802328A LUKUTEORIAN PERUSTEET OSA III

BASICS OF NUMBER THEORY PART III

Tapani Matala-aho

MATEMATIIKKA/LUTK/OULUN YLIOPISTO

SYKSY 2016

Sisältö

1 Irrationaaliluvuista

Määritelmä 1. Luku $\alpha \in \mathbb{C} \setminus \mathbb{Q}$ on irrationaalinen.

(Myös ei-rationaaliset p-adiset ($p \in \mathbb{P}$) luvut ovat irrationaalisia eli luku $\alpha \in \mathbb{C}_p \setminus \mathbb{Q}$ on irrationaalinen, missä $\mathbb{C}_p$ on kompleksilukujen kuntaa $\mathbb{C}$ vastaava p-adisten lukujen kunta.)

Esimerkki 1.

$$\sqrt{5} \notin \mathbb{Q}. \tag{1.1}$$

I todistus. Jos, olisi

$$\sqrt{5} = \frac{m}{n} \in \mathbb{Q}, \quad m \perp n, \tag{1.2}$$

niin

$$5n^2 = m^2 \quad \Rightarrow \quad 5|m^2 \quad \Rightarrow \quad 5|m \tag{1.3}$$

$$\Rightarrow \quad 5^2|m^2 = 5n^2 \quad \Rightarrow \quad 5|n^2 \quad \Rightarrow \quad 5|n. \tag{1.4}$$

Selvästi tulokset (1.3) ja (1.4) ovat ristiriidassa valinnan
$m \perp n$ kanssa. □

II todistus. Jos, olisi

$$\sqrt{5} = \frac{m}{n} \in \mathbb{Q}, \quad m \perp n, \tag{1.5}$$

niin $\exists$ sellaiset luvut $s, t \in \mathbb{Z}$, että

$$1 = sm + tn. \tag{1.6}$$

Siten

$$\sqrt{5} = sm\sqrt{5} + tn\sqrt{5} = s5n + tm \in \mathbb{Z} \tag{1.7}$$

mutta

$$2 < \sqrt{5} < 3. \tag{1.8}$$

Ristiriita. □

Määritelmä 2. Luku $m \in \mathbb{Z}$ on neliövapaa (square-free), jos ehdosta $a^2|m$, $a \in \mathbb{Z}$, välttämättä seuraa $a^2 = 1$.

Tulos (1.1) yleistyy tulokseksi (Harjoitustehtävä 46)

Lause 1. Olkoon $D \in \mathbb{Z}$, $D \neq 1$, neliövapaa. Tällöin

$$\sqrt{D} \notin \mathbb{Q}. \tag{1.9}$$

Esimerkki 2.

$$\frac{\log 2}{\log 3} \notin \mathbb{Q}. \tag{1.10}$$

Todistus. Jos olisi

$$\frac{\log 2}{\log 3} = \frac{a}{b}, \quad a, b \in \mathbb{Z}^+, \tag{1.11}$$

niin

$$2^b = 3^a \quad \Rightarrow \quad 2|3^a \quad \Rightarrow \quad 2|3 \tag{1.12}$$

mikä on mahdotonta. □

Esimerkki 3.

$$\log 2 \notin \mathbb{Q}. \tag{1.13}$$

Ei todisteta. Todistus huomattavasti vaikeampi kuin Esimerkissä 2.

Lause 2. Olkoot $n \in \mathbb{Z}_{\geq 3}$ ja $r \in \mathbb{Q}^+$. Tällöin

$$\sqrt[n]{1 + r^n} \notin \mathbb{Q}. \tag{1.14}$$

Todistus perustuu Wilesin tulokseen (**??**).

Tiedetään, että Neperin luvulle e pätee

$$e = \lim_{n \to \infty} \left(1 + \frac{1}{n}\right)^n = \sum_{k=0}^{\infty} \frac{1}{k!}. \tag{1.15}$$

Lause 3. Neperin luku e on irrationaalinen.

I Todistus. Olkoon siis vastaoletuksena

$$e = \frac{a}{b} \in \mathbb{Q}, \quad a, b \in \mathbb{Z}^+, \quad a \perp b. \tag{1.16}$$

Valitaan sellainen kokonaisluku m, että

$$m \in \mathbb{Z}^+, \quad b \leq m \tag{1.17}$$

ja merkitään

$$A = m! \left(e - \sum_{k=0}^{m} \frac{1}{k!} \right). \tag{1.18}$$

Aluksi huomataan, että

$$A = \frac{m!a}{b} - m! \sum_{k=0}^{m} \frac{1}{k!} \in \mathbb{Z}. \tag{1.19}$$

Toisaalta

$$A = m! \sum_{k=m+1}^{\infty} \frac{1}{k!}, \tag{1.20}$$

joten saadaan arviot

$$\begin{aligned} 0 < A = m! \left(\frac{1}{(m+1)!} + \frac{1}{(m+2)!} + \frac{1}{(m+3)!} + ... \right) = \\ \frac{1}{m+1} + \frac{1}{(m+1)(m+2)} + \frac{1}{(m+1)(m+2)(m+3)} + ... = \\ \frac{1}{m+1} \left(1 + \frac{1}{m+2} + \frac{1}{(m+2)(m+3)} + ... \right) < \\ \frac{1}{m+1} \left(1 + \frac{1}{m+1} + \frac{1}{(m+1)^2} + ... \right) = \frac{1}{m} \leq 1. \end{aligned} \tag{1.21}$$

Siten $A \in \mathbb{Z}$ ja $0 < A < 1$, jotka ovat ristiriidassa. □

II Todistus.

$$e^{-1} = \sum_{k=0}^{\infty} \frac{(-1)^k}{k!}. \tag{1.22}$$

Olkoon siis vastaoletuksena

$$e^{-1} = \frac{b}{a} \in \mathbb{Q}, \quad a, b \in \mathbb{Z}^+, \quad a \perp b. \tag{1.23}$$

Valitaan sellainen kokonaisluku m, että

$$m \in \mathbb{Z}^+, \quad a \leq m \tag{1.24}$$

ja merkitään

$$B = m! \left(e^{-1} - \sum_{k=0}^{m} \frac{(-1)^k}{k!} \right). \tag{1.25}$$

Aluksi huomataan, että

$$B = \frac{m!b}{a} - m! \sum_{k=0}^{m} \frac{(-1)^k}{k!} \in \mathbb{Z}. \tag{1.26}$$

Toisaalta

$$B = m! \sum_{k=m+1}^{\infty} \frac{(-1)^k}{k!}. \tag{1.27}$$

Käytetään alternoivien sarjojen ominaisuuksia. Olkoon

$$r_n > r_{n+1} > r_{n+2} > ... > 0, \quad r_n \ \to \ 0, \tag{1.28}$$

ja

$$s_n := r_n - r_{n+1} + r_{n+2} - r_{n+3} + ... \tag{1.29}$$

Tällöin

$$0 < s_n = r_n - s_{n+1} < r_n. \tag{1.30}$$

Sovelletaan tulosta (1.30), kun $r_n = \frac{1}{n!}$.

Nyt esityksestä (1.27) saadaan

$$\begin{aligned} |B| = m! \left| \sum_{k=m+1}^{\infty} \frac{(-1)^k}{k!} \right| = \\ m! \left| (-1)^{m+1} (r_{m+1} - r_{m+2} + r_{m+3} - r_{m+4} + ...) \right| \\ = m! s_{m+1} \end{aligned} \tag{1.31}$$

Siispä

$$0 < |B| = m! s_{m+1} < m! r_{m+1} = \frac{m!}{(m+1)!} = \frac{1}{m+1} \leq \frac{1}{2}. \quad (1.32)$$

Siten $B \in \mathbb{Z}$ ja $0 < |B| < 1$, jotka ovat ristiriidassa. □

2 Antiikin lukuja

2.1 Kolmio- neliö- ja tetraedriluvut

Lukuja $T_n = 1 + 2 + \cdots + n$ kutsutaan kolmioluvuiksi (triangular numbers). Aritmeettisen sarjan summakaavalla ja binomikertoimen määritelmällä saadaan

$$T_n = \binom{n+1}{2} \text{ kaikilla } n \in \mathbb{Z}^+.$$

Lukuja $\square_n = n^2$ kutsutaan neliöluvuiksi (square numbers).
Lukuja $\mathcal{T}_n = T_1 + T_2 + \cdots + T_n$ kutsutaan tetraedriluvuiksi (tetrahedral numbers). Käyttämällä Pascalin kolmion palautuskaavaa (**??**) saadaan

$$\mathcal{T}_n = \sum_{k=1}^{n} \binom{k+1}{2} = \sum_{k=1}^{n} \left(\binom{k+2}{3} - \binom{k+1}{3} \right) = \binom{n+2}{3}. \quad (2.1)$$

2.2 Pythagoraan luvut

Määritelmä 3. Kolmikko $(a, b, c) \in \mathbb{Z}^3_{\geq 1}$ on primitiivinen Pythagoraan lukukolmikko, mikäli $\text{syt}(a, b, c) = 1$ ja

$$a^2 + b^2 = c^2. \quad (2.2)$$

Tutkitaan ensin pariteettia. Oletetaan aluksi, että

$$2|a \text{ ja } 2|b,$$

mistä saadaan

$$2|c^2 \Rightarrow 2|c, \text{ ristiriita.}$$

Muut parit vastaavasti, eli ainakin kaksi luvuista on parittomia. Edelleen, jos olisi

$$\begin{aligned} &a = 2l + 1 \text{ ja } b = 2k + 1 \Rightarrow \\ &c^2 = a^2 + b^2 \equiv 2 \pmod 4, \text{ ristiriita.} \end{aligned}$$

Siis toinen luvuista a ja b on parillinen, muut parittomia. Olkoon vaikka

$$a = 2l + 1 \text{ ja } b = 2k.$$

Nyt kaikille alkuluvuille p pätee

$$p|a \text{ ja } p|b \Rightarrow p|c^2 \Rightarrow p|c, \text{ ristiriita.}$$

Vastaavasti muille pareille, joten

$$\text{syt}(a, b) = \text{syt}(a, c) = \text{syt}(b, c) = 1.$$

Lähdetään yhtälöstä (23.7), joka on yhtäpitäävää yhtälön

$$a^2 = (c - b)(c + b)$$

kanssa Koska $2 \nmid a$, niin

$$a = \prod_{i=1}^{r} p_i^{\alpha_i} \quad 2 \neq p_i \in \mathbb{P} \quad \forall i = 1, 2, \ldots, r.$$

Valitaan

$$p_i^{\alpha_i} | a$$

jolloin

$$p_i^{2\alpha_i} | (c-b)(c+b).$$

Jos

$$\begin{aligned} & p_i | c-b \text{ ja } p_i | c+b \\ \Rightarrow \quad & p_i | 2c \text{ ja } p_i | 2b \\ \Rightarrow \quad & p_i | c \text{ ja } p_i | b, \text{ ristiriita.} \end{aligned}$$

Siis joko

$$p_i^{2\alpha_i} | c-b \text{ tai } p_i^{2\alpha_i} | c+b.$$

$$\begin{aligned} \Rightarrow c-b &= \prod_{j \in J} p_j^{2\alpha_j} = \left(\prod_{j \in J} p_j^{\alpha_j} \right)^2 \text{ ja} \\ c+b &= \prod_{l \in L} p_l^{2\alpha_l} = \left(\prod_{l \in L} p_l^{\alpha_l} \right)^2, \text{ missä} \\ J \cup L &= \{1, 2, \ldots, r\} \quad J \cap L = \emptyset. \end{aligned}$$

Huomaa, että b on parillinen ja c pariton, eli

$$2 \nmid c-b \text{ ja } 2 \nmid c+b,$$

ja että $\text{syt}(c-b, c+b) = 1$. Nyt siis on olemassa sellaiset luonnolliset luvut s ja t, $\text{syt}(s,t) = 1$, että

$$\begin{cases} c+b = s^2 \\ c-b = t^2 \end{cases} \Leftrightarrow \begin{cases} c = \frac{s^2+t^2}{2} \\ b = \frac{s^2-t^2}{2} \end{cases} \text{ ja}$$

$$a^2 = s^2 t^2 \quad \Leftrightarrow \quad a = st.$$

Osoita vielä laskemalla, että kolmikko

$$(a, b, c) = (st, \frac{s^2 - t^2}{2}, \frac{s^2 + t^2}{2}) \tag{2.3}$$

toteuttaa Pythagoraan yhtälön (2.2).

Saadaan siis seuraava

Lause 4. Yhtälön

$$a^2 + b^2 = c^2 \tag{2.4}$$

primitiiviset ratkaisut saadaan parametrimuodossa

$$\begin{cases} a = st, \\ b = \frac{s^2 - t^2}{2}, \\ c = \frac{s^2 + t^2}{2}, \end{cases} \tag{2.5}$$

missä $s, t \in 2\mathbb{Z} + 1$, $s > t \geq 1$ ja $\text{syt}(s, t) = 1$.

Esimerkki 4. Olkoon $t = 1$. Annetaan luvulle s parittomia arvoja

$s = 3$	$3^2 + 4^2 = 5^2$
$s = 5$	$5^2 + 12^2 = 13^2$
$\vdots$	$\vdots$
$s = 2m + 1$	$(2m + 1)^2 + (4T_m)^2 =$
	$(2m^2 + 2m + 1)^2$.

Esimerkki 5. Olkoon $t = 2k - 1$ ja $s = 2k + 1$. Nyt

$$\begin{cases} a = 4k^2 - 1, \\ b = 4k, \\ c = 4k^2 + 1. \end{cases}$$

Saatiin siis ratkaisu, missä $c - a = 2$.

2.3 Heronin luvut

Määritelmä 4. Neliövapaa luku $n \in \mathbb{Z}^+$ on Heronin luku eli kongruentti luku, jos $\exists$ sellaiset rationaaliluvut $A, B, C \in \mathbb{Q}^+$, että

$$\begin{cases} A^2 + B^2 = C^2; \\ n = \frac{AB}{2}. \end{cases} \tag{2.6}$$

Lause 5. Neliövapaa luku $n \in \mathbb{Z}^+$ on kongruentti luku $\Leftrightarrow$
on olemassa sellaiset kokonaisluvut $d, s, t \in \mathbb{Z}^+$, että

$$\begin{cases} s, t \in 2\mathbb{Z} + 1, \quad s > t \geq 1, \quad s \perp t; \\ 4nd^2 = st(s^2 - t^2). \end{cases} \tag{2.7}$$

Todistus. "$\Rightarrow$":
Siis (2.6) toteutuu. Olkoon

$$d := p.y.j(\operatorname{den} A, \operatorname{den} B, \operatorname{den} C),$$

$$a := dA, \quad b := dB, \quad c := dC \in \mathbb{Z}^+, \tag{2.8}$$

jolloin

$$\begin{cases} a^2 + b^2 = c^2; \\ s.y.t.(a, b, c) = 1. \end{cases} \tag{2.9}$$

Siten Lauseen 4 nojalla on olemassa sellaiset $s, t \in 2\mathbb{Z} + 1$, että $s > t \geq 1$, $\operatorname{syt}(s, t) = 1$ ja

$$\begin{cases} a = st, \\ b = \frac{s^2 - t^2}{2}, \\ c = \frac{s^2 + t^2}{2}. \end{cases} \tag{2.10}$$

Edelleen

$$n = \frac{AB}{2} = \frac{1}{2}\frac{st}{d}\frac{s^2 - t^2}{2d} \Rightarrow$$

$$4nd^2 = st(s^2 - t^2). \qquad \square \tag{2.11}$$

"$\Leftarrow$":

Valitaan

$$\begin{cases} A := \frac{st}{d}; \\ B := \frac{s^2-t^2}{2d}; \\ C := \frac{s^2+t^2}{2d}. \end{cases} \tag{2.12}$$

Tällöin saadaan

$$\begin{cases} A^2 + B^2 = ... = C^2, \\ n = ... = \frac{AB}{2}. \end{cases} \tag{2.13}$$

Joten (2.6) toteutuu. □

Esimerkki 6. Olkoot

$$A = \frac{3}{2}, \quad B = \frac{20}{3}, \quad C = \frac{41}{6}. \tag{2.14}$$

Tällöin

$$\begin{cases} A^2 + B^2 = C^2, \\ \frac{AB}{2} = 5, \end{cases} \tag{2.15}$$

joten $n = 5$ on Heronin luku.

Heronin lukuja:

$5, 6, 7, 13, 14, 15, 21, 22, 23, 29, 30, 31, 34, 37, 38, 39, 41, ...$

Huomautus 1. Heronin luvut liittyvät elliptisiin käyriin

$$y^2 = x^3 - n^2 x. \tag{2.16}$$

3 Fibonaccin ja Lucasin luvut

3.1 Rekursio ja Binet'n kaava

Määritelmä 5. Luvut $f_0 = 0$, $f_1 = 1$ ja palautuskaava (eli rekursio)

$$f_{n+2} = f_{n+1} + f_n, \quad n \in \mathbb{N}, \tag{3.1}$$

muodostavat Fibonaccin luvut ja luvut $l_0 = 2$, $l_1 = 1$ sekä palautuskaava

$$l_{n+2} = l_{n+1} + l_n, \quad n \in \mathbb{N}, \tag{3.2}$$

muodostavat Lucasin luvut.

Siten Fibonaccin lukuja ovat

$$f_0 = 0, f_1 = 1, f_2 = 1, f_3 = 2, f_4 = 3, f_5 = 5, f_6 = 8, f_7 = 13, ... \tag{3.3}$$

ja Lucasin lukuja ovat

$$l_0 = 2, l_1 = 1, l_2 = 3, l_3 = 4, l_4 = 7, l_5 = 11, l_6 = 18, l_7 = 29, ... \tag{3.4}$$

Ratkaistaan rekursio

$$v_{n+2} = v_{n+1} + v_n, \quad n \in \mathbb{N}, \tag{3.5}$$

yritteellä

$$v_n = x^n, \quad x \in \mathbb{C}^*. \tag{3.6}$$

Rekursiosta (3.5) saadaan

$$x^{n+2} = x^{n+1} + x^n \quad \Leftrightarrow \quad x^2 - x - 1 = 0, \tag{3.7}$$

jonka ratkaisut ovat

$$\alpha = \frac{1+\sqrt{5}}{2}, \quad \beta = \frac{1-\sqrt{5}}{2}. \tag{3.8}$$

Lause 6. Olkoot $a, b \in \mathbb{C}$. Tällöin

$$F_n = a\alpha^n + b\beta^n \tag{3.9}$$

on rekursion (3.5) ratkaisu.

Todistus. Suoraan laskemalla saadaan

$$F_{n+2} = a\alpha^{n+2} + b\beta^{n+2} = a(\alpha^{n+1} + \alpha^n) + b(\beta^{n+1} + \beta^n) =$$

$$a\alpha^{n+1} + b\beta^{n+1} + a\alpha^n + b\beta^n = F_{n+1} + F_n. \quad \square \tag{3.10}$$

Siten Fibonaccin luvut ovat muotoa

$$f_n = a\alpha^n + b\beta^n, \tag{3.11}$$

mistä saadaan

$$f_0 = a\alpha^0 + b\beta^0, \quad f_1 = a\alpha^1 + b\beta^1. \tag{3.12}$$

Sijoitetaan alkuarvot $f_0 = 0$ ja $f_1 = 1$ yhtälöön (3.12), josta

$$a + b = 0, \quad a\frac{1+\sqrt{5}}{2} + b\frac{1-\sqrt{5}}{2} = 1 \tag{3.13}$$

ja siten $a = 1/\sqrt{5}$ ja $b = -1/\sqrt{5}$. Vastaavasti Lucasin luvuille ja siten saadaan.

Lause 7. Fibonaccin ja Lucasin luvut voidaan esittää Binet'n kaavoilla

$$f_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right), \tag{3.14}$$

$$l_n = \left(\frac{1+\sqrt{5}}{2}\right)^n + \left(\frac{1-\sqrt{5}}{2}\right)^n. \tag{3.15}$$

Siis

$$f_n = \frac{1}{\sqrt{5}}\left(\alpha^n - \beta^n\right), \quad l_n = \left(\alpha^n + \beta^n\right), \tag{3.16}$$

missä

$$\alpha = \frac{1+\sqrt{5}}{2}, \quad \beta = \frac{1-\sqrt{5}}{2}. \tag{3.17}$$

Huomaa, että

$$\alpha\beta = -1, \quad \alpha + \beta = 1, \quad \alpha - \beta = \sqrt{5}. \tag{3.18}$$

Lause 8.

$$l_n = \frac{f_{2n}}{f_n}. \tag{3.19}$$

Todistus. Suoraan laskemalla

$$\frac{f_{2n}}{f_n} = \frac{\alpha^{2n} - \beta^{2n}}{\alpha^n - \beta^n} = \alpha^n + \beta^n = l_n. \quad \square \tag{3.20}$$

Huomautus 2. Rekursioilla saadaan tarkat arvot nopeasti (laskennallinen kompleksisuus). Mutta eksplisiittisistä esityksistä (3.14) ja (3.15) saadaan likiarvo nopeasti, jolloin voi soveltaa seuraavaa tulosta.

Lause 9.

$$f_{2k} = \left\lfloor \frac{\alpha^{2k}}{\sqrt{5}} \right\rfloor \quad \forall k \in \mathbb{N}, \tag{3.21}$$

$$f_{2k+1} = \left\lceil \frac{\alpha^{2k+1}}{\sqrt{5}} \right\rceil \quad \forall k \in \mathbb{N}. \tag{3.22}$$

Todistus. Aluksi haetaan likiarvot. Koska

$$\alpha = \frac{1+\sqrt{5}}{2} = 1.6180..., \tag{3.23}$$

ja $\alpha^{-1} = \alpha - 1 = 0.6180...$, niin

$$\beta = \frac{1-\sqrt{5}}{2} = 1 - \alpha = -0.6180.... \tag{3.24}$$

Siten

$$|\beta^n/\sqrt{5}| < 1 \quad \forall \quad n \in \mathbb{N}. \tag{3.25}$$

Tarkemmin laskareissa.

3.2 Matriisiesitys

Olkoon

$$\mathbb{F} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} f_2 & f_1 \\ f_1 & f_0 \end{pmatrix}. \tag{3.26}$$

Lasketaan potensseja

$$\mathbb{F}^2 = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} f_3 & f_2 \\ f_2 & f_1 \end{pmatrix}, \tag{3.27}$$

$$\mathbb{F}^3 = \begin{pmatrix} 3 & 2 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} f_4 & f_3 \\ f_3 & f_2 \end{pmatrix}. \tag{3.28}$$

Jolloin huomataan, että alkioiksi tulee Fibonaccin lukuja.

Sovitaan vielä, että $f_{-1} = 1$, sillä tällöin pätee

$$f_1 = f_0 + f_{-1}. \tag{3.29}$$

Nyt

$$\mathbb{F}^0 = \mathbb{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} f_1 & f_0 \\ f_0 & f_{-1} \end{pmatrix}. \tag{3.30}$$

Lause 10. Olkoon

$$\mathbb{F}_n = \begin{pmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{pmatrix}. \tag{3.31}$$

Tällöin

$$\mathbb{F}^n = \mathbb{F}_n \quad \forall n \in \mathbb{N}. \tag{3.32}$$

Todistus. Induktiolla. Tapaukset $n = 0$ ja $n = 1$ kohdista (3.26) ja (3.30).

Induktio-oletus: Identiteetti (3.32) pätee, kun $n = k$.

Induktioaskel; Lasketaan

$$\mathbb{F}^{k+1} = \mathbb{F}^1\mathbb{F}^k = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} f_{k+1} & f_k \\ f_k & f_{k-1} \end{pmatrix} = \tag{3.33}$$

$$\begin{pmatrix} f_{k+1} + f_k & f_k + f_{k-1} \\ f_{k+1} & f_k \end{pmatrix} = \begin{pmatrix} f_{k+2} & f_{k+1} \\ f_{k+1} & f_k \end{pmatrix} = \mathbb{F}_{k+1}. \quad \square \tag{3.34}$$

Lause 11. Olkoot $n, m \in \mathbb{N}$, tällöin

$$f_{n+m+1} = f_{n+1}f_{m+1} + f_nf_m, \tag{3.35}$$

$$f_{2m+1} = f_{m+1}^2 + f_m^2, \tag{3.36}$$

$$f_{2m} = f_m(f_{m+1} + f_{m-1}). \tag{3.37}$$

Todistus. Sovelletaan identiteettiä

$$\mathbb{F}_{n+m} = \mathbb{F}^{n+m} = \mathbb{F}^n\mathbb{F}^m = \mathbb{F}_n\mathbb{F}_m, \tag{3.38}$$

jolloin

$$\begin{pmatrix} f_{n+m+1} & f_{n+m} \\ f_{n+m} & f_{n+m-1} \end{pmatrix} = \tag{3.39}$$

$$\begin{pmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{pmatrix} \begin{pmatrix} f_{m+1} & f_m \\ f_m & f_{m-1} \end{pmatrix} = \tag{3.40}$$

$$\begin{pmatrix} f_{n+1}f_{m+1} + f_nf_m & f_{n+1}f_m + f_nf_{m-1} \\ f_nf_{m+1} + f_{n-1}f_m & f_nf_m + f_{n-1}f_{m-1} \end{pmatrix}. \tag{3.41}$$

Vertaamalla matriisien (3.39) ja (3.41) vastinalkioita saadaan (3.35), josta edelleen saadaan (3.36) ja (3.37). □

Lause 12. Olkoon $n \in \mathbb{N}$, tällöin

$$f_{n+1}f_{n-1} - f_n^2 = (-1)^n. \tag{3.42}$$

Todistus. Otetaan determinantit tuloksesta (3.32), jolloin

$$\begin{vmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{vmatrix} = \begin{vmatrix} 1 & 1 \\ 1 & 0 \end{vmatrix}^n. \quad \square \tag{3.43}$$

Lause 13. Olkoon $n \in \mathbb{N}$, tällöin lukujen f_{n+2} ja f_{n+1} Eukleideen algoritmin pituus on n. Edelleen

$$\text{syt}(f_{n+1}, f_n) = 1. \tag{3.44}$$

Todistus. Olkoot $a = f_{n+2}$ ja $b = f_{n+1}$, jolloin

$$
\begin{aligned}
&r_0 = a,\ r_1 = b && 0 \le r_1 < r_0 \\
&r_0 = q_1 r_1 + r_2 = 1 \cdot r_1 + r_2 && 0 \le r_2 < r_1 \\
&\text{sillä } f_{n+2} = 1 \cdot f_{n+1} + f_n \\
&r_1 = q_2 r_2 + r_3 = 1 \cdot r_2 + r_3 && 0 \le r_3 < r_2 \\
&\text{sillä } f_{n+1} = 1 \cdot f_n + f_{n-1} \\
&\vdots \\
&r_k = q_{k+1} r_{k+1} + r_{k+2} = 1 \cdot r_{k+1} + r_{k+2} && 0 \le r_{k+2} < r_{k+1} \\
&\text{sillä } f_{n+2-k} = 1 \cdot f_{n+1-k} + f_{n-k} \\
&\vdots \\
&r_{n-2} = q_{n-1} r_{n-1} + r_n = 1 \cdot r_{n-1} + r_n && 1 = r_n < r_{n-1} = 2 \\
&\text{sillä } f_4 = 1 \cdot f_3 + f_2 \\
&r_{n-1} = q_n r_n = 2 \cdot 1
\end{aligned}
$$

siten

$$r_n = \text{syt}(a, b) = 1. \quad \square \tag{3.45}$$

Edelleen saadaan

Seuraus 1.

$$r_n = s_n a + t_n b \quad \Leftrightarrow \quad 1 = s_n f_{n+2} + t_n f_{n+1}, \tag{3.46}$$

missä s_n ja t_n saadaan palautuskaavoista

$$s_{k+2} = s_k - q_{k+1} s_{k+1} = s_k - s_{k+1}, \tag{3.47}$$

$$t_{k+2} = t_k - q_{k+1} t_{k+1} = t_k - t_{k+1} \quad \forall \quad 0 \le k \le n-2 \tag{3.48}$$

lähtien alkuarvoista $s_0 = t_1 = 1$, $s_1 = t_0 = 0$.

Esimerkki 7.

Olkoot $n = 5$, $f_7 = 13$, $f_6 = 8$, jolloin $q_1 = ... = q_4 = 1$ ja $q_5 = 2$. Siten $s_2 = 1, s_3 = -1, s_4 = 2, s_5 = -3$,... $t_5 = 5$ ja

$$1 = (-3) \cdot 13 + 5 \cdot 8 = f_5 f_6 - f_4 f_7. \tag{3.49}$$

Lause 14. Olkoon $a, b \in \mathbb{Z}^+$ annettu, tällöin Eukleideen algoritmin pituudelle n pätee

$$n \leq \log a / \log((1 + \sqrt{5})/2)). \tag{3.50}$$

Eukleideen algoritmissa

$$\begin{aligned}
&r_0 = a,\ r_1 = b && 0 < r_1 < r_0 \\
&r_0 = q_1 r_1 + r_2 && 0 < r_2 < r_1 \\
&\vdots \\
&r_k = q_{k+1} r_{k+1} + r_{k+2} && 0 < r_{k+2} < r_{k+1} \\
&\vdots \\
&r_{n-2} = q_{n-1} r_{n-1} + r_n && 0 < r_n < r_{n-1} \\
&r_{n-1} = q_n r_n + 0
\end{aligned}$$

osamäärien kokonaisosille pätee $q_k \geq 1$ kaikilla k.

Täten

$$r_n \geq 1 = f_2, \tag{3.51}$$

$$r_{n-1} \geq 2 = f_3, \tag{3.52}$$

$$r_{n-2} \geq 1 \cdot r_{n-1} + r_n \geq f_3 + f_2 = f_4. \tag{3.53}$$

Edelleen induktiolla saadaan

$$r_{n-h} \geq f_{h+2} \quad \forall \quad h = 0, 1, ..., n \tag{3.54}$$

ja siten

$$a = r_0 \geq f_{n+2} \geq ((1+\sqrt{5})/2)^n. \tag{3.55}$$

Epäyhtälön (3.55) todistus laskareissa. □

3.3 Generoiva sarja

Olkoon

$$F(z) = \sum_{k=0}^{\infty} f_k z^k \tag{3.56}$$

sarja, jolle haetaan lauseke tunnettujen funktioiden avulla. Vaihdetaan aluksi summausindeksi $k = n + 2$, jolloin

$$F(z) = \sum_{n=0}^{\infty} f_{n+2} z^{n+2} + f_1 z + f_0. \tag{3.57}$$

Seuraavaksi käytetään rekursiota (3.1), jolloin

$$F(z) = z \sum_{n=0}^{\infty} f_{n+1} z^{n+1} + z^2 \sum_{n=0}^{\infty} f_n z^n + f_1 z + f_0 =$$

$$z \sum_{k=1}^{\infty} f_k z^k + z^2 \sum_{k=0}^{\infty} f_k z^k + f_1 z + f_0 =$$

$$z(F(z) - f_0) + z^2 F(z) + z. \tag{3.58}$$

Yhtälöstä (3.58) saadaan ratkaisu

$$F(z) = \frac{z}{1 - z - z^2}. \tag{3.59}$$

Lause 15. Sarjalla

$$F(z) = \sum_{k=0}^{\infty} f_k z^k \tag{3.60}$$

on esitys rationaalifunktiona

$$F(z) = \frac{z}{1 - z - z^2}. \tag{3.61}$$

Määritelmä 6. Sarja

$$F(z) = \sum_{k=0}^{\infty} f_k z^k \tag{3.62}$$

on Fibonaccin lukujen generoiva sarja ja funktio

$$F(z) = \frac{z}{1 - z - z^2} \tag{3.63}$$

on Fibonaccin lukujen generoiva funktio.

Määritelmä 7. Polynomi

$$K(x) = K_f(x) = x^2 - x - 1 \tag{3.64}$$

on rekursion (3.1) karakteristinen polynomi.

Huomaa, että

$$K_f(x) = (x - \alpha)(x - \beta), \tag{3.65}$$

joten

$$F(z) = \frac{1/z}{(1/z)^2 - 1/z - 1} = \frac{1/z}{K(1/z)} =$$

$$\frac{1/z}{(1/z - \alpha)(1/z - \beta)} = \frac{z}{(1 - \alpha z)(1 - \beta z)}. \tag{3.66}$$

Jaetaan (3.66) osamurtoihin ja käytetään geometrisen sarjan summakaavaa, jolloin

$$F(z) = \frac{1}{\sqrt{5}} \left(\frac{1}{1 - \alpha z} - \frac{1}{1 - \beta z} \right) =$$

$$\sum_{k=0}^{\infty} \frac{1}{\sqrt{5}} \left(\alpha^k - \beta^k \right) z^k = \sum_{k=0}^{\infty} f_k z^k. \tag{3.67}$$

Vertaamalla sarjojen kertoimia saadaan jälleen Binet'n esitys (3.14).

3.4 Laajennus negatiivisiin indekseihin

Lauseiden 16, 17, 18 ja 19 todistuksia ei vaadita kokeessa.

Sallitaan Fibonaccin lukujen palautuskaavassa

$$f_{k+2} = f_{k+1} + f_k \tag{3.68}$$

negatiiviset indeksit, jolloin asettamalla $k = -1, -2, ...,$ saadaan

$$f_1 = f_0 + f_{-1} \Rightarrow f_{-1} = 1, \tag{3.69}$$

$$f_0 = f_{-1} + f_{-2} \Rightarrow f_{-2} = -1, \tag{3.70}$$

$$f_{-1} = f_{-2} + f_{-3} \Rightarrow f_{-3} = 2, ... \tag{3.71}$$

Sijoitetaan $k = -n$ rekursioon (3.68), jolloin

$$f_{-n} = -f_{-(n-1)} + f_{-(n-2)}. \tag{3.72}$$

Lause 16.

$$f_{-n} = (-1)^{n+1} f_n \quad \forall\ n \in \mathbb{N}. \tag{3.73}$$

Todistus. Induktiolla käyttäen rekursiota (3.72).

Äskeisen tuloksen nojalla Lause 10 laajenee myös negatiiviselle puolelle.

Lause 17. Olkoon

$$\mathbb{F}_n = \begin{pmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{pmatrix}. \tag{3.74}$$

Tällöin

$$\mathbb{F}^n = \mathbb{F}_n \quad \forall n \in \mathbb{Z}. \tag{3.75}$$

Todistus. $n \geq 0$ kts. Lause 10.

$n \leq 0$.

Alkuaskel: $n = -1$. Aluksi määrätään käänteismatriisi

$$\mathbb{F}^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \tag{3.76}$$

ja toisaalta

$$\mathbb{F}_{-1} = \begin{pmatrix} f_0 & f_{-1} \\ f_{-1} & f_{-2} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}. \tag{3.77}$$

Sitten induktio.

Edelleen, Lauseet 11 ja 12 laaajenevat negatiivisiin indekseihin.

Lause 18. Olkoot $n, m \in \mathbb{Z}$, tällöin

$$f_{n+m+1} = f_{n+1}f_{m+1} + f_n f_m, \tag{3.78}$$

$$f_{2m+1} = f_{m+1}^2 + f_m^2, \tag{3.79}$$

$$f_{2m} = f_m(f_{m+1} + f_{m-1}). \tag{3.80}$$

Huomaa, että (3.78) on yhtäpitävä kaavan

$$f_{n+m} = f_{n+1}f_m + f_n f_{m-1} \tag{3.81}$$

kanssa.

Lause 19. Olkoon $n \in \mathbb{Z}$, tällöin

$$f_{n+1}f_{n-1} - f_n^2 = (-1)^n. \tag{3.82}$$

3.5 Jaollisuustuloksia

Lause 20. Olkoot $n, r, N, M \in \mathbb{Z}$, tällöin

$$f_n | f_{rn}, \tag{3.83}$$

ja jos $(M, N) = d$, niin

$$(f_M, f_N) = f_d \tag{3.84}$$

ja jos $M \perp N$, niin

$$f_M f_N | f_{MN}. \tag{3.85}$$

Todistus. Kohta (3.83). Relaatiosta (3.80) saadaan

$$f_{2n} = f_n(f_{n+1} + f_{n-1}), \tag{3.86}$$

joten saadaan induktion alkuaskel

$$f_n | f_{2n}. \tag{3.87}$$

Sijoitetaan $m = rn$ yhtälöön (3.81), jolloin

$$f_{(r+1)n} = f_{n+1} f_{rn} + f_n f_{rn-1}, \tag{3.88}$$

jonka avulla saadaan induktioaskel ja siten (3.83) todistettua arvoilla $r \geq 1$. Koska $f_0 = 0$, niin $f_n | f_0$ aina, kun $n \in \mathbb{Z}$. Tapaus $r \leq 0$ pienin säädöin vastaavasti. □

Kohta (3.84). Nyt $M = dm$ ja $N = dk$, joillakin $m, k \in \mathbb{Z}$. siten kohdan (3.83) nojalla

$$f_d | f_M, \quad f_d | f_N. \tag{3.89}$$

Lauseen **??** nojalla on olemassa sellaiset $r, s \in \mathbb{Z}$, että

$$d = rN + sM, \tag{3.90}$$

joten jälleen kaavan (3.81) nojalla

$$f_d = f_{rN+sM} = f_{rN+1}f_{sM} + f_{rN}f_{sM-1}. \tag{3.91}$$

Jos, nyt

$$c|f_M, \quad c|f_N, \tag{3.92}$$

niin kohdan (3.83) nojalla

$$c|f_{sM}, \quad c|f_{rN}. \tag{3.93}$$

Täten kohdan (3.91) nojalla saadaan

$$c|f_d. \tag{3.94}$$

Kohdan (3.89) nojalla f_d on yhteinen tekijä ja kohdan (3.94) nojalla suurin tekijä.

□

Kohta (3.85) laskarit.

3.6 $f_n \pmod k$

Tarkastellaan Fibonaccin jonoa $(f_n) = (f_n)_{n=0}^{\infty} \pmod k$.

Esimerkki 8.

$$(f_n) \equiv (0,1,1,0,1,1,0,1,1,...) \pmod 2. \tag{3.95}$$

$$(f_n) \equiv (0,1,1,2,0,2,2,1,0,1,1,...) \pmod 3. \tag{3.96}$$

$$(f_n) \equiv (0,1,1,2,3,0,3,3,1,4,0,4,4,3,2,0,2,2,4,1,$$

$$0,1,1,...) \pmod 5. \tag{3.97}$$

$$(f_n) \equiv (0,1,1,2,3,5,8,3,1,4,5,9,4,3,7,0,7,7,...) \pmod{10}, \tag{3.98}$$

$$f_{15} = f_{30} = f_{45} = f_{60} \equiv 0,\ f_{61} = f_{62} \equiv 1 \pmod{10}. \tag{3.99}$$

Siten

$$f_{3+l} \equiv f_l \pmod{2}, \quad \forall\, l \in \mathbb{N}. \tag{3.100}$$

$$f_{8+l} \equiv f_l \pmod{3}, \quad \forall\, l \in \mathbb{N}. \tag{3.101}$$

$$f_{20+l} \equiv f_l \pmod{5}, \quad \forall\, l \in \mathbb{N}. \tag{3.102}$$

$$f_{60+l} \equiv f_l \pmod{10}, \quad \forall\, l \in \mathbb{N}. \tag{3.103}$$

Määritelmä 8. Jonon (a_l) jakso on luku $J = J_a \in \mathbb{Z}^+$, jolle pätee

$$a_{l+J} = a_l \quad \forall\, l \in \mathbb{N}. \tag{3.104}$$

Minimijakso$= MJ_a = \min\{J \in \mathbb{Z}^+ | J = jakso\}$.

Olkoon $J_f = J_f(k)$ Fibonaccin jonon jakso $\pmod{k}$.

Esimerkki 9.

$$MJ_f(2) = 3,\ MJ_f(3) = 8,\ MJ_f(5) = 20,\ MJ_f(10) = 60. \tag{3.105}$$

Lause 21.

$$MJ_f(k) \leq k^2 \quad \forall k \in \mathbb{Z}_{\geq 2}. \tag{3.106}$$

Todistus. Tarkastellaan jonoa

$$(\overline{f}_n) \subseteq \mathbb{Z}_k = \{\overline{0}, ..., \overline{k-1}\} \tag{3.107}$$

Koska

$$\#\mathbb{Z}_k^2 = \#\{(\overline{a}, \overline{b}) |\ \overline{a}, \overline{b} \in \mathbb{Z}_k\} = k^2, \tag{3.108}$$

niin joukossa

$$\{(\overline{f}_l, \overline{f}_{l+1}) |\ l = 0, 1, ..., k^2\} \tag{3.109}$$

on sellaiset alkiot, että

$$(\overline{f}_l, \overline{f}_{l+1}) = (\overline{f_h}, \overline{f}_{h+1}) \tag{3.110}$$

ja $0 \leq l < h \leq k^2$. Olkoon $J = h - l$, tällöin

$$\overline{f}_{l+J} = \overline{f}_l, \quad \overline{f}_{l+J+1} = \overline{f}_{l+1} \tag{3.111}$$

ja siten rekursion nojalla

$$\overline{f}_{n+J} = \overline{f}_n \quad \forall\ n \in \mathbb{N}, \tag{3.112}$$

missä $1 \leq J \leq k^2$. □

Esimerkki 10.

$$J_f(10) = 60 < 10^2. \tag{3.113}$$

3.7 $f_n \pmod p$

Binet'n kaavan (3.14) avulla

$$f_n = \frac{1}{2^n\sqrt{5}} \left(\left(1 + \sqrt{5}\right)^n - \left(1 - \sqrt{5}\right)^n \right) =$$

$$\frac{1}{2^n\sqrt{5}} \sum_{i=0}^{n} \binom{n}{i} \left(\sqrt{5}^i - \left(-\sqrt{5}\right)^i \right) =$$

$$\frac{1}{2^n\sqrt{5}} \left(\binom{n}{0} \cdot 0 + \binom{n}{1} \cdot 2\sqrt{5} + \binom{n}{2} \cdot 0 + \binom{n}{3} \cdot 2\sqrt{5}^3 + ... \right), \tag{3.114}$$

josta

$$2^{n-1}f_n = \sum_{j=0}^{\lfloor \frac{n-1}{2} \rfloor} \binom{n}{2j+1} 5^j. \tag{3.115}$$

Lause 22. Olkoon $p \in \mathbb{P}_{\geq 7}$.

1.) Jos,

$$5^{\frac{p-1}{2}} \equiv 1 \pmod{p}, \tag{3.116}$$

niin

$$f_{p-1} \equiv 0 \pmod{p} \quad \text{ja} \quad MJ_f(p) \leq p-1. \tag{3.117}$$

2.) Jos,

$$5^{\frac{p-1}{2}} \equiv -1 \pmod{p}, \tag{3.118}$$

niin

$$f_{p+1} \equiv 0 \pmod{p} \quad \text{ja} \quad MJ_f(p) \leq 2p+2. \tag{3.119}$$

Huomautus 3. Kurssilla Lukuteoria A osoitetaan neliöjäännösteorian avulla, että

1.) (3.116) $\Leftrightarrow p = 5m \pm 1$.

2.) (3.118) $\Leftrightarrow p = 5m \pm 2$.

Todistus. Yhtälöstä (3.115) saadaan

$$2^{p-1}f_p = \sum_{j=0}^{\frac{p-1}{2}} \binom{p}{2j+1} 5^j = \binom{p}{1} + \binom{p}{3} 5 + ... + \binom{p}{p} 5^{\frac{p-1}{2}}, \tag{3.120}$$

josta Lauseiden **??** ja **??** nojalla

$$f_p \equiv 5^{\frac{p-1}{2}} \pmod{p}. \tag{3.121}$$

Edelleen, asettamalla $n = p+1$ yhtälöön (3.115) saadaan

$$2^p f_{p+1} = \sum_{j=0}^{\lfloor \frac{p}{2} \rfloor} \binom{p+1}{2j+1} 5^j = \binom{p+1}{1} + \binom{p+1}{3} 5 + ...$$

$$+\binom{p+1}{p}5^{\frac{p-1}{2}}. \tag{3.122}$$

Tässä

$$\binom{p+1}{3} = \frac{(p+1)p(p-1)}{3\cdot 2} \equiv 0 \pmod{p} \tag{3.123}$$

ja yleisemminkin pätee

$$\binom{p+1}{k} \equiv 0 \pmod{p} \quad \forall\ 2 \leq k \leq p-1. \tag{3.124}$$

Siten yhtälön (3.122) nojalla

$$2f_{p+1} \equiv 1 + 5^{\frac{p-1}{2}} \pmod{p}. \tag{3.125}$$

Merkitään $a = 5^{\frac{p-1}{2}}$, jolloin $a^2 \equiv 1 \pmod{p}$. Nyt Lauseen **??** todistuksen nojalla $a \equiv \pm 1 \pmod{p}$.

1.) Olkoon $a \equiv 1 \pmod{p}$. Tällöin yhtälöiden (3.121) ja (3.125) nojalla

$$f_p \equiv 1, \quad f_{p+1} \equiv 1 \pmod{p}. \tag{3.126}$$

Täten, ensin rekursion avulla

$$f_{p-1} \equiv 0 \pmod{p} \tag{3.127}$$

ja edelleen rekursion nojalla

$$f_{p-1+l} \equiv f_l \pmod{p} \quad \forall l \in \mathbb{N}, \tag{3.128}$$

joten $J_f(p) = p - 1$.

2.) Olkoon $a \equiv -1 \pmod{p}$. Tällöin yhtälöiden (3.121) ja (3.125) nojalla

$$f_p \equiv -1, \quad f_{p+1} \equiv 0 = f_0 \pmod{p}. \tag{3.129}$$

Täten

$$f_{p+2} \equiv -1 = -f_1 \pmod{p}, \tag{3.130}$$

$$f_{p+3} \equiv -1 = -f_2 \pmod{p} \tag{3.131}$$

ja edelleen

$$f_{2p+1} \equiv -f_p \equiv 1 \pmod{p} \tag{3.132}$$

sekä

$$f_{2p+2} \equiv -f_{p+1} \equiv 0, \pmod{p} \tag{3.133}$$

joten $J_f(p) = 2p + 2$.

Esimerkki 11. $p = 11 \equiv 1 \pmod 5$, jolloin

$$5^{\frac{p-1}{2}} = 5^5 \equiv 1 \pmod{11}. \tag{3.134}$$

Nyt $11|f_{10}$ ja $\mathrm{MJ}_f(11) = 10 = p - 1$.

Esimerkki 12. $p = 29 \equiv -1 \pmod 5$ ja

$$5^{\frac{p-1}{2}} = 5^{14} \equiv 1 \pmod{29}. \tag{3.135}$$

Nyt $29|f_{28}$ mutta $\mathrm{MJ}_f(29) = 14 = (p-1)/2$.

Esimerkki 13. $p = 7 \equiv 2 \pmod 5$ ja

$$5^{\frac{p-1}{2}} = 5^3 \equiv -1 \pmod{7}. \tag{3.136}$$

Nyt $7|f_8$ ja $\mathrm{MJ}_f(7) = 16 = 2p + 2$.