Tampereen yliopisto

Agnesa Ujkani

KETJUMURTOLUVUT

henkilöhistoriaa ja teoriaa

Informaatioteknologian ja viestinnän tiedekunta
Pro gradu -tutkielma
Toukokuu 2024

Tiivistelmä

Agnesa Ujkani: Ketjumurtoluvut: henkilöhistoriaa ja teoriaa
Pro gradu -tutkielma
Tampereen yliopisto
Matematiikan maisteriohjelma
Toukokuu 2024

Tässä pro gradu -tutkielmassa tarkastellaan äärellisiä ja äärettömiä ketjumurtolukuja sekä Pellin yhtälöä, ja lisäksi esitetään muutamien aiheeseen liittyvien matemaatikoiden henkilöhistoriaa.

Alussa tutustutaan Fibonaccin lukuihin ja niiden taustoihin, minkä ohessa esitellään lyhyesti keskiajan maineikkain matemaatikko, Leonardo Fibonacci. Kolmannessa luvussa käsitellään lineaarisia Diofantoksen yhtälöitä ja niiden ratkaisemista.

Neljännessa luvussa keskitytään äärellisten ja äärettömien ketjumurtolukujen ominaisuuksiin ja konvergentteihin. Aluksi esitellään lyhyesti Srinivasa Ramanujanin ja Rafael Bombellin elämäntarinoita, molemmat matemaatikot liittyvät ketjumurtolukujen historiaan. Sen jälkeen määritellään äärelliset ketjumurtoluvut ja osoitetaan, että mikä tahansa rationaaliluku voidaan esittää yksinkertaisena äärellisenä ketjumurtolukuna. Seuraavaksi tarkastellaan äärellisten ketjumurtolukujen konvergentteja ja havaitaan, että konvergentit vaihtelevat parillisilla ja parittomilla indekseillä siten, että parillisen indeksin konvergentit ovat aina suurempia kuin vastaavat parittoman indeksin konvergentit. Tutustutaan myös matemaatikoihin John Wallis sekä William Brouncker. Ketjumurtoluvut ovat äärettömiä murtolukuesityksiä, jotka käyttävät jatkuvaa jakoa, ja ne mahdollistavat tarkan kuvauksen irrationaaliluvuille. Brounckerin työllä ja myöhemmillä tutkimuksilla on osoitettu, että jokaisella irrationaaliluvulla on yksikäsitteinen ketjumurtolukuesitys. Tämä on johtanut monien ketjumurtolukujen ominaisuuksien ja niiden suhteeseen irrationaalilukuihin liittyvien tulosten todistamiseen.

Lopuksi tutustutaan matemaatikko John Pelliin sekä määritellään Pellin yhtälön perusratkaisu ja tutkitaan yhtälön kaikkien positiivisten ratkaisujen muodostamista. Tutkielman päälähteenä on käytetty David M. Burtonin teosta "Elementary Number Theory".

Avainsanat: Fibonacci-luvut, Diofantoksen yhtälöt, ketjumurtoluvut, Pellin yhtälö

Sisällys

1 Johdanto

Tässä tutkielmassa käsitellään äärellisiä ja äärettömiä ketjumurtolukuja, sekä niiden sovellusta, Pellin yhtälöä. Tutkielman pääpaino on yksinkertaisissa ketjumurtoluvuissa. Tutkielma aloitetaan tutustumalla Fibonaccin lukuihin ja niiden alkuperään. Samalla esitellään lyhyesti keskiajan tunnetuin matemaatikko, Leonardo Fibonacci. Kolmannessa luvussa keskitytään Diofantoksen lineaaristen yhtälöiden käsittelyyn ja niiden ratkaisemiseen.

Neljännessä luvussa keskitytään äärellisiin sekä äärettömiin ketjumurtolukuihin. Luvussa esitellään äärellisiin ketjumurtolukuihin liittyviä määritelmiä, sekä niiden ominaisuuksia. Luvussa todistetaan äärellisten ketjumurtolukujen ja rationaalilukujen välinen yhteys, eli kuinka jokainen yksinkertainen äärellinen ketjumurtoluku esittää rationaalilukua, ja jokainen rationaaliluku vastaa yksinkertaista äärellistä ketjumurtolukua. Lisäksi neljännessä luvussa käsitellään ketjumurtolukujen konvergentteja, ja niiden tärkeimpiä ominaisuuksia. Seuraavaksi käsitellään äärettomiä ketjumurtolukuja, ja osoitetaan äärettömien ketjumurtolukujen ja irrationaalilukujen välinen yhteys. Osoitetaan, että jokainen yksinkertainen ääretön ketjumurtoluku vastaa irrationaalilukua ja vastaavasti jokainen irrationaaliluku voidaan esittää yksikäsitteisesti yksinkertaisena äärettömänä ketjumurtolukuna. Alilukujen alussa esitellään lyhyesti matemaatikot Srinivasa Ramanujan, Rafael Bombelli, John Wallis sekä William Brouncker.

Tutkielman viimeisessä luvussa käsitellään Pellin yhtälöä, $x^2 - dy^2 = 1$. Tämä osio aloitetaan esittelemällä matemaatikko John Pell. Luvussa tarkastellaan, miten $\sqrt{d}$-jaksollisen ketjumurtolukuesityksen konvergentit ja Pellin yhtälön ratkaisut liittyvät toisiinsa. Lopuksi tarkastellaan Pellin yhtälön kaikkien ratkaisuiden muodostumista luvun pituuden avulla.

2 Fibonacci

Tässä luvussa tutustutaan Fibonaccin lukuihin. Aluksi esitellään Leonardo Fibonaccin elämää ja hänen merkityksellisemmät teoksensa.

2.1 Leonardo Fibonacci 1180-1250

Fibonacci oli kenties keskiajan arvostetuin matemaatikko. Hän syntyi Pisassa Italiassa ja sai koulutuksensa Pohjois-Afrikassa, missä hänen isänsä työskenteli. Matkustaessaan Välimeren ympäri hän vieraili Espanjassa, Egyptissä, Syyriassa ja Kreikassa. Palattuaan Italiaan hän kirjoitti kuuluisan teoksensa Liber Abaci, joka esitteli latinalaiselle lännelle islamilaisen aritmetiikan ja algebralliset matemaattiset käytännöt. Fibonacci kirjoitti myös teoksen Liber Quadratorum (1225), joka keskittyi täysin Diofantoksen yhtälöön. (vrt. [1, s. 283])

2.2 Fibonaccin luvut

Tässä alaluvussa esitellään Fibonaccin Liber Abaci -teoksessa esittämä ongelma, joka liittyy kanien jälkeläisten määrään. (vrt. [3, kpl. 2]).

Oletetaan, että mies sijoittaa yhden kaniparin paikkaan, joka on täysin ympäröity seinällä. Kanien luonne on sellainen, että joka kuukausi jokainen pari synnyttää uuden parin, ja lisääntyminen alkaa toisesta kuukaudesta. Oletetaan myös, ettei yksikään kani kuole vuoden aikana. Kuinka monta paria kaneja voi syntyä yhdestä parista yhden vuoden aikana?

Ensimmäisen kuukauden alussa on siis yksi pari poikasia. Toisen kuukauden lopussa pari on lisääntymiskykyinen ja synnyttää toisen parin. Nyt on muodostunut kaksi kaniparia, joista toinen pari on täyskasvuisia ja toinen poikasia. Kolmannen kuukauden lopussa ensimmäinen pari synnyttää uuden parin ja samalla toisesta parista tulee lisääntymiskykyinen. Nyt kaneja on kolme paria, joista kaksi on täyskasvuisia ja yksi poikasia. Sama kaava pätee vuoden loppuun saakka, kuten on esitetty taulukossa 2.1.

Parien yhteismäärää eli lukuja

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, \dots$$

kutsutaan Fibonaccin luvuiksi ja lukujonoa *Fibonaccin lukujonoksi.* (vrt. [1, s. 285])

Taulukko 2.1. Kaniparien määrät

Kuukausi	Täyskasvuiset (parit)	Poikaset (parit)	Yhteensä (pareja)
1	0	1	1
2	1	0	1
3	1	1	2
4	2	1	3
5	3	2	5
6	5	3	8
7	8	5	13
8	13	8	21
9	21	13	34
10	34	21	55
11	55	34	89
12	89	55	144

Sarjan luvut ilmaistaan $u_1 = 1$, $u_2 = 1$, $u_3 = 2$ ja niin edelleen, missä u_n on n:nnes Fibonaccin luku.

$$\begin{aligned}
&2{=}1{+}1 \quad \text{tai} \quad u_3 = u_2 + u_1 \\
&3{=}2{+}1 \quad \text{tai} \quad u_4 = u_3 + u_2 \\
&5{=}3{+}2 \quad \text{tai} \quad u_5 = u_4 + u_3 \\
&8{=}5{+}3 \quad \text{tai} \quad u_6 = u_5 + u_4
\end{aligned}$$

Määritelmä 2.1. Fibonaccin luvut u_n määritellään rekursiivisesti seuraavasti:

$$\begin{aligned}
&u_1 = u_2 = 1, \\
&u_n = u_{n-1} + u_{n-2}, \quad \text{kun } n \geq 3.
\end{aligned}$$

Esimerkki 2.2. vrt. [1, s. 286] Fibonaccin luvut kasvavat nopeasti. Tämä voidaan osoittaa kaavalla $u_{5n+2} > 10^n$, kun $n \geq 1$. Tällöin,

$$u_7 > 10, u_{12} > 100, u_{17} > 1000, u_{22} > 10000 \dots$$

Lause 2.3. *Fibonaccin lukujonossa lukujen u_n ja u_{n+1} suurin yhteinen tekijä on* 1 *jokaiselle* $n \geq 1$.

Todistus. vrt. [1, s. 286-287]
Olkoon $syt(u_n, u_{n+1}) = d > 1$. Näin ollen $d \mid u_n$ ja $d \mid u_{n+1}$. Tällöin $u_{n+1} - u_n = u_{n-1}$ on myös jaollinen luvulla d. Lisäksi tiedämme, että $u_n - u_{n-1} = u_{n-2}$. Tämä tarkoittaa, että $d \mid u_{n-2}$. Sama argumentti osoittaa, että $d \mid u_{n-3}$, $d \mid u_{n-4}$, ..., ja lopulta, että $d \mid u_1 = 1$, mikä on mahdotonta. Näin ollen $syt(u_n, u_{n+1}) = 1$ kaikille $n \geq 1$. □

Lause 2.4. *Olkoot m ja n luonnollisia lukuja. Fibonaccin lukujonossa pätee*

$$u_{m+n} = u_{m-1}u_n + u_m u_{n+1}.$$

Todistus. vrt. [1, s. 288]
Todistetaan lause induktiolla luvun n suhteen, kun $m \geq 2$.
Kun $n = 1$, pätee

$$u_{m-1}u_1 + u_m u_2 = u_{m-1} \cdot 1 + u_m \cdot 1 = u_{m-1} + u_m = u_{m+1}.$$

Kun $n = 2$, pätee

$$u_{m-1}u_2 + u_m u_3 = u_{m-1} \cdot 1 + u_m \cdot 2 = (u_{m-1} + u_m) + u_m = u_{m+1} + u_m = u_{m+2}.$$

Oletetaan, että yhtälö pätee, kun $n \in \{1, 2, \ldots, k\}$ ja todistetaan, että väite pätee, kun $n = k + 1 \geq 3$. Tällöin

$$u_{m+k} = u_{m-1}u_k + u_m u_{k+1} \quad \text{ja} \quad u_{m+(k-1)} = u_{m-1}u_{k-1} + u_m u_k.$$

Tällöin

$$u_{m+k} + u_{m+(k-1)} = u_{m-1}(u_k + u_{k-1}) + u_m(u_{k+1} + u_k).$$

Fibonaccin jonon määritelmän nojalla

$$u_{m+(k+1)} = u_{m-1}u_{k+1} + u_m u_{k+2}.$$

Näin ollen väite pätee kaikilla $m \geq 2$ ja $n \geq 1$. □

Lause 2.5. *Kun* $m \geq 1$, $n \geq 1$, u_{mn} *on jaollinen luvulla* u_m.

Todistus. vrt. [1, s. 289]
Käytetään lauseen todistamisessa induktioperiaatetta. Kun $n = 1$, niin $u_{mn} = u_m$ on selvästi jaollinen itsellään. Oletetaan induktio-oletuksena, että lause pätee jollekin

$n = k$, eli u_{mk} on jaollinen luvulla u_m. Nyt osoitetaan, että $u_{m(k+1)}$ on jaollinen luvulla u_m. Käytetään Fibonaccin yhtälöä

$$u_{m(k+1)} = u_{mk-1}u_m + u_{mk}u_{m+1}.$$

Induktio-oletuksen nojalla u_{mk} on jaollinen luvulla u_m. Tällöin u_m jakaa luvun $u_{m(k+1)} = u_{mk-1}u_m + u_{mk}u_{m+1}$. Siis $u_{m(k+1)}$ on jaollinen luvulla u_m. Induktioperiaatten nojalla u_{mn} on jaollinen luvulla u_m, kun $m \geq 1, n \geq 1$. □

Apulause 2.6. *Jos $m = nq + r$, niin $syt(u_m, u_n) = syt(u_r, u_n)$.*

Todistus. vrt. [1, s. 289]
Havaitaan, että

$$\text{syt}(u_m, u_n) = \text{syt}(u_{nq+r}, u_n) = \text{syt}(u_{nq-1}u_r + u_{nq}u_{r+1}, u_n).$$

Nyt väitämme, että $\text{syt}(u_{nq-1}, u_n) = 1$. Olkoon $d = \text{syt}(u_{nq-1}, u_n)$. Tällöin d jakaa luvut u_{nq-1} ja u_n. Lisäksi u_n jakaa luvun u_{nq}. Näin ollen d jakaa luvun u_{nq}. Tämä d on lukujen u_{nq} ja u_{nq-1} positiivinen yhteinen tekijä. Mutta $\text{syt}(u_{nq-1}, u_{nq}) = 1$, joka on ristiriitaista. Siispä $d = 1$. □

Lause 2.7. *Kahden Fibonaccin luvun suurin yhteinen tekijä on jälleen Fibonaccin luku. Erityisesti, $syt(u_m, u_n) = u_d$, missä $d = syt(m, n)$.*

Todistus. vrt. [1, s. 290]
Olkoot u_m ja u_n kaksi Fibonaccin lukua. Oletetaan, että $m \geq n$. Soveltamalla lukuihin m ja n Eukleideen algoritmia, [1, s. 26-27] saadaan:

$$\begin{aligned}
m &= q_1 n + r_1 && 0 < r_1 < n \\
n &= q_2 r_1 + r_2 && 0 < r_2 < r_1 \\
r_1 &= q_3 r_2 + r_3 && 0 < r_3 < r_2 \\
&\vdots \\
r_{n-2} &= q_n r_{n-1} + r_n && 0 < r_n < r_{n-1} \\
r_{n-1} &= q_{n+1} r_n + 0.
\end{aligned}$$

Apulauseen 2.6 nojalla

$$syt(u_m, u_n) = syt(u_{r_1}, u_n) = syt(u_{r_1}, u_{r_2}) = \cdots = syt(u_{r_{n-1}}, u_{r_n}).$$

Koska $r_n \mid r_{n-1}$, niin lauseen 2.5 nojalla $u_{r_n} \mid u_{r_{n-1}}$. Tällöin $\text{syt}(u_{r_{n-1}}, u_{r_n}) = u_{r_n}$. Mutta koska r_n on viimeinen nollasta poikkeava jakojäännös Eukleideen algoritmissa lukujen m ja n välillä, se on yhtä suuri kuin $\text{syt}(m, n)$. Näin ollen $\text{syt}(u_m, u_n) = u_d$, missä $d = \text{syt}(m, n)$.

□

Seuraus 2.8. *Fibonaccin lukujonossa pätee $u_m \mid u_n$, jos ja vain jos $m \mid n$, missä $n \geq m \geq 3$.*

Todistus. Jos $u_m \mid u_n$, niin $\text{syt}(u_m, u_n) = u_m$. Tiedämme, että $\text{syt}(u_m, u_n) = u_{\text{syt}(m,n)}$. Tästä seuraa, että $\text{syt}(m, n) = m$. Siispä $m \mid n$. □

Esimerkki 2.9. Esitetään Fibonaccin luvut, jotka jakavat luvut u_{24} ja u_{36}. Lauseen 2.7 nojalla tiedämme, että

$$syt(u_m, u_n) = u_d, \quad \text{missä} \quad d = syt(m, n).$$

Kun $m = 24$ ja $n = 36$, niin

$$d = syt(24, 36) = 12.$$

Näin ollen Fibonaccin luvut, jotka jakavat sekä luvun u_{24} että luvun u_{36}, ovat ne Fibonaccin luvut, jotka jakavat luvun u_{12}. Seurauksen 2.8 nojalla luku u_m jakaa luvun u_n jos ja vain jos m jakaa luvun n, kun $n \geq m \geq 3$. Tässä tapauksessa ainoat mahdolliset arvot ovat $3, 4, 6$ ja 12. Fibonaccin luvut, jotka jakavat luvun u_{12} ovat siis u_3, u_4, u_6 ja u_{12}, sekä $u_1 = u_2 = 1$. Tällöin kaikki Fibonaccin luvut, jotka jakavat luvut u_{24} ja u_{36} ovat

$$\begin{aligned} u_1 &= u_2 = 1 \\ u_3 &= 2 \\ u_4 &= 3 \\ u_6 &= 8 \\ u_{12} &= 144. \end{aligned}$$

3 Lineaariset Diofantoksen yhtälöt

Tässä luvussa keskitytään lineaariseen Diofantoksen yhtälöön. (vrt. [2, s. 11-12])

Lause 3.1. *Olkoot a ja b luonnollisia lukuja. Jos $syt(a, b) = 1$, niin kaikki yhtälön $ax + by = c$ ratkaisut ovat muotoa $x = r + tb$, $y = s - ta$, missä r ja s ovat sellaisia, että $ar + bs = c$ ja t voi olla mikä tahansa kokonaisluku.*

Todistus. Koska $syt(a, b) = 1$, on olemassa kokonaisluvut u ja v, joille

$$au + bv = 1.$$

Näin ollen $a(cu) + b(cv) = c$ ja yhtälöllä $ax + by = c$ on ratkaisut

$$x = r = cu \quad \text{ja} \quad y = s = cv.$$

Se, että

$$x = r + tb \text{ ja } y = s - ta$$

ovat ratkaisu kaikilla kokonaisluvuilla t, seuraa siitä, että

$$a(r + tb) + b(s - ta) = (ar + bs) + (abt - abt) = c + 0 = c.$$

Olkoon nyt (x, y) mikä tahansa yhtälön $ax + by = c$ ratkaisu. Näytämme, että

$$x = r + tb \text{ ja } y = s - ta$$

jollakin kokonaisluvulla t. Pätee

$$c - c = (ax + by) - (ar + bs),$$

joten

$$a(x - r) + b(y - s) = 0. \tag{$*$}$$

Tällöin $b \mid a(x - r)$ ja koska $syt(a, b) = 1$, niin $b \mid (x - r)$. Toisin sanoen on olemassa kokonaisluku t, jolle

$$tb = x - r \text{ eli } x = r + tb.$$

Sijoittamalla tämä yhtälöön $(*)$ saadaan

$$atb + b(y - s) = 0, \text{ joten } y = s - ta.$$

Jos $syt(a, b) = d > 1$, niin jos d ei jaa lukua c, yhtälöllä $ax + by = c$ ei ole ratkaisua. Jos d jakaa luvun c, yhtälö voidaan muuttaa muotoon

$$\tfrac{a}{d}x + \tfrac{b}{d}y = \tfrac{c}{d}.$$

Tällöin, kun $syt\left(\frac{a}{d}, \frac{b}{d}\right) = 1$, lause pätee ja jos löydämme yhden ratkaisun, tiedämme kaikki ratkaisut.

$\square$

Esimerkki 3.2. vrt. [2, s.12]
Tarkastellaan yhtälöä $4x + 9y = 57$. Ensimmäiseksi jaamme yhtälön kertoimien suurimmalla yhteisellä tekijällä, joka tässä tapauksessa on 1. Tällöin saamme yhtälön

$$4x + 9y = 57.$$

Seuraavaksi, kokeilemalla tai tarkastelemalla huomaamme, että kun $x = 3$ ja $y = 5$, yhtälö toteutuu: $4 \cdot 3 + 9 \cdot 5 = 57$. Näin ollen saamme yhden ratkaisun: $x = 3$ ja $y = 5$.

Kaikkien ratkaisujen löytämiseksi ilmaisemme muuttujat x ja y parametrin t avulla. Koska muuttujien x ja y kertoimet ovat 4 ja 9, vastaavasti, voimme ilmaista ne muodossa

$$x = 3 + 9t \quad \text{ja} \quad y = 5 - 4t,$$

missä t on kokonaisluku. Näin ollen, kaikki yhtälön ratkaisut ovat muotoa

$$x = 3 + 9t \quad \text{ja} \quad y = 5 - 4t,$$

missä t on kokonaisluku.

Esimerkki 3.3. Ratkaistaan seuraavaksi yksi Burtonin kirjan tehtävistä. Eräs maanviljelijä osti yhteensä 100 eläintä, käyttäen siihen 4000 €. Vasikoita hän osti 120 € kappalehinnalla, karitsoita 50 € kappale, ja porsaita 25 € kappale. Lasketaan, kuinka monta kutakin eläintä maanviljelijä osti, kun hän hankki vähintään yhden kustakin lajista.

Asetetaan ongelma Diofantoksen yhtälöksi. Olkoon x vasikoiden lukumäärä, y karitsoiden lukumäärä ja z porsaiden lukumäärä. Tällöin saadaan

$$120x + 50y + 25z = 4000,$$

$$x + y + z = 100.$$

Erotetaan muuttuja z toisesta yhtälöstä ja sijoitetaan sen arvo ensimmäiseen yhtälöön. Tällöin Diofantoksen yhtälö saadaan muotoon

$$120x + 50y + 25(100 - x - y) = 4000,$$

joten

$$95x + 25y = 1500,$$

ja edelleen

$$19x + 5y = 300,$$

missä x y ovat positiivisia kokonaislukuja. Soveltamalla lukuihin 19 ja 5 Eukleideen algoritmia saadaan:

$$\begin{aligned} 19 &= 3 \cdot 5 + 4 \\ 5 &= 1 \cdot 4 + 1 \\ 4 &= 4 \cdot 1 + 0. \end{aligned}$$

Näin ollen $syt(19, 5) = 1$. Koska $1|300$, tämän yhtälön ratkaisu on olemassa. Nyt

$$\begin{aligned} 1 &= 5 - 4 \\ &= 5 - (19 - 3 \cdot 5) \\ &= 4 \cdot 5 - 19. \end{aligned}$$

Kerrotaan yhtälö luvulla 300 ja saadaan se muotoon

$$300 = -300 \cdot 19 + 1200 \cdot 5.$$

Tällöin $x = -300$ ja $y = 1200$, joka antaa yhden ratkaisun Diofantoksen yhtälölle. Nyt Lauseen 3.1 nojalla kaikki ratkaisut ovat muotoa

$$x = -300 + \frac{5}{1}t = -300 + 5t$$

ja

$$y = 1200 - \frac{19}{1}t = 1200 - 19t.$$

Tällöin

$$z = 100 - x - y = 100 + 300 - 5t - 1200 + 19t = -800 + 14t.$$

Esitetään seuraavaksi arvot t, joille $x, y, z > 0$:

$$\begin{aligned} -300 + 5t &> 0 & 1200 - 19t &> 0 & -800 + 14t &> 0 \\ t &> \frac{300}{5} & t &< \frac{1200}{19} & t &> \frac{800}{14} \\ t &> 60 & t &< 63,1579 & t &> 57,1429. \end{aligned}$$

Näin ollen

$$\begin{cases} x = -300 + 5t \\ y = 1200 - 19t \\ z = -800 + 14t, \end{cases}$$

missä $t = 61, 62, 63$. Tällöin

$$\begin{cases} x = 5, y = 41, z = 54 \\ x = 10, y = 22, z = 68 \\ x = 15, y = 3, z = 82. \end{cases}$$

4 Ketjumurtoluvut

Tässä luvussa tutustutaan ketjumurtolukuihin.

4.1 Srinivasa Ramanujan 1887-1920

Srinivasa Ramanujan (1887-1920) on Intian arvostetuin matemaatikko. Hänen intohimonsa matematiikkaan syttyi, kun hän 15–16-vuotiaana löysi Carrin ”Synopsis of Pure Mathematics” -teoksen, joka esitteli yli 6000 teoreemaa, suurimman osan ilman todistuksia. Ramanujan päätti itsenäisesti todistaa kaikki teoreemat. Vaikka hän menetti yliopistostipendinsä laiminlyötyään muita aineita, hän sai myöhemmin virkamiehen paikan, joka antoi hänelle aikaa jatkaa matematiikan opiskeluaan. Hänen lahjakkuutensa huomattiin, ja G. H. Hardy kutsui hänet Cambridgeen kehittämään kykyjään. Siellä Ramanujan työskenteli kolme vuotta Hardyn kanssa ja teki suuren osan parhaasta työstään. Vaikka hänen terveytensä heikkeni ja hän palasi Intiaan, hänen matemaattiset saavutuksensa ovat jättäneet pysyvän jäljen matematiikan maailmaan.

4.2 Rafael Bombelli 1526-1572

Ketjumurtoluvut saivat alkunsa Rafael Bombellilta, renessanssin viimeiseltä suurelta algebran tutkijalta Italiasta. Hän todisti, että $\sqrt{3}$ voidaan ilmaista jatkettuna murtolukuna

$$\sqrt{3} = 3 + \cfrac{4}{6 + \cfrac{4}{6 + \cfrac{4}{6 + \ddots}}}$$

Bombelli oli ensimmäinen, joka popularisoi Diofantoksen työn latinankielisessä länsimaailmassa. Alun perin hän aikoi kääntää Vatikaanin kirjaston kopion Diofantoksen Arithmetica-teoksesta (todennäköisesti sama käsikirjoitus, jonka Regiomontanus oli löytänyt), mutta muiden töiden innostamana hän ei koskaan saanut projektia valmiiksi. Sen sijaan hän otti kaikki ensimmäisen neljän kirjan ongelmat ja sulautti ne omaan Algebra-teokseensa. Vaikka Bombelli ei erottanut Diofantoksen ongelmia omiksi, hän kuitenkin myönsi vapaasti lainanneensa niitä Arithmetica-teoksesta. Ilmeisesti minkä tahansa äärellisen ketjumurtoluvun arvo on aina rationaaliluku.

4.3 Äärelliset ketjumurtoluvut

Tässä osiossa esittelemme määritelmiä, jotka liittyvät äärellisiin ketjumurtolukuihin.

Määritelmä 4.1. Äärellisellä ketjumurtoluvulla tarkoitetaan murtolukua, joka on muotoa

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}}}$$

missä $a_1, \ldots, a_n$ ovat reaalilukuja ja $a_i > 0$ kaikilla $i \in \{i, \ldots, n\}$. Äärellistä ketjumurtolukua sanotaan yksinkertaiseksi, jos kaikki luvut a_i ovat kokonaislukuja.

Lause 4.2. *Minkä tahansa rationaaliluvun voi esittää yksinkertaisena äärellisenä ketjumurtolukuna.*

Todistus. vrt. [1, s. 308-309]
Olkoon a/b, mikä tahansa rationaaliluku, missä $b > 0$. Esitetään Eukleideen algoritmi suurimman yhteisen tekijän löytämiseksi luvuille a ja b, algoritmi johtaa seuraaviin yhtälöihin

$$\begin{aligned}
a &= ba_0 + r_1 && 0 < r_1 < b \\
b &= r_1 a_1 + r_2 && 0 < r_2 < r_1 \\
r_1 &= r_2 a_2 + r_3 && 0 < r_3 < r_2 \\
&\vdots \\
r_{n-2} &= r_{n-1} a_{n-1} + r_n && 0 < r_n < r_{n-1} \\
r_{n-1} &= r_n a_n + 0.
\end{aligned}$$

Koska jokainen jakojäännös r_k on positiivinen kokonaisluku, niin kaikki luvut $a_1, a_2, \ldots, a_n$ ovat positiivisia. Näin ollen

$$
\begin{aligned}
\frac{a}{b} &= a_0 + \frac{r_1}{b} = a_0 + \frac{1}{\frac{b}{r_1}} \\
\frac{b}{r_1} &= a_1 + \frac{r_2}{r_1} = a_1 + \frac{1}{\frac{r_1}{r_2}} \\
\frac{r_1}{r_2} &= a_2 + \frac{r_3}{r_2} = a_2 + \frac{1}{\frac{r_2}{r_3}} \\
&\vdots \\
\frac{r_{n-1}}{r_n} &= a_n.
\end{aligned}
$$

Tällöin

$$\frac{a}{b} = a_0 + \frac{1}{\frac{b}{r_1}} = a_0 + \frac{1}{a_1 + \frac{1}{\frac{r_1}{r_2}}} = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\frac{r_2}{r_3}}}}.$$

Saadaan siis

$$\frac{a}{b} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}}}$$

□

Merkintöjen helpottamiseksi otamme äärellisille ketjumurtoluvuille käyttöön lyhyemmän merkinnän ja merkitsemme yllä olevaa ketjumurtolukua $\frac{a}{b}$ symbolilla $[a_0; a_1, \dots, a_n]$.

Esimerkki 4.3. Esitetään esimerkki rationaaliluvusta, joka voidaan esittää yksinkertaisena äärellisenä ketjumurtolukuna:

$$\frac{89}{23} = 3 + \frac{1}{\frac{23}{20}} = 3 + \cfrac{1}{1 + \cfrac{3}{20}} = 3 + \cfrac{1}{1 + \cfrac{1}{\frac{20}{3}}}$$

$$=3+\cfrac{1}{1+\cfrac{1}{6+\cfrac{2}{3}}}=3+\cfrac{1}{1+\cfrac{1}{6+\cfrac{1}{\frac{3}{2}}}}$$

$$=3+\cfrac{1}{1+\cfrac{1}{6+\cfrac{1}{1+\cfrac{1}{2}}}}$$

Määritelmä 4.4. Olkoon $[a_0; a_1, a_2, ..., a_n]$ ketjumurtoluku. Kaikilla $1 \leq k \leq n$, merkitään

$$C_k = [a_0; a_1, ..., a_k]$$

ja sanotaan, että C_k on ketjumurtoluvun $[a_0; a_1, \ldots, a_n]$ k:s konvergentti. Nollas konvergentti C_0 on luku a_0.

Lause 4.5. *Olkoot $a_0, a_1, a_2, \ldots, a_n$ reaalilukuja, missä luvut $a_1, a_2, \ldots, a_n$ ovat positiivisia. Määritellään jonot $p_0, p_1, \ldots, p_n$ ja $q_0, q_1, \ldots, q_n$ rekursiivisesti yhtälöillä*

$$\begin{aligned} p_0 &= a_0 & q_0 &= 1 \\ p_1 &= a_0 \cdot a_1 + 1 & q_1 &= a_1 \\ p_k &= a_k \cdot p_{k-1} + p_{k-2} & q_k &= a_k \cdot q_{k-1} + q_{k-2}, \end{aligned}$$

kun $k = 2, 3, \ldots, n$. Tällöin yksinkertaisen ketjumurtoluvun $[a_0; a_1, \ldots, a_n]$ k. konvergentti $C_k = [a_0; a_1, a_2, \ldots, a_k]$ toteuttaa yhtälön

$$C_k = \frac{p_k}{q_k}.$$

Todistus. vrt. [1, s. 312-313]

Käytetään lauseen todistamisessa induktioperiaatetta.

Kun $k = 0$, niin

$$C_0 = a_0 = \frac{a_0}{1} = \frac{p_0}{q_0}.$$

Kun $k = 1$, niin tällöin

$$C_1 = a_0 + \frac{1}{a_1} = \frac{a_1 a_0 + 1}{a_1} = \frac{p_1}{q_1}.$$

Edelleen kun $k = 2$, niin

$$C_2 = a_0 + \frac{1}{a_1 + \frac{1}{a_2}} = \frac{a_2(a_1 a_0 + 1)}{a_2 a_1 + 1} = \frac{p_2}{q_2}.$$

Väite on siis tosi kun $k = 0, 1, 2$. Oletetaan seuraavaksi, että väite on tosi kun $k = m$, missä $2 \leq m < n$. Tämä tarkoittaa, että

$$C_m = \frac{p_m}{q_m} = \frac{a_m p_{m-1} + p_{m-2}}{a_m q_{m-1} + q_{m-2}}.$$

Rekursiivisten yhtälöiden perusteella nähdään, että luvut p_{m-1}, p_{m-2} ja q_{m-2} riippuvat vain luvuista $a_0, a_1, \ldots, a_{m-1}$. Näin ollen voidaan korvata luku a_m luvulla $a_m + \frac{1}{a_{m+1}}$. Tällöin

$$\begin{aligned}
C_{m+1} &= [a_0; a_1, \ldots, a_{m-1}, a_m + \frac{1}{a_{m+1}}] \\
&= \frac{(a_m + \frac{1}{a_{m+1}})p_{m-1} + p_{m-2}}{(a_m + \frac{1}{a_{m+1}})q_{m-1} + q_{m-2}} \\
&= \frac{a_{m+1}(a_m p_{m-1} + p_{m-2}) + p_{m-1}}{a_{m+1}(a_m q_{m-1} + q_{m-2}) + q_{m-1}} \\
&= \frac{a_{m+1} p_m + p_{m-1}}{a_{m+1} q_m + q_{m-1}} \\
&= \frac{p_{m+1}}{q_{m+1}}.
\end{aligned}$$

Väite on siis tosi arvolla $k = m + 1$, joten induktioperiaatteen nojalla alkuperäinen väite pätee. □

Lause 4.6. *Jos* $C_k = \frac{p_k}{q_k}$ *on yksinkertaisen ketjumurtoluvun* $[a_0; a_1, a_2, ..., a_n]$ k*. konvergentti, niin*

$$p_k q_{k-1} - q_k p_{k-1} = (-1)^{k-1},$$

kaikilla $1 \leq k \leq n$*.*

Todistus. vrt. [1, s. 314]

Todistetaan lause induktiolla. Kun $k = 1$, niin lauseen 4.5 nojalla

$$p_1 q_0 - q_1 p_0 = (a_1 a_0 + 1) \cdot 1 - a_1 \cdot a_0 = 1 = (-1)^{1-1}$$

eli lause pitää tällöin paikkansa. Oletetaan sitten, että väite pätee kun $k = m$, missä $1 \leq m < n$. Tällöin

$$\begin{aligned} p_{m+1}q_m - q_{m+1}p_m =& (a_{m+1}p_m + p_{m-1})q_m - (a_{m+1}q_m + q_{m-1})p_m \\ =& -(p_m q_{m-1} - q_m p_{m-1}) \\ =& -(-1)^{m-1} \\ =& (-1)^m, \end{aligned}$$

joten väite pätee arvolla m+1. Induktioperiaatteen nojalla väite siis pätee. □

Seuraus 4.7. *Kun* $1 \leq k \leq n$, p_k *ja* q_k *ovat keskenään jaottomia.*

Todistus. vrt. [1, s. 314]
Jos $d = \mathrm{syt}(p_k, q_k)$, niin lauseen 4.6 nojalla $d|(-1)^{k-1}$. Tällöin siis pätee $d|1$ sekä $d|(-1)$. Tästä seuraa, että $d = 1$. Näin ollen p_k ja q_k ovat keskenään jaottomia. □

Apulause 4.8. *Olkoon* q_k *yksinkertaisen ketjumurtoluvun* $[a_0; a_1, \ldots, a_k]$ k*. konvergentin* C_k *nimittäjä. Tällöin* $q_{k-1} \leq q_k$ *kun* $1 \leq k \leq n$*. Jos* $k > 1$*, niin* $g_{k-1} < q_k$*.*

Todistus. vrt. [1, s. 317]
Käytetään induktioperiaatetta apulauseen todistamiseen. Väite on tosi, kun $k = 1$, sillä

$$q_0 = 1 \leq a_1 = q_1.$$

Oletetaan seuraavaksi, että väite pätee, kun $k = m$, missä $1 \leq m < n$.
Tällöin

$$q_{m+1} = a_{m+1}q_m + q_{m-1} > a_{m+1}q_m \geq 1 \cdot q_m = q_m.$$

Siis väite on tosi, kun $k = m + 1$. Induktioperiaatteen nojalla alkuperäinen väite pätee. □

Lause 4.9. *Olkoon* C_k *äärellisen yksinkertaisen ketjumurtoluvun* $[a_0; a_1, a_2, ..., a_n]$ k*. konvergentti. Tällöin*

$$C_0 < C_2 < C_4 < \ldots,$$

$$C_1 > C_3 > C_5 > \ldots,$$

ja jokainen konvergentti, jolla on pariton alaindeksi, on suurempi kuin jokainen konvergentti, jolla on parillinen alaindeksi.

Todistus. vrt. [1, s. 317-318]
Lauseen 4.6 nojalla huomaamme, että

$$\begin{aligned}
C_{k+2} - C_k &= (C_{k+2} - C_{k+1}) + (C_{k+1} - C_k) \\
&= \left(\frac{p_{k+2}}{q_{k+2}} - \frac{p_{k+1}}{q_{k+1}}\right) + \left(\frac{p_{k+1}}{q_{k+1}} - \frac{p_k}{q_k}\right) \\
&= \frac{(-1)^{k+1}}{q_{k+2}q_{k+1}} + \frac{(-1)^k}{q_{k+1}q_k} \\
&= \frac{(-1)^k(q_{k+2} - q_k)}{q_k q_{k+1} q_{k+2}}.
\end{aligned}$$

Apulauseen 4.8 nojalla $q_i > 0$ kaikilla $i \geq 0$ ja $q_{k+2} - q_k > 0$. Näin ollen termillä $C_{k+2} - C_k$ on sama etumerkki kuin termillä $(-1)^k$. Nyt, jos k on parillinen kokonaisluku, eli $k = 2j$, niin $C_{2j+2} > C_{2j}$. Tällöin

$$C_0 < C_2 < C_4 < \dots$$

Vastaavasti, jos k on pariton kokonaisluku, eli $k = 2j-1$, niin $C_{2j+1} < C_{2j-1}$. Tällöin

$$C_1 > C_3 > C_5 > \dots$$

Lopuksi osoitetaan, että mikä tahansa parittoman indeksin konvergentti C_{2r-1} on suurempi kuin mikä tahansa parillisen indeksin konvergentti C_{2s}. Koska $p_k q_{k-1} - q_k p_{k-1} = (-1)^{k-1}$, jakamalla yhtälön molemmat puolet luvulla $q_k q_{k-1}$ saadaan

$$C_k - C_{k-1} = \frac{p_k}{q_k} - \frac{p_{k-1}}{q_{k-1}} = \frac{(-1)^{k-1}}{q_k q_{k-1}}.$$

Tämän perusteella siis $C_{2j} < C_{2j-1}$. Kun verrataan konvergentteja C_{2j} ja C_{2j-1}, havaitaan, että

$$C_{2s} < C_{2s+2r} < C_{2s+2r-1} < C_{2r-1}.$$

Näin ollen jokainen parittomasti indeksoitu konvergentti on suurempi kuin jokainen parillisesti indeksoitu konvergentti.

Esimerkki 4.10. Esitetään luvut $3,1416$ ja $3,14159$ yksinkertaisina ketjumurtolukuna. Muutamme luvun $3,1416$ murtoluvuksi ja käytämme Eukleideen algoritmia:

$$\begin{aligned}
3,1416 &= 3 + 0,1416 \\
&= 3 + \frac{1416}{10000} \\
&= 3 + \frac{177}{1250}.
\end{aligned}$$

Nyt käyttämällä Eukleideen algoritmia saamme

$$\begin{aligned}1250 &= 7 \cdot 177 + 11\\ 177 &= 16 \cdot 11 + 1\\ 11 &= 11 \cdot 1.\end{aligned}$$

Tällöin $3,1416 = [3;7,16,11]$.

Tarkastellaan seuraavaksi lukua $3,14159$. Nyt saamme

$$\begin{aligned}3,14159 &= 3 + 0,14159\\ &= 3 + \frac{14159}{100000}.\end{aligned}$$

Käyttämällä Eukleideen algoritmia saadaan

$$\begin{aligned}100000 &= 7 \cdot 14159 + 887\\ 14159 &= 15 \cdot 887 + 854\\ 887 &= 1 \cdot 854 + 33\\ 854 &= 25 \cdot 33 + 29\\ 33 &= 1 \cdot 29 + 4\\ 29 &= 7 \cdot 4 + 1\\ 4 &= 4 \cdot 1.\end{aligned}$$

Tällöin $[3;7,15,1,25,1,7,4] = 3,14159$.

□

4.4 John Wallis 1616-1703

John Wallis oli merkittävä englatilainen matemaatikko 1600-luvulla. Hänet tunnetaan lukuisista julkaisuistaan ja häntä pidetään yhtenä aikakautensa suurimmista matemaatikoista. Wallis löysi noin vuonna 1655 äärettömän tulolausekkeen luvulle π:

$$\frac{4}{\pi} = \frac{3 \cdot 3 \cdot 5 \cdot 5 \cdot 7 \cdot 7 \ldots}{2 \cdot 4 \cdot 4 \cdot 6 \cdot 6 \cdot 8 \ldots}$$

[4, s. 44]

4.5 William Brouncker 1620-1684

William Brouncker (1620 – 1684) oli merkittävä englantilainen matemaatikko 1600-luvulla. Hän suoritti tohtorintutkinnon Oxfordin yliopistossa vuonna 1647. Brouncker oli yksi Englannin kuninkaallisen tiedeakatemian, Royal Societyn, perustajajäsenistä ja sen ensimmäinen presidentti. Hän oli ensimmäinen englantilainen, joka oli kiinnostunut ketjumurtoluvuista. Jatkamalla Wallisin työtä hän kehitti ketjumurtolukukehitelmän luvulle π:

$$\frac{4}{\pi} = 1 + \cfrac{1^2}{2 + \cfrac{3^2}{2 + \cfrac{5^2}{2 + \cfrac{7^2}{2 + \dots}}}}$$

[1, s. 320]

4.6 Äärettömät ketjumurtoluvut

Määritelmä 4.11. Äärettömällä ketjumurtoluvulla tarkoitetaan murtolukua, joka on muotoa

$$a_0 + \cfrac{b_1}{a_1 + \cfrac{b_2}{a_2 + \cfrac{b_3}{a_3 + \ddots}}}$$

missä $a_0, a_1, a_2, ...$ ja $b_1, b_2, b_3, ...$ ovat reaalilukuja.

Määritelmä 4.12. Jos $a_0, a_1, a_2, \dots$ on ääretön kokonaislukujen jono, kaikki positiivisia paitsi mahdollisesti a_0, niin äärettömän yksinkertaisen ketjumurtoluvun $[a_0; a_1, a_2, \dots]$ arvo on

$$\lim_{n\to\infty} [a_0; a_1, a_2, \dots, a_n].$$

Tarkastelemme jaksollisia ketjumurtolukuja. Jaksollinen murtoluku on muotoa

$$[a_0; a_1, \dots, a_m, b_1 \dots, b_n, b_1, \dots, b_n, \dots],$$

missä jakso $b_1, \ldots, b_n$ toistuu äärettömän monta kertaa. Merkitään tätä lukua lyhyemmin

$$[a_0; a_1, \ldots, a_m, \overline{b_1, \ldots, b_n}].$$

Yläviiva siis ilmaisee, että tämä kokonaislukujen jakso toistuu yhä uudelleen. Jos $b_1, b_2, \ldots, b_n$ on pienin jatkuvasti toistuva kokonaislukujen jakso, niin sanomme sen olevan ketjumurtolukuesityksen jakso, ja jakson pituus on n.

Esimerkki 4.13. Tarkastellaan seuraavaa yksinkertaista ääretöntä ketjumurtolukua $[0; \overline{1, 2, 3}]$. Nyt

$$[0; \overline{1, 2, 3}] = [0; 1, 2, 3, 1, 2, 3, \ldots] = 0 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{1}{2 + \ldots}}}}}$$

Kirjoitetaan $[\overline{1; 2, 3}] = x$, tällöin

$$x = 1 + \cfrac{1}{2 + \cfrac{1}{3 + \cfrac{1}{x}}}$$

Nyt saadaan

$$x = 1 + \cfrac{1}{2 + \cfrac{x}{3x + 1}}$$

Edelleen

$$(x - 1) = \frac{3x + 1}{2(3x + 1) + x},$$

josta saadaan

$$7x^2 - 8x - 3 = 0.$$

Yhtälön ratkaisut ovat

$$x = \frac{1}{7}(4 \pm \sqrt{37}).$$

Huomaamme, että $1 < x < 2$, joten valitaan ratkaisu $x = \frac{1}{7}(4 + \sqrt{37})$.
Tällöin

$$[0; \overline{1, 2, 3}] = 0 + \frac{1}{x} = \frac{7}{4 + \sqrt{37}} = 7\frac{(\sqrt{37} - 4)}{37 - 16} = \frac{\sqrt{37} - 4}{3}.$$

Lause 4.14. *Minkä tahansa äärettömän ketjumurtoluvun arvo on irrationaaliluku.*

Todistus. vrt. [1, s. 323]
Olkoon x äärettömän ketjumurtoluvun $[a_0; a_1, a_2, \ldots]$ arvo; eli x on konvergenttien

$$C_n = [a_0; a_1, a_2, \ldots, a_n] = \frac{p_n}{q_n}$$

muodostaman jonon raja-arvo. Koska x sijoittuu tarkasti peräkkäisten konvergenttien C_n ja C_{n+1} väliin, pätee

$$0 < |x - C_n| < |C_{n+1} - C_n| = \left|\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}\right| = \frac{1}{q_n q_{n+1}}.$$

Seuraavaksi tehdään vastaoletus, että x on rationaaliluku. Merkitään, että $x = \frac{a}{b}$, missä a ja $b > 0$ ovat kokonaislukuja.
Tällöin

$$0 < \left|\frac{a}{b} - \frac{p_n}{q_n}\right| < \frac{1}{q_n q_{n+1}}.$$

Kertomalla epäyhtälö puolittain positiivisella luvulla bq_n, saadaan

$$0 < |aq_n - bp_n| < \frac{b}{q_{n+1}}.$$

Valitaan n niin suureksi, että $b < q_{n+1}$. Tällöin

$$0 < |aq_n - bp_n| < 1.$$

Tämä ei ole mahdollista, koska $aq_n - bp_n$ on kokonaisluku. Siksi vastaoletus on virheellinen, mikä tarkoittaa, että alkuperäinen väite on tosi. Tämä osoittaa, että luku x on irrationaalinen.

□

Lause 4.15. *Jos äärettömät ketjumurtoluvut $[a_0; a_1, a_2, \ldots]$ ja $[b_0; b_1, b_2, \ldots]$ ovat yhtä suuret, niin $a_n = b_n$ kaikilla $n \geq 0$.*

Todistus. vrt. [5, s. 456-457]
Oletetaan, että $x = [a_0; a_1, a_2, \ldots]$. Koska $C_0 = a_0$ ja $C_1 = a_0 + \frac{1}{a_1}$ pätee

$$a_0 < x < a_0 + \frac{1}{a_1}.$$

Tiedämme, että kokonaisluku $a_1 \geq 1$, joten saamme epäyhtälön muotoon

$$a_0 < x < a_0 + 1.$$

Täten on siis voimassa $a_0 = [x]$, missä $[x]$ tarkoittaa suurinta kokonaislukua, joka on pienempi tai yhtäsuuri kuin x. Lisäksi tiedämme, että

$$[a_0; a_1, a_2, \ldots] = a_0 + \frac{1}{[a_1; a_2, a_3 \ldots]},$$

sillä

$$\begin{aligned}
x &= [a_0; a_1, a_2, \ldots] \\
&= \lim_{n\to\infty} [a_0; a_1, a_2, \ldots, a_n] \\
&= \lim_{n\to\infty} \left(a_0 + \frac{1}{[a_1; a_2, \ldots, a_n]} \right) \\
&= a_0 + \frac{1}{\lim_{n\to\infty} [a_1; a_2, \ldots, a_n]} \\
&= a_0 + \frac{1}{[a_1; a_2, a_3, \ldots]}.
\end{aligned}$$

Oletetaan, että

$$[a_0; a_1, a_2, \ldots] = [b_0; b_1, b_2, \ldots].$$

Huomaamme, että

$$a_0 = b_0 = [x]$$

ja

$$a_0 + \frac{1}{[a_1; a_2, \ldots]} = b_0 + \frac{1}{[b_1; b_2, \ldots]}.$$

Näin ollen

$$[a_1; a_2, \ldots] = [b_1; b_2, \ldots].$$

Oletetaan seuraavaksi, että $a_n = b_n$ ja

$$[a_{n+1}; a_{n+2}, \ldots] = [b_{n+1}; b_{n+2}, \ldots].$$

Päätellään samalla tavalla kuin edellä ja nähdään, että

$$a_{n+1} = b_{n+1}$$

ja edelleen

$$a_{n+1} + \frac{1}{[a_{n+2}; a_{n+3}, \dots]} = b_{n+1} + \frac{1}{[b_{n+2}; b_{n+3}, \dots]}.$$

Tällöin

$$[a_{n+2}; a_{n+3}, \dots] = [b_{n+2}; b_{n+3}, \dots].$$

Induktion nojalla $a_n = b_n$, kun $n \geq 0$. □

Seuraus 4.16. *Kaksi erilaista ääretöntä ketjumurtolukua vastaa kahta erilaista irrationaalilukua.*

Esimerkki 4.17. Määritetään irrationaaliluku, jota vastaa ääretön ketjumurtoluku $x = [2; 3, \overline{2, 5}]$. Aluksi kirjoitetaan x muodossa $x = [2; 3, y]$, missä $y = [\overline{2; 5}] = [2; 5, y]$. Yhtälö

$$y = [\overline{2; 5}] = [2; 5, y],$$

voidaan kirjoittaa muodossa

$$y = 2 + \cfrac{1}{5 + \cfrac{1}{y}}.$$

Tämä yhtälö johtaa toisen asteen yhtälöön

$$5y^2 - 10y - 2 = 0.$$

Koska $y > 0$ ja tällä yhtälöllä on vain yksi positiivinen juuri, voimme päätellä, että $y = 1 + \sqrt{\frac{7}{5}}$. Koska $x = [2; 3, y]$, saadaan

$$x = 2 + \cfrac{1}{3 + \cfrac{1}{1 + \sqrt{\frac{7}{5}}}}.$$

Lause 4.18. *Jokaisella irrationaaliluvulla on yksikäsitteinen esitys äärettömänä ketjumurtolukuna, joka saadaan käyttäen yllä kuvattua ketjumurtoluvun algoritmia.*

Seuraus 4.19. *Jos $\frac{p_n}{q_n}$ on irrationaaliluvun x n:s konvergentti, niin*

$$\left| x - \frac{p_n}{q_n} \right| < \frac{1}{q_{n+1} q_n} \leq \frac{1}{q_n^2}.$$

Apulause 4.20. *Olkoon $\frac{p_n}{q_n}$ irrationaalilukua x esittävän ketjumurtoluvun konvergentti. Jos a ja b ovat kokonaislukuja, missä $1 \leq b < q_{n+1}$,*
niin

$$|q_n x - p_n| \leq |bx - a|.$$

Todistus. vrt. [1, s. 330]

Tarkastellaan yhtälöryhmää

$$p_n\alpha + p_{n+1}\beta = a$$
$$q_n\alpha + q_{n+1}\beta = b$$

Kertoimien determinantti on $p_nq_{n+1} - q_np_{n+1} = (-1)^{n+1}$, joten yhtälöryhmällä on yksikäsitteinen kokonaislukuratkaisu

$$\alpha = (-1)^{n+1}(aq_{n+1} - bp_{n+1}), \quad \beta = (-1)^{n+1}(bp_n - aq_n)$$

On tärkeää huomata, että $\alpha \neq 0$. Itse asiassa, jos $\alpha = 0$, pätisi $aq_{n+1} = bp_{n+1}$ ja koska $\text{syt}(p_{n+1}, q_{n+1}) = 1$, tämä tarkoittaisi että $q_{n+1} \mid b$ tai $b \geq q_{n+1}$, mikä on ristiriidassa oletuksen kanssa. Tapauksessa $\beta = 0$ epäyhtälö, joka esitetään apulauseessa, on selvästi tosi. Nimittäin jos $\beta = 0$, niin $a = p_n\alpha$ ja $b = q_n\alpha$. Täten

$$|bx - a| = |\alpha||q_nx - p_n| \geq |q_nx - p_n|$$

Niinpä voimme tästä eteenpäin, olettaa että $\beta \neq 0$. Kun $\beta \neq 0$, päädymme siihen johtopäätökseen, että α ja β ovat vastakkaismerkkisiä. Jos $\beta < 0$, niin yhtälöstä $q_n\alpha = b - q_{n+1}\beta$ seuraa että $q_n\alpha > 0$ ja siten $\alpha > 0$. Toisaalta, jos $\beta > 0$, niin $b < q_{n+1}$ tarkoittaa että $b < \beta q_{n+1}$. Niinpä $\alpha q_n = b - q_{n+1}\beta < 0$, mistä seuraa, että $\alpha < 0$. Päädymme myös siihen johtopäätökseen, että koska x on kahden peräkkäisen konvergentin p_n/q_n ja p_{n+1}/q_{n+1} välissä, ovat

$$q_nx - p_n \quad \text{ja} \quad q_{n+1}x - p_{n+1}$$

ovat vastakkaismerkkisiä. Tämän päättelyn tarkoituksena on, että luvut

$$\alpha(q_nx - p_n) \quad \text{ja} \quad \beta(q_{n+1}x - p_{n+1})$$

ovat samanmerkkisiä. Tästä seuraa, että niiden summan itseisarvo on yhtäsuuri kuin niiden itseisarvojen summa. Apulauseen väite seuraa nyt helposti:

$$\begin{aligned}
|bx - a| &= |(q_n\alpha + q_{n+1}\beta)x - (p_n\alpha + p_{n+1}\beta)| \\
&= |\alpha(q_nx - p_n) + \beta|q_{n+1}x - p_{n+1}| \\
&= |\alpha||q_nx - p_n| + |\beta||q_{n+1}x - p_{n+1}| \\
&> |\alpha||q_nx - p_n| \\
&\geq |q_nx - p_n|,
\end{aligned}$$

mikä on haluttu epäyhtälö.

□

Lause 4.21. *Jos* $1 \leq b \leq q_n$*, niin rationaaliluku* $\frac{a}{b}$ *toteuttaa epäyhtälön*

$$\left|x - \frac{p_n}{q_n}\right| \leq \left|x - \frac{a}{b}\right|.$$

Todistus. vrt. [1, s. 331]
Jos pätisi

$$\left|x - \frac{p_n}{q_n}\right| > \left|x - \frac{a}{b}\right|,$$

niin saataisiin

$$|q_n x - p_n = q_n \left|x - \frac{p_n}{q_n}\right| > b \left|x - \frac{a}{b}\right| = |bx - a|,$$

mikä on ristiriidassa apulauseen 4.20 kanssa. □

Lause 4.22. *Olkoon* x *mielivaltainen irrationaaliluku. Jos rationaaliluku* $\frac{a}{b}$*, missä* $b \geq 1$ *ja* $syt(a, b) = 1$*, toteuttaa epäyhtälön*

$$\left|x - \frac{a}{b}\right| < \frac{1}{2b^2},$$

niin $\frac{a}{b}$ *on yksi irrationaaliluvun* x *jatkuvan ketjumurtolukuesityksen konvergenteista* p_n/q_n.

Todistus. vrt. [1, s. 332]
Oletetaan, että $\frac{a}{b}$ ei ole irrationaaliluvun x konvergentti. Koska tiedetään, että luvut q_k muodostavat kasvavan jonon, on olemassa yksikäsitteinen kokonaisluku n, jolle pätee $q_n \leq b < q_{n+1}$. Tälle luvulle apulause 4.20 antaa epäyhtälön

$$|q_n x - p_n| \leq |bx - a| = b \left|x - \frac{a}{b}\right| < \frac{1}{2b},$$

joka saadaan muotoon

$$\left|x - \frac{p_n}{q_n}\right| < \frac{1}{2bq_n}.$$

Olettaen, että $\frac{a}{b} \neq \frac{p_n}{q_n}$, erotus $bp_n - aq_n$ on nollasta eroava kokonaisluku, joten $1 \leq |bp_n - aq_n|$. Päätellään tästä, että

$$\frac{1}{bq_n} \leq \left|\frac{bp_n - aq_n}{bq_n}\right| = \left|\frac{p_n}{q_n} - \frac{a}{b}\right| \leq \left|\frac{p_n}{q_n} - x\right| + \left|x - \frac{a}{b}\right| < \frac{1}{2bq_n} + \frac{1}{2b^2}.$$

Tästä seuraa ristiriita $b < q_n$. Näin ollen väite pätee.

□

Esimerkki 4.23. Näytetään, että $\left|\frac{1}{3}+\frac{\sqrt{10}}{3}-\frac{18}{13}\right| < \frac{1}{2\cdot 13^2}$ ja, että $\frac{18}{13}$ on luvun $\frac{1+\sqrt{10}}{3}$ konvergentti. Arvioidaan itseisarvoa seuraavasti:

$$\left|\frac{1+\sqrt{10}}{3}-\frac{18}{13}\right| \approx |1,38743-1,38462| = 0,00281 < 0,00296 \approx \frac{1}{2\cdot 13^2}.$$

Nyt käytetään seuraavaa kaavaa:

$$x_0 = \frac{1+\sqrt{10}}{3}, \quad x_{n+1} = \frac{1}{x_n - \lfloor x_n \rfloor}.$$

Tällöin

$$\begin{aligned}
x_0 &= \frac{1}{3}+\frac{\sqrt{10}}{3} \approx 1,3874\\
x_1 &= \frac{1}{\frac{1}{3}+\frac{\sqrt{10}}{3}-1} = 1+\frac{\sqrt{10}}{2} \approx 2,5811\\
x_2 &= \frac{1}{1+\frac{\sqrt{10}}{2}-2} = \frac{2}{3}+\frac{\sqrt{10}}{3} \approx 1,7208\\
x_3 &= \frac{1}{\frac{2}{3}+\frac{\sqrt{10}}{3}-1} = \frac{1}{3}+\frac{\sqrt{10}}{3} \approx 1,3874
\end{aligned}$$

Huomaamme, että $x_3 = x_0$, joten luvut x_k toistuvat jaksollisesti. Niinpä $\frac{1+\sqrt{10}}{3} = [\overline{1;2,1}]$. Kirjoitetaan

$$[a_0; a_1, a_2, a_3, \dots] = [1; 2, 1, 1, 2, 1, 1, 2, 1, 1, \dots].$$

Lasketaan luvut p_k ja q_k, $k \geq 0$, lauseen 4.5 avulla:

$$\begin{aligned}
p_0 &= 1\cdot 1+0 = 1 & q_0 &= 1\cdot 0+1 = 1\\
p_1 &= 2\cdot 1+1 = 3 & q_1 &= 2\cdot 1+0 = 2\\
p_2 &= 1\cdot 3+1 = 4 & q_2 &= 1\cdot 2+1 = 3\\
p_3 &= 1\cdot 4+3 = 7 & q_3 &= 1\cdot 3+2 = 5\\
p_4 &= 2\cdot 7+4 = 18 & q_4 &= 2\cdot 5+3 = 13\\
p_5 &= 1\cdot 18+7 = 25 & q_5 &= 1\cdot 13+5 = 18\\
p_6 &= 1\cdot 25+18 = 43 & q_6 &= 1\cdot 18+13 = 31
\end{aligned}$$

Näin ollen $\frac{p_4}{q_4} = \frac{18}{13}$, joten $\frac{18}{13}$ on ketjumurtoluvun $\frac{1+\sqrt{10}}{3} = [\overline{1;2,1}]$ neljäs konvergentti.

5 Pellin yhtälö

5.1 John Pell 1611-1685

John Pell oli englantilainen 1600-luvulla elänyt matematiikko. Toisin kuin John Wallisilla, joka eli samaan aikaan, Pellillä oli vaikeuksia saavuttaa menestystä. Pellin yhtälö $x^2 - dy^2 = 1$ sai nimensä Pellin mukaan, vaikka yhtälön todellinen löytäjä on matemaatikko William Brouncker. Pellin yhtälö on yksi Diofantoksen vanhimmista ja tunnetuimmista yhtälöistä. (vrt. [4, s. 44])

5.2 Pellin yhtälö

Lause 5.1. *Jos p ja q ovat yhtälön $x^2 - dy^2 = 1$ positiivisia ratkaisuja, niin $\frac{p}{q}$ on luvun $\sqrt{d}$ ketjumurtolukuesityksen konvergentti.*

Todistus. vrt. [1, s. 337] Oletetaan, että $p^2 - dq^2 = 1$. Tämän perusteella saadaan

$$\left(p - q\sqrt{d}\right)\left(p + q\sqrt{d}\right) = 1.$$

Tällöin $p > q$ ja

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

Niinpä

$$0 < \frac{p}{q} - \sqrt{d} < \frac{\sqrt{d}}{q\left(q\sqrt{d} + q\sqrt{d}\right)} = \frac{\sqrt{d}}{2q^2\sqrt{d}} = \frac{1}{2q^2}.$$

Lauseen 4.22 nojalla $\frac{p}{q}$ on luvun $\sqrt{d}$ konvergentti.

□

Lause 5.2. *Jos $\frac{p}{q}$ on luvun $\sqrt{d}$ ketjumurtolukuesityksen konvergentti, niin $x = p$ ja $y = q$ on yksi yhtälön*

$$x^2 - dy^2 = k$$

ratkaisu, missä $|k| < 1 + 2\sqrt{d}$.

Todistus. vrt. [1, s. 337-338]

Jos $\frac{p}{q}$ on luvun $\sqrt{d}$ konvergentti, niin seurauksen 4.19 nojalla

$$\left|\sqrt{d} - \frac{p}{q}\right| < \frac{1}{q^2}$$

ja tällöin

$$|p - q\sqrt{d}| < \frac{1}{q}.$$

Näin ollen

$$\begin{aligned} |p + q\sqrt{d}| &= |(p - q\sqrt{d}) + 2q\sqrt{d}| \\ &\le |p - q\sqrt{d}| + |2q\sqrt{d}| \\ &< \frac{1}{q} + 2q\sqrt{d} \le (1 + 2\sqrt{d})q. \end{aligned}$$

Edelleen

$$\begin{aligned} |p^2 - dq^2| &= |p - q\sqrt{d}||p + q\sqrt{d}| \\ &< \frac{1}{q}(1 + 2\sqrt{d})q \\ &= 1 + 2\sqrt{d}. \end{aligned}$$

Väite siis pätee. □

Apulause 5.3. *Olkoon* $\sqrt{d} = [a_0; a_1, a_2, \dots]$. *Määritellään luvut* s_k *ja* t_k *rekursiivisesti*

$$s_0 = 0 \quad t_0 = 1$$

$$s_{k+1} = a_k t_k - s_k \quad t_{k+1} = \frac{d - s_{k+1}^2}{t_k} \quad k = 0, 1, 2, \dots$$

Tällöin

(a) s_k *ja* t_k *ovat kokonaislukuja, missä* $t_k \neq 0$.

(b) $t_k | (d - s_k^2)$.

(c) $x_k = (s_k + \sqrt{d})/t_k$, *kun* $k \geq 0$.

Todistus. vrt. [1, s. 340]

Todistetaan väite induktiolla luvun k suhteen, huomioiden että kolme väitettä pätevät selvästi kun $k = 0$. Oletetaan, että ne pitävät paikkansa positiiviselle kokonaisluvulle k. Koska a_k, s_k ja t_k ovat kaikki kokonaislukuja, niin myös $s_{k+1} = a_k t_k - s_k$ on kokonaisluku. Lisäksi $t_{k+1} \neq 0$, muuten pätisi $d = s_{k+1}^2$, mikä on ristiriidassa sen oletuksen kanssa, että d ei ole neliö. Nyt yhtälöstä

$$t_{k+1} = \frac{d - s_k^2 + 1}{t_k} = \frac{d - s_k^2}{t_k} + (2a_k s_k - a_k^2 t_k),$$

missä $t_k | (d - s_k)$ induktio-oletuksen mukaan, seuraa että t_{k+1} on kokonaisluku, kun taas yhtälöstä $t_k t_{k+1} = d - s_{k+1}$ seuraa, että $t_{k+1} | (d - s_{k+1}^2)$. Näin ollen

$$\begin{aligned} x_{k+1} &= \frac{1}{x_k - a_k} \\ &= \frac{t_k}{(s_k + \sqrt{d}) - t_k a_k} \\ &= \frac{t_k}{\sqrt{d} - s_{k+1}} \\ &= \frac{t_k(s_{k+1} + \sqrt{d})}{d - s_{k+1}^2} = \frac{s_{k+1} + \sqrt{d}}{t_{t+1}}. \end{aligned}$$

Näin ollen (a), (b) ja (c) pätevät tapauksessa $k + 1$, ja siten induktioperiaatteen nojalla kaikille positiivisille kokonaisluvuille. Induktioperiaatteen nojalla väitteet pätevät. □

Lause 5.4. *Jos luvut $\frac{p_k}{q_k}$ ovat luvun $\sqrt{d}$ ketjumurtolukuesityksen konvergentit, niin*

$$p_k^2 - dq_k^2 = (-1)^{k+1} t_{k+1}, \quad \textit{missä} \quad t_{k+1} > 0, \quad k = 0, 1, 2, 3, \ldots$$

Todistus. vrt. [1, s. 341]
Koska $\sqrt{d} = [a_0; a_1, a_2, \ldots, a_k, x_{k+1}]$, tiedämme että

$$\sqrt{d} = \frac{x_{k+1} p_k + p_{k-1}}{x_{k+1} q_k + q_{k-1}}.$$

Korvataan $x_{k+1} = \left(s_{k+1} + \sqrt{d}\right) / t_{k+1}$. Tällöin

$$\sqrt{d}\,(s_{k+1} q_k + t_{k+1} q_{k-1} - p_k) = s_{k+1} p_k + t_{k+1} p_{k-1} - dq_k.$$

Koska yllä olevan yhtälön oikea puoli on rationaaliluku ja $\sqrt{d}$ on irrationaaliluku, niin

$$s_{k+1} q_k + t_{k+1} q_{k-1} = p_k \quad \text{ja} \quad s_{k+1} p_k + t_{k+1} p_{k-1} = dq_k.$$

Ensimmäisen yhtälön kertominen luvulla p_k ja toisen yhtälön kertominen luvulla $-q_k$ ja näiden tulosten yhteenlasku johtaa yhtälöön

$$p_k^2 - dq_k^2 = t_{k+1}(p_k q_{k-1} - p_{k-1} q_k),$$

mutta

$$p_k q_{k-1} - p_{k-1} q_k = (-1)^{k-1} = (-1)^{k+1}.$$

Tällöin

$$p_k^2 - dq_k^2 = (-1)^{k+1} t_{k+1}.$$

Tarkastellaan seuraavaksi konvergentteja, missä

$$C_{2k} < \sqrt{d} < C_{2k+1} \quad k \geq 0.$$

Koska $C_k = \frac{p_k}{q_k}$, voidaan päätellä, että $p_k^2 - dq_k^2 < 0$, kun k on parillinen ja $p_k^2 - dq_k^2 > 0$, kun k on pariton. Näin ollen yhtälön

$$\frac{p_k^2 - dq_k^2}{p_{k-1}^2 - dq_{k-1}^2} = -\frac{t_{k-1}}{t_k} \quad k \geq 1$$

vasen puoli on aina negatiivinen. Näin ollen $\frac{t_{k+1}}{t_k}$ on positiivinen. Tällöin $t_{k+1} > 0$.

□

Seuraus 5.5. *Jos n on luvun $\sqrt{d}$ ketjumurtolukuesityksen pituus, niin $t_j = 1$ jos ja vain jos $n|j$.*

Todistus. vrt. [1, s. 341-342]
Olkoon $\sqrt{d} = [a_0; a_1, a_2, \ldots, a_n]$. Tällöin

$$x_{kn+1} = x_1 \quad k = 0, 1, \ldots$$

Niinpä

$$\frac{s_{kn+1} + \sqrt{d}}{t_{kn+1}} = \frac{s_1 + \sqrt{d}}{t_1}$$

tai

$$\sqrt{d}(t_{kn+1} - t_1) = s_{kn+1} t_1 - s_1 t_{kn+1}.$$

Koska $\sqrt{d}$ on irrationaalinen, pätee

$$t_{kn+1} = t_1 \quad \text{ja} \quad s_{kn+1} = s_1.$$

Tällöin

$$t_1 = d - s_1^2 = d - s_{kn+1}^2 = t_{kn} t_{kn+1} = t_{kn} t_1.$$

Näin ollen $t_{kn} = 1$. Siis $t_j = 1$ aina kun $n|j$. Todistetaan väite seuraavaksi toiseen suuntaan. Olkoon j positiivinen kokonaisluku, jolle $t_j = 1$ aina, kun $n|j$. Tällöin $x_j = s_j + \sqrt{d}$, joten voimme kirjoittaa

$$[x_j] = s_j + \left[\sqrt{d}\right] = s_j + a_0.$$

Luvun x_{j+1} määritelmästä seuraa, että

$$x_j = [x_j] + \frac{1}{x_{j+1}} = s_j + a_0 + \frac{1}{x_{j+1}}.$$

Edelleen

$$a_0 + \frac{1}{x_1} = x_0 = \sqrt{d} = x_j - s_j = a_0 + \frac{1}{x_{j+1}},$$

joten $x_{j+1} = x_1$. Näin ollen jakso $a_1, a_2, ..., a_j$ toistuu luvun$\sqrt{d}$ ketjumurtolukuesityksessä. Tästä seuraa, että luvun j täytyy olla jakson pituuden n monikerta.

□

Lause 5.6. *Olkoon $\frac{p_k}{q_k}$ luvun $\sqrt{d}$ ketjumurtoesityksen konvergentti ja olkoon n esityksen pituus.*
(a) Jos n on parillinen, niin kaikki yhtälön $x^2 - dy^2 = 1$ positiiviset ratkaisut ovat muotoa

$$x = p_{kn-1} \quad y = q_{kn-1} \quad k = 1, 2, 3, \ldots$$

(b) Jos n on pariton, niin kaikki yhtälön $x^2 - dy^2 = 1$ positiiviset ratkaisut ovat muotoa

$$x = p_{2kn-1} \quad y = q_{2kn-1} \quad k = 1, 2, 3, \ldots$$

Todistus. vrt. [1, s. 343]
Lauseessa 5.1 on todettu, että mikä tahansa ratkaisu x_0, y_0 yhtälölle $x^2 - dy^2 = 1$ on muotoa $x_0 = p_j$ ja $y_0 = q_j$ jollakin luvun $\sqrt{d}$ konvergentille p_j/q_j. Lauseen 5.4 nojalla,

$$p_j^2 - dq_j^2 = (-1)^{j+1} t_{j+1}.$$

Tällöin $j + 1$ on parillinen ja $t_{j+1} = 1$. Seurauksen 5.5 nojalla $n|(j + 1)$, joten $j + 1 = nk$ jollakin k. Jos n on pariton luku, niin luvun k on oltava parillinen. Kun n on parillinen, niin luku k voi olla mikä tahansa. □

Sanotaan yhtälön $x^2 - dy^2 = 1$ perusratkaisuksi ratkaisua x_0, y_0, jolle pätee $0 < x_0 < x'$ ja $0 < y_0 < y'$, missä x', y' on yhtälön $x^2 - dy^2 = 1$ mikä tahansa muu positiivinen ratkaisu.

Esimerkki 5.7. Ratkaistaan yksi Burtonin kirjan tehtävistä, jossa etsitään yhtälön $x^2 - dy^2 = 1$ perusratkaisua. Luvulle d annetaan arvot $7, 11, 18, 20$ ja 39.

a) $d = 7$:

- $y = 1$: $x^2 = 1 + 7 \cdot 1^2 = 8$, ei kokonaislukuratkaisua.
- $y = 2$: $x^2 = 1 + 7 \cdot 2^2 = 29$, ei kokonaislukuratkaisua.
- $y = 3$: $x^2 = 1 + 7 \cdot 3^2 = 64$, josta $x = 8$. Pienin positiivinen ratkaisu on siis $(x, y) = (8, 3)$.

b) $d = 11$:

- $y = 1$: $x^2 = 1 + 11 \cdot 1^2 = 12$, ei kokonaislukuratkaisua.
- $y = 2$: $x^2 = 1 + 11 \cdot 2^2 = 45$, ei kokonaislukuratkaisua.
- $y = 3$: $x^2 = 1 + 11 \cdot 3^2 = 100$, josta $x = 10$. Pienin positiivinen ratkaisu on siis $(x, y) = (10, 3)$.

c) $d = 18$:

- $y = 1$: $x^2 = 1 + 18 \cdot 1^2 = 19$, ei kokonaislukuratkaisua.
- $y = 2$: $x^2 = 1 + 18 \cdot 2^2 = 73$, ei kokonaislukuratkaisua.
- $y = 3$: $x^2 = 1 + 18 \cdot 3^2 = 163$, ei kokonaislukuratkaisua.
- $y = 4$: $x^2 = 1 + 18 \cdot 4^2 = 289$, josta $x = 17$. Pienin positiivinen ratkaisu on siis $(x, y) = (17, 4)$.

d) $d = 30$:

- $y = 1$: $x^2 = 1 + 30 \cdot 1^2 = 31$, ei kokonaislukuratkaisua.
- $y = 2$: $x^2 = 1 + 30 \cdot 2^2 = 121$, josta $x = 11$. Pienin positiivinen ratkaisu on siis $(x, y) = (11, 2)$.

e) $d = 39$:

- $y = 1$: $x^2 = 1 + 39 \cdot 1^2 = 40$, ei kokonaislukuratkaisua.
- $y = 2$: $x^2 = 1 + 39 \cdot 2^2 = 157$, ei kokonaislukuratkaisua.
- $y = 3$: $x^2 = 1 + 39 \cdot 3^2 = 352$, ei kokonaislukuratkaisua.
- $y = 4$: $x^2 = 1 + 39 \cdot 4^2 = 625$, josta $x = 25$. Pienin positiivinen ratkaisu on siis $(x, y) = (25, 4)$.

Lause 5.8. *Olkoot x_1 ja y_1 yhtälön $x^2 - dy^2 = 1$ perusratkaisu. Tällöin jokainen kokonaislukupari x_n, y_n, joka määritellään ehdolla*

$$x_n + y_n\sqrt{d} = \left(x_1 + y_1\sqrt{d}\right)^n \quad n = 1, 2, 3, \ldots$$

on positiivinen ratkaisu.

Todistus. vrt. [1, s. 344]
Koska x_1, y_1 ovat positiivisia, myös x_n, y_n ovat positiivisia kokonaislukuja. Koska pari x_1, y_1 on ratkaisu yhtälölle $x^2 - dy^2 = 1$, saamme

$$\begin{aligned} x_n^2 - dy_n^2 &= \left(x_n + y_n\sqrt{d}\right)\left(x_n - y_n\sqrt{d}\right) \\ &= \left(x_1 + y_1\sqrt{d}\right)^n \left(x_1 - y_1\sqrt{d}\right)^n \\ &= \left(x_1^2 - dy_1^2\right)^n \\ &= 1^n = 1 \end{aligned}$$

ja siten x_n, y_n on positiivinen ratkaisu.

□

Lause 5.9. *Jos x_1, y_1 on yhtälön $x^2 - dy^2 = 1$ perusratkaisu, niin jokainen positiivinen ratkaisu yhtälölle on x_n, y_n, missä x_n ja y_n ovat kokonaislukuja, jotka määräytyvät seuraavasti*

$$x_n + y_n\sqrt{d} = \left(x_1 + y_1\sqrt{d}\right)^2 \quad n = 1, 2, 3, \ldots$$

Todistus. vrt. [1, s. 345-346]
Muodostetaan vastaväite lauseen osoittamiseksi. Oletetaan, että on olemassa positiivinen ratkaisu u, v, jota ei saada kaavalla $\left(x_1 + y_1\sqrt{d}\right)^t$. Koska $x_1 + y_1\sqrt{d} > 1$, niin $\left(x_1 + y_1\sqrt{d}\right)^t$ kasvaa mielivaltaisen suureksi. Tämä tarkoittaa, että luvun $u + v\sqrt{d}$ täytyy olla kahden peräkkäisen potenssin $\left(x_1 + y_1\sqrt{d}\right)^t$ välissä, eli

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

tai

$$x_n + y_n\sqrt{d} < u + v\sqrt{d} < \left(x_n + y_n\sqrt{d}\right)\left(x_1 + y_1\sqrt{d}\right).$$

Kun kerromme tämän epäyhtälön positiivisella luvulla $x_n - y_n\sqrt{d}$ ja huomioimme, että $x_n^2 - dy_n^2 = 1$, niin saamme

$$1 < \left(x_n - y_n\sqrt{d}\right)\left(u + v\sqrt{d}\right) < x_1 + y_1\sqrt{d}.$$

Määritellään seuraavaksi kokonaisluvut r ja s yhtälöllä

$$r + s\sqrt{d} = \left(x_n - y_n\sqrt{d}\right)\left(u + v\sqrt{d}\right)$$

eli

$$r = x_n u - y_n v d \quad \text{ja} \quad s = x_n v - y_n u.$$

Tällöin

$$r^2 - ds^2 = \left(x_n^2 - dy_n^2\right)\left(u^2 - dv^2\right) = 1.$$

Näin ollen r, s on yhtälön $x^2 - dy^2 = 1$, ratkaisu, jolle pätee

$$1 < r + s\sqrt{d} < x_1 + y_1\sqrt{d}.$$

Osoitamme lopuksi parin r, s olevan positiivinen ratkaisu. Koska $1 < r + s\sqrt{d}$ ja $\left(r + s\sqrt{d}\right)\left(r - s\sqrt{d}\right) = 1$, niin huomaamme, että $0 < r - s\sqrt{d} < 1$. Tästä seuraa, että

$$2r = \left(r + s\sqrt{d}\right) + \left(r - s\sqrt{d}\right) > 1 + 0 > 0$$

ja

$$2s\sqrt{d} = \left(r + s\sqrt{d}\right) - \left(r - s\sqrt{d}\right) > 1 - 1 = 0,$$

mistä seuraa, että sekä r että s ovat positiivisia. Koska x_1, y_1 on yhtälön $x^2 - dy^2 = 1$ perusratkaisu, täytyy olla $x_1 < r$ ja $y_1 < s$. Tällöin $x_1 + y_1\sqrt{d} < r + s\sqrt{d}$, mikä on ristiriidassa aiemman epäyhtälön kanssa. Näin ollen väite pätee.

$\square$

Lähteet

[1] Burton, David, M. Elementary Number Theory. *WCB/McGraw-hill, 6th edition, 2007.*

[2] Dudley, Underwood. A Guide to Elementary Number Theory. *The Mathematical Association of America, 2009.*

[3] Koshy, T. Fibonacci and Lucas numbers with applications. *Volume 1, Hoboken, New Jersey, 2017.*

[4] Stillwell, John. Mathematics and its History. *Third edition. Undergraduate Texts in Mathematics. Springer, New York, 2010.*

[5] Rosen, Kenneth H. Elementary Number Theory and Its Applications. *Addison Wesley Longman 2000.*