TAMPEREEN YLIOPISTO
Pro gradu -tutkielma

Viivi Seppälä

Ketjumurtoluvut ja Pellin yhtälö

Informaatiotieteiden yksikkö
Matematiikka
Huhtikuu 2014

Tampereen yliopisto
Informaatiotieteiden yksikkö
SEPPÄLÄ, VIIVI: Ketjumurtoluvut ja Pellin yhtälö
Pro gradu -tutkielma, 50 s.
Matematiikka
Huhtikuu 2014

Tiivistelmä

Tässä tutkielmassa tarkastellaan äärellisiä ja äärettömiä ketjumurtolukuja, sekä niiden yhtä sovellusta, Pellin yhtälöä.

Ensimmäinen luku liittyy äärellisiin ketjumurtolukuihin. Luvussa esitellään äärelliisiin ketjumurtolukuihin liittyviä määritelmiä, sekä niiden ominaisuuksia. Luvussa todistetaan esimerkiksi äärellisten ketjumurtolukujen ja rationaalilukujen välinen yhteys. Lisäksi ensimmäisessä luvussa käsitellään hieman ketjumurtolukujen konvergentteja.

Toisessa luvussa käsitellään äärettömiä ketjumurtolukuja, ja osoitetaan esimerkiksi äärettömien ketjumurtolukujen ja irrationaalilukujen välinen yhteys. Osoitetaan, että jokainen yksinkertainen ääretön ketjumurtoluku vastaa irrationaalilukua ja vastaavasti jokainen irrationaaliluku voidaan esittää yksikäsitteisesti yksinkertaisena äärettömänä ketjumurtolukuna.

Kolmas luku keskittyy jaksollisiin ketjumurtolukuihin. Siinä käsitellään kvadraattisia irrationaalilukuja ja niiden ominaisuuksia sekä tutustutaan redusoituihin kvadraattisiin irrationaalilukuihin. Osoitetaan kvadraattisten irrationaalilukujen ja jaksollisten ketjumurtolukujen välinen yhteys, sekä redusoitujen kvadraattisten irrationaalilukujen ja täysin jaksollisten ketjumurtolukujen välinen yhteys. Lopuksi tutkitaan luvun $\sqrt{d}$ ketjumurtolukuesitystä silloin, kun luku d on positiivinen kokonaisluku eikä se ole täydellinen neliö.

Tutkielman neljännessä luvussa käsitellään Diofantoksen yhtälöiden erityistapausta, Pellin yhtälöä, joka on muotoa $x^2 - dy^2 = 1$. Tarkastellaan, miten luvun $\sqrt{d}$ jaksollisen ketjumurtolukuesityksen konvergentit ja Pellin yhtälön ratkaisut liittyvät toisiinsa. Lopuksi tutkitaan vielä, miten Pellin yhtälön kaikki ratkaisut muodostuvat.

Tutkielmassa on käytetty päälähteenä Kenneth H. Rosenin kirjaa Elementary Number Theory and Its Applications. Sivulähteitä ovat Calvin T. Longin kirja Elementary introduction to Number Theory sekä David M. Burtonin kirja Elementary Number Theory.

Sisältö

1 Johdanto

Tämän tutkielma käsittelee äärellisiä ja äärettömiä ketjumurtolukuja, sekä niiden yhtä sovellusta, Pellin yhtälöä. Tutkielman pääpaino on yksinkertaisissa ketjumurtoluvuissa.

Ensimmäinen luku liittyy äärellisiin ketjumurtolukuihin. Luvussa esitellään äärelliisiin ketjumurtolukuihin liittyviä määritelmiä, sekä niiden ominaisuuksia. Luvussa todistetaan esimerkiksi äärellisten ketjumurtolukujen ja rationaalilukujen välinen yhteys, eli kuinka jokainen yksinkertainen äärellinen ketjumurtoluku esittä rationaalilukua, ja jokainen rationaaliluku vastaa yksinkertaista äärellistä ketjumurtolukua. Lisäksi ensimmäisessä luvussa käsitellään hieman ketjumurtolukujen konvergentteja, ja niiden tärkeimpiä ominaisuuksia.

Toisessa luvussa käsittellään äärettömiä ketjumurtolukuja, ja osoitetaan esimerkiksi äärettömien ketjumurtolukujen ja irrationaalilukujen välinen yhteys. Osoitetaan, että jokainen yksinkertainen ääretön ketjumurtoluku vastaa irrationaalilukua ja vastaavasti jokainen irrationaaliluku voidaan esittää yksikäsitteisesti yksinkertaisena äärettömänä ketjumurtolukuna.

Kolmas luku keskittyy jaksollisiin ketjumurtolukuihin. Siinä käsitellään kvadraattisia irrationaalilukuja ja niiden ominaisuuksia. Tutustutaan myös redusoituihin kvadraattisiin irrationaalilukuihin. Osoitetaan kvadraattisten irrationaalilukujen ja jaksollisten ketjumurtolukujen välinen yhteys, sekä redusoitujen kvadraattisten irrationaalilukujen ja täysin jaksollisten ketjumurtolukujen välinen yhteys. Lopuksi tarkastellaan hieman luvun $\sqrt{d}$ ketjumurtolukuesitystä sellaisessa tapauksessa, kun luku d on positiivinen kokonaisluku eikä se ole täydellinen neliö.

Tutkielman neljännessä luvussa käsitellään Diofantoksen yhtälöiden erityistapausta, Pellin yhtälöä. Pellin yhtälö on muotoa $x^2 - dy^2 = 1$. Tarkastellaan, miten luvun $\sqrt{d}$ jaksollisen ketjumurtolukuesityksen konvergentit ja Pellin yhtälön ratkaisut liittyvät toisiinsa. Lopuksi tutkitaan vielä Pellin yhtälön kaikkien ratkaisuiden muodostamista luvun $\sqrt{d}$ jaksollisen ketjumurtolukuesityksen konvergenttien ja jakson pituuden avulla.

Tutkielmassa on käytetty päälähteenä Kenneth H. Rosenin kirjaa Elementary Number Theory and Its Applications. Sivulähteitä ovat Calvin T. Longin kirja Elementary introduction to Number Theory sekä David M. Burtonin kirja Elementary Number Theory.

2 Äärelliset ketjumurtoluvut

2.1 Äärellisten ketjumurtolukujen peruskäsitteitä

Tässä pykälässä esitämme muutamia määritelmiä, jotka koskevat äärellisiä ketjumurtolukuja.

Eukleideen algoritmin avulla on mahdollista esittää rationaaliluvut ketjumurtolukuina. Esimerkiksi Eukleideen algoritmi tuottaa seuraavanlaisen yhtälöiden jonon:

$$\begin{aligned} 23 &= 9 \cdot 2 + 5 \\ 9 &= 5 \cdot 1 + 4 \\ 5 &= 4 \cdot 1 + 1 \\ 4 &= 1 \cdot 4 + 0. \end{aligned}$$

Kun jaamme yhtälön molemmat puolet kyseisen yhtälön jakajalla, saamme

$$\begin{aligned} \frac{9}{23} &= 0 + \frac{9}{23} = 0 + \frac{1}{23/9} \\ \frac{23}{9} &= 2 + \frac{5}{9} = 2 + \frac{1}{9/5} \\ \frac{9}{5} &= 1 + \frac{4}{5} = 1 + \frac{1}{5/4} \\ \frac{5}{4} &= 1 + \frac{1}{4}. \end{aligned}$$

Yhdistämällä edellä esitellyt yhtälöt, huomaamme, että saamme alkuperäisen murtoluvun $\frac{9}{23}$ ilmaistua muiden murtolukujen avulla seuraavasti:

$$\begin{aligned} \frac{9}{23} &= \frac{1}{23/9} \\ &= \cfrac{1}{2 + \cfrac{5}{9}} \\ &= \cfrac{1}{2 + \cfrac{1}{9/5}} \\ &= \cfrac{1}{2 + \cfrac{1}{1 + 4/5}} \\ &= \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{5/4}}} \end{aligned}$$

$$= \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{4}}}}$$

Edellä esitettyjen yhtälöiden ketjun lopullinen muoto on ketjumurtolukuesitys äärelliselle murtoluvulle $\frac{9}{23}$.

Seuraavaksi esitämme määritelmän ketjumurtoluvuille.

Määritelmä 2.1. Äärellisellä ketjumurtoluvulla tarkoitetaan esitystä

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

missä a_0, a_1, a_2, $\ldots$, a_n ovat reaalilukuja siten, että a_1, a_2, a_3, $\ldots$, a_n ovat positiivisia. Reaalilukuja a_1, a_2, a_3, $\ldots$, a_n kutsutaan ketjumurtoluvun osanimittäjiksi. Ketjumurtolukua kutsutaan yksinkertaiseksi, jos reaaliluvut a_0, a_1, a_2, $\ldots$, a_n ovat kaikki kokonaislukuja.

Koska ketjumurtolukujen kirjoittaminen kokonaan auki murtolukumuodossa on monimutkaista, otamme käyttöön notaation $[a_0; a_1, a_2, \ldots, a_n]$ esittämään ketjumurtolukua äärellisten ketjumurtolukujen tapauksessa.

2.2 Äärelliset ketjumurtoluvut ja rationaaliluvut

Seuraavaksi tarkastelemme äärellisten ketjumurtolukujen ja rationaalilukujen välistä yhteyttä. Tulemme näyttämään, että jokainen yksinkertainen ketjumurtoluku edustaa jotakin rationaalilukua. Myöhemmin tulemme todistamaan myös, että jokainen rationaaliluku voidaan esittää yksinkertaisena äärellisenä ketjumurtolukuna.

Lause 2.1. *Jokainen yksinkertainen äärellinen ketjumurtoluku edustaa rationaalilukua.*

Todistus. (Vrt. [4, s. 443]). Todistamme lauseen käyttämällä matemaattista induktiota. Kun $n = 1$, ketjumurtolukuesitys on muotoa

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

joka on rationaalinen. Seuraavaksi tehdään induktio-oletus, että yksinkertainen ketjumurtoluku $[a_0; a_1, a_2, \ldots, a_k]$ on rationaalinen, kun $n = k$ ja kun $a_0, a_1, \ldots, a_k$

ovat positiivisia kokonaislukuja. Olkoot $a_0, a_1, \ldots, a_{k+1}$ positiivisia kokonaislukuja. Huomataan, että

$$[a_0; a_1, a_2, \ldots, a_{k+1}] = a_0 + \frac{1}{[a_1; a_2, \ldots, a_k, a_{k+1}]}.$$

Induktio-oletuksen nojalla $[a_1; a_2, \ldots, a_k, a_{k+1}]$ on rationaalinen; on siis olemassa sellaiset kokonaisluvut r ja s, $s \neq 0$, että ketjumurtoluku $[a_1; a_2, \ldots, a_k, a_{k+1}]$ on yhtäsuuri kuin r/s. Nyt siis

$$[a_0; a_1, \ldots, a_k, a_{k+1}] = a_0 + \frac{1}{r/s} = \frac{a_0 r + s}{r},$$

joka on edelleen rationaaliluku. Induktioperiaatteen mukaan väite on siis tosi. □

Huomautus 2.1. Ks. [4, s.443]. Lähdeteoksessa lauseen 12.7 todistuksessa (vrt. tutkielman lauseen 2.1 todistus) yhtälön

$$[a_0; a_1] = a_0 + \frac{1}{a_1} = \frac{a_0 a_1 + 1}{a_0}$$

tilalla pitäisi olla yhtälö

$$[a_0; a_1] = a_0 + \frac{1}{a_1} = \frac{a_0 a_1 + 1}{a_1}.$$

Seuraavaksi näytämme Eukleideen algoritmin avulla, että jokainen rationaaliluku voidaan esittää äärellisenä yksinkertaisena ketjumurtolukuna.

Lause 2.2. *Jokainen rationaaliluku voidaan esittää äärellisenä yksinkertaisena ketjumurtolukuna.*

Todistus. (Vrt. [4, s. 444]. Olkoon $x = a/b$, missä a ja b ovat kokonaislukuja ja $b > 0$. Asetetaan $r_0 = a$ ja $r_1 = b$. Nyt Eukleideen algoritmi tuottaa seuraavanlaisen yhtälöiden jonon:

$$\begin{array}{rcll}
r_0 & = & r_1 q_1 + r_2, & 0 < r_2 < r_1, \\
r_1 & = & r_2 q_2 + r_3, & 0 < r_3 < r_2, \\
r_2 & = & r_3 q_3 + r_4, & 0 < r_4 < r_3, \\
 & \vdots & & \\
r_{n-3} & = & r_{n-2} q_{n-2} + r_{n-1}, & 0 < r_{n-1} < r_{n-2}, \\
r_{n-2} & = & r_{n-1} q_{n-1} + r_n, & 0 < r_n < r_{n-1}, \\
r_{n-1} & = & r_n q_n. &
\end{array}$$

Näissä yhtälöissä termit $q_1, q_2, \ldots, q_n$ ovat positiivisia kokonaislukuja. Kun nämä yhtälöt kirjoitetaan murtolukumuotoon, saadaan yhtälöt

$$\begin{aligned}
\frac{a}{b} = \frac{r_0}{r_1} &= q_1 + \frac{r_2}{r_1} = q_1 + \frac{1}{r_1/r_2}, \\
\frac{r_1}{r_2} &= q_2 + \frac{r_3}{r_2} = q_2 + \frac{1}{r_2/r_3}, \\
\frac{r_2}{r_3} &= q_3 + \frac{r_4}{r_3} = q_3 + \frac{1}{r_3/r_4}, \\
&\vdots \\
\frac{r_{n-3}}{r_{n-2}} &= q_{n-2} + \frac{r_{n-1}}{r_{n-2}} = q_{n-2} + \frac{1}{r_{n-2}/r_{n-1}}, \\
\frac{r_{n-2}}{r_{n-1}} &= q_{n-1} + \frac{r_n}{r_{n-1}} = q_{n-1} + \frac{1}{r_{n-1}/r_n}, \\
\frac{r_{n-1}}{r_n} &= q_n.
\end{aligned}$$

Sijoittamalla murtoluvun r_1/r_2 arvo toisesta yhtälöstä ensimmäiseen yhtälöön, saamme yhtälön

$$\frac{a}{b} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{r_2/r_3}}.$$

Samalla tavalla voimme sijoittaa murtoluvun r_2/r_3 arvon kolmannesta yhtälöstä edellä esitettyyn yhtälöön, jolloin yhtälö tulee muotoon

$$\frac{a}{b} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{r_3/r_4}}}.$$

Jatkamalla tätä menettelyä huomaamme, että

$$\frac{a}{b} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{}{\ddots + q_{n-1} + \cfrac{1}{q_n}}}}.$$

Siis $\frac{a}{b} = [q_1; q_2, \ldots, q_n]$. On siis osoitettu, että jokainen rationaaliluku voidaan esittää äärellisenä yksinkertaisena kutjumurtolukuna. □

Huomautus 2.2. Ks [4, s. 444]. Lähdeteksen lauseessa 12.8 (vrt. tämän tutkielman lause 2.2) esiintyneiden termien $r + 0$, $r + 1$ ja $r + 2$ tilalla pitäisi olla termit r_0, r_1 ja r_2.

Huomaamme, että rationaalilukujen ketjumurtolukuesitykset eivät ole yksikäsitteisiä, vaan ketjumurtoluvun viimeistä termiä voidaan muuttaa. Jos $a_n > 1$, voidaan viimeinen termi kirjoittaa muodossa

$$a_n = (a_n - 1) + 1 = (a_n - 1) + \frac{1}{1}.$$

Tätä yhtälöä käyttämällä voidaan edelleen merkitä, että

$$[a_0; a_1, a_2, \ldots, a_{n-1}, a_n] = [a_0; a_1, a_2, \ldots, a_{n-1}, a_n - 1, 1].$$

Jos $a_n = 1$, silloin

$$a_{n-1} + \frac{1}{a_n} = a_{n-1} + \frac{1}{1} = a_{n-1} + 1.$$

Näin ollen

$$[a_0; a_1, a_2, \ldots, a_{n-1}, a_n] = [a_0; a_1, a_2, \ldots, a_{n-2}, a_{n-1} + 1].$$

Jokaisella rationaaliluvulla on siis kaksi ketjumurtolukuesitystä siten, että toisessa on parillinen määrä ja toisessa pariton määrä termejä. (Vrt. [1, s. 285])

Esimerkki 2.1. Tarkastellaan murtolukua $\frac{7}{11}$. Muodostetaan tekijöiden avulla seuraavat yhtälöt:

$$\begin{aligned}
\frac{7}{11} &= 0 + \frac{7}{11} = 0 + \frac{1}{11/7}, \\
\frac{11}{7} &= 1 + \frac{4}{7} = 1 + \frac{1}{7/4}, \\
\frac{7}{4} &= 1 + \frac{3}{4} = 1 + \frac{1}{4/3}, \\
\frac{4}{3} &= 1 + \frac{1}{3} = 1 + \frac{1}{3/1}.
\end{aligned}$$

Nämä yhtälöt yhdistämällä huomaamme, että

$$\frac{7}{11} = 0 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{3}}}}.$$

Tämä ketjumurtolukuesitys voidaan kirjoittaa lyhyemmin muodossa $[0; 1, 1, 1, 3]$. Kuten edellä totesimme, ketjumurtolukuesitykset eivät ole yksikäsitteisiä, joten muroluku $\frac{7}{11}$ voidaan ilmoittaa myös toisenlaisena ketjumurtolukuna. Edellä totesimme, että jos $[a_0; a_1, a_2, \ldots, a_{n-1}, a_n]$ on jonkin luvun ketjumurolukuesitys, niin $[a_0; a_1, a_2, \ldots, a_{n-1}, a_n - 1, 1]$ on myös sellainen. Tämä tarkoittaa, että $\frac{7}{11}$ voidaan esittää myös muodossa:

$$\frac{7}{11} = 0 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1}}}}},$$

joka on lyhemmin ilmaistuna $[0; 1, 1, 1, 2, 1]$. Nyt siis on voimassa

$$\frac{7}{11} = [0; 1, 1, 1, 3] = [0; 1, 1, 1, 2, 1].$$

2.3 Konvergentit

Tässä luvussa tarkastelemme lukuja, jotka on saatu äärellisestä ketjumurtoluvusta katkaisemalla esitys halutusta kohdasta.

Määritelmä 2.2. Ketjumurtolukua $[a_0; a_1, a_2, \ldots, a_k]$, missä $0 \leq k \leq n$, sanotaan ketjumurtoluvun $[a_0; a_1, a_1, \ldots, a_n]$ k. konvergentiksi. Tätä konvergenttia merkitään symbolilla C_k.

Käymme seuraavaksi läpi menetelmän, jolla ketjumurtolukujen konvergentteja voidaan muodostaa.

Lause 2.3. *Olkoot $a_0, a_1, a_2, \ldots, a_n$ reaalilukuja siten, että $a_1, a_2, \ldots, a_n$ ovat positiivisia. Määritellään jonot $p_0, p_1, \ldots, p_n$ ja $q_0, q_1, \ldots, q_n$ rekursiivisesti yhtälöillä*

$$\begin{aligned} p_0 &= a_0, & q_0 &= 1, \\ p_1 &= a_0 a_1 + 1, & q_1 &= a_1 \end{aligned}$$

ja

$$p_k = a_k p_{k-1} + p_{k-2}, \qquad q_k = a_k q_{k-1} + q_{k-2},$$

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

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

Todistus. (Vrt. [4, s. 445-446]). Todistamme tämän lauseen matemaattisella induktiolla. Kun $k = 0$, niin

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

Kun $k = 1$, huomaamme, että

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

Väite on siis tosi, kun $k = 0$ ja $k = 1$.

Seuraavaksi oletamme, että väite on tosi positiivisella kokonaisluvulla k silloin, kun $2 \leq k < n$. Tämä tarkoittaa, että

$$C_k = [a_0; a_1, \ldots, a_k] = \frac{p_k}{q_k} = \frac{a_k p_{k-1} + p_{k-2}}{a_k q_{k-1} + q_{k-2}}.$$

Rekursioyhtälöiden perusteella havaitaan, että reaaliluvut $p_{k-1}, p_{k-2}, q_{k-2}$ riippuvat ainoastaan luvuista $a_0, a_1, \ldots, a_{k-1}$. Näin ollen reaaliluku a_k voidaan korvata luvulla $a_k + 1/a_{k+1}$, jolloin huomaamme, että

$$\begin{aligned}
C_{k+1} = [a_0; a_1, \ldots, a_k, a_{k+1}] &= \left[a_o; a_1, \ldots, a_{k-1}, a_k + \frac{1}{a_{k+1}}\right] \\
&= \frac{(a_k + \frac{1}{a_{k+1}})p_{k-1} + p_{k-2}}{(a_k + \frac{1}{a_{k+1}})q_{k-1} + q_{k-2}} \\
&= \frac{a_k p_{k-1} + \frac{p_{k-1}}{a_{k+1}} + p_{k-2}}{a_k q_{k-1} + \frac{q_{k-1}}{a_{k+1}} + q_{k-2}} \\
&= \frac{a_{k+1} a_k p_{k-1} + p_{k-1} + a_{k+1} p_{k-2}}{a_{k+1} a_k q_{k-1} + a_{k+1} q_{k-2}} \\
&= \frac{a_{k+1}(a_k p_{k-1} + p_{k-2}) + p_{k-1}}{a_{k+1}(a_k q_{k-1} + q_{k-1}) + q_{k-1}} \\
&= \frac{a_{k+1} p_k + p_{k-1}}{a_{k+1} q_k + q_{k-1}} \\
&= \frac{p_{k+1}}{q_{k+1}}.
\end{aligned}$$

Väite on siis tosi arvolla $k + 1$, joten induktioperiaatteen mukaan alkuperäinen väite on todistettu todeksi. □

Huomautus 2.3. Luvut p_k ja q_k voidaan määritellä myös yhtälöillä

$$\begin{aligned}
p_{-2} &= 0, \qquad & q_{-2} = 1, \\
p_{-1} &= 1, \qquad & q_{-1} = 0
\end{aligned}$$

ja

$$p_k = a_k p_{k-1} + p_{k-2}, \qquad q_k = a_k q_{k-1} + q_{k-2},$$

kun $0 \leq k \leq n$ (vrt. [3, s. 214]).

Seuraavaksi havainnollistamme konvergenttien muodostamista esimerkin avulla.

Esimerkki 2.2. Tarkastellaan lukua $57/13$. Sen ketjumurtolukuesitys on $[4; 2, 1, 1, 2]$. Kyseisen ketjumurtolukuesityksen kaikki konvergentit on mahdollista määrittää edellä esitettyjen rekursioyhtälöiden avulla. Tällöin

$$\begin{aligned}
p_0 &= 4, & q_0 &= 1, \\
p_1 &= 4 \cdot 2 + 1 = 9, & q_1 &= 2, \\
p_2 &= 1 \cdot 9 + 4 = 13, & q_2 &= 1 \cdot 2 + 1 = 3, \\
p_3 &= 1 \cdot 13 + 9 = 22, & q_3 &= 1 \cdot 3 + 2 = 5, \\
p_4 &= 2 \cdot 22 + 13 = 57, & q_4 &= 2 \cdot 5 + 3 = 13.
\end{aligned}$$

Konvergentit $C_k \quad (k = 0, 1, \ldots, 4)$ ovat siis

$$\begin{aligned} C_0 &= p_0/q_0 = 4/1 = 4, \\ C_1 &= p_1/q_1 = 9/2, \\ C_2 &= p_2/q_2 = 13/3, \\ C_3 &= p_3/q_3 = 22/5, \\ C_4 &= p_4/q_4 = 57/13. \end{aligned}$$

Seuraavaksi esitämme ja todistamme toisen tärkeän ketjumurtolukujen konvergentteihin liittyvän ominaisuuden.

Lause 2.4. *Olkoon $C_k = p_k/q_k$ ketjumurtoluvun $[a_0; a_1, a_2, \ldots, a_n]$ k. konvergentti ja $1 \leq k \leq n$. Tällöin*

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

Todistus. (Vrt. [4, s. 447]). Todistamme lauseen matemaattisen induktion avulla. Kun $k = 1$, lauseen 2.3 rekursioyhtälöiden perusteella saamme

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

joten väite on tosi kun $k = 1$. Oletetaan sitten, että väite on tosi luvun k positiivisilla kokonaislukuarvoilla, joilla on voimassa $1 \leq k \leq n$. Nyt siis

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

Rekursioyhtälöiden sekä induktio-oletuksen avulla saadaan yhtälöketju

$$\begin{aligned} p_{k+1} q_k - p_k q_{k+1} &= (a_{k+1} p_k + p_{k-1}) q_k - p_k (a_{k+1} q_k + q_{k-1}) \\ &= a_{k+1} p_k q_k + p_{k-1} q_k - a_{k+1} p_k q_k - p_k q_{k-1} \\ &= p_{k-1} q_k - p_k q_{k-1} \\ &= -(p_k q_{k-1} - p_{k-1} q_k) \\ &= -(-1)^{k-1} \\ &= (-1)^k, \end{aligned}$$

joten väite on tosi arvolla $k+1$. Näin ollen alkuperäinen väite on induktioperiaatteen mukaan tosi. □

Seuraavaksi havainnollistamme tätä lausetta esimerkin 2.2 avulla, jolla havainnollistimme myös lausetta 2.3.

Esimerkki 2.3. Luvun $57/13$ ketjumurtolukuesitys on $[4; 2, 1, 1, 2]$. Edellisen lauseen perusteella on voimassa

$$\begin{aligned} p_0 q_1 - p_1 q_0 &= 4 \cdot 2 - 9 \cdot 1 = -1 \\ p_1 q_2 - p_2 q_1 &= 9 \cdot 3 - 13 \cdot 2 = 1 \\ p_2 q_3 - p_3 q_2 &= 13 \cdot 5 - 22 \cdot 3 = -1. \end{aligned}$$

Seuraavaksi esitämme seuraksen, joka osoittaa, että yksinkertaisen ketjumurtoluvun konvergentit ovat supistetussa muodossa, kun $k = 1, 2, \ldots$.

Seuraus 2.1. *Olkoon $C_k = p_k/q_k$ yksinkertaisen ketjumurtoluvun $[a_0; a_1, a_2, \ldots, a_n]$ k. konvergentti. Lisäksi p_k ja q_k ovat kokonaislukuja ja ne on määritelty kuten lauseessa 2.3. Tällöin kyseiset kokonaisluvut p_k ja q_k ovat suhteellisia alkulukuja.*

Todistus. (Vrt. [4, s. 447-448]). Olkoon $d = (p_k, q_k)$. Lauseen 2.4 perusteella tiedämme, että

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

Näin ollen tiedämme myös, että

$$d | (-1)^{k-1},$$

jolloin siis on voimassa sekä $d|1$ ja $d|(-1)$. Tästä seuraa, että $d = 1$. Koska $d = (p_k, q_k) = 1$, niin lukujen p_k ja q_k on oltava keskenään jaottomia, ja väite siis pätee. □

Seuraus 2.2. *Olkoon $C_k = p_k/q_k$ yksinkertaisen ketjumurtoluvun $[a_0; a_1, a_2, \ldots, a_n]$ k. konvergentti. Tällöin*

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

kaikilla kokonaisluvuilla k, missä $1 \leq k \leq n$. Lisäksi seuraava yhtälö on voimassa

$$C_k - C_{k-2} = \frac{a_k (-1)^k}{q_k q_{k-2}}$$

kaikilla kokonaisluvuilla k, missä $2 \leq k \leq n$.

Todistus. (Vrt. [4, s. 448]). Lauseen 2.4 perusteella tiedämme, että $p_k q_{k-1} - p_{k-1} q_k = (-1)^{k-1}$. Kun jaamme tämän yhtälön puolittain luvulla $q_k q_{k-1}$, saamme yhtälön

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

Näin ollen ensimmäinen yhtälö on siis voimassa.
Seuraavaksi tarkastelemme erotusta $C_k - C_{k-2}$. Huomaamme, että

$$C_k - C_{k-2} = \frac{p_k}{q_k} - \frac{p_{k-2}}{q_{k-2}} = \frac{p_k q_{k-2} - p_{k-2} q_k}{q_k q_{k-2}}.$$

Lauseen 2.3 rekursioyhtälöiden avulla tiedetään, että $p_k = a_k p_{k-1} + p_{k-2}$ ja $q_k = a_k q_{k-1} + q_{k+2}$. Lisäksi tiedämme lauseen 2.4 perusteella, että $p_{k-1} q_{k-2} - p_{k-2} q_{k-1} = (-1)^{k-2}$. Näiden tietojen avulla saamme erotuksen $C_k - C_{k-2}$ oikeanpuoleisen lausekkeen osoittajan muotoon

$$\begin{aligned}
p_k q_{k-2} - p_{k-2} q_k &= (a_k p_{k-1} + p_{k-2}) q_{k-2} - p_{k-2}(a_k q_{k-1} + q_{k-2}) \\
&= a_k p_{k-1} q_{k-2} + p_{k-2} q_{k-2} - p_{k-2} a_k q_{k-1} - p_{k-2} q_{k-2} \\
&= a_k (p_{k-1} q_{k-2} - p_{k-2} q_{k-1}) \\
&= a_k (-1)^{k-2}.
\end{aligned}$$

Nyt huomaamme, että

$$C_k - C_{k-2} = \frac{a_k(-1)^{k-2}}{q_k q_{k-2}} = \frac{a_h(-1)^k}{q_k q_{k-2}}.$$

Näin ollen toinenkin yhtälö on voimassa. $\square$

Huomautus 2.4. Ks. [4, s. 448]. Lähdeteoksen seurauksessa 12.3 (vrt. tämän tutkielman seuraus 2.2) esiintyneen yksinkertaisen ketjumurtoluvun $[a_0; a_1, a_2, \dots, a_k]$ tilalla pitäisi olla ketjumurtoluku $[a_0; a_1, a_2, \dots, a_n]$.

Lause 2.5. *Olkoon C_k yksinkertaisen ketjumurtoluvun $[a_0; a_1, a_2, \dots, a_n]$ k. konvergentti. Tällöin*

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

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

ja jokainen parittomasti indeksöity konvergentti $C_{2j+1}, j = 0, 1, 2, \dots$ on jokaista parillisesti indeksöityä konvergenttia $C_{2j}, j = 0, 1, 2, \dots$ suurempi.

Todistus. (Vrt. [4, s. 449]). Seurauksen 2.2 mukaan kun $k = 2, 3, \dots, n$, niin

$$C_k - C_{k-2} = \frac{a_k(-1)^k}{q_k q_{k-1}}.$$

Kun luku k on pariton, edellä esitetyn yhtälön oikea puoli on negatiivinen. Tiedämme siis, että silloin

$$C_k < C_{k-2}$$

on voimassa. Parittomasti indeksöidyt konvergentit muodostavat siis aidosti vähenevän jonon. Vastaavasti jos luku k on parillinen, on edellä esitetyn yhtälön oikea puoli positiivinen, jolloin saamme epäyhtälön

$$C_k > C_{k-2}.$$

Parillisesti indeksöidyt konvergentit muodostavat siis aidosti kasvavan jonon. Toisin sanoen tiedämme, että

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

Lisäksi tiedämme, että

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

On vielä osoitettava, että jokainen parittomasti indeksöity konvergentti on jokaista parillisesti indeksöityä konvergenttia suurempi. Seurauksen 2.2 mukaan tiedämme, että

$$C_{2m} - C_{2m-1} = \frac{(-1)^{2m-1}}{q_{2m} q_{2m-1}} < 0.$$

Tämän perusteella siis $C_{2m-1} > C_{2m}$. Kun vertailemme konvergentteja C_{2k} ja C_{2j-1}, huomaamme, että

$$C_{2j-1} > C_{2j+2k-1} > C_{2j+2k} > C_{2k}.$$

Näin ollen siis jokainen parittomasti indeksöity konvergentti on jokaista parillisesti indeksöityä konvergenttia suurempi. $\square$

Esimerkki 2.4. Tarkastellaan vielä aiemmin esitetyn esimerkin 2.2 ketjumurtoluvun $[4; 2, 1, 1, 2]$ konvergentteja. Esitämme konvergentit murtolukumuodossa:

$$\begin{aligned} C_0 &= 4, \\ C_1 &= \frac{9}{2} = 4,5, \\ C_2 &= \frac{13}{3} = 4,3333\ldots, \\ C_3 &= \frac{22}{5} = 4,4, \\ C_4 &= \frac{57}{13} = 4,3846. \end{aligned}$$

Huomaamme, että lauseen 2.5 mukaisesti on voimassa

$$C_0 = 4 < C_2 = 4,333\ldots < C_4 = 4,3846\ldots < C_3 = 4,4 < C_1 = 4,5.$$

3 Äärettömät ketjumurtoluvut

Tässä luvussa perehdymme hieman äärettömiin ketjumurtolukuihin ja tarkastelemme niiden ominaisuuksia aiemmin esitettyjen tulosten avulla.

3.1 Äärettömien ketjumurtolukujen peruskäsitteitä

Aluksi esitämme kaksi määritelmää äärettömiin ketjumurtolukuihin liittyen.

Määritelmä 3.1. Äärettömällä ketjumurtoluvulla tarkoitamme lauseketta

$$a_0 + \cfrac{b_1}{a_1 + \cfrac{b_2}{a_2 + \cfrac{b_3}{a_3 + \cfrac{b_4}{\ddots}}}},$$

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

Määritelmä 3.2. Yksinkertaisella äärettömällä ketjumurtoluvulla tarkoitamme lauseketta

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots}}}},$$

missä a_0 on kokonaisluku ja $a_1, a_2, a_3, \ldots$ ovat positiivisia kokonaislukuja.

Tässä luvussa käsittelemme yksinkertaisia äärettömiä ketjumurtolukuja. Näiden ketjumurtolukujen termejä $a_1, a_2, \ldots$ kutsutaan osanimittäjiksi, kuten äärellistenkin ketjumurtolukujen tapauksessa. Yksinkertaiselle ketjumurtoluvulle otamme käyttöön samankaltaisen notaation kuin äärellisille ketjumurtoluvuille, eli merkitsemme niitä $[a_0; a_1, a_2, \ldots]$.

3.2 Äärettömät ketjumurtoluvut ja irrationaaliluvut

Äärellisten ketjumurtolukujen tapauksessa tutkimme niiden ja rationaalilukujen välistä yhteyttä. Tässä pykälässä tutkimme vastaavasti äärettömien ketjumurtolukujen ja irrationaalilukujen välistä yhteyttä.

Lause 3.1. *Olkoon $a_0, a_1, a_2, \ldots$ ääretön jono kokonaislukuja siten, että $a_1, a_2, \ldots$ ovat positiivisia kokonaislukuja. Olkoon lisäksi $C_k = [a_0; a_1, a_2, \ldots, a_k]$. Tällöin konvergentit C_k lähestyvät raja-arvoa α , toisin sanoen*

$$\lim_{k\to\infty} C_k = \alpha.$$

Ennen kuin todistamme lauseen 3.1, määrittelemme, että $\alpha = [a_0; a_1, a_2, \ldots]$. Eli α on yksinkertaisen äärettömän ketjumurtoluvun arvo.

Jotta saamme lauseen 3.1 todistettua, näytämme, että parillisesti indeksöityjen konvergenttien ääretön jono on kasvava ja sillä on yläraja. Lisäksi näytämme, että parittomasti indeksöityjen konvergenttien ääretön jono on vähenevä ja sillä on olemassa alaraja. Tämän jälkeen osoitamme, että näiden kahden jonon raja-arvot ovat samat.

Todistus. (Vrt. [4, s. 452-453]). Olkoon m positiivinen parillinen kokonaisluku. Lauseen 2.5 perusteella tiedämme, että

$$C_1 > C_3 > C_5 > \ldots > C_{m-1},$$

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

ja $C_{2j} < C_{2k+1}$ aina, kun $2j \leq m$ ja $2k+1 < m$. Kun tarkastelemme kaikki mahdolliset arvot jotka m voi saada, huomaamme, että

$$C_1 > C_3 > C_5 > \ldots > C_{2n-1} > C_{2n+1} > \ldots,$$

$$C_0 < C_2 < C_4 < \ldots < C_{2n-2} < C_{2n} < \ldots$$

ja $C_{2j} < C_{2k+1}$ kaikilla positiivisilla kokonaisluvuilla j ja k. Parittomasti indeksöidyt konvergentit $C_1, C_3, C_5, \ldots$ muodostavat alhaalta rajoitetun aidosti vähenevän jonon, joka lähestyy raja-arvoa α_1. Parillisesti indeksöidyt konvergentit $C_0, C_2, C_4, \ldots$ vastaavasti muodostavat ylhäältä rajoitetun aidosti kasvavan jonon, joka lähestyy raja-arvoa α_2. Näin ollen

$$\begin{aligned} \lim_{n\to\infty} C_{2n+1} &= \alpha_1, \\ \lim_{n\to\infty} C_{2n} &= \alpha_2. \end{aligned}$$

Tarkoituksenamme on nyt osoittaa näiden kahden raja-arvon yhtäsuuruus. Seurauksen 2.2 mukaan on voimassa

$$C_{2n+1} - C_{2n} = \frac{p_{2n+1}}{q_{2n+1}} - \frac{p_{2n}}{q_{2n}} = \frac{(-1)^{(2n+1)-1}}{q_{2n+1}q_{2n}} = \frac{1}{q_{2n+1}q_{2n}}.$$

Koska $q_k > k$ kaikilla positiivisilla kokonaisluvuilla k, saamme epäyhtälön

$$\frac{1}{q_{2n+1}q_{2n}} < \frac{1}{(2n+1)(2n)},$$

ja näin ollen

$$C_{2n+1} - C_{2n} = \frac{1}{q_{2n+1}q_{2n}}$$

lähestyy nollaa. Tämä tarkoittaa, että

$$\lim_{n\to\infty} (C_{2n+1} - C_{2n}) = 0.$$

Nyt siis tiedämme, että

$$\lim_{n\to\infty}(C_{2n+1} - C_{2n}) = \lim_{n\to\infty} C_{2n+1} - \lim_{n\to\infty} C_{2n} = 0,$$

eli jonoilla $C_1, C_3, C_5, \ldots$ ja $C_0, C_2, C_4, \ldots$ on sama raja-arvo. Olemme siis osoittaneet, että $\alpha_1 = \alpha_2$, ja voimme siis päätellä, että kaikki konvergentit lähestyvät raja-arvoa $\alpha = \alpha_1 = \alpha_2$. Näin ollen väite on siis todistettu. □

Huomautus 3.1. Ks. [4, s. 478]. Lähdeteoksessa lauseen 12.13 todistuksessa (vrt. tämän tutkielman lauseen 3.1 todistus) epäyhtälön $C_{2j} > C_{2k+1}$ tilalla pitäisi olla epäyhtälö $C_{2j} < C_{2k+1}$.

Aiemmin osoitimme jo, että jokaisella rationaaliluvulla on olemassa äärellinen yksinkertainen ketjumurtolukuesitys. Seuraavaksi osoitamme, että jokaisen äärettömän yksinkertaisen ketjumurtoluvun arvo on irrationaaliluku.

Lause 3.2. *Olkoon $a_0, a_1, a_2, \ldots$ kokonaislukuja siten, että $a_1, a_2, \ldots$ ovat positiivisia. Tällöin $[a_0; a_1, a_2, \ldots]$ on irrationaalinen.*

Todistus. (Vrt. [3, s. 222]). Lauseen 3.1 perusteella tiedämme, että luku α on aidosti kasvavan jonon C_{2n} ja aidosti vähenevän jonon C_{2n+1} yhteinen raja-arvo, kun n on positiivinen kokonaisluku. Näin ollen luku α sijaitsee siis konvergenttien C_n ja C_{n+1} $(n = 0, 1, 2, \ldots)$ välissä. Tämän tiedon ja seurauksen 2.2 perusteella on voimassa

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

Seuraavaksi teemme vastaoletuksen, että α olisikin rationaaliluku. Merkitsemme, että $\alpha = a/b$, missä a ja b ovat kokonaislukuja, ja lisäksi $b > 0$. Tällöin saamme

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

Kun kerromme tämän epäyhtälön puolittain luvulla bq_n (> 0), saamme edelleen

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

Koska $q_{n+1} \geq n + 1$, niin

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

Valitsemalla kokonaisluku n, joka on $\geq b$, saadaan

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

Tämä on mahdotonta, koska $aq_n - bp_n$ on kokonaisluku. Näin ollen vastaoletus on väärä ja alkuperinen väite tosi. Luku α on siis irrationaalinen. □

Nyt olemme siis osoittaneet, että jokainen yksinkertainen ääretön ketjumurtoluku vastaa irrationaalilukua. Seuraavaksi tarkastelemme irrationaalilukujen esittämistä yksinkertaisten äärettömien ketjumurtolukujen avulla.

Lause 3.3. *Olkoon α irrationaaliluku ja merkitään lisäksi, että $\alpha = \alpha_0$. Määritellään jono $a_0, a_1, a_2, \ldots$ rekursiivisesti yhtälöillä*

$$a_k = [\alpha_k]. \qquad \alpha_{k+1} = \frac{1}{\alpha_k - a_k},$$

kun $k \geq 0$. Tällöin α on yksinkertaisen äärettömän ketjumurtoluvun $[a_0; a_1, a_2, \ldots]$ arvo.

Todistus. (Vrt. [4, s. 454-455]). Rekursiivisen määritelmän perusteella tiedämme, että a_k on kokonaisluku kaikilla luvun k arvoilla. Lisäksi matemaattisen induktion avulla voimme osoittaa, että luku α_k on irrationaalinen aina, kun k on epänegatiivinen, ja että tämän seurauksena luku α_{k+1} on olemassa. Oletuksen perusteella tiedämme, että $\alpha_0 = \alpha$ on irrationaalinen, joten

$$\alpha_0 \neq a_0 = [\alpha_0].$$

Lisäksi rekursiivisen määritelmän perusteella tiedämme, että luku

$$\alpha_1 = \frac{1}{\alpha_0 - a_0}$$

on olemassa.

Oletamme seuraavaksi, että α_k on irrationaalinen. Näin ollen luku α_{k+1} on olemassa. Voimme havaita helposti luvun α_{k+1} olevan myös irrationaalinen, nimittäin yhtälöstä

$$\alpha_{k+1} = \frac{1}{\alpha_k - a_k}$$

seuraa, että

$$\alpha_k = a_k + \frac{1}{\alpha_{k+1}}.$$

Jos α_{k+1} olisi rationaaliluku niin myös α_k olisi rationaaliluku.

Koska α_k on irrationaaliluku ja a_k on kokonaisluku, niin tiedämme, että $\alpha_k \neq a_k$. Tällöin tiedämme, että

$$a_k < \alpha_k < a_k + 1.$$

Kun vähennämme tästä epäyhtälöstä puolittain luvun a_k, saamme

$$0 < \alpha_k - a_k < 1.$$

Nyt edellä esitetyn perusteella on voimassa

$$\alpha_{k+1} = \frac{1}{\alpha_k - a_k} > 1,$$

joten tästä seuraa, että

$$a_{k+1} = [\alpha_{k+1}] \geq 1,$$

kun $k \geq 0$.Tämä tarkoittaa, että kaikki kokonaisluvut $a_1, a_2, \ldots$ ovat positiiviisia. Kun käytämme toistuvasti kaavaa

$$\alpha_k = a_k + \frac{1}{\alpha_{k+1}},$$

huomaamme, että

$$\begin{aligned}
\alpha = \alpha_0 &= a_0 + \frac{1}{\alpha_1} = [a_0; \alpha_1] \\
&= a_0 + \cfrac{1}{a_1 + \cfrac{1}{\alpha_2}} = [a_0; a_1, \alpha_2] \\
&\vdots \\
&= a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{}{\ddots \cfrac{}{+a_k + \cfrac{1}{\alpha_{k+1}}}}}} = [a_0; a_1, a_2, \ldots, a_k, \alpha_{k+1}].
\end{aligned}$$

Seuraavaksi osoitamme, että ketjumurtoluvun $[a_0; a_1, a_2, \ldots, a_k, \alpha_{k+1}]$ arvo lähestyy lukua α, kun luku k kasvaa rajatta. Lauseen 2.3 todistuksen perusteella tiedämme, että

$$\alpha = [a_0; a_1, a_2, \ldots, a_k, \alpha_{k+1}] = \frac{\alpha_{k+1} p_k + p_{k+1}}{\alpha_{k+1} q_k + q_{k+1}},$$

missä $C_j = p_j / q_j$ on ketjumurtoluvun j. konvergentti. Tällöin siis

$$\begin{aligned}
\alpha - C_k &= \frac{\alpha_{k+1} p_k + p_{k-1}}{\alpha_{k+1} q_k + q_{k-1}} - \frac{p_k}{q_k} \\
&= \frac{\alpha_{k+1} p_k q_k + p_{k-1} q_k - \alpha_{k+1} p_k q_k - p_k q_{k-1}}{(\alpha_{k+1} q_k + q_{k-1}) q_k} \\
&= \frac{-(p_k q_{k-1} - p_{k-1} q_k)}{(\alpha_{k+1} q_k + q_{k-1}) q_k} \\
&= \frac{-(-1)^{k-1}}{(\alpha_{k+1} q_k + q_{k-1}) q_k},
\end{aligned}$$

missä osoittaja $-(p_k q_{k-1} - p_{k-1} q_k)$ on sievennetty käyttämällä lausetta 2.4. Koska

$$\alpha_{k+1} q_k + q_{k-1} > a_{k+1} q_k + q_{k-1} = q_{k+1},$$

tiedämme, että

$$
\begin{aligned}
|\alpha - C_k| &= \left|\frac{-(-1)^{k-1}}{(\alpha_{k+1}q_k + q_{k-1})q_k}\right| \\
&= \frac{1}{(\alpha_{k+1}q_k + q_{k-1})q_k} \\
&< \frac{1}{(\alpha_{k+1}q_k + q_{k-1})q_k} \\
&= \frac{1}{q_k q_{k+1}}.
\end{aligned}
$$

Koska $q_k \geq k$, tiedämme, että lauseke $\frac{1}{q_k q_{k+1}}$ lähestyy arvoa 0, kun luku k kasvaa rajatta eli lähestyy ääretöntä. Näin ollen siis $\lim_{k\to\infty} C_k = \alpha$, eli luku α on yksinkertaisen äärettömän ketjumurtoluvun $[a_0; a_1, a_2, \ldots]$ arvo. □

Huomautus 3.2. Ks. [4, s.455]. Lähdeteoksessa lauseen 12.15 todistuksessa (vrt. tämän tutkielman lauseen 3.3 todistus) yksinkertaisen ketjumurtoluvun $[a_0; a_1, a_2]$ tilalla pitäisi olla ketjumurtoluku $[a_0, a_1, \alpha_2]$.

Huomautus 3.3. Ks. [4, s. 456]. Lähdeteoksessa lauseen 12.15 todistuksen (vrt. tämän tutkielman lauseen 3.3 todistus) lopussa on viitattu ehtoon $q_k > k$. Viittauksen pitäisi olla ehtoon $q_k \geq k$.

Lause 3.4. *Jos kaksi yksinkertaista ääretöntä ketjumurtolukua* $[a_0; a_1, a_2, \ldots]$ *ja* $[b_0; b_1, b_2, \ldots]$ *esittävät samaa irrationaalilukua, niin* $a_k = b_k$*, kun* $k = 0, 1, 2, \ldots$.

Todistus. (Vrt. [4, s. 456-457]). Oletetaan, että $\alpha = [a_0; a_1, a_2, \ldots]$. Koska $C_0 = a_0$ ja $C_1 = a_0 + \dfrac{1}{a_1}$, lauseen 3.1 perusteella tiedämme, että

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

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

$$a_0 < \alpha < a_0 + 1.$$

Täten on siis voimassa $a_0 = [\alpha]$. Lisäksi tiedämme, että

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

sillä

$$
\begin{aligned}
\alpha = [a_0; a_{1,2}, \ldots] &= \lim_{k\to\infty} [a_0; a_1, a_2, \ldots, a_k] \\
&= \lim_{k\to\infty} \left(a_0 + \frac{1}{[a_1; a_2, a_3, \ldots, a_k]}\right) \\
&= a_0 + \frac{1}{\lim_{k\to\infty} [a_1; a_2, \ldots, a_k]} \\
&= a_0 + \frac{1}{[a_1; a_2, a_3, \ldots]}.
\end{aligned}
$$

Oletamme, että

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

Tämän oletuksen ja käyttämiemme merkintöjen perusteella huomaamme, että

$$a_0 = b_0 = [\alpha]$$

ja

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

Näin ollen on siis voimassa, että

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

Oletetaan seuraavaksi, että $a_k = b_k$ ja $[a_{k+1}; a_{k+2}, \ldots] = [b_{k+1}; b_{k+2}, \ldots]$. Käytämme samaa päättelyä kuin edellä, ja havaitsemme, että

$$a_{k+1} = b_{k+1}.$$

Lisäksi havaitsemme, että

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

Tästä seuraa, että

$$[a_{k+2}; a_{k+3}, \ldots] = [b_{k+2}; b_{k+3}, \ldots].$$

Olemme siis osoittaneet matemaattisen induktion avulla, että $a_k = b_k$, kun $k \geq 0$. □

Huomautus 3.4. Ks. [4, s. 456-457]. Lähdeteoksessa lauseen 12.16 todistuksessa (vrt. tämän tutkielman lauseeseen 3.4 todistus) on viitattu lähdeteoksen lauseen 12.11 (vrt. tutkielman lause 2.5). Viitauksen pitäisi olla lähdeteoksen lauseeseen 12.13 (vrt. tämän tutkielman lause 3.1). Lisäksi lähdeteoksen lauseen 12.16 todistuksessa (vrt. tämän tutkielman lauseen 3.4 todistus) pitäisi yhtälön

$$a_{k+1} + \frac{1}{[a_{k+2}; a_{k+3}, \ldots]} = b_{k+1} + \frac{1}{[b_{k+1}; b_{k+3}, \ldots]}$$

tilalla olla yhtälö

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

Lauseiden 3.3 ja 3.4 perusteella tiedämme nyt, että jokainen irrationaaliluku on mahdollista esittää yksinkertaisena äärettömänä ketjumurtolukuna.

Esimerkki 3.1. Olkoon $\alpha = \sqrt{39}$. Seuraavaksi muodostamme tämän irrationaaliluvun ketjumurtolukuesityksen käyttämällä lauseen 3.3 rekursioyhtälöitä. Tällöin

$$
\begin{aligned}
a_0 &= \left[\sqrt{39}\right] = 6, \\
\alpha_1 &= \frac{1}{\sqrt{39}-6} = \frac{\sqrt{39}+6}{39-36} = \frac{\sqrt{39}+6}{3}, \\
a_1 &= \left[\frac{\sqrt{39}+6}{3}\right] = 4, \\
\alpha_2 &= \frac{1}{\frac{\sqrt{39}+6}{3}-4} = \frac{1}{\frac{\sqrt{39}-6}{3}} = \frac{3}{\sqrt{39}-6} = \frac{3(\sqrt{39}+6)}{39-36} = \sqrt{39}+6, \\
a_2 &= \left[\sqrt{39}+6\right] = 12, \\
\alpha_3 &= \frac{1}{\sqrt{39}+6-12} = \frac{1}{\sqrt{39}-6} = \frac{\sqrt{39}+6}{39-36} = \frac{\sqrt{39}+6}{3}.
\end{aligned}
$$

Koska $\alpha_3 = \alpha_1$, niin $a_3 = a_1, a_4 = a_2, \ldots$ ja näin saamme

$$\sqrt{39} = [6; 4, 12, 4, 12, 4, 12, \ldots].$$

Tämä ketjumurtoluku sisältää osanimittäjien jakson, joka toistuu jatkuvasti. Tämän vuoksi sitä kutsutaan jaksolliseksi ketjumurtoluvuksi.

Irrationaaliluvun ketjumurtolukukehitelmän konvergentit ovat hyviä approksimaatioita luvulle α. Itse asiassa, jos p_k/q_k on tämän ketjumurtolukuesityksen k. konvergentti, niin lauseen 3.3 todistuksen perusteella tiedämme, että

$$|\alpha - p_k/q_k| < 1/(q_k q_{k+1}),$$

joten tästä seuraa, että

$$|\alpha - p_k/q_k| < 1/{q_k}^2,$$

koska $q_k < q_{k+1}$.

Seuraava lause ja seurauslause osoittavat, että irrationaaliluvun α ketjumurtolukukehitelmän konvergentit ovat luvun α parhaita rationaalisia approksimaatioita. Parhaalla rationaalisella aprroksimaatiolla tarkoitamme, että konvergentti p_k/q_k on lähin sellaisista luvun α ratiolaalisista approksimaatioista, joiden nimittäjä ei ole suurempi kuin kyseessä olevan konvergentin nimittäjä.

Ennen kuin käsittelemme edellä mainitun lauseen ja seurauslauseen, esitämme apulauseen, jota tulemme tarvitsemaan lauseen 3.5 todistuksessa.

Apulause 3.1. *Jos a, b ja c ovat sellaisia positiivisia kokonaislukuja, että (a,b)=1 ja $a|bc$, niin $a|c$.*

Todistus. Ks. [4, s. 97]. □

Lause 3.5. *Olkoon α irrationaaliluku ja olkoot $p_j/q_j (j = 1,2,\dots)$ luvun α yksinkertaisen äärettömän ketjumurtolukuesityksen konvergentteja. Jos r ja s ovat kokonaislukuja ja $s > 0$ ja jos k on sellainen positiivinen kokonaisluku, että*

$$|s\alpha - r| < |q_k\alpha - p_k|,$$

niin $s \geq q_{k+1}$.

Todistus. (Vrt. [4, s. 458-459]). Ensin teemme vastaoletuksen, että $|s\alpha - r| < |q_k\alpha - p_k|$, mutta $1 \leq s < q_{k+1}$. Tarkastelemme yhtälöryhmää

$$\begin{aligned} p_k x + p_{k+1} y &= r \\ q_k x + q_{k+1} y &= s. \end{aligned}$$

Kerromme ensimmäisen yhtälön puolittain luvulla q_k ja toisen yhtälön vastaavasti luvulla p_k. Tämän jälkeen vähennämme toisen yhtälön ensimmäisestä puolittain. Tällöin saamme

$$(p_{k+1}q_k - p_k q_{k+1})y = rq_k - sp_k.$$

Lauseen 2.4 perusteella tiedämme, että $p_{k+1}q_k - p_k q_{k+1} = (-1)^k$. Tämän perusteella tiedämme, että

$$y = (-1)^k (rq_k - sp_k).$$

Tämän jälkeen kerromme ensimmäisen yhtälön luvulla q_{k+1}, ja toisen yhtälön luvulla p_{k+1}, ja vähennämme ensimmäisen yhtälön toisesta. Nyt saamme

$$(p_{k+1}q_k - p_k q_{k+1})x = sp_{k+1} - rq_{k+1}.$$

Kun käytämme edelleen lauseen 2.4 tulosta, saamme yhtälön

$$x = (-1)^k (sp_{k+1} - rq_{k+1}).$$

Seuraavaksi osoitamme, että $x \neq 0$ ja $y \neq 0$. Jos olisi $x = 0$, silloin olisi voimassa $sp_{k+1} = rq_{k+1}$. Koska $(p_{k+1}, q_{k+1}) = 1$, apulauseen 3.1 perusteella $q_{k+1}|s$. Tästä seuraa, että $q_{k+1} \leq s$, mikä on ristiriita. Näin ollen $x \neq 0$. Jos taas $y = 0$, niin tällöin on voimassa seuraavat yhtälöt $r = p_k x$ ja $s = q_k x$. Näiden yhtälöiden, sekä ehdon $|x| \geq 1$ nojalla saamme

$$\begin{aligned} |s\alpha - r| &= |q_k x\alpha - p_k x| = |x(q_k\alpha - p_k)| \\ &= |x|\,|q_k\alpha - p_k| \geq |q_k\alpha - p_k|. \end{aligned}$$

Tämä on ristiriidassa oletuksen kanssa, joten on siis voimassa, että $y \neq 0$.

Osoitamme seuraavaksi että luvut x ja y ovat erimerkkisiä. Ensin oletamme, että $y < 0$. Tiedämme, että $q_k x = s - q_{k+1}y$. Tästä seuraa, että $x > 0$, koska $q_k x > 0$ ja $q_k > 0$. Jos taas oletamme, että $y > 0$, niin epäyhtälöketjun $q_{k+1}y \geq q_{k+1} > s$ perusteella tiedämme, että $q_k x = s - q_{k+1}y < 0$. Tästä seuraa siis, että $x < 0$, sillä $q_k > 0$.

Lauseen 3.1 perusteella tiedämme, että joko epäyhtälö $p_k/q_k < \alpha < p_{k+1}q_{k+1}$ tai epäyhtälö $p_{k+1}q_{k+1} < \alpha < p_kq_k$ on voimassa. Kummassakin tapauksessa huomaamme, että luvut $q_k\alpha - p_k$ ja $q_{k+1}\alpha - p_{k+1}$ ovat erimerkkisiä.

Todistuksen alussa esitetyn yhtälöryhmän perusteella tiedämme, että

$$\begin{aligned} |s\alpha - r| &= |(q_kx + q_{k+1}y)\alpha - (p_kx + p_{k+1}y)| \\ &= |x(q_k\alpha - p_k) + y(q_{k+1}\alpha - p_{k+1})| . \end{aligned}$$

Edellisissä kappaleissa esitettyjen päätelmien perusteella tiedämme, että luvut $x(q_k\alpha - p_k)$ ja $y(q_{k+1}\alpha - p_{k+1})$ ovat samanmerkkisiä. Näin ollen niiden summan itseisarvo on sama kuin itseisarvojen summa, eli

$$\begin{aligned} |s\alpha - r| &= |x|\,|q_k\alpha - p_k| + |y|\,|q_{k+1}\alpha - p_{k+1}| \\ &\geq |x|\,|q_k\alpha - p_k| \\ &\geq |q_k\alpha - p_k| , \end{aligned}$$

koska $|x| \geq 1$. Tästä seuraa ristiriita oletuksemme kanssa. Olemme siis osoittaneet, että vastaoletus on väärä ja alkuperäinen väite on tosi. □

Huomautus 3.5. Ks. [4, s. 458]. Lähdeteoksessa lauseen 12.17 todistuksessa (vrt. tutkielman lauseen 3.5 todistus) on tehty oletukset $s \neq 0$ ja $y \neq 0$. Oletusten kuuluisi olla muotoa $x \neq 0$ ja $y \neq 0$. Lisäksi todistuksen loppuosassa on viitattu lähdeteoksen lauseeseen 12.11 (vrt. tämän tutkielman lause 2.5). Viittauksen pitäisi olla lauseeseen 12.13 (vrt. tämän tutkielman lause 3.1).

Seuraus 3.1. *Olkoon α irrationaaliluku, ja olkoot p_j/q_j , $j = 1,2,\ldots$, luvun α yksinkertaisen äärettömän ketjumurtolukuesityksen konvergentteja. Jos r/s on rationaaliluku, missä r ja s ovat kokonaislukuja ja $s > 0$, ja jos k on sellainen positiivinen kokonaisluku, että*

$$\left|\alpha - \frac{r}{s}\right| < \left|\alpha - \frac{p_k}{q_k}\right| ,$$

niin tällöin $s > q_k$.

Todistus. (Vrt. [4, s. 459]). Ensin teemme vastaoletuksen, että $s \leq q_k$ ja

$$\left|\alpha - \frac{r}{s}\right| < \left|\alpha - \frac{p_k}{q_k}\right| .$$

Kun kerromme epäyhtälön puolittain luvulla s ja otamme lisäksi huomioon ehdon $s \leq q_k$, huomaamme, että

$$s\left|\alpha - \frac{r}{s}\right| < q_k\left|\alpha - \frac{p_k}{q_k}\right| .$$

Koska $s, q_k > 0$, niin edellä esitetyn perusteella tiedämme, että

$$|s\alpha - r| < |q_k\alpha - p_k| ,$$

mikä vastaavasti on ristiriidassa lauseen 3.5 päätelmän kanssa. Näin ollen vastaoletuksemme on väärä ja alkuperäinen väite tosi. □

Lopuksi tarkastelemme vielä, millä ehdolla irrationaaliluvun rationaalinen approksimaatio on kyseisen irrationaaliluvun yksinkertaisen äärettömän ketjumurtolukuesityksen konvergentti.

Lause 3.6. *Olkoon α irrationaaliluku. Jos r/s on rationaaliluku, missä r ja s ovat kokonaislukuja ja lisäksi $s > 0$ ja $(r, s) = 1$ ja epäyhtälö*

$$\left|\alpha - \frac{r}{s}\right| < \frac{1}{2s^2}$$

on voimassa, niin r/s on luvun α yksinkertaisen ketjumurtoukusityksen konvergentti.

Todistus. (Vrt. [4, s. 460]). Ensin teemme vastaoletuksen, että r/s ei ole luvun α yksinkertaisen ketjumurtolukuesityksen konvergentti. Näin ollen on olemassa sellaiset konvergentit p_k/q_k ja p_{k+1}/q_{k+1}, että $q_k \leq s < q_{k+1}$. Lauseen 3.5 perusteella tiedämme, että

$$|q_k\alpha - p_k| \leq |s\alpha - r| = s\left|\alpha - \frac{r}{s}\right| < \frac{1}{2s}.$$

Seuraavaksi jaamme epäyhtälön

$$|q_k\alpha - p_k| < \frac{1}{2s}$$

puolittain luvulla q_k (> 0), jolloin saamme

$$\left|\alpha - \frac{p_k}{q_k}\right| < \frac{1}{2sq_k}.$$

Tiedämme, että $|sp_k - rq_k| \geq 1$ (koska tiedämme, että $r/s \neq p_k/q_k$, jolloin $sp_k - rq_k$ on nollasta eroava kokonaisluku). Tästä seuraa (kolmioepäyhtälön avulla), että

$$\begin{aligned}
\frac{1}{sq_k} &\leq \frac{|sp_k - rq_k|}{sq_k} \\
&= \left|\frac{sp_k - rq_k}{sq_k}\right| \\
&= \left|\frac{p_k}{q_k} - \frac{r}{s}\right| \\
&= \left|\frac{p_k}{q_k} - \alpha + \alpha - \frac{r}{s}\right| \\
&\leq \left|\frac{p_k}{q_k} - \alpha\right| + \left|\alpha - \frac{r}{s}\right| \\
&= \left|\alpha - \frac{p_k}{q_k}\right| + \left|\alpha - \frac{r}{s}\right| \\
&< \frac{1}{2sq_k} + \frac{1}{2s^2}.
\end{aligned}$$

Näin ollen saamme, että

$$\frac{1}{2sq_k} < \frac{1}{2s^2}.$$

Lopulta on siis voimassa

$$2sq_k > 2s^2,$$

mistä seraa, että $q_k > s$. Tämä on ristiriidassa ehdon $q_k \leq s < q_{k+1}$ kanssa, joten vastaoletus on väärä ja alkuperäinen väite on tosi. $\square$

4 Jaksolliset ketjumurtoluvut

Kutsumme ääretöntä yksinkertaista ketjumurtolukua $[a_0; a_1, a_2, \ldots]$ jaksolliseksi, jos on olemassa positiiviset kokonaisluvut N ja k siten, että $a_n = a_{n+k}$ kaikilla positiivisilla kokonaisluvuilla $n \geq N$. Käytämme notaatiota

$$[a_0; a_1, a_2, \ldots, a_{N-1}, \overline{a_N, a_{N+1}, a_{N+k-1}}],$$

kuvaamaan jaksollista ääretöntä ketjumurtolukua

$$[a_0; a_1, a_2, \ldots, a_{N-1}, a_N, a_{N+1}, \ldots, a_{N+k-1}, a_N, a_{N+1}, \ldots].$$

Esimerkiksi merkinnällä $[2; 3, \overline{1, 2}]$ tarkoitamme yksinkertaista ääretöntä ketjumurtolukua $[2; 3, 1, 2, 1, 2, 1, 2, \ldots]$. Luvussa 3 sivusimme erään esimerkin yhteydessä äärettömiä yksinkertaisia ketjumutolukuesityksiä, joissa jakso termejä toistuu. Tässä luvussa käsittelemme tarkemmin jaksollisten ketjumurtolukuesitysten ominaisuuksia

4.1 Kvadraattiset irrationaaliluvut

Määritelmä 4.1. Reaalilukua α sanotaan kvadraattiseksi irrationaaliluvuksi, jos α on irrationaalinen ja kokonaislukukertoimisen toisen asteen yhtälön juuri, eli siis

$$A\alpha^2 + B\alpha + C = 0,$$

missä A, B ja C ovat kokonaislukuja ja $A \neq 0$.

Seuraavaksi esitämme kaksi apulausetta ilman todistuksia. Nämä apulauseet helpottavat jaksollisten ketjumurtolukujen ominaisuuksien tutkimista.

Apulause 4.1. *Kahden rationaaliluvun summa ja tulo ovat rationaalisia.*

Todistus. Ks. [4, s. 14, harjoitustehtävä 3].

Apulause 4.2. *Olkoon luku α kokonaislukukertoimisen polynomin $x^n + c_{n-1}x^{n-1} + \ldots + c_1 x + c_0$ juuri. Silloin α on joko kokonaisluku tai irrationaaliluku.*

Todistus. Ks. [4, s. 103, lause 3.17].

Lause 4.1. *Reaaliluku α on kvadraattinen irrationaaliluku, jos ja vain jos on olemassa kokonaisluvut a, b ja c, joille on voimassa $b > 0$ ja $c \neq 0$ siten, että luku b ei ole täydellinen neliö ja*

$$\alpha = \frac{a + \sqrt{b}}{c}.$$

Todistus. (Vrt. [4, s. 463-464]). Jos α on kvadraattinen irrationaaliluku, niin se on selvästi irrationaalinen, ja tällöin on olemassa kokonaisluvut A, B ja C siten, että $A\alpha^2 + B\alpha + C = 0$. Toisen asteen yhtälön ratkaisukaavan perusteella tiedämme, että

$$\alpha = \frac{-B \pm \sqrt{B^2 - 4AC}}{2A}.$$

Koska α on reaaliluku, tiedämme, että $B^2 - 4AC > 0$. Koska α on irrationaalinen, niin $B^2 - 4AC$ ei ole täydellinen neliö ja $A \neq 0$. Merkitsemällä joko $a = -B$, $b = B^2 - 4AC$ ja $c = 2A$ tai $a = B$, $b = B^2 - 4AC$ ja $c = -2A$, saamme luvulle α halutun esityksen.

Oletamme seuraavaksi, että luku α on muotoa

$$\alpha = \frac{a + \sqrt{b}}{c},$$

missä a, b ja c ovat kokonaislukuja siten, että $b > 0$, $c \neq 0$ ja b ei ole täydellinen neliö. Apulauseiden 4.1 ja 4.2 perusteella havaitsemme, että α on irrationaaliluku. Koska

$$\begin{aligned}
\alpha &= \frac{a + \sqrt{b}}{c} \\
\alpha c &= a + \sqrt{b} \\
\alpha c &- a = \sqrt{b} \\
\alpha^2 c^2 + a^2 - 2ac\alpha &= b \\
c^2\alpha^2 - 2ac\alpha + (a^2 - b) &= 0,
\end{aligned}$$

on α kvadraattinen rationaaliluku. □

Huomautus 4.1. Lähdeteoksessa lemman 12.1 muotoilussa (vrt. tämän tutkielman lauseen 4.1 muotoilu) esitetään ehto $\alpha - (a + \sqrt{b})/c$. Ehdon pitäisi olla $\alpha = (a + \sqrt{b})/c$.

Lause 4.2. *Jos α on kvadraattinen irrationaaliluku ja jos r, s, t ja u ovat kokonaislukuja, niin osamäärä $(r\alpha + s)/(t\alpha + u)$ on joko rationaaliluku tai kvadraattinen irrationaaliluku.*

Todistus. (Vrt. [4, s. 464-465]). Oletamme, että α on kvadraattinen rrationaaliluku. Tällöin lauseen 4.1 perusteella on olemassa sellaiset kokonaisluvut a, b ja c ($b > 0$ ja $c \neq 0$), että luku b ei ole täydellinen neliö ja

$$\alpha = (a + \sqrt{b})/c.$$

Tällöin saamme, että

$$\begin{aligned}
\frac{r\alpha+s}{t\alpha+u} &= \left[\frac{r(a+\sqrt{b})}{c}+s\right]\Bigg/\left[\frac{t(a+\sqrt{b})}{c}+u\right] \\
&= \frac{r(a+\sqrt{b})+cs}{c}\cdot\frac{c}{t(a+\sqrt{b})+cu} \\
&= \frac{ar+r\sqrt{b}+cs}{at+t\sqrt{b}+cu} \\
&= \frac{(ar+cs)+r\sqrt{b}}{(at+cu)+t\sqrt{b}} \\
&= \frac{[(ar+cs)+r\sqrt{b}][(at+cu)-t\sqrt{b}]}{[(at+cu)+t\sqrt{b}][(at+cu)-t\sqrt{b}]} \\
&= \frac{[(ar+cs)(at+cu)-rtb]+[r(at+cu)-t(ar+cs)]\sqrt{b}}{(at+cu)^2-t^2b}.
\end{aligned}$$

Näin ollen lauseen 4.1 perusteella $(r\alpha+s)/(t\alpha+u)$ on kvadraattinen irrationaaliluku. Poikkeuksena on tilanne, jossa luvun $\sqrt{b}$ kerroin on nolla, koska tällöin kyseinen osamäärä on rationaaliluku. □

Määritelmä 4.2. Olkoon $\alpha = \dfrac{a+\sqrt{b}}{c}$ kvadraattinen irrationaaliluku. Tällöin luvun α konjugaatti α' määritellään seuraavasti

$$\alpha' = \frac{a-\sqrt{b}}{c}.$$

Lause 4.3. *Jos kvadraattinen irrationaaliluku α on yhtälön $Ax^2+Bx+C=0$ juuri, niin yhtälön toinen juuri on luku α', eli luvun α konjugaatti.*

Todistus. (Vrt. [4, s. 465]). Toisen asteen yhtälön ratkaisukaavan mukaan yhtälöllä $Ax^2+Bx+C=0$ on kaksi juurta ja ne ovat muotoa

$$\alpha = \frac{-B\pm\sqrt{B^2-4AC}}{2A}.$$

Jos luku α on toinen näistä kahdesta juuresta, niin konjugaatti α' on toinen, sillä juurilausekkeen $\sqrt{B^2-4AC}$ etumerkki vaihdetaan muodostettaessa luvusta α lukua α'. □

Lause 4.4. *Jos $\alpha_1 = (a_1+b_1\sqrt{d})/c_1$ ja $\alpha_2 = (a_2+b_2\sqrt{d})/c_2$ rationaalilukuja tai kvadraattisia irrationaalilukuja, seuraavat ominaisuudet ovat voimassa*

$$\begin{aligned}
&(i) && (\alpha_1+\alpha_2)' = \alpha_1'+\alpha_2', \\
&(ii) && (\alpha_1-\alpha_2)' = \alpha_1'-\alpha_2', \\
&(iii) && (\alpha_1\alpha_2)' = \alpha_1'\alpha_2', \\
&(iv) && (\alpha_1/\alpha_2)' = \alpha_1'/\alpha_2'.
\end{aligned}$$

Todistus. (Vrt. [4, s. 465-466]). Todistamme tuloa koskevan säännön (iii), sekä osamäärää koskevan säännön (iv). Kaksi muuta sääntöä todistetaan vastaavasti, joten sivuutamme niiden todistukset tässä.

Koska $\alpha_1 = (a_1 + b_1\sqrt{d})/c_1$ ja $\alpha_2 = (a_2 + b_2\sqrt{d})/c_2$, saadaan tulolle yhtälö

$$\begin{aligned}
\alpha_1\alpha_2 &= \frac{(a_1 + b_1\sqrt{d})}{c_1} \cdot \frac{(a_2 + b_2\sqrt{d})}{c_2} \\
&= \frac{(a_1 + b_1\sqrt{d})(a_2 + b_2\sqrt{d})}{c_1c_2} \\
&= \frac{a_1a_2 + a_1b_2\sqrt{d} + b_1\sqrt{d}\ a_2 + b_1\sqrt{d}\ b_2\sqrt{d}}{c_1c_2} \\
&= \frac{(a_1a_2 + b_1b_2d) + (a_1b_2 + b_1a_2)\sqrt{d}}{c_1c_2}.
\end{aligned}$$

Määritelmän 4.2 perusteella saamme tulon konjugaaatin $(\alpha_1\alpha_2)'$ muotoon

$$(\alpha_1\alpha_2)' = \frac{(a_1a_2 + b_1b_2d) - (a_1b_2 + b_1a_2)\sqrt{d}}{c_1c_2}.$$

Konjugaattien tulo vastaavasti vastaa määritelmän 4.2 perusteella yhtälöä

$$\begin{aligned}
\alpha_1'\alpha_2' &= \frac{(a_1 - b_1\sqrt{d})}{c_1} \cdot \frac{(a_2 - b_2\sqrt{d})}{c_2} \\
&= \frac{a_1a_2 - a_1b_2\sqrt{d} - b_1\sqrt{d}\ a_2 + b_1\sqrt{d}\ b_2\sqrt{d}}{c_1c_2} \\
&= \frac{(a_1a_2 + b_1b_2d) - (a_1b_2 + b_1a_2)\sqrt{d}}{c_1c_2}.
\end{aligned}$$

Nyt huomaamme, että $(\alpha_1\alpha_2)' = \alpha_1'\alpha_2'$, joten tuloa koskeva ominaisuus (iii) on tosi.

Koska $\alpha_1 = (a_1 + b_1\sqrt{d})/c_1$ ja $\alpha_2 = (a_2 + b_2\sqrt{d})/c_2$, saadaan osamäärälle yhtälö

$$\begin{aligned}
\frac{\alpha_1}{\alpha_2} &= \frac{(a_1 + b_1\sqrt{d})/c_1}{(a_2 + b_2\sqrt{d})/c_2} \\
&= \frac{c_2(a_1 + b_1\sqrt{d})}{c_1(a_2 + b_2\sqrt{d})} \\
&= \frac{c_2(a_1 + b_1\sqrt{d})(a_2 - b_2\sqrt{d})}{c_1(a_2 + b_2\sqrt{d})(a_2 - b_2\sqrt{d})} \\
&= \frac{c_2a_1a_2 - c_2a_1b_2\sqrt{d} + c_2a_2b_1\sqrt{d} - c_2b_1b_2d}{c_1({a_2}^2 - {b_2}^2d)} \\
&= \frac{(c_2a_1a_2 - c_2b_1b_2d) + (c_2a_2b_1 - c_2a_1b_2)\sqrt{d}}{c_1({a_2}^2 - {b_2}^2d)}.
\end{aligned}$$

Määritelmän 4.2 perusteella tiedämme nyt, että voimme esittää osamäärän α_1/α_2 konjugaatin $(\alpha_1/\alpha_2)'$ yhtälönä

$$\left(\frac{\alpha_1}{\alpha_2}\right)' = \frac{(c_2a_1a_2 - c_2b_1b_2d) - (c_2a_2b_1 - c_2a_1b_2)\sqrt{d}}{c_1({a_2}^2 - {b_2}^2)}.$$

Konjugaattien osamäärä α_1'/α_2' vastaavasti vastaa määritelmän 4.2 perusteella yhtälöä

$$
\begin{aligned}
\frac{\alpha_1'}{\alpha_2'} &= \frac{(a_1 - b_1\sqrt{d})/c_1}{(a_2 - b_2\sqrt{d})/c_2} \\
&= \frac{c_2(a_1 - b_1\sqrt{d})(a_2 + b_2\sqrt{d})}{c_1(a_2 - b_2\sqrt{d})(a_2 + b_2\sqrt{d})} \\
&= \frac{c_2a_1a_2 + c_2a_1b_2\sqrt{d} - c_2a_2b_1\sqrt{d} - c_2b_1b_2d}{c_1({a_2}^2 - {b_2}^2d)} \\
&= \frac{(c_2a_1a_2 - c_2b_1b_2d) - (c_2a_2b_1 - c_2a_1b_2)\sqrt{d}}{c_1({a_2}^2 - {b_2}^2d)}.
\end{aligned}
$$

Nyt huomaamme, että $(\alpha_1/\alpha_2)' = \alpha_1'/\alpha_2'$, joten osamäärää koskeva sääntö (iv) on tosi. □

Huomautus 4.2. Ks. [4, s. 465]. Lähdeteoksen apulauseen 14.4 (vrt. tämän tutkielman lause 4.4) toisen ehdon tulisi olla $(\alpha_1 - \alpha_2)' = \alpha_1' - \alpha_2'$, eikä $(\alpha_1 + \alpha_2)' = \alpha_1' - \alpha_2'$.

Lause 4.5. *(Lagrangen lause) Irrationaaliluvun yksinkertainen ääretön ketjumurtolukuesitys on jaksollinen, jos ja vain jos luku on kvadraattinen irrationaaliluku.*

Lauseen todistus on jaettu kahteen osaan. Tämä on mahdollista, sillä kehäpäättelyä ei synny, vaikka todistusten osien välissä esitetäänkin lauseet 4.6 ja 4.7 todistuksineen.

Todistus. (Vrt. [4, s. 466-467]). Olkoon yksinkertainen ketjumurtoluku α jaksollinen. Tällöin voimme merkitä, että

$$\alpha = [a_0; a_1, a_2, \ldots, a_{N-1}, \overline{a_N, a_{N+1}, \ldots, a_{N+k}}].$$

Lisäksi merkitsemme, että

$$\beta = [\overline{a_N, a_{N+1}, \ldots, a_{N+k}}].$$

Tällöin

$$\beta = [a_N; a_{N+1}, \ldots, a_{N+k}, \beta],$$

ja lauseen 2.3 avulla saamme, että

$$\beta = \frac{\beta p_k + p_{k-1}}{\beta q_k + q_{k-1}},$$

missä p_k/q_k ja p_{k-1}/q_{k-1} ovat ketjumurtoluvun $[a_N; a_{N+1}, \ldots, a_{N+k}]$ konvergentteja. Koska luvun β yksinkertainen ketjumurtolukuesitys on ääretön, niin tiedämme, että β on irrationaaliluku.Voimme esittää yhtälön

$$\beta = \frac{\beta p_k + p_{k-1}}{\beta q_k + q_{k-1}}$$

muodossa

$$q_k\beta^2 + (q_{k-1} - p_k)\beta - p_{k-1} = 0,$$

joten määritelmän 4.1 perusteella havaitsemme, että luku β on kvadraattinen irrationaaliluku. Nyt huomaaamme, että

$$\alpha = [a_0; a_1, a_2, \ldots, a_{N-1}, \beta],$$

joten lauseen 2.3 perusteella saamme

$$\alpha = \frac{\beta p_{N-1} + p_{N-2}}{\beta q_{N-1} + q_{N-2}},$$

missä p_{N-1}/q_{N-1} ja p_{N-2}/q_{N-2} ovat ketjumurtoluvun $[a_0; a_1, a_2, \ldots, a_{N-1}]$ konvergentteja. Koska tiedämme,että β on kvadraattinen irrationaaliluku, niin lauseen 4.2 perusteella tiedämme, että myös α on kvadraattinen irrationaaliluku (tiedämme, että α on irrationaaliluku, koska yksinkertainen ketjumurtolukuesitys on ääretön). □

Esimerkki 4.1. Olkoon $x = [2; \overline{1, 4}]$. Lauseen 4.5 perusteella tiedämme, että x on kvadraattinen irrationaaliluku. Merkitsemme, että $x = [2; y]$, missä $y = [\overline{1; 4}]$, kuten lauseen 4.5 todistuksessa. Tiedämme, että $y = [1, 4, y]$, joten

$$y = 1 + \cfrac{1}{4 + \cfrac{1}{y}} = 1 + \cfrac{1}{\cfrac{4y+1}{y}} = 1 + \frac{y}{4y+1} = \frac{5y+1}{4y+1}.$$

Nyt saamme muodostettua toisen asteen yhtälön

$$4y^2 - 4y - 1 = 0.$$

Koska tiedämme, että $y > 0$, niin toisen asteen yhtälön ratkaisukaavan avulla saamme

$$y = \frac{4 + \sqrt{(-4)^2 - 4 \cdot 4 \cdot (-1)}}{2 \cdot 4} = \frac{1 + \sqrt{2}}{2}$$

Koska $x = 2 + \dfrac{1}{y}$, niin saamme

$$x = 2 + \frac{2}{1+\sqrt{2}} = 2 + \frac{2(1-\sqrt{2}}{1-2} = 2 + \frac{2-2\sqrt{2}}{-1} = \frac{-2+2-2\sqrt{2}}{-1} = 2\sqrt{2}.$$

Siis $x = 2\sqrt{2}$.

Lauseen 4.5 perusteella voimme nyt selvittää jaksollisia ketjumurtolukuja vastaavat kvadraattiset irrationaaliluvut. Myöhemmin tulemme esittämään lauseen, jonka avulla voimme määrittää kvadraattisia irrationaalilukuja vastaavat ketjumurtoluvut.

Lause 4.6. *Jos α on kvadraattinen irrationaaliluku, niin se voidaan kirjoittaa muodossa*

$$\alpha = \frac{P + \sqrt{d}}{Q},$$

missä P, Q ja d ovat kokonaislukuja siten, että $Q \neq 0$, $d > 0$, d ei ole täydellinen neliö ja $Q|(d - P^2)$.

Todistus. (Vrt. [4, s. 467-468]). Koska α on kvadraattinen irrationaaliluku, lauseen 4.1 perusteella tiedämme, että luvulle α pätee

$$\alpha = \frac{a + \sqrt{b}}{c},$$

missä a, b ja c ovat kokonaislukuja, $b > 0$ ja $c \neq 0$. Kun lavennamme tämän murtoluvun luvulla $|c|$, saamme muodon

$$\alpha = \frac{a\,|c| + |c|\,\sqrt{b}}{c\,|c|} = \frac{a\,|c| + \sqrt{bc^2}}{c\,|c|}.$$

Olkoon nyt $P = a\,|c|$, $Q = c\,|c|$ ja $d = bc^2$. Tällöin P, Q ja d ovat kokonaislukuja. Lisäksi tiedämme, että $Q \neq 0$, koska $c \neq 0$ ja $d > 0$ koska $b > 0$. Tiedämme vielä, että luku d ei ole täydellinen neliö, koska luku b ei ole täydellinen neliö. Lopulta tiedämme, että $Q|(d - P^2)$, sillä voimme kirjoittaa luvun $d - P^2$ muodossa $d - P^2 = bc^2 - a^2c^2 = c^2(b - a^2) = \pm Q(b - a^2)$. □

Seuraavasi esitämme menetelmän, jolla voimme määrittää kvadraattisia irrationaalilukuja vastaavat ketjumurtoluvut.

Lause 4.7. *Olkoon α kvadraattinen irrationaaliluku. Kirjoitetaan se muodossa*

$$\alpha = \frac{P_0 + \sqrt{d}}{Q_0},$$

missä $P_0.Q_0, d$ ovat kokonaislukuja siten, että $Q_0 \neq 0$, $d > 0$, d ei ole täydellinen neliö ja $Q_0|(d - P_0^2)$. Määrittelemme rekursiivisesti, että

$$\begin{aligned} \alpha_k &= (P_k + \sqrt{d})/Q_k, \\ a_k &= [\alpha_k], \\ P_{k+1} &= a_k Q_k - P_k, \\ Q_{k+1} &= (d - P_{k+1}^2)/Q_k, \end{aligned}$$

kun $k = 0, 1, 2, \ldots$. Silloin $\alpha = [a_0; a_1, a_2, \ldots]$.

Todistus. (Vrt. [4, s. 468-469]). Todistamme ensin matemaattisella induktiolla, että luvut P_k ja Q_k ovat kokonaislukuja ja että $Q_k \neq 0$ ja $Q_k|(d - P_k^2)$. Tämä väite on oletuksen nojalla tosi, kun $k = 0$. Seuraavaksi oletamme, että P_k ja Q_k ovat kokonaislukuja, ja että $Q_k \neq 0$ ja $Q_k|(d - P_k^2)$. Tällöin tiedämme, että

$$P_{k+1} = a_k Q_k - P_k$$

on kokonaisluku. Luvun Q_{k+1} voimme kirjoittaa edellä esitettyjen rekursiokaavojen avulla seuraavasti

$$\begin{aligned} Q_{k+1} &= \frac{d - P_{k+1}^2}{Q_k} \\ &= \frac{d - (a_k Q_k - P_k)^2}{Q_k} \\ &= \frac{d - a_k^2 Q_k^2 + 2a_k Q_k P_k - P_k^2}{Q_k} \\ &= \frac{d - P_k^2}{Q_k} + (2a_k Q_k P_k - a_k^2 Q_k). \end{aligned}$$

Induktio-oletuksen perusteella tiedämme, että $Q_k | (d - P_k^2)$. Tästä seuraa, että Q_{k+1} on kokonaisluku. Tiedämme, että d ei ole täydellinen neliö, joten $d \neq P_{k+1}^2$. Tästä seuraa, että $Q_{k+1} = (d - P_{k+1}^2)/Q_k \neq 0$. Koska

$$Q_k = \frac{d - P_{k+1}^2}{Q_{k+1}},$$

tiedämme, että $Q_{k+1} | (d - P_{k+1}^2)$. Tämä päättää induktiotodistuksen.

Seuraavaksi todistamme lauseen 3.3 avulla, että kokonaisluvut $a_0, a_1, a_2, \ldots$ vastaavat luvun α ketjumurtolukukehitelmän $[a_0; a_1, a_2, \ldots]$ termejä. Jos voimme osoittaa, että

$$\alpha_{k+1} = \frac{1}{\alpha_k - a_k},$$

kun $k = 0, 1, 2, \ldots$, niin silloin tiedämme, että $\alpha = [a_0; a_1, a_2, \ldots]$. Lauseen muotoilussa esitettyjen rekursiokaavojen perusteella saamme yhtälön

$$\begin{aligned} \alpha_k - a_k &= \frac{P_k + \sqrt{d}}{Q_k} - a_k \\ &= \frac{\sqrt{d} - (a_k Q_k - P_k)}{Q_k} \\ &= \frac{\sqrt{d} - P_{k+1}}{Q_k} \\ &= \frac{(\sqrt{d} - P_{k+1})(\sqrt{d} + P_{k+1})}{Q_k(\sqrt{d} + P_{k+1})} \\ &= \frac{d - P_{k+1}^2}{Q_k(\sqrt{d} + P_{k+1})} \\ &= \frac{Q_k Q_{k+1}}{Q_k(\sqrt{d} + P_{k+1})} \\ &= \frac{Q_{k+1}}{\sqrt{d} + P_{k+1}} \\ &= \frac{1}{\alpha_{k+1}}. \end{aligned}$$

Olemme siis osoittaneet, että $\alpha_{k+1} = 1/(\alpha_k - a_k)$. Näin ollen $\alpha = [a_0; a_1, a_2, \ldots]$. $\square$

Huomautus 4.3. Ks. [4, s. 468]. Lähdeteoksessa lauseen 12.20 induktiotodistuksen (vrt. tämän tutkielman lauseen 4.7 todistus) lopussa on käytetty ehtoa $d \neq P_k^2$. Ehdon pitäisi olla $d \neq P_{k+1}^2$. Lisäksi ehdon $\alpha_{k+1} = 1/(\alpha_k - a_k)$ todistuksessa tulisi yhtälöketjussa olla lausekkeen

$$(\sqrt{d} - P_{k+1})(\sqrt{d} + P_{k+1})/Q_k(\sqrt{d} + P_{k+1})$$

tilalla lauseke

$$(\sqrt{d} - P_{k+1})(\sqrt{d} + P_{k+1})/(Q_k(\sqrt{d} + P_{k+1})).$$

Esimerkki 4.2. Määritämme kvadraattisen irrationaaliluvun $\alpha = (3 + \sqrt{5})/2$ ketjumurtolukuesityksen käyttämällä lauseen 4.7 rekursioyhtälöitä. Ensin muodostamme aloitusarvot P_0, Q_0, d ja a_0. Nyt $5 - 3^2 = -4$. Selvästi 2 jakaa luvun -4. Aloitusarvot ovat siis

$$P_0 = 3, Q_0 = 2, d = 5, a_0 = [\alpha] = \left[\frac{3+\sqrt{5}}{2}\right] = 2.$$

Näiden arvojen ja rekursioyhtälöiden avulla saamme

$$\begin{aligned}
P_1 &= a_0 \cdot Q_0 - P_0 = 2 \cdot 2 - 3 = 1, & \alpha_1 &= \frac{P_1 + \sqrt{d}}{Q_1} = \frac{1+\sqrt{5}}{2},\\
Q_1 &= \frac{d - P_1^2}{Q_0} = \frac{5 - 1^2}{2} = 2, & a_1 &= [\alpha_1] = \left[\frac{1+\sqrt{5}}{2}\right] = 1,\\
P_2 &= a_1 \cdot Q_1 - P_1 = 1 \cdot 2 - 1 = 1, & \alpha_2 &= \frac{P_2 + \sqrt{d}}{Q_2} = \frac{1+\sqrt{5}}{2},\\
Q_2 &= \frac{d - P_2^2}{Q_1} = \frac{5 - 1^2}{2} = 2, & a_2 &= [\alpha_2] = \left[\frac{1+\sqrt{5}}{2}\right] = 1,\\
P_3 &= a_2 \cdot Q_2 - P_2 = 1 \cdot 2 - 1 = 1, & \alpha_3 &= \frac{P_3 + \sqrt{d}}{Q_3} = \frac{1+\sqrt{5}}{2},\\
Q_3 &= \frac{d - P_3^2}{Q_2} = \frac{5 - 1^2}{2} = 2, & a_3 &= [\alpha_3] = \left[\frac{1+\sqrt{5}}{2}\right] = 1.
\end{aligned}$$

Huomaamme, että $P_1 = P_2$ ja $Q_1 = Q_2$, joten algoritmi alkaa toistaa itseään. Näin ollen

$$\frac{3+\sqrt{5}}{2} = [2; 1, 1, 1, 1, 1, \ldots] = [2; \overline{1}].$$

Todistus. (Vrt. [4, s. 470-471]). Lauseen 4.5 todistus jatkuu. Olkoon α kvadraattinen irrationaaliluku. Silloin sen yksinkertainen ääretön ketjumurtolukuesitys on jaksollinen.

Lauseen 4.6 perusteella voimme kirjoittaa luvun α muodossa

$$\alpha = \frac{P_0 + \sqrt{d}}{Q_0}.$$

Lisäksi lauseen 4.7 perusteella on voimassa yhtälö $\alpha = [a_0; a_1, a_2, \ldots]$, sekä rekursiokaavat

$$\begin{aligned}
\alpha_k &= (P_k + \sqrt{d})/Q_k, \\
a_k &= [\alpha_k], \\
P_{k+1} &= a_k Q_k - P_k, \\
Q_{k+1} &= (d - P_{k+1}^2)/Q_k,
\end{aligned}$$

kun $k = 0, 1, 2, \ldots$.

Tiedämme, että $\alpha = [a_0; a_1, a_2, \ldots]$, joten lauseen 2.3 perusteella voimme kirjoittaa

$$\alpha = \frac{p_{k-1}\alpha_k + p_{k-2}}{q_{k-1}\alpha_k + q_{k-2}}.$$

Kun otamme konjugaatit molemmin puolin yhtälöä ja käytämme lausetta 4.4, saamme yhtälön

$$\alpha' = \frac{p_{k-1}\alpha'_k + p_{k-2}}{q_{k-1}\alpha'_k + q_{k-2}}.$$

Tästä yhtälöstä voimme ratkaista konjugaatin α'_k, jolloin saamme

$$\alpha'_k = \frac{-q_{k-2}}{q_{k-1}} \left(\frac{\alpha' - \dfrac{p_{k-2}}{q_{k-2}}}{\alpha' - \dfrac{p_{k-1}}{q_{k-1}}} \right).$$

Huomaamme, että $p_{k-2}/q_{k-2} \to \alpha$ ja $p_{k-1}/q_{k-1} \to \alpha$, kun $k \to \infty$. Tästä seuraa, että

$$\left(\alpha' \frac{p_{k-2}}{q_{k-2}}\right) / \left(\alpha' - \frac{p_{k-1}}{q_{k-1}}\right) \to 1.$$

Näin ollen on siis olemassa sellainen kokonaisluku N, että $\alpha'_k < 0$, kun $k \geq N$. Koska $\alpha_k > 0$, kun $k > 1$, niin tiedämme, että

$$\alpha_k - \alpha'_k = \frac{P_k + \sqrt{d}}{Q_k} - \frac{P_k - \sqrt{d}}{Q_k} = \frac{2\sqrt{d}}{Q_k} > 0,$$

joten $Q_k > 0$, kun $k \geq N$.

Rekursiokaavojen perusteella tiedämme, että $Q_k Q_{k+1} = d - P_{k+1}^2$, joten kun $k \geq N$, niin on voimassa seuraava epäyhtälö

$$0 < Q_k < Q_k Q_{k+1} = d - P_{k+1}^2 \leq d.$$

Lisäksi tiedämme, että kun $k \geq N$, niin

$$P_{k+1}^2 < d = P_{k+1}^2 + Q_k Q_{k+1},$$

minkä perusteella saamme

$$-\sqrt{d} < P_{k+1} < \sqrt{d}.$$

Ehdoista $0 < Q_k \leq d$ ja $-\sqrt{d} < P_{k+1} < \sqrt{d}$, jotka ovat voimassa kun $k \geq N$ havaitsemme, että on olemassa vain äärellinen määrä mahdollisia arvoja kokonaislukuparille P_k, Q_k, kun $k > N$. Koska kokonaislukuindeksejä k on äärettömän monta (kun $k \geq N$), niin on olemassa sellaiset kokonaislukuindeksit i ja j, että $P_i = P_j$ ja $Q_i = Q_j$, kun $i < j$. Rekursiokaavojen perusteella $\alpha_k = (P_k + \sqrt{d})/Q_k$ joten tästä seuraa, että $\alpha_i = \alpha_j$. Tästä seuraa, että $a_i = a_j, a_{i+1} = a_{j+1}, a_{i+2} = a_{j+2}, \ldots$. Näin ollen siis

$$\begin{aligned}\alpha &= [a_0; a_1, a_2, \ldots, a_{i-1}, a_i, a_{i+1}, \ldots, a_{j-1}, a_i, a_{i+1}, \ldots, a_{j-1}, \ldots] \\ &= [a_0; a_1, a_2, \ldots, a_{i-1}, \overline{a_i, a_{i+1}, \ldots, a_{j-1}}].\end{aligned}$$

Olemme siis osoittaneet, että luvun α yksinkertainen ketjumurtolukuesitys on jaksollinen. □

Huomautus 4.4. Ks. [4, s. 470-471]. Lähdeteoksessa lauseen 12.19 todistuksen jatko-osassa (vrt. tämän tutkielman todistuksen lauseen 4.5 todistuksen jatko-osa) on viitattu teoksen lauseeseen 12.11. Viittauksen pitäisi olla lauseeseen 12.9 (vrt. tämän tutkielman lause 2.3). Lisäksi todistuksen lopussa epäyhtälön $P_{k+1}^2 \leq d = P_{k+1}^2 - Q_k Q_{k+1}$ tilalla pitäisi olla epäyhtälö $P_{k+1}^2 < d = P_{k+1}^2 + Q_k Q_{k+1}$. Vastaavasti epäyhtälön $0 \leq Q_k \leq d$ tilalla pitäisi olla epäyhtälö $0 < Q_k \leq d$.

4.2 Täysin jaksollisten ketjumurtolukujen ominaisuuksia

Tässä pykälässä tutkimme täysin jaksollisia ketjumurtolukuja. Täysin jaksollisilla ketjumurtoluvuilla tarkoitamme ketjumurtolukuja, joilla toistuva jakso alkaa heti ketjumurtolukuesityksen alusta.

Määritelmä 4.3. Yksinkertainen ketjumurtoluku $[a_0; a_1, a_2, \ldots]$ on täysin jaksollinen, jos on olemassa kokonaisluku n siten, että $a_k = a_{n+k}$, kun $k = 0, 1, 2, \ldots$, jolloin siis

$$[a_0, a_1, a_2, \ldots] = [\overline{a_0; a_1, a_2, \ldots, a_{n-1}}].$$

Määritelmä 4.4. Kvadraattista irrationaalilukua α kutsutaan redusoiduksi, jos $\alpha > 1$ ja $-1 < \alpha' < 0$, missä α' on luvun α konjugaatti.

Lause 4.8. *Kvadraattisen irrationaaliluvun α yksinkertainen ketjumurtolukuesitys on täysin jaksollinen, jos ja vain jos α on redusoitu. Edelleen jos α on redusoitu ja $\alpha = [\overline{a_0; a_1, a_2, \ldots, a_n}]$, niin luvun $-1/\alpha$ ketjumurtolukuesitys on $[\overline{a_n; a_{n-1}, \ldots, a_0}]$.*

Todistus. (Vrt. [4, s. 471-473]). Ensin oletamme, että α on kvadraattinen irrationaaliluku. Lauseen 3.3 perusteella tiedämme, että luvun α ketjumurtolukuesityksen termeille on voimassa seuraavaa

$$a_k = [\alpha_k], \qquad \alpha_{k+1} = \frac{1}{\alpha_k - a_k},$$

kun $k = 0, 1, 2, \ldots$ ja $\alpha_0 = \alpha$. Nyt tiedämme, että

$$\frac{1}{\alpha_{k+1}} = \alpha_k - a_k.$$

Käyttämällä hyväksi konjugaatteja, sekä lausetta 4.4, saamme yhtälön

$$\frac{1}{\alpha'_{k+1}} = \alpha'_k - a_k.$$

Todistamme matemaattisen induktion avulla, että $-1 < \alpha'_k < 0$, kun $k = 0, 1, 2, \ldots$. Ensin huomaamme, että koska $\alpha_0 = \alpha$ on redusoitu, niin $-1 < \alpha'_0 < 0$. Seuraavaksi oletamme, että $-1 < \alpha'_k < 0$. Nyt $a_k \geq 1$, kun $k = 0, 1, 2, \ldots$ (huomaa, että $a_0 \geq 1$, koska $\alpha > 1$). Täten

$$\frac{1}{\alpha'_{k+1}} < -1.$$

Näin ollen $-1 < \alpha'_{k+1} < 0$ ja induktioperiaatteen mukaan väite on tosi.

Seuraavaksi havaitsemme, että

$$\alpha'_k = a_k + \frac{1}{\alpha'_{k+1}},$$

ja koska $-1 < \alpha'_k a_0$, tiedämme, että

$$-1 < a_k + 1/\alpha'_{k+1} < 0.$$

Lopulta siis

$$-1 - \frac{1}{\alpha'_k} < a_k < -\frac{1}{\alpha'_k},$$

josta seuraa, että

$$a_k = \left[-\frac{1}{\alpha'_k} \right].$$

Koska α on kvadraattinen irrationaaliluku, tiedämme lauseen 4.5 perusteella, että on olemassa sellaiset ei-negatiiviset kokonaislukuindeksit i ja j, $i < j$, että $\alpha_i = \alpha_j$. Tästä seuraa, että $-1/\alpha'_i = -1/\alpha'_j$. Koska $a_{i-1} = [-1/\alpha'_i]$ ja $a_{j-1} = [-1/\alpha'_j]$, niin $a_{i-1} = a_{j-1}$. Lisäksi koska $\alpha_{i-1} = a_{i-1} + 1/\alpha_i$ ja $\alpha_{j-1} = a_{j-1} + 1/\alpha_j$, tiedämme, että $\alpha_{i-1} = \alpha_{j-1}$. Kun jatkamme tätä päättelyä, havaitsemme, että $\alpha_{i-2} = \alpha_{j-2}$, $\alpha_{i-3} = \alpha_{j-3}$ ja lopulta, että $\alpha_0 = \alpha_{j-i}$. Koska

$$\begin{aligned} \alpha_0 = \alpha &= [a_0; a_1, \ldots, a_{j-i-1}, \alpha_{j-i}] \\ &= [a_0; a_1, \ldots, a_{j-i-1}, \alpha_0] \\ &= [\overline{a_0; a_1, \ldots, a_{j-i-1}}], \end{aligned}$$

niin näemme, että luvun α yksinkertainen ääretön ketjumurtolukuesitys on täysin jaksollinen.

Jotta saamme todistettua toisen suunnnan, oletamme, että α on kvadraatttinen irrationaaliluku ja sen ketjumurtolukuesitys $\alpha = [\overline{a_0; a_1, a_2, \ldots, a_k}]$ on täysin jaksollinen. Voimme merkitä myös, että $\alpha = [a_0;_1, a_2, \ldots, a_k, \alpha]$. Lauseen 2.3 perusteella tiedämme, että

$$\alpha = \frac{\alpha p_k + p_{k-1}}{\alpha q_k + q_{k-1}},$$

missä p_{k-1}/q_{k-1} ja p_k/q_k ovat luvun α ketjumurtolukuesityksen $(k-1)$. ja k. konvergentti. Edellä mainitusta yhtälöstä seuraa, että

$$q_k\alpha^2 + (q_{k-1} - p_k)\alpha - p_{k-1} = 0.$$

Olkoon β sellainen kvadraattinen irrationaaliluku, että $\beta = [\overline{a_k; a_{k-1}, \ldots, a_1, a_0}, \beta]$. Tällöin luvun β ketjumurtolukuesityksen termit ovat luvun α ketjumurtolukuesityksen termit käänteisessä järjestyksessä. Merkitsemme, että $\beta = [a_k; a_{k-1}, \ldots, a_1, a_0, \beta]$. Lauseen 2.3 todistuksen avulla saamme, että

$$\beta = \frac{\beta p'_k + p'_{k-1}}{\beta q'_k + q'_{k-1}},$$

missä p'_{k-1}/q'_{k-1} ja p'_k/q'_k ovat luvun β ketumurtolukusityksen $(k-1)$. ja k. konvergentti. Tiedämme, että

$$\frac{p_k}{p_{k-1}} = [a_k; a_{k-1}, \ldots, a_1, a_0] = \frac{p'_k}{q'_k}$$

ja

$$\frac{q_k}{q_{k-1}} = [a_k; a_{k-1}, \ldots, a_2, a_1] = \frac{p'_{k-1}}{q'_{k-1}}.$$

Koska p'_{k-1}/q'_{k-1} ja p'_k/q'_k ovat konvergentteja, ne ovat supistetussa muodossa. Lauseen 2.4 perusteella tiedämme, että $p_k q_{k-1} - p_{k-1} q_k = (-1)^{k-1}$. Jos $d = (p_{k-1}, p_k)$ niin $d|(-1^{k-1}$. Samoin, jos $d = (q_{k-1}, q_k)$, niin $d|(-1)^{k-1}$. Kummassakin tapauksessa $d = 1$. Tällöin siis luvut p_{k-1} ja p_k ovat keskenään jaottomia, samoin kuin luvut q_{k-1} ja q_k. Siis myös luvut p_k/p_{k-1} ja q_k/q_{k-1} ovat supistetussa muodossa. Näin ollen on voimassa, että

$$p'_k = p_k, \qquad q'_k = p_{k-1}$$

ja

$$p'_{k-1} = q_k, \qquad q'_{k-1} = q_{k-1}.$$

Kun sijoitamme nämä arvot yhtälöön

$$\beta = \frac{\beta p'_k + p'_{k-1}}{\beta q'_k + q'_{k-1}},$$

saamme

$$\beta = \frac{\beta p_k + q_k}{\beta p_{k-1} + q_{k-1}}.$$

Tämän johdosta tiedämme, että

$$p_{k-1}\beta^2 + (q_{k-1} - p_k)\beta - q_k = 0.$$

Kun jaamme yhtälön puolittain luvulla $-\beta^2$, saamme

$$q_k(-1/\beta)^2 + (q_{k-1} - p_k)(-1/\beta) - p_{k-1} = 0.$$

Näiden yhtälöiden perusteella havaitsemme, että toisen asteen yhtälön

$$q_k x^2 + (q_{k-1} - p_k)x - p_{k-1} = 0$$

kaksi juurta ovat luvut α ja $-1/\beta$. Lauseen 4.3 perusteella tiedämme, että $\alpha' = -1/\beta$. Koska $\beta = [\overline{a_n; a_{n-1}, \ldots, a_1, a_0}]$, niin huomaamme, että $\beta > 1$, joten $-1/\alpha' = -1/\beta < 0$. Näin ollen α on redusoitu kvadraattinen irrationaaliluku. Lisäksi koska $\beta = -1/\alpha'$ niin

$$-1/\alpha' = [\overline{a_n; a_{n-1}, \ldots, a_1, a_0}].$$

□

Huomautus 4.5. Ks. [4, s. 471-473]. Lähdeteoksessa lauseen 12.21 todistuksessa (vrt. tämän tutkielman lauseen 4.8 todistus) on alussa viitattu lauseeseen 12.17. Viittauksen pitäisi olla lauseeseen 12.15 (vrt. tämän tutkielman lause 3.3). Lisäksi yhtälön $\alpha_0 = \alpha_{j-1}$ tilalla tulisi olla yhtälö $\alpha_0 = \alpha_{j-i}$. Samoin yhtälön $\alpha_0 = \alpha = [a_0; a_1, \ldots, a_{j-i-1}, \alpha_{j-1}]$ tilalla tulisi olla yhtälö $\alpha_0 = \alpha = [a_0; a_1, \ldots, a_{j-i-1}, \alpha_{j-i}]$. Lauseen 12.21 todistuksessa on viitattu kaksi kertaa lauseeseen 12.11. Viittausten tulisi olla lähdeteoksen lauseeseen 12.9 (vrt. tämän tutkielman lause 2.3). Lisäksi viittauksen 12.12 tulisi olla lauseen 12.10 (vrt. tämän tutkielman lause 2.4).

Seuraavaksi tutkimme luvun $\sqrt{D}$ yksinkertaista jaksollista ketjumurtolukuesitystä. Oletamme, että D on positiivinen kokonaisluku eikä se lisäkso ole täydellinen neliö. Luku $\sqrt{D}$ ei ole redusoitu, koska sen konjugaatille $-\sqrt{D}$ ei ole voimassa $-1 < -\sqrt{D} < 0$. Kvadraattinen irrationaaliluku $[\sqrt{D}] + \sqrt{D}$ vastaavasti on redusoitu, koska sen konjugaatille $[\sqrt{D}] - \sqrt{D}$ on voimassa $-1 < [\sqrt{D}] - \sqrt{D} < 0$. Lauseen 4.8 perusteella tiedämme nyt, että luvulla $[\sqrt{D}] + \sqrt{D}$ on täysin jaksollinen ketjumurtolukuesitys. Tiedämme, että tämän ketjumurtolukuesityksen ensimmäinen termi on $[[\sqrt{D}] + \sqrt{D}] = 2[\sqrt{D}] = 2a_0$, missä $a_0 = [\sqrt{D}]$, joten voimme kirjoittaa

$$
\begin{aligned}
[\sqrt{D}] + \sqrt{D} &= [\overline{2a_0; a_1, a_2, \ldots, a_n}] \\
&= [2a_0; a_1, a_2, \ldots, a_n, 2a_0, a_1, \ldots, a_n].
\end{aligned}
$$

Kun vähennämme yhtälön molemmilta puolilta luvun $a_0 = [\sqrt{D}]$, saamme

$$
\begin{aligned}
\sqrt{D} &= [a_0; a_1, a_2, \ldots, 2a_0, a_1, a_2, \ldots, 2a_0, \ldots] \\
&= [a_0; \overline{a_1, a_2, \ldots, a_n, 2a_0}].
\end{aligned}
$$

Tutkimme vielä hieman luvun $\sqrt{D}$ ketjumurtolukuesityksen osanimittäjiä $a_1, a_2, \ldots, a_n$. Lauseen 4.8 perusteella tiedämme, että luvun $-1/([\sqrt{D}] - \sqrt{D})$ ketjumurtolukuesitys saadaan luvun $[\sqrt{D}] + \sqrt{D}$ ketjumurtolukuesityksestä kääntämällä termit päinvastaiseen järjestykseen. Tällöin siis

$$
-1/([\sqrt{D}] - \sqrt{D}) = 1/(\sqrt{D} - [\sqrt{D}] = [\overline{a_n; a_{n-1}, \ldots, a_1, 2a_0}].
$$

Toisaalta tiedämme, että

$$
\begin{aligned}
\sqrt{D} + [\sqrt{D}] &= a_0 + \frac{1}{[a_1; a_2, \ldots, a_n, 2a_0, a_1, \ldots, a_n, 2a_0, \ldots]} - a_0 \\
&= 0 + \frac{1}{[a_1; a_2, \ldots, a_n, 2a_0, a_1, \ldots, a_n, 2a_0, \ldots]} \\
&= [0; \overline{a_1, a_2, \ldots, a_n, 2a_0}].
\end{aligned}
$$

Tällöin tiedämme, että luvun $\sqrt{D} - [\sqrt{D}]$ käänteisluvulle $1/(\sqrt{D} - [\sqrt{D}]$ pätee

$$
1/(\sqrt{D} - [\sqrt{D}] = [\overline{a_1, a_2, \ldots, a_n, 2a_0}].
$$

Kun vertailemme näitä kahta luvun $1/(\sqrt{D} - [\sqrt{D}]$ ketjumurtolukuesitystä, huomaamme, että

$$
a_1 = a_n, a_2 = a_{n-1}, \ldots, a_n = a_1,
$$

joten luvun $\sqrt{D}$ ketjumurtoluesityksen jakso on symmetrinen ensimmäisestä termistä toiseksi viimeiseen termiin saakka. Lopulta saamme luvun $\sqrt{D}$ ketjumurtolukuesityksen muotoon

$$
\sqrt{D} = [a_0; \overline{a_1, a_2, \ldots, a_2, a_2, 2a_0}]
$$

Voimme muodostaa luvun $\sqrt{D}$ ketjumurtolukuesityksen lauseen 3.3 rekursioyhtälöiden avulla. Ketjumurtolukuesityksiä löytyy myös valmiiksi taulukoituna kirjallisuudesta (ks. esim. [4, s. 552, taulukko E.5]).

Esimerkki 4.3. Lukujen $\sqrt{43}$ ja $\sqrt{65}$ ketjumurtolukuesitykset ovat

$$\sqrt{43} = [6; \overline{1, 1, 3, 1, 5, 1, 3, 1, 1, 12}]$$

ja

$$\sqrt{65} = [8; \overline{16}].$$

Ensimmäisen esityksen jakson pituus on 10. Jakson alkuosa on symmetrinen ensimmäisestä termistä toiseksi viimeiseen termiin saakka. Jakson viimeinen termi on kaksinkertainen esityksen ensimmäiseen termiin verrattuna. Toisen esityksen jakson pituus on 1, mutta tässä tapauksessa jakson symmetrinen alkuosa puuttuu. Tässäkin tapauksessa jakson viimeinen termi (ja myös ainoa) on kaksinkertainen esityksen ensimmäiseen termiin verrattuna. (Ks. [4, s. 552, taulukko E.5]).

5 Pellin yhtälö

Tässä luvussa tarkastelemme Diofantoksen yhtälöä, joka on muotoa $x^2 - dy^2 = n$, missä luvut d ja n ovat kokonaislukuja. Kun $d < 0$ ja $n < 0$, niin yhtälölle ei ole ratkaisua. Kun $d < 0$ ja $n > 0$, niin yhtälöllä voi olla korkeintaan äärellinen määrä ratkaisuita, koska yhtälöstä $x^2 - dy^2 = n$ seuraa, että $|x| \leq \sqrt{n}$ ja $|y| \leq \sqrt{n/|d|}$. Lisäksi huomaamme, että kun luku d on täydellinen neliö ($d = D^2$), niin silloin

$$x^2 - dy^2 = x^2 - D^2y^2 = n.$$

Näin ollen, kun d on täydellinen neliö, niin jokainen yhtälön ratkaisu vastaa samanaikaisesti ratkaisua seuraaviin yhtälöihin

$$x + Dy = a$$

ja

$$x - Dy = b,$$

missä a ja b ovat kokonaislukuja siten, että $ab = n$. Tässä tapauksessa on olemassa vain äärellinen määrä ratkaisuja, ja ratkaisut löytyvät luvun n tekijöistä. Näin ollen olemme tässä luvussa kiinnostuneita yhtälöstä $x^2 - dy^2 = n$, missä d ja n ovat kokonaislukuja, ja lisäksi d on positiivinen, eikä se ole täydellinen neliö. Yhtälön $x^2 - dy^2 = n$ erityistapausta, kun $n = 1$, kutsutaan Pellin yhtälöksi John Pellin mukaan. Vaikka yhtälön on nimetty hänen mukaansa ja hän olikin aikansa suuria matemaatikkoja, hän näytteli hyvin pientä osaa yhtälön $x^2 - dy^2 = 1$ ratkaisuita etsittäessä.

Seuraavaksi esittelemme lauseen, joka osoittaa, että luvun $\sqrt{d}$ yksinkertainen ketjumurtolukuesitys on hyvin hyödyllinen kyseistä yhtälöä käsiteltäessä.

Lause 5.1. *Olkoot d ja n kokonaislukuja. Lisäksi olkoot voimassa seuraavat ehdot, $d > 0$, d ei ole täydellinen neliö ja $|n| < \sqrt{d}$. Jos $x^2 - dy^2 = n$, niin silloin x/y on luvun $\sqrt{d}$ yksinkertaisen ketjumurtolukuesityksen konvergentti.*

Todistus. (Vrt. [4, s. 506-507]). Tarkastelemme ensin tapausta, kun $n > 0$. Koska $x^2 - dy^2 = n$, niin tiedämme, että

$$(x + y\sqrt{d})(x - y\sqrt{d}) = n.$$

Tästä yhtälöstä näemme, että $x - y\sqrt{d} > 0$, joten $x > y\sqrt{d}$. Tästä johtuen tiedämme, että

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

Koska $0 < n < \sqrt{d}$, niin huomaamme, että

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

Nyt tiedämme, että $0 < \dfrac{x}{y} - \sqrt{d} < \dfrac{1}{2y^2}$, joten lauseen 3.6 perusteella tiedämme, että luvun x/y on oltava luvun $\sqrt{d}$ yksinkertaisen ketjumurtolukuesityksen konvergentti.

Olkoon sitten $n < 0$. Kun jaamme yhtälön $x^2 - dy^2 = n$ molemmat puolet luvulla $-d$, saamme

$$y^2 - (1/d)x^2 = -n/d.$$

Voimme nyt tarkastella tilannetta samanlaisella argumentoinnilla kuin tilannetta $n > 0$. Silloin luku y/x on luvun $1/\sqrt{d}$ yksinkertaisen ketjumurtolukuesityksen konvergentti. Näin ollen tiedämme että $x/y = 1/(x/y)$ on oltava yksinkertaisen ketjumurtolukuesityksen $\sqrt{d} = 1/(1/\sqrt{d})$ konvergentti. □

Olemme osoittaneet, että yhtälön $x^2 - dy^2 = n$ ratkaisut ovat luvun $\sqrt{d}$ yksinkertaisen ketjumnurtolukuesityksen konvergentteja. Esitämme seuraavaksi uudelleen lauseen 4.7, koska se on hyödyllinen apu siihen, kuinka näitä konvergentteja käytetään yhtälön $x^2 - dy^2 = n$ ratkaisuiden löytämiseksi.

Lause 5.2. *Olkoon d positiivinen kokonaisluku, joka ei ole täydellinen neliö. Määrittelemme, että*

$$\begin{aligned}
\alpha_k &= (P_k + \sqrt{d})/Q_k, \\
a_k &= [\alpha_k], \\
P_{k+1} &= a_k Q_k - P_k, \\
Q_{k+1} &= (d - P_{k+1}^2)/Q_k,
\end{aligned}$$

kun $k = 0, 1, 2, \ldots$. Olkoon p_k/q_k on luvun $\sqrt{d}$ yksinkertaisen kaetjumurtolukuesityksen k. konvergentti. Tällöin on voimassa seuraava yhtälö

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

Määritelmä 5.1. Pellin yhtälön perusratkaisulla tarkoitetaan yhtälön $x^2 - dy^2 = 1$ pienintä positiivista ratkaisua, eli sellaista ratkaisua x_0, y_0, jolle on voimassa $x_0 < x'$ ja $y_0 < y'$, kaikilla muilla positiivisillla ratkaisuilla x', y'.

Lause 5.3. *Olkoon d positiivinen kokonaisluku, joka ei ole täydellinen neliö. Olkoon p_k/q_k luvun $\sqrt{d}$ yksinkertaisen ketjumurtoluvun k. konvergentti, kun $k = 1,2,3,\ldots$. Olkoon lisäksi n tämän ketjumurtoluvun jakson pituus. Tällöin kun n on parillinen, yhtälön $x^2 - dy^2 = 1$ ratkaisut ovat $x = p_{jn-1}$ ja $y = q_{jn-1}$, kun $j = 1,2,3,\ldots$. Lisäksi kun n on parillinen, yhtälöllä $x^2 - dy^2 = -1$ ei ole ratkaisua. Kun n on pariton, yhtälön $x^2 - dy^2 = 1$ ratkaisut ovat $x = p_{2jn-1}$ ja $y = q_{2jn-2}$, kun $j = 1,2,3,\ldots$. Lisäksi kun n on pariton, yhtälön $x^2 - dy^2 = -1$ ratkaisut ovat muotoa $x = p_{(2j-1)n-1}$ ja $y = q_{(2j-1)n-1}$, kun $j = 1,2,3,\ldots$.*

Todistus. (Vrt. [4, s. 508-509]). Lauseen 5.1 mukaan tiedämme, että jos x_0, y_0 on yhtälön $x^2 - dy^2 = \pm 1$ positiivinen ratkaisu, niin silloin $x_0 = p_k$ ja $y_0 = q_k$, missä p_k/q_k on luvun $\sqrt{d}$ yksinkertaisen ketjumurtolukuesityksen konvergentti. Toisaalta lauseen 5.2 perusteella tiedämme, että

$$p_k^2 - dq_k^2 = (-1)^{k-1} Q_{k+1},$$

missä Q_{k+1} on määritelty kuten lauseessa 5.2.

Tiedämme, että luvun $\sqrt{d}$ yksinkertaisen ketjumurtolukuesityksen jakson pitus on n, joten tästä seuraa, että $Q_{jn} = Q_0 = 1$, kun $j = 1,2,3,\ldots$, koska $\sqrt{d} = \dfrac{P_0 + \sqrt{d}}{Q_0}$. Tällöin

$$p_{jn-1}^2 - dq_{jn-1}^2 = (-1)^{jn} Q_{nj} = (-1)^{jn}.$$

Tästä yhtälöstä seuraa, että kun n on parillinen, niin p_{jn-1}, q_{jn-1} on yhtälön $x^2 - dy^2 = 1$ ratkaisu, kun $j = 1,2,3,\ldots$. Siinä tapauksessa, että n on pariton, niin p_{2jn-1}, q_{2jn-1} on yhtälön $x^2 - dy^2 = 1$ ratkaisu. Lisäksi $p_{2(j-1)n-1}, q_{2(j-1)n-1}$ on yhtälön $x^2 - dy^2 = -1$ ratkaisu, kun $j = 1,2,3,\ldots$.

Jotta saamme osoitettua, että yhtälöillä $x^2 - dy^2 = 1$ ja $x^2 - dy^2 = -1$ ei ole muita ratkaisuja kuin edellä esitetyt, meidän on osoitettava, että jos $Q_{k+1} = 1$, niin siitä seuraa, että $n|k$ ja lisäksi on osoitettava, että $Q_j \neq -1$ kun $j = 1,2,3,\ldots$.Ensin huomaamme, että jos $Q_{k+1} = 1$, niin

$$\alpha_{k+1} = P_{k+1} + \sqrt{d}.$$

Koska $\alpha_{k+1} = [a_{k+1}; a_{k+2}, \ldots]$, niin luvun α_{k+1} ketjumurtolukuesitys on täysin jaksollinen. Näin ollen tiedämme, että $-1 < \alpha_{k+1} = P_{k+1} - \sqrt{d} < 0$. Tästä seuraa, että $P_{k+1} = [\sqrt{d}]$ joten $\alpha_k = \alpha_0$ ja $n|k$.

Seuraavaksi osoitamme, että $Q_j \neq -1$, kun $j = 1,2,3,\ldots$. Ensin huomaamme, että jos $Q_j = 1$ niin siitä seuraa $\alpha_j = -P_j - \sqrt{d}$. Koska luvulla α_j on täysin jaksollinen yksinkertainen ketjumurtolukuesitys, niin huomaamme, että

$$-1 < \alpha_j' = -P_j + \sqrt{d} < 0$$

ja

$$\alpha_j = -P_j - \sqrt{d} > 1.$$

Ensimmäisestä epäyhtälöstä huomaamme, että $P_j > -\sqrt{d}$, ja toisesta huomaamme, että $P_j < -1 - \sqrt{d}$. Nämä kaksi epäyhtälöä ovat ristiriidassa keskenään, joten saamme, että $Q_j \neq -1$.

Näin ollen olemme siis löytäneet kaikki ratkaisut yhtälöille $x^2 - dy^2 = 1$ ja $x^2 - dy^2 = -1$, missä x ja y ovat kokonaislukuja, joten todistus on valmis. □

Esimerkki 5.1. Tarkastelemme Pellin yhtälöä $x^2 - 23y^2 = 1$. Luvun $\sqrt{23}$ ketjumurtolukuesitys on $[4; \overline{1,3,1,8}]$. Esityksen jakson pituus on 4, joten yhtälön positiiviset ratkaisut ovat lauseen 5.3 perusteella muotoa $x = p_{4k-1}, y = q_{4k-1}$, kun $k = 1,2,3,\ldots$. Pienin positiivinen ratkaisu (jota kutsutaan myös perusratkaisuksi) on $x_1 = p_3, y_1 = q_3$. Lauseessa 2.3 esitettyjen rekursioyhtälöiden perusteella saamme, että $p_3 = 24$ ja $q_3 = 5$, joten perusratkaisu on $x_1 = 24$ ja $y_1 = 5$.

Esimerkki 5.2. Tarkastelemme Pellin yhtälöä $x^2 - 65y^2 = 1$. Luvun $\sqrt{65}$ ketjumurtolukuesitys on $[8; \overline{16}]$. Esityksen jakson pituus on 1, joten yhtälön positiiviset ratkaisut ovat lauseen 5.3 perusteella muotoa $x = p_{2k-1}, y = q_{2k-1}$, kun $k = 1,2,3,\ldots$. Pienin positiivinen ratkaisu (jota kutsutaan myös perusratkaisuksi) on $x_1 = p_1, y_1 = q_1$. Lauseessa 2.3 esitettyjen rekursioyhtälöiden perusteella saamme, että $p_1 = 129$ ja $q_1 = 8$, joten perusratkaisu on $x_1 = 129$ ja $y_1 = 8$.

Viimeisenä esittelemme vielä, kuinka Pellin yhtälön $x^2 - dy^2 = 1$ kaikki positiiviset ratkaisut muodostetaan.

Lause 5.4. *Olkoon x_1, y_1 Pellin yhtälön $x^2 - dy^2 = 1$ perusratkaisu (d on positiivinen kokonaisluku, joka ei ole täydelinen neliö). Tällöin kaikki positiiviset ratkaisut x_k, y_k saadaan yhtälöllä*

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

kun $k = 1,2,3,\ldots$.

Todistus. (Vrt. [4, s. 510-511]). Meidän on osoitettava, että x_k, y_k on ratkaisu, kun $k = 1,2,3,\ldots$ Lisäksi on osoitettava, että jokainen ratkaisua on muotoa x_k, y_k jollakin luvun k positiivisella kokonaislukuarvolla.

Ensin osoitamme, että x_k, y_k on ratkaisu. Huomaamme, että kun otamme konjugaatit, saamme $x_k - y_k\sqrt{d} = (x_1 - y_1\sqrt{d})^k$, koska lauseeen 4.3 perusteella tiedämme, että potenssin konjugaatti on konjugaatin potenssi. Todellakin

$$[(x_1 + y_1\sqrt{d})^k]' = [(x_1 + y_1\sqrt{d})']^k = (x_1 - y_1\sqrt{d})^k.$$

Tästä saamme, että

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

Näin ollen saamme, että

$$\begin{aligned} x_k^2 - dy_k^2 &= (x_k + y_k\sqrt{d})(x_k - y_k\sqrt{d}) \\ &= (x_1 + y_1\sqrt{d})^k(x_1 - y_1\sqrt{d})^k \\ &= (x_1^2 - dy_1^2)^k \\ &= 1^k = 1. \end{aligned}$$

Tämän perusteella x_k, y_k on ratkaisu, kun $k = 1,2,3,\ldots$.

Seuraavaksi osoitamme, että jokainen positiivinen ratkaisu on muotoa x_k, y_k jollakin $k = 1,2,3,\ldots$. Teemme vastaoletuksen, että X, Y on positiivinen ratkaisu, joka ei ole muotoa x_k, y_k. On olemassa sellainen kokonaisluku n, että

$$(x_1 + y_1\sqrt{d})^n < X + Y\sqrt{d} < (x_1 + y_1\sqrt{d})^{n+1}.$$

Voimme kertoa tämän epäyhtälön puolittain luvulla $(x_1+y_1\sqrt{d})^{-n}$. Koska $x_1^2-dy_1^2 = 1$, ja siitä seuraa, että $x_1 - y_1\sqrt{d} = (x_1 + y_1\sqrt{d})^{-1}$, niin saamme

$$1 < (x_1 - y_1\sqrt{d})^{-n}(X + Y\sqrt{d}) < x_1 + y_1\sqrt{d},$$

Olkoon sitten

$$s + t\sqrt{d} = (x_1 - y_1\sqrt{d})^n(X + Y\sqrt{d}).$$

Huomaamme, että

$$\begin{aligned} s^2 - dt^2 &= (s - t\sqrt{d})(s + t\sqrt{d}) \\ &= (x_1 + y_1\sqrt{d})^n(X - Y\sqrt{d})(x_1 - y_1\sqrt{d})^n(X + Y\sqrt{d}) \\ &= (x_1^2 - dy_1^2)^n(X^2 - dY^2) \\ &= 1. \end{aligned}$$

Nyt huomaamme, että s,t on yhtälön $x^2 - dy^2 = 1$ ratkaisu ja lisäksi tiedämme, että $1 < s + t\sqrt{d} < x_1 + y_1\sqrt{d}$. Tiedämme, että $s + t\sqrt{d} > 1$, joten $0 < (s + t\sqrt{d})^{-1} = s - t\sqrt{d} < 1$. Näin ollen

$$s = \frac{1}{2}\left[(s + t\sqrt{d}) + (s - t\sqrt{d})\right] > 0$$

ja

$$t = \frac{1}{2\sqrt{d}}\left[(s + t\sqrt{d}) - (s - t\sqrt{d}\right] > 0.$$

Tämä tarkoittaa, että s,t on positiivinen ratkaisu. Tämä puolestaan tarkoittaa, että $s \geq x_1$ ja $t \geq y_1$, koska x_1, y_1 on pienin positiivinen kokonaisratkaisu. Tämä on ristiriidassa epäyhtälön $s + t\sqrt{d} < x_1 + y_1\sqrt{d}$ kanssa. Näin ollen siis ratkaisun X, Y täytyy olla muotoa x_k, y_k, jollakin $k = 1,2,3\ldots$. □

Esimerkki 5.3. Tarkastelemme Pellin yhtälöä $x^2 - 26y^2 = 1$. Luvun $\sqrt{26}$ ketjumurtolukuesitykseksi saadaan $[5; \overline{10}]$. Näin ollen pienin positiivinen ratkaisu on

$x_1 = 51, y_1 = 10$. Lauseen 5.4 perusteella saamme kaksi muuta positiivista ratkaisua. Nyt siis

$$\begin{aligned} x_2 + y_2\sqrt{26} &= (51 + 10\sqrt{26})^2 \\ &= 5201 + 1020\sqrt{26}, \end{aligned}$$

jolloin $x_1 = 5201, y_1 = 1020$.Vastaavalla tavalla saamme

$$\begin{aligned} x_3 + y_3\sqrt{26} &= (51 + 10\sqrt{26})^3 \\ &= 530451 + 104030\sqrt{26}, \end{aligned}$$

jolloin $x_1 = 530451, y_1 = 104030$.

Lähteet

[1] Burton, David M. *Elementary Number Theory*. WCB/McGraw-Hill, third edition, 1997.

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

[3] Long, Calvin T. *Elementary Introduction to Number Theory*. Waveland press, third edition, 1995.

[4] Rosen, Kenneth H. *Elementary Number Theory and Its Applicatons*. Addison Wesley Longman, fourth edition, 2000.