TAMPEREEN YLIOPISTO
Pro gradu-tutkielma

Ville Helenius

Katsaus ketjumurtolukuihin

Matematiikan, tilastotieteen ja filosofian laitos
Matematiikka
Huhtikuu 2000

Sisällysluettelo

Johdanto

Tämän Pro gradu-tutkielman tarkoitus on luoda katsaus ketjumurtolukujen ominaisuuksiin. Tarkastelu rajoittuu lähinnä yksinkertaisiin ketjumurtolukuihin. Lukijan odotetaan hallitsevan analyysin ja lukuteorian peruskäsitteet ja -tulokset. Analyysin osalta odotetaan erityisesti lukujonojen suppenemiseen liittyvät tulokset tunnetuiksi. Lukuteorian osalta riittää peruskäsitteiden tunteminen.

Luvussa 1 esitetään suurin osa määritelmistä ja merkinnöistä. Lisäksi tutustutaan ketjumurtolukujen perusominaisuuksiin sekä luodaan katsaus neliökuntiin.

Luvussa 2 tutustutaan reaalilukujen ja yksinkertaisten ketjumurtolukujen väliseen relaatioon. Lisäksi esitetään menetelmä, jolla reaalilukuja esitetään ketjumurtolukuina. Luku 2 myötäilee kirjojen [2] ja [4] esitystä.

Luvussa 3 tutustutaan kvadraattisten irrationaalilukujen ja jaksollisten ketjumurtolukujen väliseen relaatioon. Erityistä huomiota kiinnitetään luvun $\sqrt{N}$ ketjumurtolukukehitelmään, koska sillä on keskeinen sija lukuteoriassa. Luku 3 myötäilee kirjojen [2] ja [4] esitystapaa pykälän 1 osalta. Pykälän 2 osalta kirja [5] on ollut keskeisellä sijalla.

Luvussa 4 käsitellään irrationaalilukujen approksimointia. Erityisesti tutkitaan ketjumurtolukujen konvergenttien asemaa irrationaalilukujen approksimaationa. Lukuteoriassa sama asia tunnetaan Diofantoksen approksimaatioina. Luku 4 noudattaa kirjaa [1].

Luvussa 5 käsitellään ketjumurtolukujen teorian tunnetuinta sovellusta eli ketjumurtolukujen käyttöä ratkaistaessa Pellin yhtälöä. Luku 5 noudattaa kirjojen [3] ja [5] esitystä.

Seuraavaksi kerron hiukan ketjumurtolukujen historiasta ja merkityksestä matematiikkaan.

1600-luvulla elänyt matemaatikko John Wallis (1620-1684) oli ensimmäinen, joka tutki yleisesti ketjumurtolukujen teoriaa. Aiemmin ketjumurtolukuja oli käytetty vain joissakin erikoistapauksissa. John Wallis esitti esimerkiksi ketjumurtolukujen konvergenttien laskemismenetelmän sekä esitti joitakin nykyään tunnettuja perustuloksia.

1700-luvulla Leonard Euler (1707-1783) ja Joseph Louis Lagrange (1736-1813) kehittivät lisää ketjumurtolukujen teoriaa. Euler esitti muun muassa Neperin luvun e ketjumurtolukukehitelmän. Lagrange taas osoitti kvadraattisten irrationaalilukujen ja jaksollisten ketjumurtolukujen välisen relaation.

1800-luvulla ketjumurtolukujen teoriaa kehitettiin kaikkein vahvimmin. Esimerkiksi siirryttiin tutkimaan ketjumurtolukuja, joiden termit ovat kompleksilukuja. Tunnetuimpia matemaatikkoja, jotka kehittivät ketjumurtolukujen teoriaa olivat Jacobi, Perron, Hermite, Gauss, Cauchy sekä Stieljes. Erityisesti Oscar Perron tunnetaan erinomaisesta ketjumurtolukujen teoriaa käsittelevästä oppikirjasta *Die lehre von den Kettenbrüchen*.

Ketjumurtoluvuilla on tärkeä asema erityisesti lukuteoriassa, koska ketjumurtoluvut ovat tehokas työkalu moneen lukuteorian ongelman ratkaisuun. Esimerkiksi lukujen tekijöihin jaossa voi ketjumurtoluvuista olla apua. Tässä tutkielmassa ei käsitellä kuitenkaan tätä ongelmaa, koska ketjumurtolukuihin perustuvaa determinististä algoritmia ei tunneta. Ketjumurtolukuja käytetään myös muissa matematiikan osa-alueissa.

Luku 1. Perustuloksia

§ 1.1. Määritelmiä ja merkintöjä

Määritelmä 1.1.1. Päättyvällä ketjumurtoluvulla tarkoitetaan lauseketta

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

missä luvut $a_1, a_2, \ldots, a_n \in \mathbf{R}_+$ ja luku $a_0 \in \mathbf{R}$. Lausekkeelle (1) käytetään merkintää

$$[a_0, a_1, \ldots, a_n]. \tag{2}$$

Kyseisen ketjumurtoluvun *indeksijoukolla* I tarkoitetaan tällöin joukkoa $\{0, 1, \ldots, n\}$.

Määritelmä 1.1.2. Päättymättömällä ketjumurtoluvulla tarkoitetaan lauseketta

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots}}}}, \tag{3}$$

missä luvut $a_1, a_2, a_3, \ldots \in \mathbf{R}_+$ ja luku $a_0 \in \mathbf{R}$. Lausekkeelle (3) käytetään merkintää

$$[a_0, a_1, a_2, \ldots]. \tag{4}$$

Kyseisen ketjumurtoluvun *indeksijoukolla* I tarkoitetaan tällöin joukkoa $\{0, 1, 2, \ldots\}$.

Määritelmä 1.1.3. Lukuja $a_1, a_2, a_3, \ldots$ sanotaan ketjumurtoluvun *osanimittäjiksi*. Mikäli $a_0 \in \mathbf{Z}$ ja osanimittäjät ovat positiivisia kokonaislukuja, niin ketjumurtolukua sanotaan *yksinkertaiseksi*.

Määritelmä 1.1.4. Päättymätöntä ketjumurtolukua sanotaan *jaksolliseksi*, mikäli on olemassa sellaiset luvut $N \in \mathbf{N}$ ja $k \in \mathbf{Z}_+$, että aina kun $n \geq N$, niin $a_n = a_{n+k}$. Ketjumurtoluvulle $[a_0, a_1, \ldots, a_N, a_{N+1}, \ldots, a_{N+k-1}, a_N, a_{N+1}, \ldots]$ otetaan käyttöön merkintä

$$[a_0, a_1, \ldots, a_{N-1}, \overline{a_N, a_{N+1}, \ldots, a_{N+k-1}}]. \tag{5}$$

Määritelmä 1.1.5. Ketjumurtolukua $[\overline{a_0, a_1, \ldots, a_k}]$ sanotaan *täysin jaksolliseksi ketjumurtoluvuksi*.

Määritelmä 1.1.6. Olkoon ketjumurtoluvun indeksijoukko I ja olkoon $k \in I$. Silloin *astetta* k olevalla ketjumurtoluvun *konvergentilla* tarkoitetaan ketjumurtoluvun osaa $[a_0, a_1, \ldots, a_k]$. Kyseiselle konvergentille otetaan käyttöön merkintä c_k.

Määritelmä 1.1.7. Olkoon $x \in \mathbf{R}$. Määritellään rekursioyhtälöt

$$\varepsilon_0 = x,\ a_0 = \lfloor \varepsilon_0 \rfloor,\ \varepsilon_k = \frac{1}{\varepsilon_{k-1} - a_{k-1}},\ a_k = \lfloor \varepsilon_k \rfloor. \tag{1}$$

Määritelmä 1.1.8. Olkoon $a_0 \in \mathbf{R}$ ja olkoot $a_1, a_2, \ldots \in \mathbf{R}_+$. Määritellään tällöin rekursioyhtälöt

$$\begin{aligned} p_{-2} &= 0,\ p_{-1} = 1, \\ q_{-2} &= 1,\ q_{-1} = 0, \\ p_k &= a_k p_{k-1} + p_{k-2}, \\ q_k &= a_k q_{k-1} + q_{k-2} \quad (k = 0, 1, 2, ...). \end{aligned} \tag{2}$$

Määritelmä 1.1.9. Olkoon $N \in \mathbf{Z}_+$, joka ei ole täydellinen neliö. Määritellään tällöin rekursioyhtälöt

$$
\begin{aligned}
C_{-2} &= N,\ C_{-1} = 1,\ B_{-1} = 0, \\
A_k &= \left\lfloor \frac{\sqrt{N} + B_{k-1}}{C_{k-1}} \right\rfloor, \\
B_k &= A_k C_{k-1} - B_{k-1}, \\
C_k &= C_{k-2} + A_k(B_{k-1} - B_k)\ (k = 0, 1, 2, \ldots).
\end{aligned} \tag{3}
$$

§ 1.2. Konvergentit

Lause 1.2.1. *Olkoon ketjumurtoluvun indeksijoukko I ja olkoon $k \in I$. Lisäksi olkoot ketjumurtoluvun astetta k olevan konvergentin c_k termit $a_0, a_1, \ldots, a_k$. Silloin $c_k = \frac{p_k}{q_k}$, missä luvut p_k ja q_k ovat määritelty rekursioyhtälöillä (2).*

Todistus. Todistetaan induktiolla ketjumurtoluvun asteen k suhteen. Kun $k = 0$, niin $\frac{p_0}{q_0} = \frac{a_0}{1} = a_0 = [a_0] = c_0$, joten tässä tapauksessa väite on tosi. Valitaan mielivaltainen $k \in I$. Tehdään induktio-oletus, että väite on tosi konvegenteille, joiden aste on $\leq k$. Nyt mikäli $k+1 \in I$, niin osoitetaan, että $c_{k+1} = \frac{p_{k+1}}{q_{k+1}}$. Oletetaan nyt, että $k+1 \in I$. Ketjumurtolukujen määritelmien perusteella $c_{k+1} = [a_0, a_1, \ldots, a_{k-1}, a_k, a_{k+1}] = [a_0, a_1, \ldots, a_{k-1}, a_k + \frac{1}{a_{k+1}}] = c'_k$. Koska konvergentti c'_k on astetta k ja eroaa konvergentista c_k vain viimeisen termin osalta, niin induktio-oletuksen perusteella

$$\begin{aligned}
c'_k = \frac{p'_k}{q'_k} &= \frac{\left(a_k + \frac{1}{a_{k+1}}\right) p'_{k-1} + p'_{k-2}}{\left(a_k + \frac{1}{a_{k+1}}\right) q'_{k-1} + q'_{k-2}} \\
&= \frac{\left(a_k + \frac{1}{a_{k+1}}\right) p_{k-1} + p_{k-2}}{\left(a_k + \frac{1}{a_{k+1}}\right) q_{k-1} + q_{k-2}} = \frac{a_k p_{k-1} + \frac{1}{a_{k+1}} p_{k-1} + p_{k-2}}{a_k q_{k-1} + \frac{1}{a_{k+1}} q_{k-1} + q_{k-2}} \\
&= \frac{a_k p_{k-1} + p_{k-2} + \frac{1}{a_{k+1}} p_{k-1}}{a_k q_{k-1} + q_{k-2} + \frac{1}{a_{k+1}} q_{k-1}} = \frac{p_k + \frac{1}{a_{k+1}} p_{k-1}}{q_k + \frac{1}{a_{k+1}} q_{k-1}} \\
&= \frac{a_{k+1} p_k + p_{k-1}}{a_{k+1} q_k + q_{k-1}} = \frac{p_{k+1}}{q_{k+1}}.
\end{aligned}$$

Siis $c_{k+1} = \frac{p_{k+1}}{q_{k+1}}$, joten induktioperiaatteen mukaan väite on tosi. □
Jatkossa käytetään astetta k oleville konvergenteille myös merkintää $\frac{p_k}{q_k}$, missä luvut p_k ja q_k ovat määritelty rekursioyhtälöillä (2).

Seuraavaksi esitellään konvergenttien ominaisuuksia.

Lause 1.2.2. *Olkoon ketjumurtoluvun indeksijoukko I ja olkoon $k \in I$. Silloin konvergenteille $\frac{p_k}{q_k}$ ja $\frac{p_{k-1}}{q_{k-1}}$ on voimassa yhtälö*

$$p_k q_{k-1} - q_k p_{k-1} = (-1)^{k+1}. \tag{4}$$

Todistus. Todistetaan induktiolla indeksin k suhteen. Kun $k = 0$, niin $p_0 q_{-1} - q_0 p_{-1} = a_0 \cdot 0 - 1 \cdot 1 = -1 = (-1)^{0+1}$, joten tässä tapauksessa väite on tosi. Valitaan mielivaltainen $n \in I$. Tehdään induktio-oletus, että väite on tosi aina, kun $k \leq n$. Osoitetaan, että väite on tosi, kun $k = n + 1$ ja $n + 1 \in I$. Oletetaan nyt, että $n + 1 \in I$. Nyt käyttämällä rekursioyhtälöitä (2) ja induktio-oletusta saadaan yhtälö

$$\begin{aligned}
p_{n+1} q_n - q_{n+1} p_n &= (a_{n+1} p_n + p_{n-1}) q_n - (a_{n+1} q_n + q_{n-1}) p_n \\
&= a_{n+1} p_n q_n + p_{n-1} q_n - a_{n+1} q_n p_n - q_{n-1} p_n \\
&= p_{n-1} q_n - q_{n-1} p_n \\
&= (-1)(p_n q_{n-1} - q_n p_{n-1}) \\
&= (-1) \cdot (-1)^{n+1} = (-1)^{(n+1)+1}.
\end{aligned}$$

Siis induktioperiaatteen mukaan väite on tosi. □

Lauseen 1.2.2 suora seuraus on se, että kun $k, k+1 \in I$, niin on voimassa yhtälö

$$c_{k+1} - c_k = \frac{p_{k+1}}{q_{k+1}} - \frac{p_k}{q_k} = \frac{(-1)^k}{q_{k+1}q_k}. \tag{5}$$

Lause 1.2.3. *Olkoon* $[a_0, a_1, \ldots, a_k]$ *päättyvä ketjumurtoluku, missä* $k \geq 1$. *Oletetaan lisäksi, että sen astetta* k *oleva konvergentti on* $\frac{p_k}{q_k}$. *Silloin on voimassa yhtälö*

$$\frac{q_k}{q_{k-1}} = [a_k, a_{k-1}, \ldots, a_1]. \tag{6}$$

Todistus. Todistetaan induktiolla luvun k suhteen. Kun $k = 1$, niin $\frac{q_1}{q_0} = \frac{a_1}{1} = a_1 = [a_1]$, joten tässä tapauksessa väite on tosi. Valitaan mielivaltainen $n \in \mathbf{Z}_+$. Tehdään induktio-oletus, että väite on tosi aina, kun $k \leq n$. Seuraavaksi osoitetaan, että väite on tosi, kun $k = n+1$. Nyt käyttämällä rekursioyhtälöitä (2) ja induktio-oletusta saadaan yhtälö

$$\begin{aligned}\frac{q_{n+1}}{q_n} &= \frac{a_{n+1}q_n + q_{n-1}}{q_n} \\ &= a_{n+1} + \frac{q_{n-1}}{q_n} \\ &= a_{n+1} + \frac{1}{\frac{q_n}{q_{n-1}}} \\ &= a_{n+1} + \frac{1}{[a_n, a_{n-1}, \ldots, a_1]} \\ &= [a_{n+1}, a_n, \ldots, a_1].\end{aligned}$$

Siis induktioperiaatteen mukaan väite on tosi. □

Lause 1.2.4. *Olkoon* $[a_0, a_1, \ldots, a_k]$ *päättyvä ketjumurtoluku, missä* $a_0 > 0$ *ja* $k \geq 0$. *Oletetaan lisäksi, että sen astetta* k *oleva konvergentti on* $\frac{p_k}{q_k}$. *Silloin on voimassa yhtälö*

$$\frac{p_k}{p_{k-1}} = [a_k, a_{k-1}, \ldots, a_0]. \tag{7}$$

Todistus. Todistetaan induktiolla luvun k suhteen. Kun $k = 0$, niin $\frac{p_0}{p_{-1}} = \frac{a_0}{1} = a_0 = [a_0]$, joten tässä tapauksessa väite on tosi. Valitaan mielivaltainen $n \in \mathbf{N}$. Tehdään induktio-oletus, että väite on tosi aina, kun $k \leq n$. Seuraavaksi osoitetaan, että väite on tosi, kun $k = n + 1$. Nyt käyttämällä rekursioyhtälöitä (2) ja induktio-oletusta saadaan yhtälö

$$\begin{aligned}\frac{p_{n+1}}{p_n} &= \frac{a_{n+1}p_n + p_{n-1}}{p_n} \\ &= a_{n+1} + \frac{p_{n-1}}{p_n} \\ &= a_{n+1} + \frac{1}{\frac{p_n}{p_{n-1}}} \\ &= a_{n+1} + \frac{1}{[a_n, a_{n-1}, \ldots, a_0]} \\ &= [a_{n+1}, a_n, \ldots, a_0].\end{aligned}$$

Siis induktioperiaatteen mukaan väite on tosi. $\square$

Seuraavaksi tutkitaan edellisiä lauseita siinä tapauksessa, että kyseessä ovat yksinkertaiset ketjumurtoluvut.

Apulause 1.2.1. *Yksinkertaisten ketjumurtolukujen konvergentit $\frac{p_k}{q_k}$ $(k \in I)$ ovat rationaalilukuja. Erityisesti $p_k \in \mathbf{Z}$ ja $q_k \in \mathbf{Z}_+$.*

Todistus. Todistetaan induktiolla. Koska $\frac{p_0}{q_0} = a_0 \in \mathbf{Z} \subseteq \mathbf{Q}$ ja $p_0 = a_0 \in \mathbf{Z}, q_0 = 1 \in \mathbf{Z}_+$, niin väite on tässä tapauksessa tosi. Valitaan mielivaltainen $n \in I$. Tehdään induktio-oletus, että lause on voimassa konvergenteille, joiden aste k on $\leq n$. Oletetaan lisäksi, että astetta $k+1$ oleva konvergentti on olemassa. Todistetaan, että astetta $k + 1$ oleva konvergentti toteuttaa lauseen. Nyt koska $a_{k+1} \in \mathbf{Z}_+$, niin rekursioyhtälöiden (2) ja induktio-oletuksesta perusteella $p_{k+1} = a_{k+1}p_k + p_{k-1} \in \mathbf{Z}$ ja $q_{k+1} = a_{k+1}q_k + q_{k-1} \in \mathbf{Z}+$. Siis $\frac{p_{k+1}}{q_{k+1}} \in \mathbf{Q}$, joten induktioperiaatteen mukaan väite on tosi. $\square$

Apulause 1.2.2. *Yksinkertaisten ketjumurtolukujen konvergenttien $\frac{p_k}{q_k}$ $(k \in I)$ nimittäjille q_k on voimassa epäyhtälö $q_k \geq k$.*

Todistus. Todistetaan induktiolla. Väite on tosi, kun $k = 0$,

$k = 1$ tai $k = 2$, koska $q_0 = 1 > 0$, $q_1 = a_1 \geq 1$ ja $q_2 = a_2 q_1 + q_0 \geq 1 \cdot 1 + 1 = 2$. Valitaan mielivaltainen $n \in I$, joka on ≥ 2. Tehdään induktio-oletus, että $q_k \geq k$, kun $k \leq n$. Nyt rekursioyhtälöiden (2) ja induktio-oletuksen mukaan $q_{n+1} = a_{n+1} q_n + q_{n-1} \geq n + n - 1 = 2n - 1 = n + n - 1 \geq n + 2 - 1 = n + 1$, joten induktioperiaatteen mukaan väite on tosi. □

Apulause 1.2.3. *Olkoon yksinkertainen ketjumurtoluku muotoa $[a_0, a_1, \ldots, a_n]$, missä $a_0 \geq 1$ ja $n > 0$. Silloin konvergentti $\frac{p_n}{q_n}$ on > 1.*

Todistus. Todistetaan induktiolla luvun n suhteen. Kun $n = 1$, niin $\frac{p_1}{q_1} = a_0 + \frac{1}{a_1} \geq 1 + \frac{1}{a_1} > 1$, joten tässä tapauksessa väite on tosi. Valitaan mielivaltainen $k > 0$. Tehdään induktio-oletus, että lause on tosi, kun $n = k$. Osoitetaan, että lause on tosi myös, kun $n = k + 1$. Nyt koska $\frac{p_{k+1}}{q_{k+1}} = a_0 + \frac{1}{[a_1, a_2, \ldots, a_{k+1}]}$, $a_1 \geq 1$ sekä $k + 1 - 1 = k$, niin induktio-oletuksen mukaan $[a_1, a_2, \ldots, a_{k+1}] > 1$. Siis $\frac{p_{k+1}}{q_{k+1}} > a_0 \geq 1$, joten induktioperiaatteen mukaan väite on tosi. □

Lause 1.2.5. *Yksinkertaisten ketjumurtolukujen konvergentit $\frac{p_k}{q_k}$ ovat supistetussa muodossa.*

Todistus. Apulauseen 1.2.1 mukaan $p_k \in \mathbf{Z}$ ja $q_k \in \mathbf{Z}_+$ aina, kun $k \in I$. Oletetaan, että luvuilla p_k ja q_k olisi yhteinen tekijä d, joka on > 1. Lauseen 1.2.2 mukaan $p_k q_{k-1} - q_k p_{k-1} = (-1)^{k+1}$. Siis luku d jakaisi luvut $-1, 1$, mikä on mahdotonta, koska $d > 1$. Täten konvergentit $\frac{p_k}{q_k}$ ovat supistetussa muodossa. □

Lause 1.2.6. *Olkoon ketjumurtoluvun indeksijoukko I ja olkoot $k + 1, k \in I$. Silloin konvergenteille $\frac{p_{k+1}}{q_{k+1}}$ ja $\frac{p_{k-1}}{q_{k-1}}$ on voimassa yhtälö*

$$p_{k+1} q_{k-1} - q_{k+1} p_{k-1} = (-1)^{k+1} a_{k+1}. \tag{8}$$

Todistus. Todistetaan induktiolla indeksin k suhteen. Kun $k = 0$, niin $p_1 q_{-1} - q_1 p_{-1} = (a_0 a_1 + 1) \cdot 0 - a_1 \cdot 1 = -1 \cdot a_1 = (-1)^{0+1} a_1$, joten tässä tapauksessa väite on tosi. Valitaan mielivaltainen $n \in I$. Tehdään induktio-oletus, että väite on tosi aina, kun $k \leq n$. Osoitetaan, että väite on tosi, kun $k = n+1$ ja $n+1, n+2 \in I$. Oletetaan nyt, että $n+1, n+2 \in I$. Nyt käyttämällä lausetta 1.2.2, rekursioyhtälöitä (2) ja induktio-oletusta saadaan yhtälö

$$\begin{aligned}
p_{n+2}q_n - q_{n+2}p_n &= (a_{n+2}p_{n+1} + p_n)q_n - (a_{n+2}q_{n+1} + q_n)p_n \\
&= a_{n+2}p_{n+1}q_n + p_nq_n - a_{n+2}q_{n+1}p_n - q_np_n \\
&= a_{n+2}(p_{n+1}q_n - q_{n+1}p_n) \\
&= (-1)^{n+1+1}a_{n+2} = (-1)^{n+2}a_{n+2}.
\end{aligned}$$

Siis induktioperiaatteen mukaan väite on tosi. □

Lauseen 1.2.6 suora seuraus on se, että kun $k, k+2 \in I$, niin on voimassa yhtälö

$$c_{k+2} - c_k = \frac{p_{k+2}}{q_{k+2}} - \frac{p_k}{q_k} = \frac{(-1)^k a_{k+2}}{q_{k+2}q_k}. \tag{9}$$

§ 1.3. Neliökunnista

Määritelmä 1.3.1. Olkoon $N \in \mathbf{Z}_+$, joka ei ole täydellinen neliö. Olkoot $s, t \in \mathbf{Q}$. Silloin lukua $s + t\sqrt{N}$ sanotaan *kvadraattiseksi irrationaaliluvuksi.*

Määritelmä 1.3.2. Merkitään joukkoa $\{s + t\sqrt{N} | s, t \in \mathbf{Q}\}$ merkinnällä $\mathbf{Z}_{\sqrt{N}}$. Olkoot $x, y \in \mathbf{Z}_{\sqrt{N}}$. Merkitään $x = s_1 + t_1\sqrt{N}$, $y = s_2 + t_2\sqrt{N}$. Määritellään yhteen- ja kertolasku seuraavasti

$$\begin{aligned}
x + y &= (s_1 + s_2) + (t_1 + t_2)\sqrt{N}, \\
x \cdot y &= (s_1s_2 + Nt_1t_2) + (s_1t_1 + s_2t_2)\sqrt{N}.
\end{aligned}$$

Määritelmä 1.3.3. Olkoon $x \in \mathbf{Z}_{\sqrt{N}}$. Merkitään seuraavasti $x = s + t\sqrt{N}$, missä $s, t \in \mathbf{Q}$. Määritellään luvun x liittoluku $\overline{x}$ seuraavasti $\overline{x} = s - t\sqrt{N}$.

Lause 1.3.1. *Joukko $\mathbf{Z}_{\sqrt{N}}$ muodostaa määritelmän 1.3.2* *mukaisen yhteen- ja kertolaskun suhteen algebrallisen struktuurin kunta.*

Todistus. Sivuutetaan.

Lause 1.3.2. *Olkoot $x, y \in \mathbf{Z}_{\sqrt{N}}$. Silloin lukujen x, y liittoluvuille on voimassa seuraavat laskusäännöt*

$$
\begin{aligned}
\overline{x+y} &= \overline{x} + \overline{y}, \\
\overline{xy} &= \overline{x} \cdot \overline{y}, \\
\overline{x-y} &= \overline{x} - \overline{y}, \\
\overline{\left(\frac{x}{y}\right)} &= \frac{\overline{x}}{\overline{y}}, \text{ kun } y \neq 0.
\end{aligned}
$$

Todistus. Todistetaan vain ensimmäinen sääntö. Muut säännöt todistetaan vastaavasti. Käytetään merkintöjä $x = x_1 + x_2\sqrt{N}$ ja $y = y_1 + y_2\sqrt{N}$, missä $x_1, x_2, y_1, y_2 \in \mathbf{Q}$. Määritelmien 1.3.2 ja 1.3.3 perusteella

$$
\begin{aligned}
\overline{x+y} &= \overline{(x_1 + x_2\sqrt{N}) + (y_1 + y_2\sqrt{N})} \\
&= \overline{(x_1 + y_1) + (x_2 + y_2)\sqrt{N}} \\
&= (x_1 + y_1) - (x_2 + y_2)\sqrt{N} \\
&= (x_1 - x_2\sqrt{N}) + (y_1 - y_2\sqrt{N}) \\
&= \overline{x} + \overline{y}.
\end{aligned}
$$

Siis ensimmäinen sääntö on tosi. □

Lause 1.3.3. *Olkoon $x \in \mathbf{Z}_{\sqrt{N}}$. Silloin on olemassa sellaiset $a, b, c \in \mathbf{Z}$, että $x, \overline{x}$ ovat toisen asteen yhtälön $ax^2 + bx + c = 0$ ratkaisut.*

Todistus. Merkitään $x = s + t\sqrt{N}$, missä $s, t \in \mathbf{Q}$. Merkitään $s = \frac{s_1}{s_2}$ ja $t = \frac{t_1}{t_2}$, missä $s_1, t_1 \in \mathbf{Z}$ ja $s_2, t_2 \in \mathbf{Z}_+$. Valitaan

$$
\begin{aligned}
a &= (s_2 t_2)^2, \\
b &= -2 s_1 s_2 t_1 t_2, \\
c &= (s_1 t_2)^2 - (s_2 t_1)^2 N.
\end{aligned}
$$

Selvästikin näin valitut luvut a, b, c ovat kokonaislukuja. Osoitetaan vielä, että tällöin yhtälön $ax^2 + bx + c = 0$ ratkaisut ovat x ja $\overline{x}$. Soveltamalla toisen asteen yhtälön ratkaisukaavaa $x = \frac{-b \pm \sqrt{b^2-4ac}}{2a}$ saadaan

$$x = \frac{-(-2s_1s_2t_1t_2) \pm \sqrt{(-2s_1s_2t_1t_2)^2 - 4(s_2t_2)^2((s_1t_2)^2 - (s_2t_1)^2N)}}{2(s_2t_2)^2}$$

, josta saadaan $x = \frac{s_1t_1 \pm s_2t_1\sqrt{N}}{s_2t_2} = \frac{s_1}{s_2} \pm \frac{t_1}{t_2}\sqrt{N} = s \pm t\sqrt{N}$. Siis x ja $\overline{x}$ ovat yhtälön ratkaisut. $\square$

Lause 1.3.4. *Olkoot $a, b, c \in \mathbf{Z}$ ja olkoon lisäksi $a \neq 0$. Olkoot toisen asteen yhtälön $ax^2 + bx + c = 0$ ratkaisut x_1 ja x_2. Mikäli $x_1, x_2 \in \mathbf{R} \setminus \mathbf{Q}$, niin luvut x_1 ja x_2 ovat kvadraattisia irrationaalilukuja.*

Todistus. Soveltamalla yhtälöön toisen asteen yhtälön ratkaisukaavaa saadaan $x_1 = \frac{-b+\sqrt{b^2-4ac}}{2a}$ ja $x_2 = \frac{-b-\sqrt{b^2-4ac}}{2a}$. Koska luvut x_1 ja x_2 oletettiin irrationaaliluvuiksi, niin luku $b^2 - 4ac$ ei ole täydellinen neliö. Nyt merkitään $N = b^2 - 4ac$, $t = \frac{1}{2a}$ ja $s = \frac{-b}{2a}$. Selvästikin $s, t \in \mathbf{Q}$, joten $x_1 = s + t\sqrt{N}$ ja $x_2 = s - t\sqrt{N}$. Siis luvut x_1 ja x_2 ovat kvadraattisia irrationaalilukuja. $\square$

Määritelmä 1.3.4. Olkoon $x \in \mathbf{Z}_{\sqrt{N}}$. Mikäli $x > 0$ ja $-1 < \overline{x} < 0$, niin lukua x sanotaan *redusoiduksi kvadraattiseksi irrationaaliluvuksi.*

Apulause 1.3.1. *Seuraava yhtälö on voimassa*

$$au^2 + bu + c = a(u-v)^2 + (2av+b)(u-v) + (av^2 + bv + c).$$

Todistus. Apulause saadaan suoraan laskemalla

$$\begin{aligned}
&a(u-v)^2 + (2av+b)(u-v) + (av^2+bv+c) \\
&= au^2 - 2auv + av^2 + 2avu + bu - 2av^2 - bv + av^2 + bv + c \\
&= au^2 + bu + c.
\end{aligned}$$

$\square$

Luku 2. Reaalilukujen esittämisestä ketjumurtolukuina

§ 2.1. Rationaaliluvut

Kun tässä luvussa puhutaan ketjumurtoluvuista, niin tarkoitetaan yksinkertaisia ketjumurtolukuja.

Lause 2.1.1. *Olkoot $a_0, a_1, \ldots, a_n$ päättyvän ketjumurtoluvun termit. Olkoot $\frac{p_k}{q_k}$ $(k = 0, 1, \ldots, n)$ tämän ketjumurtoluvun konvergentteja. Silloin on olemassa sellainen rationaaliluku x, että $x = [a_0, a_1, \ldots, a_n]$.*

Todistus. Tulos seuraa suoraan apulauseesta 1.2.1, kun valitaan $x = \frac{p_n}{q_n}$. $\square$

Apulause 2.1.1. *Olkoon I se indeksijoukko, missä rekursioyhtälöt (1) ovat määritelty. Silloin rekursioyhtälöissä (1) $a_0 \in \mathbf{Z}$ ja $a_k \in \mathbf{Z}_+$ aina, kun $k \in I$ ja $k > 0$.*

Todistus. Rekursioyhtälöistä (1) seuraa suoraan, että $a_0 = \lfloor x \rfloor \in \mathbf{Z}$. Koska rekursio-yhtälöissä (1) $a_{k+1} = \lfloor \varepsilon_{k+1} \rfloor = \left\lfloor \frac{1}{\varepsilon_k - a_k} \right\rfloor$ ja $\frac{1}{\varepsilon_k - a_k} > 1$, niin $a_{k+1} \geq 1$. Siis $a_k \in \mathbf{Z}_+$ aina, kun $k \in I$ ja $k > 0$. $\square$

Apulause 2.1.2. *Olkoon I se indeksijoukko, missä rekursioyhtälöt (1) ovat määritelty. Silloin on voimassa yhtälö $x = [a_0, a_1, \ldots, a_{k-1}, \varepsilon_k]$ aina, kun $k \in I$.*

Todistus. Indeksijoukko I on $\{0, 1, \ldots, n\}$, mikäli on olemassa sellainen $n \in \mathbf{N}$, että $\varepsilon_n = a_n$. Muutoin $I = \{0, 1, 2, \ldots\}$. Todistetaan lause induktiolla. Kun $k = 0$, niin $x = [\varepsilon_0] = \varepsilon_0$, joten tässä tapauksessa väite on tosi. Valitaan mielivaltainen $n \in I$. Tehdään induktio-oletus, että lause on tosi, kun $k = n$. Nyt osoitetaan, että lause on tosi myös, kun $k = n + 1$ ja $n + 1 \in I$. Rekursioyhtälöiden (1) perusteella $\varepsilon_k = a_k + \frac{1}{\varepsilon_{k+1}}$. Nyt induktio-oletuksen mukaan $x = [a_0, a_1, \ldots, a_{n-1}, \varepsilon_n] = [a_0, a_1, \ldots, a_{n-1}, a_n + \frac{1}{\varepsilon_{n+1}}] = [a_0, a_1, \ldots, a_{n-1}, a_n, \varepsilon_{n+1}]$. Siis induktio-periaatteen mukaan väite on tosi. □

Lause 2.1.2. *Jokainen $x \in \mathbf{Q}$ voidaan esittää yksikäsitteisesti päättyvänä ketjumurtolukuna, kun annetaan lisäehto, että ketjumurtoluku ei pääty lukuun 1, paitsi kun $x = 1$.*

Todistus. Valitaan mielivaltainen $x \in \mathbf{Q}$. Nyt mikäli $x = 1$, niin $x = 1 = [1]$. Oletetaan nyt, että $x \neq 1$. Luku x voidaan esittää muodossa $\frac{s_0}{t_0}$, missä $s_0 \in \mathbf{Z}$ ja $t_0 \in \mathbf{Z}_+$. Sovelletaan rekursioyhtälöitä (1) lukuun x. Osoitetaan, että $\varepsilon_k \in \mathbf{Q}$ aina, kun $k \in I$. Tulemme merkitsemään $\varepsilon_k = \frac{s_k}{t_k}$. Osoitetaan lisäksi, että $t_{k+1} < t_k$. Todistetaan induktiolla. Kun $k = 0$, niin $\varepsilon_0 = x = \frac{s_0}{t_0} \in \mathbf{Q}$, joten tässä tapauksessa väite on tosi. Valitaan mielivaltainen $n \in I$. Tehdään induktio-oletus, että kun $k = n$, niin $\varepsilon_n = \frac{s_n}{t_n}$ sekä $t_n < t_{n-1}$. Nyt rekursioyhtälöiden (1) perusteella

$$\begin{aligned}
\varepsilon_{n+1} &= \frac{1}{\varepsilon_n - a_n} \\
&= \frac{1}{\frac{s_n}{t_n} - \left\lfloor \frac{s_n}{t_n} \right\rfloor} \\
&= \frac{t_n}{s_n - \left\lfloor \frac{s_n}{t_n} \right\rfloor t_n}.
\end{aligned}$$

Merkitään $s_{n+1} = t_n$ ja $t_{n+1} = s_n - \left\lfloor \frac{s_n}{t_n} \right\rfloor t_n$. Koska $\varepsilon_n - a_n < 1$, niin $t_{n+1} < t_n$. Lisäksi $\varepsilon_{n+1} = \frac{s_{n+1}}{t_{n+1}} \in \mathbf{Q}$. Induktioperiaatteen mukaan väite on todistettu. Koska $t_0 > t_1 > t_2 > \cdots$ ja $t_0 \in \mathbf{Z}_+$, niin on olemassa sellainen $n \in \mathbf{N}$, että $t_n = 1$. Siis $\varepsilon_n = s_n = \lfloor s_n \rfloor = \lfloor \varepsilon_n \rfloor = a_n$, joten rekursioyhtälöt (1) ovat määritelty indeksijoukossa $\{0, 1, \ldots, n\}$. Nyt apulauseen 2.1.2 mukaan $x = [a_0, a_1, \ldots, a_{n-1}, \varepsilon_n] = [a_0, a_1, \ldots, a_n]$. Edelleen apulauseen 2.1.1 mukaan $a_0 \in \mathbf{Z}$ ja $a_1, a_2, \ldots, a_n \in \mathbf{Z}_+$. Tutkitaan vielä lukua a_n.

Kun $n = 0$, niin oletuksen mukaan $a_0 = x \neq 1$. Kun $n > 0$, niin $a_n = s_n = t_{n-1} > t_n = 1$. Siis olemme osoittaneet, että rekursioyhtälöistä (1) voidaan muodostaa päättyvä yksinkertainen ketjumurtoluku luvulle x, joka ei pääty lukuun 1. Osoitamme vielä, että tämä esitys on yksikäsitteinen. Olkoon nyt $[a_0, a_1, \ldots, a_n]$ ja $[b_0, b_1, \ldots, b_m]$ kaksi sellaista luvun x ketjumurtolukukehitelmää, jotka eivät pääty lukuun 1. Oletetaan lisäksi, että $n \leq m$. Mikäli $n = 0$, niin $\lfloor x \rfloor = a_0 = \lfloor [b_0, b_1, \ldots, b_m] \rfloor$. Mikäli $m = 0$, niin $a_0 = b_0$ ja yksikäsitteisyys on selvä. Oletetaan, että $m > n$. Nyt koska $[b_1, b_2, \ldots, b_m]$ ei pääty lukuun 1, niin apulauseen 1.2.3 mukaan $[b_1, b_2, \ldots, b_m] > 1$, joten $\lfloor [b_0, b_1, \ldots, b_m] \rfloor = \left\lfloor b_0 + \frac{1}{[b_1, b_2, \ldots, b_m]} \right\rfloor = b_0$. Siis $\frac{1}{[b_1, b_2, \ldots, b_m]} = 0$, mikä on mahdotonta, joten $m = n$. Oletetaan, nyt, että $n > 0$. Koska ketjumurtoluvut eivät oletuksen mukaan pääty lukuun 1, niin apulauseen 1.2.3 mukaan $[b_1, b_2, \ldots, b_m] > 1$ ja $[a_1, a_2, \ldots, a_n] > 1$, joten $\lfloor [a_0, a_1, \ldots, a_n] \rfloor = \left\lfloor a_0 + \frac{1}{[a_1, a_2, \ldots, a_n]} \right\rfloor = a_0 = \lfloor [b_0, b_1, \ldots, b_m] \rfloor = \left\lfloor b_0 + \frac{1}{[b_1, b_2, \ldots, b_m]} \right\rfloor = b_0$. Siis myös tässä tapauksessa $a_0 = b_0$. Edelleen saadaan $[a_1, a_2, \ldots, a_n] = [b_1, b_2, \ldots, b_m]$. Kun toistetaan edellisten kaltaisia päättelyitä, niin saadaan yhtälöt

$a_1 = b_1, a_2 = b_2, \ldots, a_n = b_n$. Lisäksi vielä $n = m$. Siis ketjumurtolukukehitelmä on yksikäsitteinen. □

Tutkitaan vielä lukuun 1 päättyvää yksinkertaista ketjumurtolukua $[a_0, a_1, \ldots, a_n, 1]$, missä $n > 0$. Tämä voidaan esittää myös muodossa $[a_0, a_1, \ldots, a_n + \frac{1}{1}]$, joka on $= [a_0, a_1, \ldots, a_n + 1]$. Tällöin viimeinen termi $a_n + 1$ on > 1, joten lukuun 1 päättyvä ketjumurtoluku voidaan esittää myös lyhyemmässä muodossa siten, että se ei pääty lukuun 1.

Olemme todistaneet tässä pykälässä, että jokainen rationaaliluku voidaan esittää yksikäsitteisesti päättyvänä yksinkertaisena ketjumurtolukuna. Tämä esitys saadaan rekursioyhtälöistä (1). Toisaalta olemme todistaneet, että jokainen päättyvä yksinkertainen ketjumurtoluku esittää jotain rationaalilukua. Siis rationaaliluvut ja päättyvät yksinkertaiset ketjumurtoluvut ovat yhtäpitäviä.

Esimerkki 2.1.1. Muodostetaan luvun $\frac{7}{4}$ ketjumurtolukuesitys. Käyttämällä rekursioyhtälöitä (1) saadaan

$$\frac{7}{4} = 1 + \frac{3}{4} = 1 + \frac{1}{\frac{4}{3}} = 1 + \frac{1}{1 + \frac{1}{3}}.$$

Eli $\frac{7}{4} = [1, 1, 3]$, joka on helppo tarkastaa rekursioyhtälöiden (2) avulla.

Esimerkki 2.1.2. Muutetaan luku $\frac{119}{68}$ supistetuun muotoon. Muodostetaan luvun $\frac{119}{68}$ ketjumurtolukukehitelmä. Toimitaan kuten esimerkissä 2.1.1, jolloin saadaan

$$\frac{119}{68} = 1 + \frac{51}{68} = 1 + \frac{1}{\frac{68}{51}} = 1 + \frac{1}{1 + \frac{17}{51}} = 1 + \frac{1}{1 + \frac{1}{\frac{51}{17}}} = 1 + \frac{1}{1 + \frac{1}{3}}.$$

Eli $\frac{119}{68} = \frac{7}{4}$. Lukujen suurin yhteinen tekijä oli siis $\frac{68}{4} = 17$.

Esimerkki 2.1.3. Ratkaistaan lineaarinen Diofantoksen yhtälö $ax + by = 1$. Lukujen a ja b suurimman yhteisen tekijän täytyy olla 1, jotta yhtälö on ratkeava. Oletetaan, että yhtälö on ratkeava. Voidaan lisäksi olettaa, että $b > 0$, koska $by = (-b)(-y)$. Muodostetaan luvun $\frac{a}{b}$ ketjumurtolukukehitelmä. Olkoon se nyt $[a_0, a_1, \ldots, a_n]$. Eli $p_n = a$ ja $q_n = b$. Lauseen 1.2.2 perusteella $p_n q_{n-1} - q_n p_{n-1} = (-1)^{n+1}$. Jos n on parillinen, niin valitaan $x = -q_{n-1}$ ja $y = p_{n-1}$. Jos n on pariton, niin valitaan $x = q_{n-1}$ ja $y = -p_{n-1}$. Näin valituille luvuille x ja y on voimassa yhtälö $ax + by = 1$.

§ 2.2. Irrationaaliluvut

Määritelmä 2.2.1. Olkoot päättymättömän yksinkertaisen ketjumurtoluvun termit $a_0, a_1, \ldots$. Olkoot $\frac{p_k}{q_k}$ $(k = 0, 1, \ldots)$ tämän ketjumurtoluvun konvergentteja. Olkoon $x \in \mathbf{R}$. Silloin voidaan merkitä $x = [a_0, a_1, \ldots]$, mikäli $\lim_{k \to \infty} \frac{p_k}{q_k} = x$.

Lause 2.2.1. *Yksinkertaisen päättymättömän ketjumurtoluvun $[a_0, a_1, \ldots]$ konvergentit c_k $(k = 0, 1, \ldots)$ muodostavat epäyhtälöketjun*

$$c_0 < c_2 < \cdots < c_{2k} < \cdots < c_{2k+1} < \cdots < c_3 < c_1. \tag{10}$$

Todistus. Valitaan mielivaltainen $k \in \mathbf{N}$. Yhtälön (9) mukaan $c_{2k+2} - c_{2k} = \frac{(-1)^{2k+2} a_{2k+2}}{q_{2k+2} q_{2k}} > 0$ ja $c_{2k+3} - c_{2k+1} = \frac{(-1)^{2k+3} a_{2k+3}}{q_{2k+3} q_{2k+1}} < 0$. Siis $c_{2k+2} > c_{2k}$ ja $c_{2k+3} < c_{2k+1}$, joten on osoitettu, että
$c_0 < c_2 < c_4 < \cdots$ ja $\cdots < c_5 < c_3 < c_1$. Valitaan mielivaltaiset $k, l \in \mathbf{N}$. Merkitään $m = \max\{k, l\}$. Tiedetään, että $c_{2k} \leq c_{2m}$ ja $c_{2m+1} \leq c_{2l+1}$. Nyt yhtälön (5) mukaan $c_{2m+1} - c_{2m} = \frac{(-1)^{2m}}{q_{2m+1} q_{2m}} > 0$, joten $c_{2k} \leq c_{2m} < c_{2m+1} \leq c_{2l+1}$. Siis on todistettu, että
$c_0 < c_2 < \cdots < c_{2k} < \cdots < c_{2k+1} < \cdots < c_3 < c_1$. □

Lause 2.2.2. *Olkoot yksinkertaisen päättymättmän ketjumurtoluvun termit* $a_0, a_1, \ldots$. *Olkoot* c_k $(k = 0, 1, \ldots)$ *tämän ketjumurtoluvun konvergentteja. Silloin on olemassa sellainen* $l \in \mathbf{R}$, *että* $\lim_{k\to\infty} c_k = l$.

Todistus (vrt. [4], s. 66–67). Osoitetaan aluksi, että on olemassa sellaiset $l_1, l_2 \in \mathbf{R}$, että $\lim_{k\to\infty} c_{2k} = l_1$ ja $\lim_{k\to\infty} c_{2k+1} = l_2$. Koska $c_0, c_2, c_4, \ldots$ muodostavat aidosti kasvavan jonon, joka on ylhäältä rajoitettu luvulla c_1, niin analyysin perustulosten nojalla voidaan sanoa, että on olemassa sellainen $l_1 \in \mathbf{R}$, että $\lim_{k\to\infty} c_{2k} = l_1$. Vastaavasti koska $c_1, c_3, c_5, \ldots$ muodostavat aidosti vähenevän jonon, joka on alhaalta rajoitettu luvulla c_0, niin on olemassa sellainen $l_2 \in \mathbf{R}$, että $\lim_{k\to\infty} c_{2k+1} = l_2$. Osoitetaan seuraavaksi, että $\lim_{k\to\infty}(c_{2k+1} - c_{2k}) = 0$. Valitaan mielivaltainen $\varepsilon > 0$. Valitaan $n_0 = \lceil \frac{1}{\varepsilon} \rceil + 1$. Valitaan mielivaltainen $n > n_0$. Apulauseen 1.2.2 mukaan $q_{2n+1} > q_{2n} > q_n \geq n$. Nyt yhtälön (5) perusteella

$$\begin{aligned} |c_{2n+1} - c_{2n}| &= \left| \frac{p_{2n+1}}{q_{2n+1}} - \frac{p_{2n}}{q_{2n}} \right| \\ &= \left| \frac{(-1)^{2n+1}}{q_{2n+1} q_{2n}} \right| < \frac{1}{n} < \varepsilon. \end{aligned}$$

Siis on osoitettu, että $\lim_{k\to\infty}(c_{2k+1} - c_{2k}) = 0$. Nyt $l_2 - l_1 = \lim_{k\to\infty} c_{2k+1} - \lim_{k\to\infty} c_{2k} = \lim_{k\to\infty}(c_{2k+1} - c_{2k}) = 0$, joten $l_1 = l_2$. Merkitään $l = l_1 = l_2$. Täten $\lim_{k\to\infty} c_k = l$. □

Apulause 2.2.1. *Olkoon* $[a_0, a_1, \ldots]$ *sellainen yksinkertainen päättymätön ketjumurtoluku, että* $a_0 \in \mathbf{Z}_+$. *Olkoon* $x = [a_0, a_1, \ldots]$.

Silloin $x > 1$.

Todistus. Apulauseen 1.2.3 mukaan $c_k > 1$ ($k = 1, 2, \ldots$), joten $\lim_{k\to\infty} c_k \geq 1$. Koska $[a_1, a_2, \ldots]$ on yksinkertainen päättymätön ketjumurtoluku, jonka ensimmäinen termi $a_1 \in \mathbf{Z}_+$, niin on olemassa $l \geq 1$ siten, että $l = [a_1, a_2, \ldots]$. Siis $[a_0, a_1, \ldots] = a_0 + \frac{1}{[a_1, a_2, \ldots]} = a_0 + \frac{1}{l} \geq 1 + \frac{1}{l} > 1$, joten $x > 1$. □

Lause 2.2.3. *Jokainen $x \in \mathbf{R} \setminus \mathbf{Q}$ voidaan esittää yksikäsitteisesti yksinkertaisena päättymättömänä ketjumurtolukuna.*

Todistus (vrt. [4], s. 68–70). Sovelletaan rekursioyhtälöitä (2) lukuun x. Osoitetaan induktiolla, että $\varepsilon_k \in \mathbf{R} \setminus \mathbf{Q}$ ($k = 0, 1, \ldots$). Kun $k = 0$, niin $x = \varepsilon_0 \in \mathbf{R} \setminus \mathbf{Q}$. Valitaan mielivaltainen $n \in \mathbf{N}$. Tehdään induktio-oletus, että $\varepsilon_n \in \mathbf{R} \setminus \mathbf{Q}$. Siis $\varepsilon_n > a_n$. Rekursioyhtälöiden (1) mukaan $\varepsilon_{n+1} = \frac{1}{\varepsilon_n - a_n} > 1$. Jos nyt $\varepsilon_{n+1} \in \mathbf{Q}$, niin $\varepsilon_n = a_n + \frac{1}{\varepsilon_{n+1}} \in \mathbf{Q}$, joka on ristiriidassa induktio-oletuksen kanssa. Siis $\varepsilon_{n+1} \in \mathbf{R} \setminus \mathbf{Q}$, joten induktioperiaatteen mukaan väite on todistettu. Koska $\varepsilon_k \in \mathbf{R} \setminus \mathbf{Q}$ ($k = 0, 1, \ldots$), niin rekursioyhtälöt (1) ovat määritelty aina, kun $k \in \mathbf{N}$. Apulauseen 2.1.1 mukaan rekursioyhtälöissä (1) $a_0 \in \mathbf{Z}$ ja $a_k \in \mathbf{Z}_+$, kun $k > 0$. Siis rekursioyhtälöillä (1) saadaan muodostettua luvusta x päättymätön yksinkertainen ketjumurtoluku $[a_0, a_1, \ldots]$. Nyt riittää osoittaa, että $x = [a_0, a_1, \ldots]$ eli $\lim_{k\to\infty} \frac{p_k}{q_k} = x$. Apulauseen 2.1.2 mukaan $x = [a_0, a_1, \ldots, a_k, \varepsilon_{k+1}]$ ($k = 0, 1, \ldots$). Valitaan mielivaltainen $\varepsilon > 0$. Merkitään $k_0 = \lceil \frac{1}{\varepsilon} \rceil + 1$. Valitaan mielivaltainen $k \geq k_0$. Nyt

$$\begin{aligned}
\left| x - \frac{p_k}{q_k} \right| &= \left| \frac{\varepsilon_{k+1} p_k + p_{k-1}}{\varepsilon_{k+1} q_k + q_{k-1}} - \frac{p_k}{q_k} \right| \\
&= \left| \frac{\varepsilon_{k+1} p_k q_k + p_{k-1} q_k - \varepsilon_{k+1} q_k p_k - q_{k-1} p_k}{\varepsilon_{k+1} q_k^2 + q_k q_{k-1}} \right| \\
&= \left| \frac{p_{k-1} q_k - q_{k-1} p_k}{\varepsilon_{k+1} q_k^2 + q_k q_{k-1}} \right| \\
&= \left| \frac{(-1)^k}{\varepsilon_{k+1} q_k^2 + q_k q_{k-1}} \right| \\
&= \frac{1}{\varepsilon_{k+1} q_k^2 + q_k q_{k-1}} < \frac{1}{q_k^2} < \frac{1}{k} < \varepsilon.
\end{aligned}$$

Siis $\lim_{k\to\infty} \frac{p_k}{q_k} = x$, joten rekursioyhtälöillä (1) saadaan luvusta x yksinkertainen päättymätön ketjumurtoluku, joka on $= x$. Vielä pitää todistaa, että näin saatu esitys on yksikäsitteinen. Oletetaan, että luvulla x on kaksi ketjumurtolukuesitystä $[a_0, a_1, \ldots]$ ja $[b_0, b_1, \ldots]$. Apulauseen 2.2.1 mukaan $l_1 = [a_1, a_2, \ldots] > 1$ ja $l_2 = [b_1, b_2, \ldots] > 1$, joten $\lfloor x \rfloor = \left\lfloor a_0 + \frac{1}{l_1} \right\rfloor = a_0$ ja $\lfloor x \rfloor = \left\lfloor b_0 + \frac{1}{l_2} \right\rfloor = b_0$ eli $a_0 = b_0$. Siis myös $l_1 = l_2$, joten edelleen vastaavalla päättelyllä voidaan osoittaa myös, että $a_1 = b_1, a_2 = b_2, \ldots$. Olemme siis osoittaneet, että luvun x ketjumurtolukukehitelmä on yksikäsitteinen. □

Huomautus 2.2.1. Edellisen lauseen todistuksessa tuli esiin se mielenkiintoinen seikka, että

$$\left| x - \frac{p_n}{q_n} \right| < \frac{1}{q_n^2} \ (n = 0, 1, \ldots).$$

Yhtälailla on helppo huomata, että

$$\left| x - \frac{p_n}{q_n} \right| > \frac{1}{q_n(q_{n+1} + q_n)} \ (n = 0, 1, \ldots).$$

Apulause 2.2.2. *Olkoot $\frac{p_k}{q_k}$ $(k = 0, 1, \ldots)$ luvun x konvergentteja. Silloin $x < \frac{p_k}{q_k}$, kun k on parillinen ja $x > \frac{p_k}{q_k}$, kun k on pariton.*

Todistus. Apulauseen 2.1.2 ja lauseen 1.2.1 perusteella

$$\begin{aligned} x - \frac{p_k}{q_k} &= \frac{\varepsilon_{k+1} p_k + p_{k-1}}{\varepsilon_{k+1} q_k + q_{k-1}} - \frac{p_k}{q_k} \\ &= \frac{p_{k-1} q_k - q_{k-1} p_k}{q_k(\varepsilon_k q_k + q_{k-1})} \\ &= \frac{(-1)^k}{q_k(\varepsilon_k q_k + q_{k-1})}. \end{aligned}$$

Koska $q_k(\varepsilon_k q_k + q_{k-1}) > 0$, niin $x - \frac{p_k}{q_k} > 0$, kun k on parillinen ja $x - \frac{p_k}{q_k} < 0$, kun k on pariton. □

Esimerkki 2.2.1. Lasketaan yksinkertaisen päättymättömän ketjumurtoluvun $[1, 1, 1, \ldots]$ arvo.

Ratkaisu saadaan, kun sijoitetaan $x = [1, 1, 1, \ldots]$ ja huomataan, että $x = [1, 1, 1, \ldots] = 1 + \frac{1}{[1,1,1,\ldots]} = 1 + \frac{1}{x}$. Yhtälöstä

$x = 1 + \frac{1}{x}$ saadaan toisen asteen yhtälö $x^2 - x - 1 = 0$, jonka ratkaisut ovat $x_1 = \frac{1+\sqrt{5}}{2}$ ja $x_2 = \frac{1-\sqrt{5}}{2}$. Koska $x_2 < 0$ ja $x_1 > 0$, niin täytyy valita $x = x_1$, koska apulauseen 2.2.1 mukaan $x > 1$. Eli ketjumurtoluvun $[1, 1, 1, \ldots]$ arvo on $\frac{1+\sqrt{5}}{2}$.

Esimerkki 2.2.2. Muodostetaan luvun $\frac{1+\sqrt{5}}{2}$ ketjumurtolukukehitelmä.

Käytetään rekursioyhtälöitä (1), jolloin $\varepsilon_0 = \frac{1+\sqrt{5}}{2}$, $a_0 = \lfloor \frac{1+\sqrt{5}}{2} \rfloor = 1, \varepsilon_1 = \frac{1}{\varepsilon_0 - a_0} = \frac{1}{\frac{1+\sqrt{5}}{2} - 1} = \frac{1}{\frac{\sqrt{5}-1}{2}} = \frac{2}{\sqrt{5}-1} = \frac{2(\sqrt{5}+1)}{5-1} = \frac{1+\sqrt{5}}{2} = \varepsilon_0$. Selvästi $\varepsilon_0 = \varepsilon_1 = \cdots$ ja edelleen $a_0 = a_1 = \cdots$, joten luvun $\frac{1+\sqrt{5}}{2}$ ketjumurtolukukehitelmä on $[1, 1, 1, \ldots]$, kuten pitikin.

§ 2.3. Logaritmien laskemisesta

Määritelmä 2.3.1. Olkoot reaaliluvut b_0 ja b_1 sellaisia, että $b_0 > b_1 > 1$. Määritellään, että n_k on sellainen positiivinen kokonaisluku, että $b_k^{n_k} \leq b_{k-1} < b_k^{n_k+1}$ $(k = 1, 2, \ldots)$, missä $b_k = \frac{b_{k-2}}{b_{k-1}^{n_{k-1}}}$ $(k = 2, 3, \ldots)$.

Lause 2.3.1. *Olkoot luvut* $n_1, n_2, \ldots$ *määritelmän 2.3.1 mukaiset. Silloin* $\log_{b_1} b_0 = [n_1, n_2, \ldots]$.

Todistus. Muodostetaan luvun $\log_{b_1} b_0$ ketjumurtolukukehitelmä $[a_0, a_1, \ldots]$ rekursioyhtälöillä (1). Osoitetaan, että $a_0 = n_1$, $a_1 = n_2, \ldots$. Todistetaan induktiolla. Koska $b_0 = b_1^{[a_0, a_1, \ldots]} = b_1^{a_0} b_1^{\frac{1}{[a_1, a_2, \ldots]}}$, niin $b_1^{a_0} \leq b_0 < b_1^{a_0+1}$, joten $a_0 = n_1$. Edelleen, koska $\frac{b_0}{b_1^{a_0}} = b_2 = b_1^{\frac{1}{[a_1, a_2, \ldots]}}$, niin $b_2^{[a_1, a_2, \ldots]} = b_1$. Valitaan mielivaltainen $k \geq 0$. Tehdään induktio-oletus, että $a_k = n_{k+1}$ ja $b_k = b_{k+1}^{[a_k, a_{k+1}, \ldots]}$. Siis $\frac{b_k}{b_{k+1}^{n_{k+1}}} = b_{k+2} = b_{k+1}^{\frac{1}{[a_{k+1}, a_{k+2}, \ldots]}}$ eli $b_{k+1} = b_{k+2}^{[a_{k+1}, a_{k+2}, \ldots]}$. Täten $b_{k+2}^{a_{k+1}} \leq b_{k+1} < b_{k+2}^{a_{k+1}+1}$, joten $a_{k+1} = n_{k+2}$. Induktioperiaatteen mukaan $a_0 = n_1,\ a_1 = n_2, \ldots$. Siis $\log_{b_1} b_0 = [n_1, n_2, \ldots]$. $\square$

Esimerkki 2.3.1. Lasketaan likiarvo luvulle $\log_2 10$. Muodostetaan luvut $n_1,\ n_2, \ldots$ määritelmän 2.3.1 osoittamalla tavalla. Saadaan

$$2^3 < 10 < 2^4$$

$$\left(\frac{10}{8}\right)^3 < 2 < \left(\frac{10}{8}\right)^4$$

$$\left(\frac{1024}{1000}\right)^9 < \frac{10}{8} < \left(\frac{1024}{1000}\right)^{10}$$

$$\vdots$$

eli lauseen 2.3.1 perusteella $\log_2 10 = [3, 3, 9, \ldots]$. Approksimoidaan lukua $\log_2 10$ konvergentilla $[3, 3, 9]$, joka on yhtä suuri kuin $\frac{93}{28}$. Huomautuksen 2.2.1 perusteella $\left|\log_2 10 - \frac{93}{28}\right| < \frac{1}{28^2} = \frac{1}{784} < 0,002$. Näin luvulle $\log_2 10$ saadaan likiarvo $3,32$.

Luku 3. Jaksolliset ketjumurtoluvut

§ 3.1. Kvadraattiset irrationaaliluvut

Lause 3.1.1. *Olkoon jaksollinen ketjumurtoluku muotoa* $[a_0, a_1, \ldots, a_{k-1}, \overline{a_k, a_{k+1}, \ldots, a_{k+h}}]$. *Olkoon tämän ketjumurtoluvun arvo* α. *Silloin luku* α *on kvadraattinen irrationaaliluku.*

Todistus (vrt. [2], s. 88–89). Apulauseen 2.1.2 mukaan $\alpha = [a_0, a_1, \ldots, a_{n-1}, \varepsilon_n]$ $(n = 0, 1, \ldots)$. Tiedetään myös, että ε_n on irrationaaliluku. Koska ketjumurtoluku on jaksollinen, niin $\varepsilon_n = \varepsilon_{n+h}$, kun $n \geq k$. Ottamalla huomioon rekursioyhtälöt (2) saadaan yhtälö (11)

$$\alpha = \frac{\varepsilon_n p_{n-1} + p_{n-2}}{\varepsilon_n q_{n-1} + q_{n-2}} = \frac{\varepsilon_{n+h} p_{n+h-1} + p_{n+h-2}}{\varepsilon_{n+h} q_{n+h-1} + q_{n+h-2}} = \frac{\varepsilon_n p_{n+h-1} + p_{n+h-2}}{\varepsilon_n q_{n+h-1} + q_{n+h-2}}$$

. Ristiinkertomalla yhtälö (11) saadaan toisen asteen yhtälö

$$a\varepsilon_n^2 + b\varepsilon_n + c = 0, \tag{12}$$

missä

$$\begin{aligned}
a &= q_{n+h-1}p_{n-1} - p_{n+h-1}q_{n-1},\\
b &= q_{n+h-2}p_{n-1} + q_{n+h-1}p_{n-2} - p_{n+h-1}q_{n-2} - p_{n+h-2}q_{n-1},\\
c &= p_{n-2}q_{n+h-2} - q_{n-2}p_{n+h-2},
\end{aligned}$$

joten lauseen 1.3.4 mukaan ε_n on kvadraattinen irrationaaliluku, kun $n \geq k$. Ratkaisemalla yhtälöstä (11) ε_n luvun α suhteen saadaan

$\varepsilon_n = \frac{p_{n-2}-q_{n-2}\alpha}{q_{n-1}\alpha-p_{n-1}}$. Sijoittamalla tämä yhtälöön (12) ja sieventämällä saadaan yhtälö

$$
\begin{aligned}
(aq_{n-2}^2 + cq_{n-1}^2 - bq_{n-2}q_{n-1})\alpha^2 + \\
(bp_{n-2}q_{n-1} + bq_{n-2}p_{n-1} - 2ap_{n-2}q_{n-2} - 2cp_{n-1}q_{n-1})\alpha + \\
(ap_{n-2}^2 + cp_{n-1}^2 + bp_{n-1}p_{n-2}) = 0.
\end{aligned}
$$

Koska luku α on irrationaaliluku, joka toteuttaa kokonaislukukertoimisen toisen asteen yhtälön, niin lauseen 1.3.4 mukaan luku α on kvadraattinen irrationaaliluku. $\square$

Lause 3.1.2. *Olkoon täysin jaksollinen ketjumurtoluku muotoa* $[\overline{a_0, a_1, \ldots, a_k}]$. *Olkoon tämän ketjumurtoluvun arvo* α. *Silloin luku* α *on redusoitu kvadraattinen irrationaaliluku.*

Todistus (vrt. [4], s. 93–95). Merkitään $\beta = [\overline{a_k, a_{k-1}, \ldots, a_0}]$. Eli luku β on täysin jaksollisen ketjumurtoluvun arvo, missä ketjumurtoluvun termit ovat päinvastaisessa järjestyksessä kuin luvun α ketjumurtolukuesityksessä. Koska kyseessä ovat täysin jaksolliset ketjumurtoluvut, niin saadaan yhtälöt $\alpha = \frac{\alpha p_k + p_{k-1}}{\alpha q_k + q_{k-1}}$ ja $\beta = \frac{\beta p'_k + p'_{k-1}}{\beta q'_k + q'_{k-1}}$. Lauseen 1.2.4 yhtälön (7) mukaan $p'_k = p_k$, $q'_k = p_{k-1}$ ja lauseen 1.2.3 yhtälön (6) mukaan $p'_{k-1} = q_k$, $q'_{k-1} = q_{k-1}$. Siis $\beta = \frac{\beta p_k + q_k}{\beta p_{k-1} + q_{k-1}}$. Näin ollen saadaan toisen asteen yhtälöt $q_k\alpha^2 + (p_k - q_{k-1})\alpha - p_{k-1} = 0$ ja $p_{k-1}\beta^2 + (p_k - q_{k-1})\beta - q_k = 0$, joista jälkimmäinen on yhtäpitävä yhtälön $q_k(-\frac{1}{\beta})^2 + (p_k - q_{k-1})(-\frac{1}{\beta}) - p_{k-1} = 0$ kanssa. Koska lukujen α ja β ketjumurtolukuesityksessä kaikki termit ovat positiivisia kokonaislukuja, niin apulauseen 2.2.1 mukaan $\alpha > 1$ ja $\beta > 1$, joten $-1 < -\frac{1}{\beta} < 0$. Koska yhtälöllä $q_k x^2 + (p_k - q_{k-1})x - p_{k-1} = 0$ on ratkaisut α ja $-\frac{1}{\beta}$, niin luku α on redusoitu kvadraattinen irrationaaliluku lauseen 1.3.4 ja määritelmän 1.3.4 perusteella. $\square$

Lause 3.1.3. *Jokainen kvadraattinen irrationaaliluku* α *voidaan esittää jaksollisena ketjumurtolukuna.*

Todistus (vrt. [2], s. 89–91). Koska luku α on kvadraattinen irrationaaliluku, niin luku α toteuttaa lauseen 1.3.3 mukaan kokonaislukukertoimisen toisen asteen yhtälön $ax^2 + bx + c = 0$. Apulauseen 2.1.2

mukaan $\alpha = \frac{\varepsilon_n p_{n-1}+p_{n-2}}{\varepsilon_n q_{n-1}+q_{n-2}}$. Sijoittamalla yhtälöön ja sieventämällä saadaan yhtälö

$$A_n\varepsilon_n^2 + B_n\varepsilon_n + C_n = 0, \tag{13}$$

missä

$$\begin{aligned}
A_n &= ap_{n-1}^2 + bp_{n-1}q_{n-1} + cq_{n-1}^2,\\
B_n &= 2ap_{n-1}p_{n-2} + b(p_{n-1}q_{n-2} + p_{n-2}q_{n-1}) + 2cq_{k-1}q_{k-2},\\
C_n &= ap_{k-2}^2 + bp_{k-2}q_{k-2} + cq_{k-2}^2.
\end{aligned}$$

Osoitetaan seuraavaksi, että on olemassa sellainen positiivinen luku M, että $|A_n| < M$, $|B_n| < M$, $|C_n| < M$. Helposti nähdään, että

$$\begin{aligned}
A_n &= q_{n-1}^2\left(a\left(\frac{p_{n-1}}{q_{n-1}}\right)^2 + b\left(\frac{p_{n-1}}{q_{n-1}}\right) + c\right),\\
C_n &= q_{n-2}^2\left(a\left(\frac{p_{n-2}}{q_{n-2}}\right)^2 + b\left(\frac{p_{n-2}}{q_{n-2}}\right) + c\right).
\end{aligned}$$

Merkitään $u = \frac{p_{n-1}}{q_{n-1}}$ ja $v = \alpha$. Kun otetaan huomioon, että $a\alpha^2 + b\alpha + c = 0$, niin apulauseen 1.3.1 perusteella $A_n = q_{n-1}^2\left(\frac{p_{n-1}}{q_{n-1}} - \alpha\right)\left(2a\alpha + b + a\left(\frac{p_{n-1}}{q_{n-1}} - \alpha\right)\right)$. Nyt huomautuksen 2.2.1 mukaan $\left|\alpha - \frac{p_{n-1}}{q_{n-1}}\right| < \frac{1}{q_{n-1}^2}$, joten

$$|A_n| < |2a\alpha + b| + \frac{|a|}{q_{n-1}^2} \leq |2a\alpha + b| + |a|.$$

Aivan vastaavasti osoitetaan, että

$$|C_n| < |2a\alpha + b| + \frac{|a|}{q_{n-2}^2} \leq |2a\alpha + b| + |a|.$$

Suoraan laskemalla voidaan osoittaa helposti, että $B_n^2 - 4A_nC_n = b^2 - 4ac$. Siis

$$|B_n| < \sqrt{|b^2 - 4ac| + 4(|2a\alpha + b| + |a|)^2}.$$

Nyt kun merkitään

$$M = \max\left\{|2a\alpha + b| + |a|, \sqrt{|b^2 - 4ac| + 4(|2a\alpha + b| + |a|)^2}\right\},$$

niin $|A_n| < M$, $|B_n| < M$, $|C_n| < M$. Nyt selvästikin yhtälöitä (13) on korkeintaan $(2M+1)^3$ kappaletta, joten Dirichletin laatikkoperiaatteen mukaan on olemassa vähintään 3 sellaista indeksin arvoa n_1, n_2, n_3, että

$$\begin{aligned} A_{n_1} &= A_{n_2} = A_{n_3}, \\ B_{n_1} &= B_{n_2} = B_{n_3}, \\ C_{n_1} &= C_{n_2} = C_{n_3}. \end{aligned}$$

Koska yhtälöllä $A_{n_1}x^2 + B_{n_1}x + C_{n_1} = 0$ on vain kaksi ratkaisua, niin kahden luvuista ε_{n_1}, ε_{n_2}, ε_{n_3} täytyy olla yhtä suuret. Olkoon nyt merkinnät valittu siten, että $\varepsilon_{n_1} = \varepsilon_{n_2}$ ja $n_1 < n_2$. Merkitään $h = n_2 - n_1$. Siis $\varepsilon_{n_1} = \varepsilon_{n_1+h}$ ja $a_{n_1} = a_{n_1+h}$. Nyt rekursioyhtälöiden (1) perusteella $\varepsilon_{n_1+1} = \frac{1}{\varepsilon_{n_1} - a_{n_1}} = \frac{1}{\varepsilon_{n_1+h} - a_{n_1+h}} = \varepsilon_{n_1+h+1}$. Toistamalla tätä päättelyä huomataan, että $\varepsilon_{k+h} = \varepsilon_k$ aina, kun $k \geq n_1$, joten myös $a_{k+h} = a_k$ aina, kun $k \geq n_1$. Määritelmän 1.1.4 mukaan kyseinen ketjumurtoluku on siis jaksollinen. $\square$

Lause 3.1.4. *Jokainen redusoitu kvadraattinen irrationaaliluku x voidaan esittää täysin jaksollisena ketjumurtolukuna.*

Todistus. Koska x on redusoitu kvadraattinen irrationaaliluku, niin $-1 < \overline{x} < 0$. Rekursioyhtälöiden (1) mukaan $\varepsilon_k = a_k + \frac{1}{\varepsilon_{k+1}}$, joten $\overline{\varepsilon}_k = \overline{a_k + \frac{1}{\varepsilon_{k+1}}} = \overline{a}_k + \frac{1}{\overline{\varepsilon}_{k+1}} = a_k + \frac{1}{\overline{\varepsilon}_{k+1}}$. Todistetaan induktiolla, että $-1 < \overline{\varepsilon}_k < 0$ $(k = 0, 1, \ldots)$. Kun $k = 0$, niin $-1 < \overline{\varepsilon}_0 = \overline{x} < 0$. Valitaan mielivaltainen $n \in \mathbf{N}$. Tehdään induktio-oletus, että $-1 < \overline{\varepsilon}_n < 0$. Koska $\overline{\varepsilon}_n - a_n < -1$, niin $-1 < \overline{\varepsilon}_{n+1} = \frac{1}{\overline{\varepsilon}_n - a_n} < 0$, joten induktioperiaatteen mukaan väite on todistettu. Koska $a_k - \overline{\varepsilon}_k = -\frac{1}{\overline{\varepsilon}_{k+1}}$ ja $-1 < \overline{\varepsilon}_k < 0$, niin $a_k = \lfloor a_k - \overline{\varepsilon}_k \rfloor = \left\lfloor -\frac{1}{\overline{\varepsilon}_{k+1}} \right\rfloor$, kun $k \geq 0$. Oletetaan, että ketjumurtolukukehitelmä ei ole täysin jaksollinen. Tiedetään kuitenkin lauseen 3.1.3 mukaan, että kyseinen ketjumurtoluku on jaksollinen. Olkoon ketjumurtolukukehitelmä nyt jaksollinen indeksin arvosta k, joka on > 0 ja olkoon jakson pituus h. Siis $\varepsilon_k = \varepsilon_{k+h}$ ja $a_k = a_{k+h}$. Edelleen myös $\overline{\varepsilon}_k = \overline{\varepsilon}_{k+h}$. Nyt tiedetään, että $a_{k-1} = \left\lfloor -\frac{1}{\bar{\varepsilon}_k} \right\rfloor = \left\lfloor -\frac{1}{\bar{\varepsilon}_{k+h}} \right\rfloor = a_{k+h-1}$, joten ketjumurtoluku olisi jaksollinen indeksin arvosta $k-1$, joka on ristiriidassa oletuksen kanssa, joten $k = 0$. $\square$

§ 3.2. Luvun $\sqrt{N}$ ketjumurtolukukehitelmä

Tässä pykälässä oletamme, että luku $N \in \mathbf{Z}_+$ sekä luku N ei ole täydellinen neliö. Siis luku $\sqrt{N}$ on irrationaaliluku, joten sillä on päättymätön yksinkertainen ketjumurtolukukehitelmä. Tulemme tarkastelemaan tätä ketjumurtolukukehitelmää.

Apulause 3.2.1. *Luvun $\sqrt{N}$ ketjumurtolukukehitelmä on jaksollinen ja muotoa $[a_0, \overline{a_1, \ldots, a_n, 2a_0}]$.*

Todistus. Rekursioyhtälöiden (1) perusteella $a_0 = \lfloor \sqrt{N} \rfloor$. Koska luku $\sqrt{N} + \lfloor \sqrt{N} \rfloor$ on selvästikin redusoitu kvadraattinen irrationaaliluku, niin luvulla $\sqrt{N} + \lfloor \sqrt{N} \rfloor$ on lauseen 3.1.4 mukaan täysin jaksollinen ketjumurtolukukehitelmä. Olkoon $\sqrt{N} + \lfloor \sqrt{N} \rfloor = [\overline{a'_0, a'_1, \ldots, a'_n}]$. On helppo todeta, että $a'_0 = 2a_0$. Siis $\sqrt{N} = [a_0, \overline{a'_1, \ldots, a'_n, a'_0}]$. Nyt kun muutetaan merkintöjä siten, että $a'_1 = a_1$, $a'_2 = a_2, \ldots, a'_n = a_n$, niin saadaan yhtälö $\sqrt{N} = [a_0, \overline{a_1, a_2, \ldots, a_n, 2a_0}]$. $\square$

Rekursioyhtälöillä (1) voitaisiin muodostaa luvun $\sqrt{N}$ ketjumurtolukukehitelmä, mutta tulemme käyttämään rekursioyhtälöitä (3).

Apulause 3.2.2. *Rekursioyhtälöille (3) on voimassa yhtälö*

$$B_n^2 + C_n C_{n-1} = N \ (n = -1, 0, 1, 2, \ldots). \tag{14}$$

Todistus. Todistetaan induktiolla indeksin n suhteen. Kun $n = -1$, niin $B_{-1}^2 + C_{-1}C_{-2} = 0^2 + 1 \cdot N = N$, joten tässä tapauksessa väite on tosi. Valitaan mielivaltainen $k \in \{-1, 0, 1, 2, \ldots\}$. Tehdään induktio-oletus, että $B_k^2 + C_k C_{k-1} = N$. Rekursioyhtälöiden (3) sekä induktio-oletuksen perusteella

$$\begin{aligned}
&B_{k+1}^2 + C_{k+1}C_k \\
&= (A_{k+1}C_k - B_k)^2 + (C_{k-1} + A_{k+1}(B_k - B_{k+1}))C_k \\
&= A_{k+1}^2 C_k^2 - 2A_{k+1}C_kB_k + B_k^2 + C_kC_{k-1} \\
&\quad + A_{k+1}B_kC_k - A_{k+1}B_{k+1}C_k \\
&= A_{k+1}C_k(A_{k+1}C_k - (B_{k+1} + B_k)) + B_k^2 + C_kC_{k-1} \\
&= A_{k+1}C_k(A_{k+1}C_k - A_{k+1}C_k) + B_k^2 + C_kC_{k-1} \\
&= B_k^2 + C_kC_{k-1} = N,
\end{aligned}$$

joten induktioperiaatteen mukaan väite on tosi. □

Lause 3.2.1. *Olkoot $A_0, A_1, \ldots$ saatu rekursioyhtälöistä (3). Silloin $\sqrt{N} = [A_0, A_1, \ldots]$.*

Todistus. Tiedetään, että rekursioyhtälöillä (1) saadaan luvulle $\sqrt{N}$ ketjumurtolukukehitelmä $[a_0, a_1, \ldots]$, joten riittää osoittaa, että $a_0 = A_0,\ a_1 = A_1, \cdots$. Todistetaan induktiolla. Rekursioyhtälöiden (1) ja (3) mukaan
$a_0 = \lfloor \sqrt{N} \rfloor = \left\lfloor \frac{\sqrt{N}+0}{1} \right\rfloor = \left\lfloor \frac{\sqrt{N}+B_{-1}}{C_{-1}} \right\rfloor = A_0$. Lisäksi $\frac{\sqrt{N}+B_{-1}}{C_{-1}} = \varepsilon_0$.
Valitaan mielivaltainen $n \in \mathbf{N}$. Tehdään induktio-oletus, että
$a_n = A_n$ ja $\frac{\sqrt{N}+B_{n-1}}{C_{n-1}} = \varepsilon_n$. Nyt rekursioyhtälöiden (1) ja (3), induktio-oletuksen ja apulauseen 3.2.2 perusteella

$$\begin{aligned}
\varepsilon_{n+1} &= \frac{1}{\varepsilon_n - a_n} = \frac{1}{\frac{\sqrt{N}+B_{n-1}}{C_{n-1}} - A_n} \\
&= \frac{1}{\frac{\sqrt{N}+B_{n-1}-A_nC_{n-1}}{C_{n-1}}} = \frac{1}{\frac{\sqrt{N}-B_n}{C_{n-1}}} \\
&= \frac{C_{n-1}(\sqrt{N}+B_n)}{N - B_n^2} = \frac{C_{n-1}(\sqrt{N}+B_n)}{C_nC_{n-1}} \\
&= \frac{\sqrt{N}+B_n}{C_n}.
\end{aligned}$$

Siis $a_{n+1} = \lfloor \varepsilon_{n+1} \rfloor = \left\lfloor \frac{\sqrt{N}+B_n}{C_n} \right\rfloor = A_{n+1}$, joten induktioperiaatteen mukaan väite on tosi. □

Seuraavaksi tutkitaan hieman tarkemmin rekursioyhtälöiden (3) lukuja B_k ja C_k. Määritelmästä 1.1.9 huomataan suoraan, että $B_k, C_k \in \mathbf{Z}$. Esitetään seuraavaksi muutama apulause lukuja B_k ja C_k koskien.

Apulause 3.2.3. *Rekursioyhtälöille (3) on voimassa seuraavat epäyhtälöt*

$$0 < A_n \leq 2A_0,\ 0 < B_n \leq A_0,\ 0 < C_n \leq 2A_0. \tag{15}$$

Todistus (vrt. [5], s. 182–183). Todistetaan induktiolla indeksin n suhteen. Kun $n = 0$, niin $0 < A_0 < 2A_0$, $0 < B_0 = A_0$, $0 < C_0 = N - A_0^2 \leq 2A_0$, joten tässä tapauksessa väite on tosi. Valitaan mielivaltainen $k \in \mathbf{N}$. Tehdään induktio-oletus, että $0 < A_k \leq 2A_0$, $0 < B_k \leq A_0$, $0 < C_k \leq 2A_0$. Lauseen 3.2.1 perusteella $A_{k+1} > 0$. Koska $\varepsilon_{k+1} - A_{k+1} = \frac{\sqrt{N}+B_k}{C_k} - A_{k+1} = \frac{\sqrt{N}+B_k - A_{k+1}C_k}{C_k} = \frac{\sqrt{N}-B_{k+1}}{C_k} > 0$, niin $B_{k+1} \leq A_0 < \sqrt{N}$. Apulauseen 3.2.2 mukaan $B_{k+1}^2 + C_{k+1}C_k = N$, joten $C_{k+1} > 0$. Koska $\varepsilon_{k+2} = \frac{\sqrt{N}+B_{k+1}}{C_{k+1}} > 1$, niin $C_{k+1} \leq 2A_0 < 2\sqrt{N}$. Oletetaan, että $B_{k+1} \leq 0$. Silloin $C_k \leq A_{k+1}C_k \leq B_k < \sqrt{N}$, joten $\varepsilon_{k+1} - A_{k+1} = \frac{\sqrt{N}-B_{k+1}}{C_k} \geq \frac{\sqrt{N}}{C_k} > \frac{\sqrt{N}}{\sqrt{N}} = 1$, joka on mahdotonta, koska $0 < \varepsilon_{k+1} - A_{k+1} < 1$. Siis $B_{k+1} > 0$. Koska $C_k \geq 1$ ja $B_k \leq A_0$, niin $A_{k+1} \leq 2A_0$. Siis induktioperiaatteen mukaan väite on tosi. $\square$

Apulause 3.2.4. *Rekursioyhtälöissä (3) $A_{n+1} = 2A_0$, jos ja vain jos $C_n = 1$.*

Todistus. Oletetaan, että $A_{n+1} = 2A_0$. Eli $2A_0 = A_{n+1} = \left\lfloor \frac{\sqrt{N}+B_n}{C_n} \right\rfloor = \left\lfloor \frac{A_0+B_n}{C_n} \right\rfloor \leq \frac{A_0+B_n}{C_n} \leq \frac{2A_0}{C_n}$, joten $C_n \leq 1$. Koska $1 \leq C_n \leq 1$, niin $C_n = 1$. Oletetaan nyt, että $C_n = 1$. Apulauseen 3.2.3 mukaan $C_{n-1} < 2\sqrt{N}$. Apulauseen 3.2.2 perusteella $C_{n-1} = N - B_n^2 = (\sqrt{N}+B_n)(\sqrt{N}-B_n)$. Siis $(\sqrt{N}+B_n)(\sqrt{N}-B_n) < 2\sqrt{N}$ eli $\sqrt{N}-B_n < \frac{2\sqrt{N}}{\sqrt{N}+B_n} < \frac{2\sqrt{N}}{\sqrt{N}} = 2$, joten $B_n \geq A_0 - 1$. Oletetaan nyt, että $B_n = A_0 - 1$. Silloin, koska $N - A_0^2 \geq 1$, niin $C_{n-1} = N - B_n^2 = N - (A_0-1)^2 = N - A_0^2 + 2A_0 - 1 \geq 1 + 2A_0 - 1 = 2A_0$, joten

$C_{n-1} = 2A_0$. Nyt $A_n = \left\lfloor \frac{A_0+B_{n-1}}{C_{n-1}} \right\rfloor \leq \left\lfloor \frac{A_0+A_0}{2A_0} \right\rfloor = 1$, joten $A_n = 1$ ja $B_{n-1} = A_0$. Rekursioyhtälöiden (3) mukaan $B_n = A_n C_{n-1} - B_{n-1} = A_0$, joka on mahdotonta, koska oletettiin, että $B_n = A_0 - 1$, joten $B_n = A_0$. Siis $A_{n+1} = \left\lfloor \frac{A_0+B_n}{C_n} \right\rfloor = A_0 + A_0 = 2A_0$. □

Apulause 3.2.5. *Luvun $\sqrt{N}$ ketjumurtolukukehitelmässä $[A_0, \overline{A_1, A_2, \ldots, A_n, 2A_0}]$ on voimassa epäyhtälöt $A_0, A_1, \ldots, A_n < 2A_0$.*

Todistus. Tiedetään, että $\varepsilon_1 = \frac{\sqrt{N}+B_0}{C_0} = \frac{\sqrt{N}+A_0}{N-A_0^2}$. Koska $A_{n+1} = 2A_0$, niin apulauseen 3.2.4 nojalla $B_n = A_0$ ja $C_n = 1$. Rekursioyhtälöiden (3) perusteella $B_{n+1} = 2A_0 - A_0 = A_0$. Apulauseen 3.2.2 perusteella $C_{n+1} = N - B_{n+1}^2 = N - A_0^2$. Siis $\varepsilon_{n+1} = \frac{\sqrt{N}+B_{n+1}}{C_{n+1}} = \frac{\sqrt{N}+A_0}{N-A_0^2} = \varepsilon_1$. Täten huomataan, että ketjumurtoluvussa uusi jakso alkaa heti sen osanimittäjän jälkeen, jonka arvo on $= 2A_0$, joten $A_0, A_1, \ldots, A_n < 2A_0$. □

Apulause 3.2.6. *Luvun $\sqrt{N}$ ketjumurtolukukehitelmässä $[A_0, \overline{A_1, A_2, \ldots, A_n, 2A_0}]$ indeksille n on voimassa epäyhtälö $n < 2N$.*

Todistus. Koska $B_k < \sqrt{N}$ ja $C_k < 2\sqrt{N}$ $(k = 0, 1, \ldots)$, niin erisuuria lukuja $\frac{\sqrt{N}+B_k}{C_k}$ on vähemmän kuin $\sqrt{N} \cdot 2\sqrt{N}$ kappaletta. Siis ketjumurtoluvun jakson pituus $n+1$ on pienempi kuin $2N$. Eli saadaan epäyhtälö $n < 2N$. □

Esimerkki 3.2.1. Muodostetaan luvun $\sqrt{11}$ ketjumurtolukukehitelmä. Käyttämällä rekursioyhtälöitä (3) saadaan kaavio

n	0	1	2	3
B_n	3	3	3	3
C_n	2	1	2	1
A_n	3	3	6	3.

Täten $\sqrt{11} = [3, \overline{3, 6}]$.

Luku 4. Irrationaalilukujen rationaaliluku approksimoinnista

§ 4.1. Approksimointi konvergenteilla

Apulause 4.1.1. *Olkoon x irrationaaliluku. Olkoot $\frac{p_k}{q_k}$ $(k = 0, 1, 2, \ldots)$ luvun x ketjumurtolukukehitelmän $[a_0, a_1, \ldots]$ konvergentteja. Silloin on voimassa epäyhtälö*

$$|q_n x - p_n| < |q_{n-1} x - p_{n-1}|, \text{ kun } n \geq 1. \tag{16}$$

Todistus. Apulauseen 2.1.2 ja rekursioyhtälöiden (2) perusteella $\left|x - \frac{p_n}{q_n}\right| = \frac{1}{q_n(\varepsilon_{n+1}q_n + q_{n-1})}$, josta edelleen saadaan yhtälö $|q_n x - p_n| = \frac{1}{q_n \varepsilon_{n+1} + q_{n-1}}$. Koska $q_n \varepsilon_{n+1} + q_{n-1} > q_n a_{n+1} + q_{n-1} = q_{n+1}$ ja $q_n \varepsilon_{n+1} + q_{n-1} < q_n(a_{n+1} + 1) + q_{n-1} = q_{n+1} + q_n \leq q_{n+2}$, niin $\frac{1}{q_{n+2}} < |q_n x - p_n| < \frac{1}{q_{n+1}}$. Koska luvut q_k $(k = 0, 1, \ldots)$ muodostavat kasvavan lukujonon, niin $|q_n x - p_n| < \frac{1}{q_{n+1}} < |q_{n-1} x - p_{n-1}|$. □

Epäyhtälöstä (16) saadaan, kun merkitään $c_n = \frac{p_n}{q_n}$ ja $c_{n-1} = \frac{p_{n-1}}{q_{n-1}}$ myös epäyhtälö

$$|x - c_n| < |x - c_{n-1}|. \tag{17}$$

Lause 4.1.1. *Olkoon $\frac{p_k}{q_k}$ luvun x konvergentti, missä $k > 0$. Olkoon $\frac{p}{q}$ sellainen rationaaliluku, että $0 < q \leq q_k$ ja $\frac{p}{q} \neq \frac{p_k}{q_k}$. Silloin on voimassa epäyhtälö*

$$|q_k x - p_k| \leq |qx - p|. \tag{18}$$

Todistus (vrt. [2], s. 93–94). Oletetaan ensin, että $q_k = q$. Silloin $\left|\frac{p_k}{q_k} - \frac{p}{q}\right| = \left|\frac{p_k}{q_k} - \frac{p}{q_k}\right| = \left|\frac{p_k - p}{q_k}\right| \geq \frac{1}{q_k}$, koska $p_k \neq p$. Toisaalta $\left|x - \frac{p_k}{q_k}\right| = \frac{1}{q_k(\varepsilon_k q_k + q_{k-1})} \leq \frac{1}{q_k q_{k+1}} \leq \frac{1}{2q_k}$, koska apulauseen 1.2.2 mukaan $q_{k+1} \geq q_2 \geq 2$. Näiden epäyhtälöiden perusteella $\frac{1}{q_k} \leq \left|\frac{p_k}{q_k} - \frac{p}{q}\right| \leq \left|x - \frac{p_k}{q_k}\right| + \left|x - \frac{p}{q}\right| \leq \left|x - \frac{p}{q}\right| + \frac{1}{2q_k}$, josta edelleen $\left|x - \frac{p_k}{q_k}\right| \leq \frac{1}{2q_k} \leq \left|x - \frac{p}{q}\right|$. Koska oletettiin, että $q = q_k$, niin $|q_k x - p_k| \leq |qx - p|$. Mikäli $q = q_0 = 1 < q_1$, niin ainoat mahdolliset luvun p arvot ovat $\lceil x \rceil$ ja $\lfloor x \rfloor$, jotta $|x - p| < 1$. Tämä on välttämätöntä, koska $\left|x - \frac{p_k}{q_k}\right| < 1$. Jos nyt $p = \lfloor x \rfloor = p_0$, niin apulauseen 4.1.1 perusteella $|q_k x - p_k| < |q_0 x - p_0| = |qx - p|$. Jos taas $p = \lceil x \rceil$, niin koska $\frac{p_1}{q_1} > x$ ja $\frac{p_1}{q_1} = a_0 + \frac{1}{a_1} \leq a_0 + \frac{1}{2}$, niin $|qx - p| > |q_0 x - p_0| > |q_k x - p_k|$. Jatkossa voidaan siis olettaa, että $q > 1$. Lisäksi lause on osoitettu todeksi siinä tapauksessa, että jos $q = q_k$, kun $k \geq 1$. Voidaan siis olettaa, että on olemassa sellainen indeksin arvo n, että $q_{n-1} < q < q_n \leq q_k$. Voidaan myös olettaa, että lukujen p ja q suurin yhteinen tekijä on 1. Määritellään yhtälöryhmä

$$\begin{aligned} up_n + vp_{n-1} &= p, \\ uq_n + vq_{n-1} &= q. \end{aligned}$$

Ratkaisemalla yhtälöryhmästä luvut u ja v saadaan ratkaisut $u = (-1)^{n+1}(pq_{n-1} - p_{n-1}q)$ ja $v = (-1)^{n+1}(p_n q - pq_n)$. Koska $\frac{p}{q}$ ei ole luvun x konvergentti, niin sekä $u \neq 0$ että $v \neq 0$. Oletetaan, että $u > 0$. Koska $q = uq_n + vq_{n-1} < q_n$, niin $q - uq_n = vq_{n-1} < 0$. Siis $v < 0$. Oletetaan, että $u < 0$. Koska $vq_{n-1} = q_n - uq_n > 0$, niin $v > 0$. Siis luvut u ja v ovat erimerkkisiä. Apulauseen 2.2.2 perusteella myös luvut $q_n x - p_n$ ja $q_{n-1}x - p_{n-1}$ ovat erimerkkisiä. Siis luvut $u(q_n x - p_n)$ ja $v(q_{n-1}x - p_{n-1})$ ovat samanmerkkisiä. Koska $qx - p = u(q_n x - p_n) + v(q_{n-1}x - p_{n-1})$, niin

$$\begin{aligned} |qx - p| &= |u(q_n x - p_n) + v(q_{n-1}x - p_{n-1})| \\ &= |u(q_n x - p_n)| + |v(q_{n-1}x - p_{n-1})| \\ &> |v(q_{n-1}x - p_{n-1})| \\ &\geq |q_{n-1}x - p_{n-1}|. \end{aligned}$$

Siis apulauseen 4.1.1 perusteella

$$\begin{aligned} |qx - p| &> |q_{n-1}x - p_{n-1}| \\ &> |q_n x - p_n| \\ &\geq |q_k x - p_k|. \end{aligned}$$

□

Lause 4.1.2. *Jos* $\left|x - \frac{p}{q}\right| < \frac{1}{2q^2}$, *niin* $\frac{p}{q}$ *on luvun* x *ketjumurtolukukehitelmän konvergentti.*

Todistus (vrt. [2], s. 94). Oletetaan, että luku $\frac{p}{q}$ ei ole luvun x konvergentti. Silloin on olemassa sellainen indeksi k, että $q_{k-1} \leq q < q_k$. Lauseen 4.1.1 todistuksesta nähdään, että $|q_{k-1}x - p_{k-1}| \leq |qx - p|$. Koska $|qx - p| < \frac{1}{2q}$, niin $\left|x - \frac{p_{k-1}}{q_{k-1}}\right| < \frac{1}{2qq_{k-1}}$. Koska $q \geq q_{k-1}$, niin $\left|x - \frac{p}{q}\right| < \frac{1}{2q^2} \leq \frac{1}{2qq_{k-1}}$. Nyt

$$\begin{aligned} \left|\frac{p}{q} - \frac{p_{k-1}}{q_{k-1}}\right| &= \left|x - x + \frac{p}{q} - \frac{p_{k-1}}{q_{k-1}}\right| \\ &\leq \left|x - \frac{p}{q}\right| + \left|x - \frac{p_{k-1}}{q_{k-1}}\right| \\ &< \frac{1}{qq_{k-1}}, \end{aligned}$$

mutta toisaalta

$$\begin{aligned} \left|\frac{p}{q} - \frac{p_{k-1}}{q_{k-1}}\right| &= \left|\frac{pq_{k-1} - qp_{k-1}}{qq_{k-1}}\right| \\ &\geq \frac{1}{qq_{k-1}}. \end{aligned}$$

Tämän ristiriidan perusteella $\frac{p}{q}$ on luvun x konvergentti. □

Lause 4.1.3. *Olkoon* $c \in (0, 1)$. *Silloin on olemassa sellainen* $x \in \mathbf{R}$, *että luvun* x *ketjumurtolukukehitelmässä on sellainen konvergentti* $\frac{p_k}{q_k}$, *että* $\left|x - \frac{p_k}{q_k}\right| > \frac{c}{q_k^2}$.

Todistus (vrt. [1], s. 29). Merkitään $n = \left[\frac{2}{\frac{1}{c} - 1}\right] + 1$. Siis $n > \frac{2}{\frac{1}{c}-1}$, joten $\frac{2}{n} < \frac{1}{c} - 1$. Edellisen perusteella $\frac{1}{1+\frac{2}{n}} > c$. Valitaan

$x = [0, n, 1, n]$. Lauseen 2.1.1 mukaan $x \in \mathbf{R}$ ja $\frac{p_3}{q_3} = x$. Koska

$$\begin{aligned} \left| x - \frac{p_1}{q_1} \right| &= \left| \frac{p_3}{q_3} - \frac{p_1}{q_1} \right| \\ &= \frac{1}{n(n+2)} \\ &= \frac{1}{q_1^2(1+\frac{2}{n})} \\ &> \frac{c}{q_1^2}, \end{aligned}$$

niin väite on tosi. $\square$

Lause 4.1.4. *Olkoot luvut* $\frac{p_k}{q_k}$ *ja* $\frac{p_{k-1}}{q_{k-1}}$ *luvun* x *peräkkäiset konvergentit. Silloin on voimassa ainakin toinen epäyhtälöistä* $\left| x - \frac{p_k}{q_k} \right| < \frac{1}{2q_k^2}$ *ja* $\left| x - \frac{p_{k-1}}{q_{k-1}} \right| < \frac{1}{2q_{k-1}^2}$.

Todistus (vrt. [1], s. 30). Koska luku x on lauseen 2.2.2 mukaan lukujen $\frac{p_k}{q_k}$ ja $\frac{p_{k-1}}{q_{k-1}}$ välissä, niin $\left| x - \frac{p_k}{q_k} \right| + \left| x - \frac{p_{k-1}}{q_{k-1}} \right| = \left| \frac{p_k}{q_k} - \frac{p_{k-1}}{q_{k-1}} \right|$. Yhtälön (5) perusteella $\left| \frac{p_k}{q_k} - \frac{p_{k-1}}{q_{k-1}} \right| = \frac{1}{q_k q_{k+1}} < \frac{1}{q_k q_{k-1}}$. Koska lukujen $\frac{1}{q_k^2}$ ja $\frac{1}{q_{k-1}^2}$ geometrinen keskiarvo on pienempi tai yhtä suuri kuin niiden aritmeettinen keskiarvo, niin $\frac{1}{q_k q_{k-1}} \le \frac{1}{2q_k^2} + \frac{1}{2q_{k-1}^2}$, joten $\left| x - \frac{p_k}{q_k} \right| + \left| x - \frac{p_{k-1}}{q_{k-1}} \right| < \frac{1}{2q_k^2} + \frac{1}{2q_{k-1}^2}$. Jos nyt $\left| x - \frac{p_k}{q_k} \right| \ge \frac{1}{2q_k^2}$, niin $\left| x - \frac{p_{k-1}}{q_{k-1}} \right| < \frac{1}{2q_{k-1}^2}$. $\square$

Apulause 4.1.2. *Määritellään* $\varphi_k = \frac{q_{k-2}}{q_{k-1}}$ *ja* $\psi_k = \varphi_k + \varepsilon_k$, *kun* $k \ge 1$. *Kun* $k \ge 2$, $\psi_k \le \sqrt{5}$ *ja* $\psi_{k-1} \le \sqrt{5}$, *niin* $\varphi_k > \frac{\sqrt{5}-1}{2}$.

Todistus. Lauseen 1.2.3 perusteella $\frac{1}{\varphi_{n+1}} = \frac{q_n}{q_{n-1}} = a_n + \varphi_n$, kun $n \ge 1$. Koska $\varepsilon_n = a_n + \frac{1}{\varepsilon_{n+1}}$, niin $\frac{1}{\varphi_{n+1}} + \frac{1}{\varepsilon_{n+1}} = \varphi_n + \varepsilon_n = \psi_n$. Oletusten mukaan $\psi_k \le \sqrt{5}$ ja $\psi_{k-1} \le \sqrt{5}$, joten $\varphi_k + \varepsilon_k \le \sqrt{5}$ ja $\frac{1}{\varphi_k} + \frac{1}{\varepsilon_k} \le \sqrt{5}$. Täten $(\sqrt{5} - \varphi_k)\left(\sqrt{5} - \frac{1}{\varphi_k}\right) \ge 1$ ja koska $\varphi_k \in \mathbf{Q}$, niin $5 - \sqrt{5}\left(\varphi_k + \frac{1}{\varphi_k}\right) > 0$. Edellisen perusteella $\varphi^2 - \sqrt{5}\varphi_k < -1$, joka on yhtäpitävä epäyhtälön

$$
\begin{aligned}
\left(\frac{\sqrt{5}}{2}-\varphi_k\right)^2 &= \varphi^2-\sqrt{5}\varphi_k+\left(\frac{\sqrt{5}}{2}\right)^2 \\
&< -1+\left(\frac{\sqrt{5}}{2}\right)^2 \\
&= \frac{1}{4}
\end{aligned}
$$

kanssa. Eli $\frac{\sqrt{5}}{2}-\varphi_k<\frac{1}{2}$, josta saadaan $\varphi_k>\frac{\sqrt{5}-1}{2}$. □

Lause 4.1.5. *Olkoot luvut $\frac{p_k}{q_k}$, $\frac{p_{k-1}}{q_{k-1}}$ ja $\frac{p_{k-2}}{q_{k-2}}$ luvun x peräkkäiset konvergentit. Silloin on voimassa ainakin yksi epäyhtälöistä $\left|x-\frac{p_k}{q_k}\right|<\frac{1}{\sqrt{5}q_k^2}$, $\left|x-\frac{p_{k-1}}{q_{k-1}}\right|<\frac{1}{\sqrt{5}q_{k-1}^2}$ ja $\left|x-\frac{p_{k-2}}{q_{k-2}}\right|<\frac{1}{\sqrt{5}q_{k-2}^2}$.*

Todistus (vrt. [1], s. 31-33). Olkoot luvut φ_k ja ψ_k määritelty kuten apulauseessa 4.1.2. Tehdään vasta-oletus, että $\left|x-\frac{p_n}{q_n}\right|\geq\frac{1}{\sqrt{5}q_n^2}$ $(n=k-2,k-1,k)$. Apulauseen 2.1.2 perusteella

$$
\begin{aligned}
\left|x-\frac{p_n}{q_n}\right| &= \left|\frac{\varepsilon_{n+1}p_n+p_{n-1}}{\varepsilon_{n+1}q_n+q_{n-1}}\right| \\
&= \frac{1}{q_n(\varepsilon_{n+1}q_n+q_{n-1})} \\
&= \frac{1}{q_n^2\left(\varepsilon_{n+1}+\frac{q_{n-1}}{q_n}\right)} \\
&= \frac{1}{q_n^2\left(\varepsilon_{n+1}+\varphi_{n+1}\right)} \\
&= \frac{1}{q_n^2\psi_{n+1}}.
\end{aligned}
$$

Nyt oletuksen perusteella $\psi_{n+1}\leq\sqrt{5}$ $(n=k-2,k-1,k)$, joten apulauseen 4.1.2 perusteella $\varphi_k>\frac{\sqrt{5}-1}{2}$ ja $\varphi_{k+1}>\frac{\sqrt{5}-1}{2}$. Nyt $a_k=\frac{1}{\varphi_{k+1}}-\varphi_k<\frac{2}{\sqrt{5}-1}-\frac{\sqrt{5}-1}{2}=1$, joka on mahdotonta, koska $a_k\in\mathbf{Z}_+$.

Siis vasta-oletus hylätään, joten väite on tosi. $\square$

Lause 4.1.6. *Olkoon $c \in \left(0, \frac{1}{\sqrt{5}}\right)$. Silloin on olemassa sellainen $x \in \mathbf{R} \setminus \mathbf{Q}$, että vain äärellinen määrä luvun x konvergentteja $\frac{p_k}{q_k}$ toteuttaa epäyhtälön $\left|x - \frac{p_k}{q_k}\right| < \frac{c}{q_k^2}$.*

Todistus (vrt. [1], s. 33–34). Merkitään $x = [1, 1, 1, \ldots]$. Esimerkin 2.2.1 perusteella $x = \frac{\sqrt{5}+1}{2}$. Selvästikin $\varepsilon_n = x$ $(n = 0, 1, \ldots)$, joten on voimassa yhtälö $x = \frac{xp_n + p_{n-1}}{xq_n + q_{n-1}}$. Siis on voimassa yhtälö $\left|x - \frac{p_n}{q_n}\right| = \frac{1}{q_n(xq_n + q_{n-1})} = \frac{1}{q_n^2\left(x + \frac{q_{n-1}}{q_n}\right)}$. Lauseen 1.2.3 mukaan $\frac{q_n}{q_{n-1}} = \overbrace{[1, 1, \ldots, 1]}^{n \text{ kpl}}$. Nyt tiedetään, että $\lim_{n\to\infty} \frac{q_n}{q_{n-1}} = x$, joten $\frac{q_{n-1}}{q_n} = \frac{1}{x} + \xi_n = \frac{\sqrt{5}-1}{2} + \xi_n$, missä $\lim_{n\to\infty} \xi_n = 0$. Siis $\left|x - \frac{p_n}{q_n}\right| = \frac{1}{q_n^2\left(\frac{\sqrt{5}-1}{2} + \frac{\sqrt{5}-1}{2} + \xi_n\right)} = \frac{1}{q_n^2\left(\sqrt{5} + \xi_n\right)}$. Koska $\lim_{n\to\infty} \xi_n = 0$, niin on olemassa sellainen indeksi k_0, että aina, kun $k \geq k_0$, niin $\xi_k < \frac{1}{c} - \sqrt{5}$. Siis kun $k \geq k_0$, niin $\left|x - \frac{p_k}{q_k}\right| = \frac{1}{q_k^2\left(\sqrt{5} + \xi_k\right)} > \frac{c}{q_k^2}$. Eli epäyhtälö $\left|x - \frac{p_k}{q_k}\right| < \frac{c}{q_k^2}$ on voimassa korkeintaan konvergenteille $\frac{p_n}{q_n}$ $(n = 0, 1, \ldots, k_0 - 1)$. $\square$

Olemme tähän mennessä osoittaneet, että jokaista irrationaalilukua x kohti on olemassa ääretön määrä sellaisia kokonaislukupareja p ja q, että $\left|x - \frac{p}{q}\right| < \frac{1}{\sqrt{5}q^2}$. Lisäksi nämä kokonaisluvut p ja q ovat luvun x konvergenttien osoittajia ja nimittäjiä. Olemme lisäksi todenneet, että jos edellistä ehtoa tiukennetaan, niin kokonaislukupareja p ja q ei yleisesti ole äärettömästi. Tiedetään myös, että kaikki kokonaislukuparit p ja q, jotka toteuttavat epäyhtälön $\left|x - \frac{p}{q}\right| < \frac{1}{2q^2}$, ovat luvun x konvergenttien osoittajia ja nimittäjiä. On myös osoitettu, että luvulla x voi olla sellaisia konvergentteja, että epäyhtälö $\left|x - \frac{p}{q}\right| < \frac{c}{q^2}$ ei ole voimassa, kun $c < 1$.

Lause 4.1.7. *Olkoon $x \in \mathbf{R} \setminus \mathbf{Q}$. Olkoot sen ketjumurtolukukehitelmän termit $a_1, a_2, \ldots$ rajoitetut. Silloin on olemassa sel-*

lainen $c \in \mathbf{R}_+$*, että epäyhtälöllä* $\left|x - \frac{p}{q}\right| < \frac{c}{q^2}$ *ei ole kokonaisluku-ratkaisuja* p, q*.*

Todistus (vrt. [1], s. 36–38). Koska ketjumurtoluvun termit ovat rajoitetut, niin on olemassa sellainen $M > 0$, että $a_1, a_2, \dots < M$. Koska $\left|x - \frac{p_n}{q_n}\right| > \frac{1}{q_n(q_{n+1}+q_n)} = \frac{1}{q_n^2(a_{n+1}+1+\frac{q_{n-1}}{q_n})} > \frac{1}{q_n^2(a_{n+1}+2)}$ $(n = 0, 1, \ldots)$, niin $\left|x - \frac{p_n}{q_n}\right| > \frac{1}{q_n^2(M+2)}$. Valitaan mielivaltainen $p \in \mathbf{Z}$ ja mielivaltainen $q \in \mathbf{Z}_+$. Olkoon k sellainen indeksi, että $q_{k-1} < q \le q_k$. Lauseen 4.1.1 perusteella

$$
\begin{aligned}
\left|x - \frac{p}{q}\right| &\ge \left|x - \frac{p_k}{q_k}\right| \\
&> \frac{1}{q_k^2(M+2)} \\
&= \frac{1}{q^2(M+2)}\left(\frac{q}{q_k}\right)^2 \\
&> \frac{1}{q^2(M+2)}\left(\frac{q_{k-1}}{q_k}\right)^2 \\
&= \frac{1}{q^2(M+2)}\left(\frac{q_{k-1}}{a_k q_{k-1} + q_{k-2}}\right)^2 \\
&> \frac{1}{q^2(M+2)} \cdot \frac{1}{(a_k+1)^2} \\
&> \frac{1}{q^2(M+2)} \cdot \frac{1}{(M+1)^2} \\
&= \frac{1}{(M+2)(M+1)^2q^2}.
\end{aligned}
$$

Kun valitaan $c = \frac{1}{(M+2)(M+1)^2}$, niin yksikään kokonaislukupari p, q ei toteuta epäyhtälöä $\left|x - \frac{p}{q}\right| < \frac{c}{q^2}$, koska $\left|x - \frac{p}{q}\right| > \frac{1}{(M+2)(M+1)^2q^2} = \frac{c}{q^2}$. □

Lause 4.1.8. *Olkoon* $x \in \mathbf{R} \setminus \mathbf{Q}$*. Olkoot sen ketjumurtolukukehitelmän termit* $a_1, a_2, \ldots$ *rajoittamattomat. Silloin jokaista*

$c \in \mathbf{R}_+$ *kohti epäyhtälöllä* $\left|x - \frac{p}{q}\right| < \frac{c}{q^2}$ *on äärettömästi kokonaislukuratkaisuja* p *ja* q.

Todistus (vrt. [1], s. 37). Koska termejä ei ole rajoitettu, niin on olemassa sellainen indeksijoukko $\{k_1, k_2, k_3, \dots\}$, että $a_{k_1+1}, a_{k_2+1}, \dots > \frac{1}{c}$. Nyt koska

$$\begin{aligned}\left|x - \frac{p_{k_n}}{q_{k_n}}\right| &= \frac{1}{q_{k_n}(\varepsilon_{k_n+1}q_{k_n} + q_{k_n-1})} \\ &< \frac{1}{a_{k_n+1}q_{k_n}^2} \\ &< \frac{c}{q_{k_n}^2} \ (n = 1, 2, \dots),\end{aligned}$$

niin selvästikin epäyhtälöllä $\left|x - \frac{p}{q}\right| < \frac{c}{q^2}$ on äärettömästi kokonaislukuratkaisuja p ja q. □

Lause 4.1.9. *Olkoon* α *astetta* n *oleva algebrallinen irrationaaliluku. Silloin on olemassa sellainen* $c \in \mathbf{R}_+$, *että epäyhtälöllä* $\left|\alpha - \frac{p}{q}\right| \le \frac{c}{q^n}$ *ei ole kokonaislukuratkaisuja* p *ja* q.

Todistus (vrt. [1], s. 45–47). Koska α on astetta n oleva algebrallinen irrationaaliluku, niin se toteuttaa kokonaislukukertoimisen n asteen polynomiyhtälön $P(x) = a_0 + a_1x + \cdots + a_nx^n = 0$. Eli $P(\alpha) = 0$, joten $P(x) = (x - \alpha)P_1(x)$, missä $P_1(x)$ on $n-1$ asteen polynomi. Osoitetaan, että $P_1(\alpha) \neq 0$. Oletetaan, että $P_1(\alpha) = 0$. Silloin olisi sellainen astetta $n-2$ oleva polynomi $P_2(x)$, että $P_1(x) = (x-\alpha)P_2(x)$, joten $P(x) = (x-\alpha)^2P_2(x)$. Koska $P'(x)$ on kokonaislukukertoiminen $n-1$ asteen polynomi ja toisaalta $P'(x) = (x-\alpha)(2P_2(x) + (x-\alpha)P_2'(x))$ eli $P'(\alpha) = 0$, niin tällöin α olisi astetta $n-1$ oleva algebrallinen irrationaaliluku. On siis päädytty ristiritaan, joten $P_1(\alpha) \neq 0$. Koska $P_1(x)$ on polynomi, niin $P_1(x)$ on myös jatkuva, joten on olemassa sellainen δ-säteinen luvun α ympäristö, että $P_1(x) \neq 0$, kun $x \in [\alpha - \delta, \alpha + \delta]$. Olkoot p ja q mielivaltaisia kokonaislukuja ja olkoon vielä $q > 0$. Mikäli $\left|\alpha - \frac{p}{q}\right| \le \delta$, niin $P_1\left(\frac{p}{q}\right) \neq 0$. Silloin $\frac{p}{q} - \alpha = \frac{P\left(\frac{p}{q}\right)}{P_1\left(\frac{p}{q}\right)} = \frac{a_0 + a_1\left(\frac{p}{q}\right) + \cdots + a_n\left(\frac{p}{q}\right)^n}{P_1\left(\frac{p}{q}\right)} =$

$\frac{a_0q^n+a_1pq^{n-1}+\cdots+a_np^n}{q^nP_1(\frac{p}{q})}$. Selvästikin luku $a_0q^n + a_1pq^{n-1} + \cdots + a_np^n$ on kokonaisluku. Lisäksi se on nollasta eriävä, koska α on irrationaaliluku. Merkitään

$$M = \sup\{|P_1(x)| : x \in [\alpha - \delta, \alpha + \delta]\} + 1.$$

Nyt saadaan epäyhtälö $\left|\alpha - \frac{p}{q}\right| > \frac{1}{Mq^n}$. Mikäli $\left|\alpha - \frac{p}{q}\right| > \delta$, niin saadaan epäyhtälö $\left|\alpha - \frac{p}{q}\right| > \frac{\delta}{q^n}$. Nyt kun valitaan $c = \min\left\{\delta, \frac{1}{M}\right\}$, niin $\left|\alpha - \frac{p}{q}\right| > \frac{c}{q^n}$, joka on voimassa kaikille kokonaislukupareille p, q. Siis epäyhtälöllä $\left|\alpha - \frac{p}{q}\right| \leq \frac{c}{q^n}$ ei ole kokonaislukuratkaisuja. $\square$

Seuraus 4.1.9. *Jos jokaista $c \in \mathbf{R}_+$ ja $n \in \mathbf{N}$ kohti on olemassa sellaiset kokonaisluvut p, q, että $\left|\alpha - \frac{p}{q}\right| \leq \frac{c}{q^n}$, niin luku α on transcendenttiluku.*

Seuraus 4.1.9 on siinä mielessä merkittävä, että sitä voidaan käyttää todistettaessa jotain lukua transcendenttiseksi. Seuraava esimerkki osoittaa, että transcendenttilukuja ylipäätään on olemassa.

Esimerkki 4.1.1. Määritellään yksinkertaisen päättymättömän ketjumurtoluvun $[a_0, a_1, a_2, \ldots]$ termit seuraavasti $a_0 = 0$, $a_{k+1} = q_k^{k-1} + 1$ $(k = 0, 1, \ldots)$, missä q_k on määritelty rekursioyhtälöillä (2). Olkoon kyseisen ketjumurtoluvun arvo α. Tällöin $\left|\alpha - \frac{p_k}{q_k}\right| < \frac{1}{q_kq_{k+1}} < \frac{1}{q_k^2a_{k+1}} < \frac{1}{q_k^2q_k^{k-1}} = \frac{1}{q_k^{k+1}}$, kun $k \geq 0$. Valitaan mielivaltainen $c \in \mathbf{R}_+$ ja mielivaltainen $n \in \mathbf{N}$. Valitaan $k = \max\left\{\left\lceil\frac{1}{c}\right\rceil, n\right\}$. Silloin $\frac{1}{c} \leq q_k$ ja $q_k^k \geq q_k^n$, joten $\left|\alpha - \frac{p_k}{q_k}\right| < \frac{1}{q_k^{k+1}} \leq \frac{c}{q_k^n}$. Seurauksen 4.1.9 perusteella α on transcendenttiluku.

Esimerkissä 4.1.1 olisi voitu luvut a_k $(k = 1, 2, \ldots)$ valita itse asiassa äärettömän monella tavalla, kunhan $a_{k+1} > q_k^{k-1}$. Täten olisi helppo osoittaa, että transcendenttilukujen joukko on ylinumeroituva käyttämällä Cantorin diagonalisointimenetelmää.

Luku 5. Pellin yhtälö $x^2 - Ny^2 = 1$

§ 5.1. Perusratkaisu

Tässä luvussa tarkastelemme niin sanottua Pellin yhtälöä $x^2 - Ny^2 = 1$, missä $N \in \mathbf{Z}_+$ ja luku N ei ole täydellinen neliö. Yhtälölle pyritään löytämään positiiviset kokonaislukuratkaisut x ja y. Myöhemmin osoitetaan, että yhtälö on aina ratkeava sekä ratkaisuja on äärettömän monta. Mielenkiintoiseksi ongelman tekee se, että ratkaisut saadaan luvun $\sqrt{N}$ ketjumurtolukukehitelmän konvergenteista.

Määritelmä 5.1.1. Lukua $x + y\sqrt{N}$ sanotaan Pellin yhtälön ratkaisuksi, mikäli $x^2 - Ny^2 = 1$ ja $x, y \in \mathbf{Z}_+$.

Määritelmä 5.1.2. Pellin yhtälön $x^2 - Ny^2 = 1$ *perusratkaisulla* tarkoitetaan lukua

$$\min\left\{x + y\sqrt{N} : x^2 - Ny^2 = 1 : x, y \in \mathbf{Z}_+\right\}.$$

Lause 5.1.1. *Olkoon $x + y\sqrt{N}$ Pellin yhtälön $x^2 - Ny^2 = 1$ ratkaisu. Silloin $\frac{x}{y}$ on luvun $\sqrt{N}$ ketjumurtolukukehitelmän konvergentti.*

Todistus. Koska $x^2 - Ny^2 = 1$ ja $y > 0$, niin $\left(\frac{x}{y}\right)^2 - N = \left(\frac{x}{y} - \sqrt{N}\right)\left(\frac{x}{y} + \sqrt{N}\right) = \frac{1}{y^2}$. Täten $\frac{x}{y} - \sqrt{N} = \frac{1}{y^2\left(\frac{x}{y}\right) + \sqrt{N}} < \frac{1}{2y^2\sqrt{N}} < \frac{1}{2y^2}$. Koska $\frac{x}{y} > \sqrt{N}$, niin $\left|\frac{x}{y} - \sqrt{N}\right| =$

$\frac{x}{y} - \sqrt{N}$, joten $\left|\frac{x}{y} - \sqrt{N}\right| < \frac{1}{2y^2}$. Lauseen 4.1.2 perusteella $\frac{x}{y}$ on luvun $\sqrt{N}$ konvergentti. $\square$

Lause 5.1.2. *Olkoon luvun $\sqrt{N}$ ketjumurtolukukehitelmä $[A_0, A_1, \ldots]$. Olkoot B_k, C_k $(k = 0, 1, \ldots)$ saatu rekursioyhtälöillä (3). Silloin on voimassa yhtälö*

$$p_k^2 - Nq_k^2 = (-1)^{k+1} C_k \ (k = 0, 1, \ldots). \tag{19}$$

Todistus (vrt. [5], s. 184). Apulauseen 2.1.2 perusteella $\sqrt{N} = \frac{\varepsilon_{k+1} p_k + p_{k-1}}{\varepsilon_{k+1} q_k + q_{k-1}}$. Lauseen 3.3.1 todistuksesta nähdään, että $\varepsilon_{k+1} = \frac{\sqrt{N} + B_k}{C_k}$, joten $\sqrt{N} = \frac{\frac{\sqrt{N}+B_k}{C_k} p_k + p_{k-1}}{\frac{\sqrt{N}+B_k}{C_k} q_k + q_{k-1}}$. Kun tätä lauseketta sievennetään, niin saadaan yhtälö

$$\sqrt{N}(p_k - C_k q_{k-1} - B_k q_k) = Nq_k - C_k p_{k-1} - B_k p_k.$$

Koska $\sqrt{N}$ on irrationaaliluku, niin

$$\begin{aligned} p_k - C_k q_{k-1} - B_k q_k &= 0, \\ Nq_k - C_k p_{k-1} - B_k p_k &= 0 \end{aligned}$$

eli

$$\begin{aligned} p_k &= C_k q_{k-1} + B_k q_k, \\ Nq_k &= C_k p_{k-1} + B_k p_k. \end{aligned}$$

Edelleen yhdistämällä nämä yhtälöt saadaan yhtälö

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

$\square$

Lause 5.1.3. *Olkoon $\sqrt{N} = [a_0, \overline{a_1, a_2, \ldots, a_n, 2a_0}]$. Määritellään $k = n$, kun n on pariton ja $k = 2n+1$, kun n on parillinen. Silloin on voimassa yhtälö*

$$p_k^2 - Nq_k^2 = 1. \tag{20}$$

Lisäksi $p_k + q_k\sqrt{N}$ *on Pellin yhtälön perusratkaisu.*

Todistus. Lauseen 5.1.2 perusteella $p_k^2 - Nq_k^2 = (-1)^{k+1}C_k$. Koska $a_{k+1} = 2a_0$, niin apulauseen 3.2.4 perusteella $C_k = 1$, joten koska vielä $(-1)^{k+1} = 1$, niin $p_k^2 - Nq_k^2 = 1$. Koska Pellin yhtälön ratkaisut saadaan luvun $\sqrt{N}$ konvergenteista, niin riittää tarkastella konvergentteja $\frac{p_s}{q_s}$, kun $s < k$. Koska apulauseen 3.2.4 mukaan $C_s = 1$ vain, kun $a_{s+1} = 2a_0$ ja apulauseen 3.2.5 mukaan $a_1, a_2, \ldots, a_n < 2a_0$, niin $a_{s+1} = 2a_0$ vain, kun $s = n$ tai $s = 2n+1$. Jos nyt $k = n$, niin $p_k + q_k\sqrt{N}$ on Pellin yhtälön perusratkaisu. Jos n on parillinen, niin $k = 2n+1$ ja $p_n^2 - Nq_n^2 = -1$. Siis $p_k + q_k\sqrt{N}$ on Pellin yhtälön perusratkaisu. Siis molemmissa tapauksissa $p_k + q_k\sqrt{N}$ on Pellin yhtälön perusratkaisu. □

Esimerkki 5.1.1. Ratkaistaan Pellin yhtälö $x^2 - 6y^2 = 1$. Muodostetaan luvun $\sqrt{6}$ ketjumurtolukukehitelmä rekursioyhtälöillä (3). Tällöin $\sqrt{6} = [2, \overline{2, 4}]$. Lauseen 5.4.3 perusteella $p_1^2 - 6q_1^2 = 1$. Rekursioyhtälöiden (2) perusteella $p_1 = 5$ ja $q_1 = 2$. Siis $5 + 2 \cdot \sqrt{6}$ on Pellin yhtälön $x^2 - 6y^2 = 1$ perusratkaisu. Tarkastetaan vielä tulos: $5^2 - 6 \cdot 2^2 = 25 - 6 \cdot 4 = 1$.

Esimerkki 5.1.2. Ratkaistaan Pellin yhtälö $x^2 - 13y^2 = 1$. Muodostetaan luvun $\sqrt{13}$ ketjumurtolukukehitelmä rekursioyhtälöillä (3). Tällöin $\sqrt{13} = [3, \overline{1, 1, 1, 1, 6}]$. Lauseen 5.4.3 perusteella

$p_{2\cdot 4+1}^2 - 13q_{2\cdot 4+1}^2 = 1$. Rekursioyhtälöiden (2) perusteella $p_9 = 649$ ja $q_9 = 180$. Siis $649 + 180 \cdot \sqrt{13}$ on Pellin yhtälön $x^2 - 13y^2 = 1$ perusratkaisu. Tarkastetaan vielä tulos:

$649^2 - 13 \cdot 180^2 = 421201 - 13 \cdot 32400 = 421201 - 421200 = 1.$

§ 5.2. Muut ratkaisut

Kuten olemme jo aiemmin todenneet Pellin yhtälöllä

$x^2 - Ny^2 = 1$ on äärettömästi ratkaisuja.

Lause 5.2.1. *Olkoon* $x_1 + y_1\sqrt{N}$ *Pellin yhtälön* $x^2 - Ny^2 = 1$ *perusratkaisu. Silloin yhtälön kaikki ratkaisut* $x_n + y_n\sqrt{N}$ $(n = 1, 2, \ldots)$ *saadaan kaavalla*

$$
\begin{aligned}
x_n &= x_1 x_{n-1} + N y_1 y_{n-1}, \\
y_n &= y_1 x_{n-1} + x_1 y_{n-1}, \quad \text{kun } n > 1.
\end{aligned} \tag{21}
$$

Todistus (vrt. [3], s. 198–199). Todistetaan induktiolla luvun n suhteen, että luvut $x_n + y_n\sqrt{N}$ $(n = 2, 3, \ldots)$ ovat Pellin yhtälön ratkaisuja. Kun $n = 2$, niin $x_2 = x_1^2 + Ny_1^2$ ja $y_2 = 2y_1x_1$. Siis

$$
\begin{aligned}
x_2^2 - Ny_2^2 &= x_1^4 + N^2y_1^4 + 2N(x_1y_1)^2 - 4N(x_1y_1)^2 \\
&= x_1^4 + N^2y_1^4 - 2N(x_1y_1)^2 \\
&= (x_1^2 - Ny_1^2)^2 = 1^2 = 1,
\end{aligned}
$$

joten $x_2 + y_2\sqrt{N}$ on Pellin yhtälön ratkaisu. Valitaan mielivaltainen $n > 1$. Tehdään induktio-oletus, että $x_n + y_n\sqrt{N}$ on Pellin yhtälön ratkaisu. Osoitetaan, että $x_{n+1} + y_{n+1}\sqrt{N}$ on Pellin yhtälön ratkaisu. Kaavan (21) ja induktio-oletuksen perusteella

$$
\begin{aligned}
x_{n+1}^2 - Ny_{n+1}^2 &= (x_1x_n + Ny_1y_n)^2 - N(y_1x_n + x_1y_n)^2 \\
&= x_1^2x_n^2 + N^2y_1^2y_n^2 + 2Nx_1y_1x_ny_n \\
&\quad - Ny_1^2x_n^2 - Nx_1^2y_n^2 - 2Nx_1y_1x_ny_n \\
&= x_1^2(x_n^2 - Ny_n^2) - Ny_1^2(x_n^2 - Ny_n^2) \\
&= x_1^2 - Ny_1^2 = 1.
\end{aligned}
$$

Siis $x_{n+1} + y_{n+1}\sqrt{N}$ on Pellin yhtälön ratkaisu, joten induktioperiaatteen mukaan luvut $x_n + y_n\sqrt{N}$ $(n = 2, 3, \ldots)$ ovat Pellin yhtälön ratkaisuja. Pitää vielä osoittaa, että muita ratkaisuja ei ole. Oletetaan, että on olemassa sellainen Pellin yhtälön ratkaisu $u + v\sqrt{N}$, että $u + v\sqrt{N} \neq x_n + y_n\sqrt{N}$ $(n = 1, 2, \ldots)$. Olkoon nyt n sellainen indeksi, että $x_n + y_n\sqrt{N} < u + v\sqrt{N} < x_{n+1} + y_{n+1}\sqrt{N}$. On helppo huomata, että $x_{n+1} + y_{n+1}\sqrt{N} = (x_n + y_n\sqrt{N})(x_1 + y_1\sqrt{N})$, ja $x_n - y_n\sqrt{N} > 0$. Yhdistämällä nämä tulokset yllä olevaan epäyhtälöön saadaan epäyhtälö $1 < (u + v\sqrt{N})(x_n - y_n\sqrt{N}) < x_1 + y_1\sqrt{N}$. Merkitään $x = ux_n - vy_nN$ ja $y = vx_n - uy_n$. Edelleen on helppo todeta, että $(u + v\sqrt{N})(x_n - y_n\sqrt{N}) = x + y\sqrt{N}$ ja $(u - v\sqrt{N})(x_n + y_n\sqrt{N}) = x - y\sqrt{N}$. Kertomalla nämä yhtälöt keskenään saadaan yhtälö $x^2 - Ny^2 = (u^2 - Nv^2)(x_n^2 - Ny_n)^2 = 1$. Siis $x + y\sqrt{N}$ on Pellin yhtälön ratkaisu. Tiedetään, että $1 < (u + v\sqrt{N})(x_n - y_n\sqrt{N}) = x + y\sqrt{N}$ ja $0 < x - y\sqrt{N} = \frac{1}{x+y\sqrt{N}}$, joten on mahdotonta, että $x < 0$ tai $y < 0$. Edelleen tiedetään, että $x + y\sqrt{N} = (u + v\sqrt{N})(x_n - y_n\sqrt{N}) < x_1 + y_1\sqrt{N}$, mikä on mahdotonta, koska $x_1 + y_1\sqrt{N}$ oletettiin perusratkaisuksi. Siis Pellin yhtälöllä ei ole muita ratkaisuja kuin edellä osoitetut. □

Huomautus 5.2.1. Yhtälöistä (21) seuraa selvästi, että $x_{n+1} > x_n$ ja $y_{n+1} > y_n$ $(n = 1, 2, \ldots)$.

Lause 5.2.2. *Olkoon* $[a_0, \overline{a_1, a_2, \ldots, a_n, 2a_0}]$ *luvun* $\sqrt{N}$ *ketjumurtolukukehitelmä. Silloin Pellin yhtälön* $x^2 - Ny^2 = 1$ *kaikki ratkaisut ovat*

$$\begin{cases} p_{n+t(n+1)} + q_{n+t(n+1)}\sqrt{N}, \text{ kun } n \text{ on pariton} \\ p_{2n+1+2t(n+1)} + q_{2n+1+2t(n+1)}\sqrt{N}, \text{ kun } n \text{ on parillinen} \end{cases},$$

missä $t \in \mathbf{N}$.

Todistus. Merkitään $k = n + t(n + 1)$, kun n on pariton ja $k = 2n + 1 + 2t(n + 1)$, kun n on parillinen. Selvästi $(-1)^{k+1} = 1$ ja $a_{k+1} = 2a_0$ $(t = 0, 1, \ldots)$. Apulauseen 3.2.4 mukaan $C_k = 1$, joten lauseen 5.1.2 perusteella $p_k^2 - Nq_k^2 = (-1)^{k+1}C_k = 1$ $(t = 0, 1, \ldots)$. Osoitetaan vielä, että ei ole muita ratkaisuja. Selvästikin luku $2a_0$ esiintyy luvun $\sqrt{N}$ ketjumurtolukukehitelmässä ainoastaan indekseillä $n + t(n + 1) + 1$ $(t = 0, 1, 2, \ldots)$, koska apulauseen 3.2.5 mukaan muilla indeksin arvoilla ketjumurtoluvun termit ovat pienempiä kuin $2a_0$. Edelleen apulauseen 3.2.4 perusteella $C_k = 1$ vain kun $k = n + t(n + 1)$ $(t = 0, 1, \ldots)$. Mikäli n on parillinen, niin $(-1)^{k+1} = -1$, kun t on parillinen. Parittomat luvun t arvot ovat muotoa $t = 2s + 1$ $(s = 0, 1, \ldots)$, joten saadaan $k = n + (2s + 1)(n + 1) = 2n + 1 + 2s(n + 1)$. Lauseen 5.1.2 perusteella Pellin yhtälö on siis ratkeava vain yllä osoitetuilla luvun $\sqrt{N}$

konvergenteilla. Lauseen 5.1.1 perusteella kaikki ratkaisut ovat luvun $\sqrt{N}$ konvergentteja. Siis muita ratkaisuja ei ole. □

Seuraus 5.2.1. *Lauseet 5.2.1 ja 5.2.2 antavat samat ratkaisut Pellin yhtälölle* $x^2 - Ny^2 = 1$.

Huomautus 5.2.2. Laskennallisesti lauseen 5.2.1 tapa on nopeampi kuin lauseen 5.2.2 tapa, koska lauseen 5.2.2 tapauksessa joudutaan mahdollisesti laskemaan useita konvergentteja ennen kuin haettu konvergentti saadaan.

Esimerkki 5.2.1. Etsitään Pellin yhtälön $x^2 - 6y^2 = 1$ kaikki sellaiset ratkaisut, että $x < 1000$ ja $y < 1000$. Esimerkin 5.1.1 perusteella yhtälön perusratkaisu on $5+2\sqrt{6}$. Kun sovelletaan kaavaa (21), niin saadaan ratkaisut

$$\begin{gathered} 5 + 2\sqrt{6}, \\ 49 + 40\sqrt{6}, \\ 725 + 298\sqrt{6}, \\ 7201 + 2940\sqrt{6}, \\ \vdots \end{gathered}$$

Kolme ylintä ratkaisua ovat ainoat ratkaisut, jotka täyttävät annetut ehdot. Tarkastetaan vielä laskemalla:

$$\begin{aligned} 5^2 - 6 \cdot 2^2 &= 1, \\ 49^2 - 6 \cdot 40^2 &= 1, \\ 725^2 - 6 \cdot 298^2 &= 1. \end{aligned}$$

Kirjallisuus

[1] Khinchin, A. Ya.: Continued fractions. Dover Publications, Inc., New York 1997.

[2] LeVeque, William J.: Elementary theory of numbers. Dover Publications, Inc., New York 1990.

[3] Nagell, Trygve: Introduction to number theory. Chelsea Publishing Company, New York 1981.

[4] Olds, C. D.: Continued fractions. The Mathematical Association of America, New York 1963.

[5] Shanks, Daniel: Solved and unsolved problems in number theory. Chelsea Publishing Company, New York 1978.