Lamén lause

Erik Kiljander

LuK-tutkielma
Toukokuu 2026

MATEMATIIKAN JA TILASTOTIETEEN LAITOS

Tarkastajat:
FM Tarmo Taipale

TURUN YLIOPISTO, Matematiikan ja tilastotieteen laitos

LuK-tutkielma
Pääaine: Matematiikka
Tekijä: Erik Kiljander
Otsikko: Lamén lause
Ohjaaja: FM Tarmo Taipale
Sivumäärä: 10 sivua
Aika: Toukokuu 2026

Tässä LuK-tutkielmassa esitetään ja todistetaan Lamén lause. Lause arvioi, kuinka nopeasti Eukleideen algoritmi löytää suurimman yhteisen tekijän kahdelle kokonaisluvulle. Algoritmin nopeus riippuu tutkittavien kokonaislukujen logaritmisesta suuruudesta eli numeroiden lukumäärästä luvuissa. Tutkielmassa esitellään lyhyesti jaollisuuden perusteita ja Eukleideen algoritmi. Lisäksi käsitellään Fibonaccin lukuja ja todistetaan niihin liittyviä aputuloksia. Tutkitaan, miten Fibonaccin lukujono liittyy Eukleideen algoritmin analysointiin.

Asiasanat: Lamén lause, Gabriel Lamé, Fibonacci, Eukleideen algoritmi, algoritmin analysointi, suurin yhteinen tekijä.

Sisällys

1 Johdanto

Ranskalainen matemaatikko Gabriel Lamé (1795–1870) esitti vuonna 1844 lauseen, joka arvioi, kuinka nopeasti *Eukleideen algoritmi* löytää suurimman yhteisen tekijän (a, b) kokonaisluvuille $a \geq b > 0$. Lauseen mukaan algoritmin tarvitsemien vaiheiden lukumäärä on enintään viisi kertaa numeroiden lukumäärä luvussa b.

Lamén lausetta pidetään merkittävimpänä työnä varhaisessa *algoritmien analysoinnissa*. Algoritmin analysoinnilla tarkoitetaan, että arvioidaan algoritmin tehokkuutta. Toisin sanoen lasketaan, kuinka monta askelta algoritmi suorittaa, kun sille annetaan tietyn kokoinen syöte. Tällainen analysointi on erittäin tärkeää esimerkiksi tietotekniikassa, joten algoritmien tutkimus on moderni ja hyvin ajankohtainen matematiikan ala.

Eukleideen algoritmi on yksi vanhimmista edelleen käytössä olevista matematiikan algoritmeista. Vaikka algoritmi on nimetty Eukleideen mukaan, arvellaan, että menetelmä tunnettiin jo ennen häntä [1, s. 403]. Koska Eukleideen algoritmi on niin historiallisesti merkittävä, se on yksi ensimmäisistä algoritmeista, jonka tehokkuutta analysoitiin kvantitatiivisesti.

Eukleideen algoritmin analysoinnissa hyödynnetään *Fibonaccin lukuja.* Fibonaccin luvut ovat tunnettu lukujono

$$1, 1, 2, 3, 5, 8, 13, 21, ...,$$

jossa kukin luku on kahden edellisen summa. Jonon jäsenet siis noudattavat rekursiokaavaa

$$F_n = F_{n-1} + F_{n-2}.$$

Fibonaccin luvut ilmenevät monissa matematiikan tuloksissa useilta matematiikan osa-alueilta; lukuisia esimerkkejä on esitelty lähteessä [2]. Luvut liittyvät myös Eukleideen algoritmiin, sillä algoritmin jakojäännöksiä voi arvioida alaspäin Fibonaccin luvuilla. Lamén lauseen todistus perustuu tähän menetelmään.

Lamé on tunnetuin Eukleideen algoritmia analysoineista matemaatikoista, mutta hän ei ollut ensimmäinen, joka ymmärsi Fibonaccin lukujen ja Eukleideen algoritmin välisen yhteyden. Monet ranskalaiset matemaatikot olivat tutkineet aihetta jo aiemmin 1700–1800 -luvuilla, kuten kerrotaan lähteessä [1].

Tässä tutkielmassa kerätään yhteen Lamén lauseen todistamisessa tarvittavat tulokset. Luvussa 2 pohjustetaan jaollisuuden perusteita ja esitellään Eukleideen algoritmi. Luvussa 3 tutkitaan Fibonaccin lukujonoa ja sen ominaisuuksia. Lopuksi luvussa 4 todistetaan Lamén lause. Kunkin luvun alussa esitellään lisäksi aiheeseen liittyvää historiallista taustaa.

2 Kokonaislukujen jaollisuus

Lamén lause käsittelee Eukleideen algoritmia, joten on olennaista ymmärtää, miten tämä algoritmi toimii. Perehdytään siksi lukuteorian ja jaollisuuden perusteisiin.

2.1 Historiallinen tausta

Muinaiset egyptiläiset ja babylonialaiset osasivat kerto- ja jakolaskuja, mutta heidän aritmetiikkansa oli vielä alkeellista. Egyptiläiset käyttivät vain murtolukuja, jotka olivat muotoa $\frac{1}{n},\ n = 2, 3, 4, ...$ ja lisäksi lukua $\frac{2}{3}$ [3, s. 10]. Babylonialaisten kerto- ja jakolasku puolestaan perustui valmiiksi taulukoituihin arvoihin [3, s. 12].

Varsinainen jaollisuuden tutkimus sai länsimaissa alkunsa antiikin Kreikassa. Kreikkalaisten matematiikka oli luonteeltaan geometrista. He hahmottivat jaollisuutta niin sanottujen yhteismitallisten janojen avulla. Janoja a ja b sanottiin yhteismitallisiksi, jos ne olivat jonkin kolmannen janan monikertoja eli jos oli olemassa sellainen jana c ja positiiviset kokonaisluvut m ja n, että $a = mc$ ja $b = nc$. [3, s. 38]

Pythagoraan (n. 580–500 eaa.) koulukunta oli lukuteorian tutkimuksen edelläkävijöitä. Pythagoralaisilta ovat peräisin esimerkiksi alkulukujen ja täydellisten lukujen käsitteet. He johtivat lukuteoreettisia tuloksia geometrisista argumenteista. Luvuiksi he hyväksyivät vain positiiviset kokonaisluvut. [3, s. 36–38.]

Eukleides (n. 325–265 eaa.) oli antiikin merkittävimpiä matemaatikkoja. Hänen pääteoksensa *Alkeet* on kattava esitys aikansa matemaattisesta tietoudesta. Se koostuu 13 kirjasta, joissa johdetaan kymmenestä aksioomasta lähtien satoja lauseita. Ensimmäisissä kirjoissa käsitellään geometrisia ongelmia. Seitsemännessä kirjassa Eukleides alkaa tutkia lukuteoriaa. Kirjassa määritellään esimerkiksi alkuluvut ja yhdistetyt luvut sekä esitetään Eukleideen algoritmi suurimman yhteisen tekijän löytämiseksi. [3, s. 43–45.]

2.2 Jakoalgoritmi ja suurin yhteinen tekijä

Palautetaan nyt mieleen jaollisuuden perusteita. Tässä luvussa kaikki muuttujat $a, b, c, ...$ ovat kokonaislukuja. Tarkastellaan ensin tavallista *jakoalgoritmia*: Olkoon $b \neq 0$. Jokaisella kokonaisluvulla a on yksikäsitteinen esitys

$$a = qb + r,$$

missä $0 \leq r < |b|$. Esitystä kutsutaan *jakoyhtälöksi*. Siinä q on *osamäärä* (quotient) ja r on *jakojäännös* (remainder). [4, s. 3.]

Määritelmä 1. Jos jakoyhtälössä jakojäännös $r = 0$ eli jos $a = qb$ jollakin kokonaisluvulla q, niin silloin b *jakaa* a:n ja merkitään $b|a$. [4, s. 4.]

Määritelmä 2. Kokonaislukujen a ja b *suurin yhteinen tekijä* $(a, b) = d$ on suurin kokonaisluku d, joka jakaa sekä a:n että b:n. [4, s. 4]

Todistetaan seuraavaksi jakoalgoritmin avulla suurinta yhteistä tekijää koskeva lemma. Eukleideen algoritmi pohjautuu tähän ominaisuuteen.

Lemma 1. *Olkoon k kokonaisluku. Silloin $d = (a, b) = (a + kb, b)$.*

Todistus. Jos $b = 0$, väite on triviaali. Oletetaan, että $b \neq 0$. Näytetään, että jos $d|b$, niin $d|a$ jos ja vain jos $d|(a + kb)$.

Suuntaan ($\Rightarrow$): Jos $d|b$ ja $d|a$, niin $b = xd$ ja $a = yd$ joillakin $x, y \in \mathbb{Z}$. Silloin

$$a + kb = yd + kxd = (y + kx)d.$$

Koska $y + kx \in \mathbb{Z}$, niin $d|(a + kb)$.

Suuntaan ($\Leftarrow$): Jos $d|b$ ja $d|(a + kb)$, niin $b = xd$ ja $a + kb = yd$ joillakin $x, y \in \mathbb{Z}$. Silloin

$$a + kb = a + kxd = yd$$

eli $a = (y - kx)d$. Koska $y - kx \in \mathbb{Z}$, niin $d|a$. [4, s. 5.] □

2.3 Eukleideen algoritmi

Eukleideen algoritmi on menetelmä, jolla etsitään kokonaislukujen $a \geq b > 0$ suurin yhteinen tekijä (a, b). Valitaan $a = r_0$ ja $b = r_1$ ja muodostetaan vähenevä jono positiivisia kokonaislukuja $r_0 > r_1 > ... > r_i > ... > r_n > r_{n+1} = 0$ kirjoittamalla jakoyhtälöitä allekkain seuraavasti:

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

Lause 1. *Eukleideen algoritmissa etsitty suurin yhteinen tekijä (a, b) on viimeinen nollasta poikkeava jakojäännös r_n.*

Todistus. Todistetaan induktiolla, että kaikilla $0 \leq i \leq n$ pätee $(a, b) = (r_i, r_{i+1})$. Alkuaskel $i = 0$ toteutuu, koska valittiin $(a, b) = (r_0, r_1)$. Lemman 1 perusteella

$$(r_i, r_{i+1}) = (r_i - q_{i+1} r_{i+1},\ r_{i+1}) = (r_{i+2}, r_{i+1}) = (r_{i+1}, r_{i+2}).$$

Jos siis oletetaan $(a, b) = (r_i, r_{i+1})$, niin silloin pätee myös $(a, b) = (r_{i+1}, r_{i+2})$ eli induktioaskel toteutuu. Siispä $(a, b) = (r_i, r_{i+1})$ kaikilla $0 \leq i \leq n$. Sijoitetaan $i = n$, jolloin

$$(a, b) = (r_n, r_{n+1}) = (r_n, 0) = r_n. \quad [4, \text{s. } 6.]$$

□

Lasketaan vielä esimerkkinä Eukleideen algoritmilla lukujen 252 ja 198 suurin yhteinen tekijä $(252, 198)$.

$$\begin{aligned} 252 &= 1 \cdot 198 + 54 \\ 198 &= 3 \cdot 54 + 36 \\ 54 &= 1 \cdot 36 + 18 \\ 36 &= 2 \cdot 18 \end{aligned}$$

Suurimmaksi yhteiseksi tekijäksi saadaan siis $(252, 198) = 18$.

Yllä olevassa esimerkissä tarvitaan vain neljä vaihetta suurimman yhteisen tekijän löytämiseksi. Pienille kokonaisluvuille suurimman yhteisen tekijän löytäminen onkin yleensä helppoa. Suuremmilla luvuilla laskettaessa tarvitaan kuitenkin usein enemmän vaiheita, ja suuret laskutoimitukset kuluttavat tietokoneiden laskentatehoa. Siksi voi olla hyödyllistä arvioida algoritmin tehokkuutta etukäteen esimerkiksi Lamén lauseen avulla.

3 Fibonaccin luvut

Lamén lauseen todistus pohjautuu Fibonaccin lukuihin, joten esitellään ne seuraavaksi. Johdetaan lisäksi Fibonaccin luvuille suora laskukaava ja alaraja.

3.1 Historiallinen tausta

Fibonacci (1170–1250), oikealta nimeltään Leonardo Pisano, oli italialainen matemaatikko. Nuorena hän opiskeli Algeriassa Bugian kaupungissa, missä hän tutustui tuolloisen arabimaailman matemaattiseen sivistykseen. Fibonacci julkaisi vuonna 1202 kuuluisimman teoksensa *Liber abaci*, jossa hän esitteli arabialaisen lukujärjestelmän eurooppalaiselle yleisölle. Kirjan saaman suosion myötä arabialaiset luvut yleistyivät myös Euroopassa.

Teoksessaan Fibonacci käsittelee pääosin kahden tyyppisiä aritmeettisia ongelmia. Hän tutkii täydellisiä lukuja ja useamman kuin kahden muuttujan lineaarisia yhtälöryhmiä. Teoksessa esitetään myös kuuluisa jänisongelma: "Mies pitää jänisparia suljetussa aitauksessa. Jänikset lisääntyvät ja tuottavat uuden parin kerran kuukaudessa. Jänikset tulevat lisääntymiskykyisiksi kahden kuukauden iässä. Kuinka monta jänisparia miehellä on vuoden kuluttua, jos oletetaan, että yksikään jänis ei kuole vuoden aikana?"

Fibonacci havaitsi, että kuukauden päästä jänispareja oli 1, kahden kuukauden päästä 2, kolmen kuukauden päästä 3, neljän kuukauden päästä 5 ja niin edelleen. Toisin sanoen hän huomasi jänisparien lukumäärän noudattavan jonoa 1,1,2,3,5,8,13,21,...,. Myöhemmin tämä lukujono on nimetty hänen mukaansa Fibonaccin jonoksi. [2, s. 14–15.]

3.2 Rekursiivinen määritelmä

Fibonaccin jonossa kukin luku on kahden edellisen luvun summa. Nykylähteissä merkitään usein ensimmäiseksi Fibonaccin luvuksi $F_0 = 0$, jolloin jonolle saadaan seuraava rekursiivinen määritelmä:

Määritelmä 3. Olkoot $n \geq 0$ kokonaislukuja. Fibonaccin lukujono (F_n) noudattaa rekursiota

$$\begin{aligned} &F_0 = 0 \\ &F_1 = 1 \\ &F_n = F_{n-1} + F_{n-2}, \quad n \geq 2. \quad [5, \text{s. } 13.] \end{aligned}$$

Yhtälö $F_n = F_{n-1}+F_{n-2}$ on niin sanottu toisen kertaluvun lineaarinen homogeeninen rekursioyhtälö. Yleisesti tällainen yhtälö on muotoa

$$a_n = Aa_{n-1} + Ba_{n-2},$$

missä $A, B \in \mathbb{R}$ ja $B \neq 0$. [5, s. 13.] Sijoitetaan yhtälöön $a_n = x^n$, missä $x \neq 0$. Silloin

$$x^n = Ax^{n-1} + Bx^{n-2}.$$

Jaetaan puolittain termillä x^{n-2}, jolloin päädytään rekursioyhtälöä vastaavaan *karakteristiseen yhtälöön*

$$x^2 = Ax + B.$$

Todistetaan karakteristista yhtälöä koskeva lemma, jota tarvitaan, kun johdetaan laskukaavoja rekursiivisille lukujonoille.

Lemma 2. *Jos karakteristisella yhtälöllä $x^2 = Ax + B$ on kaksi erisuurta juurta α ja β, niin on olemassa yksikäsitteiset luvut $K_1, K_2 \in \mathbb{C}$, joille*

$$a_n = K_1\alpha^n + K_2\beta^n$$

kaikilla kokonaisluvuilla $n \geq 0$.

Todistus. Todistetaan väite induktiolla. Koska $B \neq 0$, niin myös $\alpha \neq 0$ ja $\beta \neq 0$. Valitaan sellaiset luvut K_1 ja K_2, jotka toteuttavat väitteen arvoilla $n = 0$ ja $n = 1$. Toisin sanoen ne toteuttavat yhtälöparin

$$\begin{cases} a_0 &= K_1\alpha^0 + K_2\beta^0 \\ a_1 &= K_1\alpha^1 + K_2\beta^1, \end{cases}$$

josta saadaan ratkaistua

$$K_1 = \frac{a_1 - a_0\beta}{\alpha - \beta}, \quad K_2 = \frac{a_0\alpha - a_1}{\alpha - \beta}.$$

Olkoon sitten $k \geq 2$. Oletetaan, että väite toteutuu, kun $n < k$, ja osoitetaan, että silloin se toteutuu myös arvolla $n = k$. Nyt

$$\begin{aligned} a_k &= Aa_{k-1} + Ba_{k-2} \\ &= A(K_1\alpha^{k-1} + K_2\beta^{k-1}) + B(K_1\alpha^{k-2} + K_2\beta^{k-2}) \\ &= K_1(A\alpha^{k-1} + B\alpha^{k-2}) + K_2(A\beta^{k-1} + B\beta^{k-2}) \\ &= K_1\alpha^{k-2}(A\alpha + B) + K_2\beta^{k-2}(A\beta + B). \end{aligned}$$

Koska α ja β ovat yhtälön $x^2 = Ax + B$ juuria, niin

$$\begin{aligned} a_k &= K_1\alpha^{k-2}(A\alpha + B) + K_2\beta^{k-2}(A\beta + B) \\ &= K_1\alpha^{k-2}\alpha^2 + K_2\beta^{k-2}\beta^2 \\ &= K_1\alpha^k + K_2\beta^k. \end{aligned}$$

Siis väite toteutuu kaikilla kokonaisluvuilla $n \geq 0$. [5, s. 14.] □

3.3 Binet'n kaava

Suurten Fibonaccin lukujen laskeminen rekursiivisesti on työlästä, koska myös kaikki edeltävät luvut täytyy laskea. Johdetaan siksi niin sanottu Binet'n kaava, jolla saadaan laskettua järjestyslukua n vastaava Fibonaccin luku suoraan luvun n funktiona.

Lause 2. *(Binet) Olkoon $n \geq 0$ kokonaisluku. Fibonaccin luku F_n on muotoa*

$$F_n = \frac{1}{\sqrt{5}}\alpha^n - \frac{1}{\sqrt{5}}\beta^n,$$

missä $\alpha = \frac{1+\sqrt{5}}{2}$ ja $\beta = \frac{1-\sqrt{5}}{2}$.

Todistus. Fibonaccin lukujen rekursioyhtälöä

$$F_n = F_{n-1} + F_{n-2}$$

vastaa karakteristinen yhtälö

$$x^2 - x - 1 = 0.$$

Toiseen asteen yhtälön ratkaisukaavalla saadaan

$$x = \frac{-(-1) \cdot \sqrt{(-1)^2 - 4 \cdot 1 \cdot (-1)}}{2 \cdot 1} = \frac{1 \pm \sqrt{5}}{2},$$

eli karakteristisen yhtälön juuret ovat

$$\alpha = \frac{1+\sqrt{5}}{2}, \quad \beta = \frac{1-\sqrt{5}}{2}.$$

Lemman 2 perusteella on olemassa yksikäsitteiset vakiot $K_1, K_2 \in \mathbb{C}$, joilla

$$F_n = K_1\alpha^n + K_2\beta^n.$$

Sijoitetaan alkuarvot $n = 0$ ja $n = 1$, jolloin saadaan yhtälöpari

$$\begin{cases} F_0 = 0 = K_1(\frac{1+\sqrt{5}}{2})^0 + K_2(\frac{1-\sqrt{5}}{2})^0 \\ F_1 = 1 = K_1(\frac{1+\sqrt{5}}{2})^1 + K_2(\frac{1-\sqrt{5}}{2})^1. \end{cases}$$

Sen ratkaisuiksi saadaan

$$K_1 = \frac{1}{\sqrt{5}}, \quad K_2 = -\frac{1}{\sqrt{5}}.$$

Siispä

$$F_n = \frac{1}{\sqrt{5}}\alpha^n - \frac{1}{\sqrt{5}}\beta^n. \quad [2, \text{s. } 52\text{–}53.]$$

□

Lukua $\alpha = \frac{1+\sqrt{5}}{2}$ kutsutaan *kultaisen leikkauksen* suhdeluvuksi. Se on tunnettu vakio, joka esiintyy useissa matemaattisissa tuloksissa. Kultainen leikkaus ilmenee myös luonnossa; esimerkiksi monien kasvien lehdet kasvavat spiraaleina, jotka noudattavat kultaisen leikkauksen suhdetta [2, s. 49–50].

Todistetaan vielä lemma, joka antaa Fibonaccin luvuille alarajan kultaisen leikkauksen luvun α avulla. Lemmaa tarvitaan Lamén lauseen todistamiseen.

Lemma 3. *Kokonaisluvuilla $n \geq 3$ pätee*

$$F_n > \alpha^{n-2},$$

missä $\alpha = \frac{1+\sqrt{5}}{2}$.

Todistus. Todistetaan väite induktiolla. Selvästi

$$F_3 = 2 > \left(\frac{1+\sqrt{5}}{2}\right)^{3-2} = 1.6180...$$
$$F_4 = 3 > \left(\frac{1+\sqrt{5}}{2}\right)^{4-2} = 2.6180...,$$

joten alkuaskel toteutuu. Oletetaan sitten, että $\alpha^{k-2} < F_k$ kaikilla $k \leq n$. Koska α on yhtälön $x^2 - x - 1 = 0$ ratkaisu, niin $\alpha^2 = \alpha + 1$. Siispä

$$\begin{aligned} \alpha^{n-1} &= \alpha^2\alpha^{n-3} \\ &= (\alpha + 1)\alpha^{n-3} \\ &= \alpha^{n-2} + \alpha^{n-3}. \end{aligned}$$

Induktio-oletuksen mukaan $\alpha^{n-2} < F_n$ ja $\alpha^{n-3} < F_{n-1}$, joten

$$\alpha^{n-1} = \alpha^{n-2} + \alpha^{n-3} < F_n + F_{n-1} = F_{n+1}. \quad [6, \text{lem2.}]$$

□

4 Eukleideen algoritmin analysointi

Eukleideen algoritmin tarvitsemien vaiheiden lukumäärä kasvaa, kun sille annetaan yhä pidempiä lukuja syötteeksi. Täsmällisemmin sanottuna vaiheiden lukumäärä riippuu syötelukujen logaritmisesta suuruudesta. Algoritmin analysoinnissa on tavoitteena löytää mahdollisimman tarkka yläraja tälle lukumäärälle.

4.1 Historiallinen tausta

Fibonaccin lukujen yhteys Eukleideen algoritmiin on keskeinen osa algoritmin analysointia, ja myös Lamén lauseen tulos perustuu siihen. Monet ranskalaiset matemaatikot olivat kuitenkin huomanneet yhteyden jo aiemmin. Esimerkiksi Thomas Fantet de Lagny (1660–1734) tutki ketjumurtolukujen yhteyttä Fibonaccin lukuihin. De Lagny ei itse huomannut tutkimuksensa liittyvän Eukleideen algoritmiin, mutta käytännössä hänen tuloksensa kertoi, että algoritmi tarvitsee eniten vaiheita silloin, kun sille annetaan syötteeksi kaksi peräkkäistä Fibonaccin lukua (F_{n+2}, F_{n+1}). [1, s. 404–406.]

Ensimmäinen suoraan Eukleideen algoritmia analysoinut matemaatikko oli Antoine-André-Louis Reynaud (1771–1844). Vuonna 1811 hän todisti, että Eukleideen algoritmi tarvitsee korkeintaan b vaihetta löytääkseen kokonaislukujen $a \geq b > 0$ suurimman yhteisen tekijän. Vuonna 1821 Reynaud esitti parannellun tuloksen, joka antoi ylärajaksi $b/2 + 2$ vaihetta. Myös Lamé viittasi myöhemmin omassa julkaisussaan Reynaudin tulokseen. [1, s. 408–409.]

Émile Léger (1795–1838) huomasi vuonna 1838 yhteyden, joka oli jäänyt de Lagnylta huomaamatta: Eukleideen algoritmi tarvitsee eniten vaiheita, kun se laskee kahden peräkkäisen Fibonaccin luvun suurimman yhteisen tekijän (F_{n+2}, F_{n+1}). Léger ei kuitenkaan antanut havainnolleen täsmällistä todistusta. [1, s. 410.]

Pierre-Joseph-Étienne Finck (1797–1870) julkaisi vuonna 1841 ensimmäisen täsmällisen analyysin Eukleideen algoritmista. Hän todisti Fibonaccin lukujen avulla, että algoritmi tarvitsee korkeintaan $2 \log_2 b + 1$ vaihetta suurimman yhteisen tekijän löytämiseksi. Tämä yläraja on jo lähes yhtä tarkka kuin Laméllа. [1, s. 413.] Onkin tärkeää tunnustaa Lamén edeltäjien työ, vaikka hänen lauseensa vuodelta 1844 on jäänyt tunnetuimmaksi analyysiksi Eukleideen algoritmista.

4.2 Lamén lause

Todistetaan lopuksi Lamén tulos.

Lause 3. *(Lamé) Olkoot $a > b \geq 0$ kokonaislukuja ja olkoon k numeroiden lukumäärä luvussa b. Silloin Eukleideen algoritmi tarvitsee korkeintaan $5k$ vaihetta suurimman yhteisen tekijän (a, b) löytämiseksi.*

Todistus. Yleisyyttä menettämättä voidaan olettaa $a > b \geq 2$. Valitaan $a = r_0$ ja $b = r_1$. Nähdään, että Eukleideen algoritmi

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

tarvitsee n vaihetta suurimman yhteisen tekijän r_n löytämiseksi. Selvästi osamäärät $q_1, q_2, ..., q_{n-1} \geq 1$. Koska r_i ja q_i ovat luonnollisia lukuja ja $r_n < r_{n-1}$, niin viimeisessä vaiheessa $q_n \geq 2$.

Kirjoitetaan jakojäännökset $r_{n-1}, r_{n-2}, ..., r_2, r_1$ allekkain ja arvioidaan kutakin jakojäännöstä alaspäin edellisten avulla. Huomataan, että arviot voi esittää Fibonaccin lukuina. Ensinnäkin $r_n > 0$, joten $r_n \geq 1 = F_2$. Lisäksi

$$\begin{aligned}
r_{n-1} &= q_n r_n \geq 2 \cdot 1 = 2 = F_3 \\
r_{n-2} &= q_{n-1} r_{n-1} + r_n \geq 1 \cdot r_{n-1} + r_n \geq F_3 + F_2 = F_4 \\
&\ldots \\
r_2 &= q_3 r_3 + r_4 \geq 1 \cdot r_3 + r_4 \geq F_{n-1} + F_{n-2} = F_n \\
r_1 &= q_2 r_2 + r_3 \geq 1 \cdot r_2 + r_3 \geq F_n + F_{n-1} = F_{n+1}.
\end{aligned}$$

Jos siis Eukleideen algoritmissa on n vaihetta, niin $r_1 = b \geq F_{n+1}$. Silloin lemman 3 perusteella $b > \alpha^{(n+1)-2} = \alpha^{n-1}$. Otetaan epäyhtälöstä puolittain logaritmi.

$$\begin{aligned}
\log_{10} b &> \log_{10} \alpha^{n-1} \\
&= (n-1) \cdot \log_{10} \alpha \\
&= (n-1) \cdot \log_{10} \frac{1+\sqrt{5}}{2} \\
&= (n-1) \cdot 0.2089... \\
&> (n-1) \cdot \frac{1}{5}
\end{aligned}$$

Siispä $n - 1 < 5 \log_{10} b$. Olkoon nyt

$$10^{k-1} \leq b < 10^k,$$

jolloin luvussa b on k paikkaa kymmenjärjestelmässä, toisin sanoen k numeroa. Otetaan puolittain logaritmi, jolloin

$$\log_{10} b < \log_{10} 10^k = k.$$

Kun tämä kerrotaan puolittain viidellä, saadaan

$$n - 1 < 5 \log_{10} b < 5k.$$

Koska n ja k ovat luonnollisia lukuja ja $n - 1 < 5k$, niin $n \leq 5k$. [2, s. 62–63.] □

5 Yhteenveto

Lamén lause on hyvä esimerkki matematiikan kumulatiivisesta luonteesta, jossa vanhan tiedon päälle rakennetaan uutta. Lause sitoo yhteen Eukleideen algoritmin antiikin ajoilta, keskiaikaiset Fibonaccin luvut sekä modernin algoritmien analysoinnin. Yksittäinen lause voi yhdistää teoriaa historian eri aikakausilta, koska matemaattinen tieto ei vanhene.

Lisäksi Lamén lauseen todistuksessa käytetään tietoa matematiikan eri osa-alueilta. Algoritmien analysoinnissa tarvitaan lukuteoriaa. Diskreeteissä lukuteorian ongelmissa puolestaan käytetään apuna analyysin jatkuvia menetelmiä, esimerkiksi logaritmifunktiota. Lamén lause havainnollistaa, kuinka matematiikan eri osa-alueet ovat yhteydessä toisiinsa ja tukevat toisiaan.

Viitteet

[1] Shallit, J. (1994) *Origins of the analysis of Euclidean algorithm*, Historia Mathematica, vol 21:4, s. 401-419

[2] Grimaldi, R. P. (2012) *Fibonacci and Catalan numbers: an introduction* (1st edition), John Wiley & Sons

[3] Halava, V., Pirttimäki, T. (2021) *Matematiikan historia*, Turun yliopisto

[4] Honkala, I., Jutila, M. (2011) *Lukuteoria*, Turun yliopisto

[5] Honkala, I. (2015) *Kombinatoriikka*, Turun yliopisto

[6] Raji, W. (2021) *Lame's Theorem*, https://math.libretexts.org/@go/page/8972, luettu 4.3.2026