivisten kokonaislukuratkaisujen perheet ovat

$$\begin{aligned}
x_m^{(1)} &= 15r_m^{(1)} + 36s_m^{(1)} + 3, & y_m^{(1)} &= 3r_m^{(1)} + 3, & z_m^{(1)} &= 12, \quad \text{kun } m \geq 1,\\
x_m^{(2)} &= 12r_m^{(2)} + 16s_m^{(2)} + 4, & y_m^{(2)} &= 4r_m^{(2)} + 4, & z_m^{(2)} &= 8, \quad \text{kun } m \geq 1,\\
x_m^{(3)} &= 12r_m^{(3)} + 18s_m^{(3)} + 6, & y_m^{(3)} &= 6r_m^{(3)} + 6, & z_m^{(3)} &= 6, \quad \text{kun } m \geq 1,\\
x_m^{(4)} &= 15r_m^{(4)} + 25s_m^{(4)} + 10, & y_m^{(4)} &= 10r_m^{(4)} + 10, & z_m^{(4)} &= 5, \quad \text{kun } m \geq 1.
\end{aligned}$$

Lähteet

[1] William W. Adams & Larry Joel Goldstein. *Introduction to Number Theory*. Prentice-Hall, Inc., Englewood Cliffs, New Jersey, 1976.

[2] Titu Andreescu. *A note on the equation* $(x+y+z)^2 = xyz$. General Mathematics 10 (2002), 17–22.

[3] Keith Conrad. *Pell's Equation, I*, Expository papers, University of Connecticut, [Verkkodokumentti], [Viitattu 11.05.2017].
URL: http://www.math.uconn.edu/~kconrad/blurbs/ugradnumthy/pelleqn1.pdf

[4] Keith Conrad. *Pell's Equation, II*, Expository papers, University of Connecticut, [Verkkodokumentti], [Viitattu 11.05.2017].
URL: http://www.math.uconn.edu/~kconrad/blurbs/ugradnumthy/pelleqn2.pdf

[5] Kenneth H. Rosen. *Elementary Number Theory and Its Applications*. 6th edition. Addison-Wesley, USA, 2011.