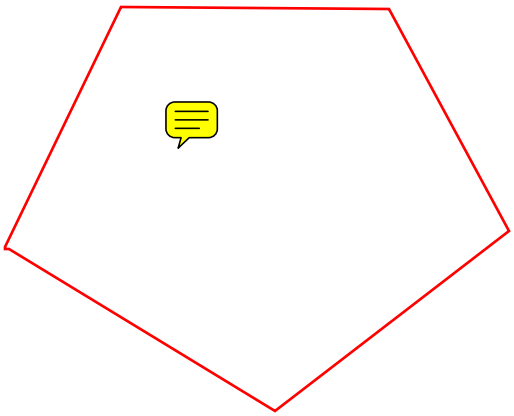

LUKUTEORIA I

Tapani Matala-aho

19. helmikuuta 2009

Sisältö

~~TIEDOTE: Kevät 2009~~

~~1. Välikoe ma 9.3.2009 klo 14–18 L1.~~

~~1. välikokeen alue: Kappaleet 1–10.~~

~~2. Välikoe ma 11.5.2009 klo 14–18 L1~~

LUKUTEORIA, NUMBER THEORY, THÉORIE DES NOMBRES

1 Johdanto

Työn alla.....

Lukuteoria eli aritmetiikka tutkii erityisesti kokonaislukuihin liittyviä kysymyksiä. Aritmetiikan määritelmästä: Ensinnäkin, alkeisaritmetiikka eli alkeismatematiikka voidaan käsittää kokonaislukujen ja niiden laskutoimitusten-yhteenlasku, vähennyslasku, kertolasku ja jakolasku-muodostamaksi järjestelmäksi. Esimerkiksi korttipeli voidaan ajatella matemaattiseksi järjestelmäksi, jossa lukuja vastaavat kortit ja laskutoimituksia pelin säännöt. Toisaalta aritmetiikka laajasti katsottuna sisältää myös tutkimukselliset kysymykset ja niiden tarkasteluun kehitetyt työkalut. Tällöin termit lukuteoria ja aritmetiikka samaistetaan-kuten voi nähdä alan päälehtien Acta Arithmetica ja Journal of Number Theory nimistä.

LÄHTEITÄ:

G.H. Hardy E.M. Wright: An Introduction to the Theory of Numbers.
Kenneth H. Rosen: Elementary number theory and its applications.
Number Theory Web
American Mathematical monthly

Voit ilmoittaa löytämäsi painovirheet ja muut töpeksinnät E-mail osoitteeseen:

etunimi.sukunimi@oulu.fi
Tapani Matala-aho

2 Merkintöjä

2.1 Lukujoukot

$\mathbb{N} = \{0, 1, 2, \ldots, GOOGOL^{10}, \ldots\} = \{\text{ei-negatiiviset kokonaisluvut}\}$.

$\mathbb{P} = \{2, 3, 5, 7, 11, \ldots\} = \{\text{alkuluvut}\}$.

$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\} = \{\text{kokonaisluvut}\}$.

$\mathbb{Z}^+ = \{1, 2, 3, \ldots\} = \mathbb{N}\backslash\{0\} = \{\text{positiiviset kokonaisluvut}\}$.

$\mathbb{Z}^- = \{-1, -2, -3, \ldots\} = \mathbb{Z}\backslash\mathbb{N} = \{\text{negatiiviset kokonaisluvut}\}$.

$\mathbb{Q} = \{\frac{m}{n} \mid m \in \mathbb{Z}, n \in \mathbb{Z}^+\} = \{\text{rationaaliluvut}\}$.

$\mathbb{R} = \{x \mid x = \sum_{k=l}^{\infty} a_k 10^{-k},\ l \in \mathbb{Z};\ a_k \in \{0, \ldots, 9\}\} = \{\text{reaaliluvut }\}$.

$\mathbb{C} = \mathbb{R}(i) = \{a + ib|\ a, b \in \mathbb{R}, i^2 = -1\} = \{\text{ kompleksiluvut}\}$

$\mathbb{C} \setminus \mathbb{Q} = \{\text{ Irrationaaliluvut }\}$.

$\mathbb{Z}_{\geq m} = \{k \in \mathbb{Z}|\ k \geq m\}$. $\mathbb{R}_{\leq 0} = \{r \in \mathbb{R}|\ r \leq 0\}, ...$

$\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$, $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$,

Olkoot a, b lukuja ja J lukujoukko:

$$aJ + b = \{aj + b \mid j \in J\}.$$

ESIM: $J = \mathbb{Z},\ b \in \mathbb{Z},\ n \in \mathbb{Z}^+$, tällöin merkitään

$$\overline{b} = n\mathbb{Z} + b,$$

joka on jakojäännösluokka (mod n) ja

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{b} \mid b \in \{0, 1, \ldots, n-1\}\},$$

joka on jakojäännösrengas (mod n).

$\exists!$ $\Leftrightarrow \exists$ täsmälleen yksi.

$A \subsetneqq B \Leftrightarrow A \subseteq B$ ja $A \neq B$.

$\#A = |A|$ = Joukon A alkioiden lukumäärä.

Olkoon $A = \{a_1, ..., a_m\}$, tällöin

$$\sum_{a \in A} f(a) = f(a_1) + ... + f(a_m),$$

$$\prod_{a \in A} f(a) = f(a_1) \cdots f(a_m).$$

Jos $A = \varnothing$, niin

$$\sum_{a \in A} f(a) = 0, \quad \prod_{a \in A} f(a) = 1$$

(tyhjä summa ja tulo). Edelleen "Summaus n. tekijöiden yli"

$$\sum_{d|n} f(d) = f(d_1) + ... + f(d_k),$$

missä $d_i \in \mathbb{Z}^+$ ovat n:n erilliset tekijät. "Summaus n. alkutekijöiden yli"

$$\sum_{p|n} f(p) = \sum_{p|n, p \in \mathbb{P}} f(p).$$

"Tulo n. alkutekijöiden yli"

$$\prod_{p|n} f(p) = \prod_{p|n, p \in \mathbb{P}} f(p).$$

2.2 Porrasfunktiot

Määritelmä 2.1. Lattiafunktio (eli porrasfunktio):

$$\lfloor\ \rfloor : \mathbb{R} \to \mathbb{Z},$$

$$\lfloor x \rfloor = [x] = \max\{n \in \mathbb{Z} \mid n \leqslant x\}$$

aina, kun $x \in \mathbb{R}$.

ESIM: Jos $x \in \mathbb{R}_{\geq 0}$, niin tällöin $\lfloor x \rfloor$ on x:n kokonaisosa, mutta esimerkiksi $\lfloor -1.2 \rfloor = -2$.

Määritelmä 2.2. Kattofunktio:

$$\lceil\ \rceil : \mathbb{R} \to \mathbb{Z},$$

$$\lceil x \rceil = \min\{n \in \mathbb{Z} \mid x \leq n\}$$

aina, kun $x \in \mathbb{R}$.

Apulause. *Olkoon $x \in \mathbb{R}$ muotoa*

$$x = k + c, \quad k \in \mathbb{Z},\ 0 \leq c < 1. \tag{2.1}$$

Tällöin

$$k = \lfloor x \rfloor. \tag{2.2}$$

Edelleen

$$\lceil x \rceil = -\lfloor -x \rfloor \quad \forall x \in \mathbb{R}, \tag{2.3}$$

$$\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1 \quad \forall x \in \mathbb{R} \tag{2.4}$$

$$\lfloor x + k \rfloor = \lfloor x \rfloor + k \quad \forall x \in \mathbb{R}, \forall k \in \mathbb{Z}, \tag{2.5}$$

$$\lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x + y \rfloor \quad \forall x, y \in \mathbb{R}, \tag{2.6}$$

$$\lfloor x \rfloor \lfloor y \rfloor \leq \lfloor xy \rfloor \quad \forall x, y \in \mathbb{R}_{\geq 0}. \tag{2.7}$$

3 Kokonaislukurengas $\mathbb{Z}$

3.1 Jaollisuus, alkuluvut

Määritelmä 3.1. Olkoot $a, b \in \mathbb{Z}$. Tällöin

$$b|a \quad \Leftrightarrow \quad \exists c \in \mathbb{Z}: \quad a = bc. \tag{3.1}$$

Kun $b|a$, niin b jakaa (divides) a:n eli b on a:n tekijä (factor) eli a on b:n monikerta (multiple).

Merkitään: $b \nmid a$, kun b ei jaa a:ta.

Asetetaan "aksiomi":

$$\text{Jos} \quad b|1, \text{niin} \quad b = \pm 1. \tag{3.2}$$

3.2 Voidaan todistaa itseisarvon ja järjestyksen ominaisuuksilla.
ESIM.1:

$$0|0, \quad 0 \nmid a \neq 0. \tag{3.3}$$

Merkintöjä: Olkoot $d, n \in \mathbb{Z}, d \geq 2$, tällöin

$$d^s||n \;\Leftrightarrow\; d^s|n \; ja \; d^{s+1} \nmid n. \tag{3.4}$$

Olkoon $k \in \mathbb{Z}$, tällöin

$$k\mathbb{Z} = \{ka|\ a \in \mathbb{Z}\} = \tag{3.5}$$

k:lla jaollisten kokonaislukujen joukko eli k:n monikerrat.

ESIM 2:

$$3^4||162, \quad 1\mathbb{Z} = \mathbb{Z}, \quad 0\mathbb{Z} = \{0\}. \tag{3.6}$$

Määritelmä 3.2. Olkoon $q \in \mathbb{Z}$ annettu ja olkoon $d|q, d \in \mathbb{Z}$. Jos $d \in \{1, -1, q, -q\}$, niin d on luvun q triviaali tekijä. Jos $d \notin \{1, -1, q, -q\}$, niin d on luvun q aito tekijä.

Määritelmä 3.3. Luku $q \in \mathbb{Z}$ on jaoton (irreducible) $\Leftrightarrow$ Jos $d|q$, niin $d = \pm 1$ tai $d = \pm q$.

Siten jaottomalla kokonaisluvulla q on vain triviaalit tekijät $1, -1, q, -q$.

Määritelmä 3.4. Luku $p \in \mathbb{Z}$, $p \geq 2$ on alkuluku (prime) $\Leftrightarrow$
Jos $d|p$, niin $d = \pm 1$ tai $d = \pm p$.

Merkintä: Alkulukujen joukko

$$\mathbb{P} = \{p|\ p\ on\ alkuluku\}.$$

Siten $p \in \mathbb{P} \Leftrightarrow p$ on jaoton ja $p \geq 2$, joten

$$\mathbb{P} = \{p|\ 2, 3, 5, 7, 11, ..., 101, ...\}.$$

Alkutekijä=alkulukutekijä=(prime factor).

Määritelmä 3.5. Luku $n \in \mathbb{Z}$, on yhdistetty (composite) luku $\Leftrightarrow$
n:llä on ainakin 2 alkutekijää.

ESIM. 3: -4 on yhdistetty. 0 on yhdistetty. -3 ei ole yhdistetty eikä alkuluku mutta on jaoton.

Määritelmä 3.6. Luvun $n \in \mathbb{Z}_{\geq 2}$ esitys

$$n = p_1^{r_1} \cdots p_t^{r_t}, \quad p_i \in \mathbb{P}, \quad r_i \in \mathbb{Z}^+ \tag{3.7}$$

on luvun n luonnollinen alkulukuesitys (kanoninen alkulukuhajoitelma, prime factorization).

Jos, $m/n \in \mathbb{Q}^*$, niin

$$\frac{m}{n} = p_0^{r_0} p_1^{r_1} \cdots p_t^{r_t}, \quad p_i \in \mathbb{P}, \quad p_0 = -1 \quad r_i \in \mathbb{Z}. \tag{3.8}$$

ESIM. 4:

$$-1 = (-1)^1 2^0 3^0, \quad \frac{40}{128} = \frac{2^3 5}{2^7} = 2^{-4} 5^1 \tag{3.9}$$

3.2 Jakoalgoritmi

Lause 3.1. *Olkoot $a, b \in \mathbb{Z}$ ja $b \neq 0$. Tällöin*

$$\exists! q \in \mathbb{Z} \quad ja \quad \exists! r \in \mathbb{N} :$$

$$a = qb + r, \quad 0 \leq r < |b|. \tag{3.10}$$

Kun $b \in \mathbb{Z}^+$, niin

$$q = \left\lfloor \frac{a}{b} \right\rfloor . \tag{3.11}$$

ESIM. 5: $b = 3$,

$$a = -13 = (-5) \cdot 3 + 2, \quad q = -5, \ r = 2, \quad \left\lfloor \frac{a}{b} \right\rfloor = -5 \tag{3.12}$$

$$a = 13 = 4 \cdot 3 + 1, \quad q = 4, \ r = 1, \quad \left\lfloor \frac{a}{b} \right\rfloor = 4 \tag{3.13}$$

Määritelmä 3.7. Jaettaessa luku a luvulla b, on jakoalgoritmista saatu luku r jakojäännös (remainder) ja osamäärän (quotient) a/b kokonaisosa (integral part) on luku q, kun $a/b \geq 0$ ja $b \geq 1$.

Määritelmä 3.8. Olkoot $a, b \in \mathbb{Z}$ annettu. Tällöin luku $d \in \mathbb{N}$ on lukujen a ja b suurin yhteinen tekijä (greatest common divisor) eli $d = \text{syt}(a, b) = (a, b)$ mikäli

$$\begin{aligned} &a) \qquad d|a \quad \text{ja} \quad d|b; \\ &b) \qquad c|a \quad \text{ja} \quad c|b \quad \Rightarrow \quad c|d. \end{aligned}$$

Jos $(a, b) = 1$, niin sanotaan, että a ja b ovat keskenään jaottomia (relatively prime) ja merkitään $a \perp b$.

ESIM: a)

$$23 \perp 32 \quad \Leftrightarrow (23, 32) = 1 \tag{3.14}$$

b)

$$(0, a) = a \quad \forall a \in \mathbb{Z}, \tag{3.15}$$

erityisesti

$$(0,0) = 0. \tag{3.16}$$

HUOM: Usein esiintyy myös määritelmä, jossa vaaditaan, että $d \in \mathbb{Z}^+$, jolloin $(0,0) \not\exists$ (Muutoin saadaan samat tulokset).

Määritelmä 3.9. Olkoot $a, b \in \mathbb{Z}$ annettu. Tällöin luku $f \in \mathbb{N}$ on lukujen a ja b pienin yhteinen jaettava(least common multiple) eli $f =$pyj(a,b) mikäli

$$\begin{aligned} &a) \qquad a|f \quad \text{ja} \quad b|f; \\ &b) \qquad a|g \quad \text{ja} \quad b|g \quad \Rightarrow \quad f|g. \end{aligned}$$

Lause 3.2. *Olkoot*

$$a = \prod_{i=1}^{m} p_i^{r_i}, \quad b = \prod_{i=1}^{m} p_i^{s_i}, \quad p_i \in \mathbb{P},\ r_i, s_i \in \mathbb{N}.$$

Tällöin

$$syt(a,b) = \prod_{i=1}^{m} p_i^{\min(r_i,s_i)}, \tag{3.17}$$

$$pyj(a,b) = \prod_{i=1}^{m} p_i^{\max(r_i,s_i)}. \tag{3.18}$$

ESIM. 6: Olkoot $a = 3 \cdot 5^2 \cdot 7, \quad b = 3^2 \cdot 5 \cdot 7$, nyt

$$syt(a,b)pyj(a,b) = 3 \cdot 5 \cdot 7 \cdot 3^2 \cdot 5^2 \cdot 7 = ab. \tag{3.19}$$

Lause 3.3. *Olkoot $a, b \in \mathbb{Z}^+$, tällöin*

$$ab = syt(a,b)pyj(a,b). \tag{3.20}$$

TOD: (Harj.) Osoita ensin, että

$$\min(r_i, s_i) + \max(r_i, s_i) = r_i + s_i. \tag{3.21}$$

3.3 Eukleideen algoritmi

Jakoalgoritmin nojalla saadaan

E.A.=Eukleideen algoritmi.

E.A. Olkoot $a \in \mathbb{Z}$, $b \in \mathbb{Z}^+$ annettu ja $1 \leq b < |a|$.

$$
\begin{aligned}
& r_0 = a,\ r_1 = b && 0 \leq r_1 < |r_0| \\
& r_0 = q_1 r_1 + r_2 && 0 \leq r_2 < r_1 \\
& \vdots \\
& r_k = q_{k+1} r_{k+1} + r_{k+2} && 0 \leq r_{k+2} < r_{k+1} \\
& \vdots \\
& r_{n-2} = q_{n-1} r_{n-1} + r_n && 0 \leq r_n < r_{n-1} \\
& \exists\, n \in \mathbb{N}: \quad r_n \neq 0,\ r_{n+1} = 0 \\
& r_{n-1} = q_n r_n \\
& r_n = \mathrm{syt}(a, b).
\end{aligned}
$$

Tässä n = Eukleideen algoritmin pituus (length), jolle pätee

$$n \leq |a| - 1. \tag{3.22}$$

Asetetaan nyt

$$R_k = \begin{pmatrix} r_k \\ r_{k+1} \end{pmatrix},\ Q_k = \begin{pmatrix} q_k & 1 \\ 1 & 0 \end{pmatrix},\ k \in \mathbb{N}, \tag{3.23}$$

jolloin

$$\det Q_k = -1, \quad {Q_k}^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & -q_k \end{pmatrix}. \tag{3.24}$$

Nähdään, että

$$(E.A.) \Leftrightarrow R_k = Q_{k+1} R_{k+1},\ \forall k = 0, \ldots, n-1, \tag{3.25}$$

jolloin pätee

$$1) \quad R_0 = Q_1 Q_2 \ldots Q_k R_k. \tag{3.26}$$

Merkitään

$$S_0 = \begin{pmatrix} s_0 & t_0 \\ s_1 & t_1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \tag{3.27}$$

ja

$$S_k = \begin{pmatrix} s_k & t_k \\ s_{k+1} & t_{k+1} \end{pmatrix} = {Q_k}^{-1} \dots {Q_2}^{-1} {Q_1}^{-1}, \tag{3.28}$$

jolloin

$$2) \quad R_k = S_k R_0. \tag{3.29}$$

Nyt

$$3) \quad S_{k+1} = Q_{k+1}^{-1} S_k \tag{3.30}$$

eli

$$\begin{pmatrix} s_{k+1} & t_{k+1} \\ s_{k+2} & t_{k+2} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_{k+1} \end{pmatrix} \begin{pmatrix} s_k & t_k \\ s_{k+1} & t_{k+1} \end{pmatrix} = \begin{pmatrix} s_{k+1} & t_{k+1} \\ s_k - q_{k+1}s_{k+1} & t_k - q_{k+1}t_{k+1} \end{pmatrix} \tag{3.31}$$

$\Leftrightarrow$ 4) Palautuskaavat eli rekursiot (recurrence):

$$\begin{cases} s_{k+2} = s_k - q_{k+1}s_{k+1}, \ k = 0, 1, \dots \\ t_{k+2} = t_k - q_{k+1}t_{k+1}, \ k = 0, 1, \dots \end{cases} \tag{3.32}$$

Yhtälöstä 2) saadaan

$$r_n = s_n a + t_n b, \tag{3.33}$$

josta edelleen saadaan

Lause 3.4. *:*

$$5) \quad syt(a, b) = s_n a + t_n b, \tag{3.34}$$

missä n on E.A:n pituus.

Seuraus 1. *Olkoot $a, b, c \in \mathbb{Z}$. Tällöin, jos*

$$a|bc \quad ja \quad a \perp c, \tag{3.35}$$

niin

$$a|b. \tag{3.36}$$

Seuraus 2. *Olkoot $a, b, c \in \mathbb{Z}$. Tällöin, jos*

$$a|c \quad ja \quad b|c \quad ja \quad a \perp b, \tag{3.37}$$

niin

$$ab|c. \tag{3.38}$$

Seuraus 3. *Olkoot $a, b \in \mathbb{Z}$ ja $p \in \mathbb{P}$. Tällöin, jos*

$$p|ab, \tag{3.39}$$

niin

$$p|a \quad tai \quad p|b. \tag{3.40}$$

Määritelmä 3.10. Olkoot $a_1, ..., a_m \in \mathbb{Z}$ annettu. Tällöin luku $d_m \in \mathbb{N}$ on lukujen $a_1, ..., a_m$ suurin yhteinen tekijä eli $d_m = \text{syt}(a_1, ..., a_m) = (a_1, ..., a_m)$ mikäli

$$\begin{aligned} a) \quad & d_m|a_i \quad \forall i = 1, ..., m; \\ b) \quad & c|a_i \quad \forall i = 1, ..., m \quad \Rightarrow \quad c|d_m. \end{aligned}$$

Esim: Olkoot $m_1, \ldots, m_r \in \mathbb{Z}^+$ pareittain keskenään jaottomia (pairwise relatively prime) eli $m_i \perp m_j \ \forall i \neq j$. Tällöin

$$(a_1, ..., a_r) = 1. \tag{3.41}$$

HUOM: Edellinen ei päde välttämättä vastakkaiseen suuntaan, sillä esimerkiksi

$$(6, 9, 5) = 1 \quad \text{mutta} \quad (6, 9) = 3. \tag{3.42}$$

Määritelmä 3.11. Olkoot $a_1, ..., a_m \in \mathbb{Z}$ annettu. Tällöin luku $f_m \in \mathbb{N}$ on lukujen $a_1, ..., a_m$ pienin yhteinen jaettava eli f_m =pyj$(a_1, ..., a_m)$ mikäli

$$\begin{aligned} &a) \qquad a_i | f_m \quad \forall i = 1, ..., m; \\ &b) \qquad a_i | c \quad \forall i = 1, ..., m \quad \Rightarrow \quad f_m | c. \end{aligned}$$

Lause 3.5. *Olkoon $d_m = (a_1, ..., a_m)$, tällöin on olemassa sellaiset $l_1, ..., l_m \in \mathbb{Z}$, että*

$$d_m = l_1 a_1 + ... + l_m a_m. \tag{3.43}$$

Todistus: Induktiolla.

Perusaskel: $m = 2 \Leftrightarrow 5)$.

Induktio-oletus: Väite tosi, kun $m = k$.

Induktioaskel: Olkoon $m = k + 1$.

1. Osoitetaan ensin, että

$$d_{k+1} = (d_k, a_{k+1}). \tag{3.44}$$

a.) Koska

$$d_{k+1} | a_1, ..., a_k, a_{k+1}, \tag{3.45}$$

niin

$$d_{k+1} | d_k, \ a_{k+1} \tag{3.46}$$

eli on yhteinen tekijä.

b.) Jos

$$c | d_k, \ a_{k+1}, \tag{3.47}$$

niin

$$c | a_1, ..., a_k, a_{k+1}. \tag{3.48}$$

Siten

$$c|d_{k+1}, \tag{3.49}$$

joten on suurin tekijä. a.)+b.)$\Rightarrow d_{k+1} = (d_k, a_{k+1})$.

2. Induktio-oletuksesta saadaan, että

$$\exists \quad h_i \in \mathbb{Z} : \quad d_k = h_1 a_1 + ... + h_k a_k \tag{3.50}$$

ja

$$\exists \quad j_i \in \mathbb{Z} : \quad (d_k, a_{k+1}) = j_1 d_k + j_2 a_{k+1}. \tag{3.51}$$

Siten

$$d_{k+1} = (d_k, a_{k+1}) =$$

$$j_1(h_1 a_1 + ... + h_k a_k) + j_2 a_{k+1} = l_1 a_1 + ... + l_{k+1} a_{k+1}. \tag{3.52}$$

Joten induktioaskel on todistettu ja induktioperiaatteen nojalla alkuperäinen lauseen väite on tosi. □

3.4 Kongruenssi

Määritelmä 3.12. Olkoon $n \in \mathbb{Z}^+$ annettu ja $a, b \in \mathbb{Z}$. Jos

$$n|a - b, \tag{3.53}$$

niin tällöin asetetaan

$$a \equiv b \pmod{n} \tag{3.54}$$

eli a on kongruentti b:n kanssa modulo n.

Huomaa, että

$$n|a - b \Leftrightarrow a = b + l \cdot n, \text{ jollakin } l \in \mathbb{Z} \Leftrightarrow a \in b + n\mathbb{Z} = \overline{b}. \tag{3.55}$$

Lemma 3.1. *Keskenään kongruenteilla luvuilla on samat jakojäännökset ja Vice Versa.*

Kongruentit luvut kuuluvat samaan jakojäännösluokkaan (mod n):

$$a \equiv b \pmod{n} \quad \Leftrightarrow \quad \overline{a} = \overline{b}. \tag{3.56}$$

Siispä joukkoa

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{a} | a = 0, 1, 2, \ldots, n-1\} = \mathbb{Z}_n \tag{3.57}$$

kutsutaan jakojäännösrenkaaksi, missä on laskutoimitukset

$$\overline{a} + \overline{b} = \overline{a+b}, \tag{3.58}$$

$$\overline{a}\overline{b} = \overline{ab}. \tag{3.59}$$

HUOM: Usein lasketaan vain pelkillä edustajilla eli jakojäännöksillä $0, 1, 2, ..., n-1 = -1 \pmod{n}$.

ESIM:

$$-1 + 1 = n - 1 + 1 = n = 0, \quad (-1)^{-1} = -1, \tag{3.60}$$

$$2^{-1} = \frac{1}{2} = \frac{p+1}{2}, \quad p \in \mathbb{P}_{p \geq 3}. \tag{3.61}$$

Olkoon R-ykkösellinen rengas.

Määritelmä 3.13. Joukko

$$R^* = \{\text{yksiköt}\} = \{u \in R \mid \exists\ u^{-1} \in R :\ uu^{-1} = 1\} = \tag{3.62}$$

on renkaan R yksikköryhmä.

Jos $R = K$-kunta, niin $K^* = K \backslash \{0\}$.

Lemma 3.2. *Joukko*

$$\{\overline{a} \in \mathbb{Z}_n |\ a \perp n\}$$

on renkaan $\mathbb{Z}_n$ yksikköryhmä eli

$$\mathbb{Z}_n^* = \{\overline{a} \in \mathbb{Z}_n |\ a \perp n\}. \tag{3.63}$$

Huomaa,että ehdosta $a \perp n$ seuraa Eukleideen algoritmin kohdan 5) nojalla, että

$$1 = s_m a + t_m n, \tag{3.64}$$

missä m on E.A:n pituus. Siten

$$s_m a \equiv 1 \pmod{n} \Leftrightarrow \overline{a}^{-1} = \overline{s_m}. \tag{3.65}$$

Erityisesti, jos $p \in \mathbb{P}$, niin $\mathbb{Z}_p$ on kunta ja

$$\mathbb{Z}_p^* = \{\overline{a} \in \mathbb{Z}_p |\ a \perp p\} = \{\overline{1}, \overline{2}, ..., \overline{p-1}\}. \tag{3.66}$$

Määritelmä 3.14. Olkoon $n \geq 2$. Jos $a \perp n$, niin $\overline{a}$ on alkuluokka (mod n) ja

$$\mathbb{Z}_n^* = \{\overline{a} \in \mathbb{Z}_n |\ a \perp n\}$$

on renkaan $\mathbb{Z}_n$ kertolaskuryhmä (multiplication group of the ring).

Eulerin funktio $\varphi(n)$ määritellään asettamalla

$$\varphi(n) = \#\{k \in \mathbb{Z}^+ \mid 1 \leqslant k \leqslant n-1,\ k \perp n\}. \tag{3.67}$$

Joten, ryhmän $\mathbb{Z}_n^*$ kertaluku (order) on $\#\mathbb{Z}_n^* = \varphi(n)$.

Lemma 3.3.

$$\varphi(MN) = \varphi(M)\varphi(N),\ \forall M \perp N. \tag{3.68}$$

Eli φ on multiplikatiivinen ja koska

$$\varphi(p^m) = p^m(1 - \frac{1}{p}),\ \forall p \in \mathbb{P},\ \forall m \in \mathbb{Z}^+, \tag{3.69}$$

niin saadaan

Lemma 3.4. *Olkoon* $n = {p_1}^{a_1} \dots {p_k}^{a_k},\ p_i \in \mathbb{P}$. *Tällöin*

$$\varphi(n) = n \prod_{p|n} (1 - \frac{1}{p})\ \textit{eli} \tag{3.70}$$

$$\varphi(n) = {p_1}^{a_1} \dots {p_k}^{a_k}(1 - \frac{1}{p_1}) \dots (1 - \frac{1}{p_k}) \tag{3.71}$$

Lause 3.6. *KIINALAINEN JÄÄNNÖSLAUSE: Olkoot* $m_1, \ldots, m_r \in \mathbb{Z}^+$ *pareittain keskenään jaottomia (pairwise relatively prime) eli*

$$m_i \perp m_j \quad \forall i \neq j \tag{3.72}$$

ja olkoot $a_1, \ldots, a_r \in \mathbb{Z}$ *annettu. Tällöin yhtälöryhmän*

$$\begin{cases} x \equiv a_1 \ (mod\ m_1), \\ \vdots \\ x \equiv a_r \ (mod\ m_r) \end{cases} \tag{3.73}$$

ratkaisut ovat

$$x = x_0 + l \cdot M, \ l \in \mathbb{Z}, \quad M = m_1 \ldots m_r = m_k M_k, \tag{3.74}$$

ja

$$x_0 = n_1 M_1 a_1 + \ldots + n_r M_r a_r, \tag{3.75}$$

missä

$$n_k M_k \equiv 1 \ (mod\ m_k). \tag{3.76}$$

"Ratkaisu on yksikäsitteinen (solution is unique) (mod M)".

Tod: Lasketaan

$$M_k = \prod_{i \neq k} m_i \equiv 0 \ (\text{mod}\ m_j) \quad \forall j \neq k. \tag{3.77}$$

Joten

$$x_0 \equiv n_k M_k a_k \equiv 1 \cdot a_k = a_k \ (\text{mod}\ m_k) \quad \forall k = 1, ..., r \tag{3.78}$$

ja siten x_0 on ratkaisu.

Olkoon x ratkaisu, tällöin

$$x - x_0 \equiv 0 \ (\text{mod}\ m_k) \quad \forall k = 1, ..., r. \tag{3.79}$$

Koska $m_i \perp m_j \ \forall i \neq j$, niin

$$x - x_0 \equiv 0 \pmod{m_1 \cdots m_r} \tag{3.80}$$

eli

$$x \equiv x_0 \pmod{M}. \quad \square \tag{3.81}$$

4 Kertomat, binomikertoimet

Määritellään luvun $n \in \mathbb{N}$ kertoma $n!$ induktiivisesti asettamalla

Määritelmä 4.1.

$$0! = 1, \tag{4.1}$$

$$n! = n \cdot (n-1)!, \quad \forall n \in \mathbb{Z}^+. \tag{4.2}$$

Ja kertoman yleistys, Pochammerin symboli $(a)_n$, seuraavasti.

Määritelmä 4.2. Olkoon $a \in \mathbb{C}$. Tällöin

$$(a)_0 = 1, \tag{4.3}$$

$$(a)_n = (a + n - 1) \cdot (a)_{n-1}, \quad \forall n \in \mathbb{Z}^+. \tag{4.4}$$

Erityisesti

$$(1)_n = n!. \tag{4.5}$$

Määritelmä 4.3. Olkoot $a \in \mathbb{C}$ ja $k \in \mathbb{N}$. Tällöin luvut

$$\binom{a}{k} = (-1)^k \frac{(-a)_k}{k!} \tag{4.6}$$

ovat binomikertoimia "a yli k:n".

Tutkitaan erikoistapauksia.

Olkoon aluksi $k = 0$. Tällöin

$$\binom{a}{k} = \binom{a}{0} = \frac{(-a)_0}{0!} = 1 \quad \forall \quad a \in \mathbb{C}. \tag{4.7}$$

Kun $k \in \mathbb{Z}^+$, niin

$$\binom{a}{k} = (-1)^k \frac{(-a)(-a+1)\cdots(-a+k-1)}{k!} = \frac{a(a-1)\cdots(a-k+1)}{k!} \quad \forall a \in \mathbb{C}. \tag{4.8}$$

Olkoon vielä $a = n \in \mathbb{Z}^+$, jolloin

$$\binom{n}{k} = \frac{n(n-1)\cdots(n-k+1)}{k!} = \frac{n(n-1)\cdots(n-k+1)(n-k)!}{k!(n-k)!}, \tag{4.9}$$

joten

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} \quad \forall \quad 0 \leq k \leq n. \tag{4.10}$$

Jos $k \geq n+1$, niin

$$\binom{n}{k} = (-1)^k \frac{(-n)\cdots(-n+j)\cdots(-n+k-1)}{k!}, \tag{4.11}$$

missä $0 \leq j \leq k-1$. Siten, kun $j = n$, niin $-n + j = 0$ ja

$$\binom{n}{k} = 0 \quad \forall k \geq n+1. \tag{4.12}$$

Olkoon $a = -n \in \mathbb{Z}^-$, jolloin

$$\binom{-n}{k} = (-1)^k \frac{n(n+1)\cdots(n+k-1)}{k!} = (-1)^k \frac{(n+k-1)!}{k!(n-1)!}, \tag{4.13}$$

joten

$$\binom{-n}{k} = (-1)^k \binom{n+k-1}{k} \quad \forall k \geq 0. \tag{4.14}$$

4.1 Palautuskaava, Pascalin kolmio

Lause 4.1. *Olkoon $a \in \mathbb{C}$. Tällöin*

$$\binom{a+1}{k+1} = \binom{a}{k+1} + \binom{a}{k} \quad \forall k \in \mathbb{N}. \tag{4.15}$$

Todistus. Lasketaan väitteen oikea puoli käyttäen binomikertoimien esitystä (4.8), jolloin

$$\begin{gathered}
\binom{a}{k+1} + \binom{a}{k} = \\
\frac{a(a-1)\cdots(a-(k+1)+1)}{(k+1)!} + \frac{a(a-1)\cdots(a-k+1)}{k!} = \\
\frac{a(a-1)\cdots(a-k+1)(a-k)}{k!(k+1)} + \frac{a(a-1)\cdots(a-k+1)}{k!} = \\
\frac{a(a-1)\cdots(a-k+1)}{k!}\left(\frac{a-k}{k+1}+1\right) = \\
\frac{(a+1)(a+1-1)\cdots(a+1-(k+1)+1)}{(k+1)!} = \binom{a+1}{k+1}.
\end{gathered} \tag{4.16}$$

Siis saatiin väitteen vasen puoli. □

Erikoistapauksena saadaan

Lause 4.2.

$$\binom{n+1}{k+1} = \binom{n}{k+1} + \binom{n}{k} \quad \forall k, n \in \mathbb{N}. \tag{4.17}$$

Jonka avulla (I tapa) voidaan todistaa.

Lause 4.3.

$$\binom{n}{k} \in \mathbb{Z}^+ \quad \forall \quad 0 \leq k \leq n \in \mathbb{N}. \tag{4.18}$$

Todistus. Voidaan olettaa, että $0 \leq k \leq n$. Induktio n:n suhteen.

Aluksi $n = 0, 1$.

$$\binom{0}{0} = \binom{1}{0} = \binom{1}{1} = 1. \tag{4.19}$$

Induktio-oletus: Väite tosi, kun $n = l$.

Induktioaskel: Olkoon $n = l + 1$. Tällöin

$$\binom{l+1}{k+1} = \binom{l}{k+1} + \binom{l}{k} \quad \forall \quad 1 \leq k+1 \leq l, \tag{4.20}$$

mistä

$$\binom{l+1}{k+1} \in \mathbb{Z}^+ \quad \forall \quad 1 \leq k+1 \leq l. \tag{4.21}$$

Lisäksi

$$\binom{l+1}{l+1} = \binom{l+1}{0} = 1. \quad \square \tag{4.22}$$

Tuloksen (4.18) nojalla

$$\frac{(n-k+1)(n-k+2)\cdots(n-1)n}{k!} \in \mathbb{Z}^+, \tag{4.23}$$

joten

$$k!|(n-k+1)(n-k+2)\cdots(n-1)n, \tag{4.24}$$

mistä saadaan.

Lause 4.4.

$$k!|(m+1)(m+2)\cdots(m+k) \quad \forall k, m \in \mathbb{N}. \tag{4.25}$$

Edelleen

Lause 4.5. *Olkoon $p \in \mathbb{P}$, tällöin*

$$p \left| \binom{p}{k} \right. \qquad \forall \quad 1 \leq k \leq p-1. \tag{4.26}$$

Todistus. Tuloksen (4.24) nojalla

$$k!|(p-k+1)(p-k+2)\cdots(p-1)p, \tag{4.27}$$

Koska $p \perp k!$, niin (4.27) johtaa relaatioon

$$k!|(p-k+1)\cdots(p-1) = l \cdot k!, \tag{4.28}$$

jollakin $l \in \mathbb{Z}$. Siten

$$\binom{p}{k} = \frac{(p-k+1)(p-k+2)\cdots(p-1)p}{k!} = l \cdot p \equiv 0 \pmod{p}. \quad \square \tag{4.29}$$

4.2 p-valuaatio kokonaisluvuille

Tarkastellaan alkuluvun p esiintymistä kokonaisluvussa k (myöhemmin esitetään p-valuaation määritelmä rationaaliluvulle).

Määritelmä 4.4. Olkoot $p \in \mathbb{P}$, $k \in \mathbb{Z} \setminus \{0\}$, $r \in \mathbb{N}$ ja

$$p^r || k. \tag{4.30}$$

Tällöin asetetaan

$$v_p(k) = r. \tag{4.31}$$

Kertaa vielä, että

$$p^r || k \quad \Leftrightarrow \quad k = p^r c, \quad p \not| c \in \mathbb{Z} \setminus \{0\}. \tag{4.32}$$

Lause 4.6. *Laskusääntöjä. Olkoon $p \in \mathbb{P}$ ja $n, m \in \mathbb{Z} \setminus \{0\}$, tällöin*

$$v_p(1) = 0. \tag{4.33}$$

$$v_p(n) \geq 0. \tag{4.34}$$

$$v_p(nm) = v_p(n) + v_p(m). \tag{4.35}$$

$$v_p(n!) = v_p(1) + v_p(2) + ... + v_p(n), \quad n \geq 1. \tag{4.36}$$

$$n = \prod_{p \leq n} p^{v_p(n)} = \prod_{p \in \mathbb{P}} p^{v_p(n)}. \tag{4.37}$$

Määritelmä 4.5. Olkoot $p \in \mathbb{P}$, $k \in \mathbb{Z} \setminus \{0\}$ $l \in \mathbb{Z}^+$. Asetetaan tällöin

$$w_{p^l}(k) = 1 \quad \text{jos} \quad p^l | k; \tag{4.38}$$

$$w_{p^l}(k) = 0 \quad \text{jos} \quad p^l \nmid k. \tag{4.39}$$

Lause 4.7. *Olkoot $p \in \mathbb{P}$, $k \in \mathbb{Z} \setminus \{0\}$, $r \in \mathbb{N}$ ja $v_p(k) = r$. Tällöin*

$$v_p(k) = \sum_{i=1}^{r} w_{p^i}(k) = \sum_{i=1}^{\infty} w_{p^i}(k). \tag{4.40}$$

Lause 4.8. *Olkoot $n \in \mathbb{Z}^+$ ja*

$$A_p = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor, \quad p \in \mathbb{P}. \tag{4.41}$$

Tällöin

$$a) \quad v_p(n!) = A_p. \tag{4.42}$$

$$b). \quad p^{A_p} \,||n! \quad \forall p|n!. \tag{4.43}$$

$$c). \quad n! = \prod_{p \le n} p^{A_p}. \tag{4.44}$$

Huomaa, että $\lfloor n/p^i \rfloor = 0$, kun $p^i > n$. Siten summat A_p ovat äärellisiä.

Todistus. Laskarit: Välillä $[1, n]$ olevien luvulla p^i jaollisten lukujen lkm=

$$\#\{k \in \mathbb{Z}^+ |\ 1 \le k \le n,\ p^i|k\} = \left\lfloor \frac{n}{p^i} \right\rfloor. \tag{4.45}$$

Toisaalta

$$\left\lfloor \frac{n}{p^i} \right\rfloor = w_{p^i}(1) + w_{p^i}(2) + ... + w_{p^i}(n). \tag{4.46}$$

Esimerkiksi

$$1, ..., 1 \cdot p, ..., 2 \cdot p, ..., p \cdot p, ..., \left\lfloor \frac{n}{p} \right\rfloor \cdot p, ..., n \tag{4.47}$$

missä pätee

$$w_p(1) = w_p(2) = ... = w_p(p-1) = w_p(p+1) = ... = 0 \tag{4.48}$$

$$w_p(p) = w_p(2p) = ... = w_p(\left\lfloor \frac{n}{p} \right\rfloor p) = 1. \tag{4.49}$$

Nyt

$$w_p(1) + w_p(2) + ... + w_p(n) = \left\lfloor \frac{n}{p} \right\rfloor; \tag{4.50}$$

$$w_{p^2}(1) + w_{p^2}(2) + ... + w_{p^2}(n) = \left\lfloor \frac{n}{p^2} \right\rfloor; \tag{4.51}$$

...

$$w_{p^r}(1) + w_{p^r}(2) + ... + w_{p^r}(n) = \left\lfloor \frac{n}{p^r} \right\rfloor, \tag{4.52}$$

missä

$$p^r \leq n < p^{r+1}, \quad \Rightarrow \quad \left\lfloor \frac{n}{p^{r+1}} \right\rfloor = 0. \tag{4.53}$$

Lasketaan yhtälöt (4.50–4.52) puolittain yhteen, jolloin saadaan

$$v_p(1) + v_p(2) + ... + v_p(n) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + ... + \left\lfloor \frac{n}{p^r} \right\rfloor. \tag{4.54}$$

Siten

$$v_p(n!) = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor = A_p, \quad p \in \mathbb{P}. \tag{4.55}$$

Edelleen

$$n! = \prod_{p \leq n} p^{v_p(n!)}. \quad \square \tag{4.56}$$

Lauseen 4.3 II todistus. Kertomien alkutekijäkehitelmien nojalla

$$\frac{n!}{k!(n-k)!} = \prod_{p \leq n} p^{B_p}, \tag{4.57}$$

missä

$$B_p = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor - \left\lfloor \frac{k}{p^i} \right\rfloor - \left\lfloor \frac{n-k}{p^i} \right\rfloor. \tag{4.58}$$

Tuloksen (2.6)

$$\lfloor a \rfloor + \lfloor b \rfloor \leq \lfloor a + b \rfloor \tag{4.59}$$

avulla saadaan

$$\left\lfloor \frac{k}{p^i} \right\rfloor + \left\lfloor \frac{n-k}{p^i} \right\rfloor \leq \left\lfloor \frac{k}{p^i} + \frac{n}{p^i} - \frac{k}{p^i} \right\rfloor = \left\lfloor \frac{n}{p^i} \right\rfloor. \tag{4.60}$$

Siten $B_p \in \mathbb{N}$ ja

$$\prod_{p \leq n} p^{B_p} \in \mathbb{Z}^+, \tag{4.61}$$

joka identiteetin (4.57) kanssa todistaa, että

$$\binom{n}{k} \in \mathbb{Z}^+ \quad \forall \quad 0 \leq k \leq n \in \mathbb{N}. \quad \square$$

4.3 Binomisarja, Binomikehitelmä

Sarjaa

$$(1+t)^a = \sum_{k=0}^{\infty} \binom{a}{k} t^k, \quad a \in \mathbb{C} \tag{4.62}$$

sanotaan Binomisarjaksi. Olkoon $a = n \in \mathbb{N}$, jolloin

$$(1+t)^n = \sum_{k=0}^{n} \binom{n}{k} t^k. \tag{4.63}$$

Asetetaan $t = A/B$, jolloin yhtälöstä (4.63) saadaan Binomikehitelmä:

$$(A+B)^n = \sum_{k=0}^{n} \binom{n}{k} A^k B^{n-k} = \sum_{0 \le k \le n, k+l=n} \binom{n}{k} A^k B^l. \tag{4.64}$$

Kun, $a = -1$ ja $t = -x$, niin saadaan Geometrinen sarja:

$$\frac{1}{1-x} = \sum_{k=0}^{\infty} x^k. \tag{4.65}$$

Ja yleisemmin, jos $a = -n \in \mathbb{Z}^-$ ja $t = -x$, niin

$$\frac{1}{(1-x)^n} = \sum_{k=0}^{\infty} \binom{n+k-1}{k} x^k \tag{4.66}$$

identiteetin (4.14) nojalla.

5 Hieman polynomialgebraa

Olkoon R ykkösellinen rengas. Tällöin

$$R[x] = \{P(x) \mid P(x) = \sum_{k=0}^{n} p_k x^k;\ p_k \in R,\ n \in \mathbb{N}\} \tag{5.1}$$

on R-kertoimisten polynomien joukko. Jos $p_n \neq 0$, niin polynomin aste $\deg P(x) = n$, erityisesti $\deg 0(x) = -\infty$. Pääpolynomiksi (monic polynomial) sanotaan polynomia, missä korkeimman potenssin kerroin $p_n = 1$.

Määritelmä 5.1. Olkoot

$$P(x) = \sum_{k=0}^{n} p_k x^k,$$

$$Q(x) = \sum_{k=0}^{n} q_k x^k \in R[x],$$

jolloin asetetaan

$$\begin{aligned} &P(x) = Q(x) \Leftrightarrow \forall k(p_k = q_k); \\ &P(x) + Q(x) = \sum_{k \geqslant 0} (p_k + q_k) x^k; \\ &P(x)Q(x) = \sum_{k \geqslant 0} r_k x^k, \end{aligned} \tag{5.2}$$

missä

$$r_k = \sum_{i=0}^{k} p_i q_{k-i} = \sum_{i+j=k} p_i q_j, \tag{5.3}$$

joka on Cauchyn kertosääntö.

Tällöin $R[x]$ on rengas, missä

$$0(x) = 0 + 0 \cdot x + 0 \cdot x^2 + \ldots \tag{5.4}$$

on nolla-alkio ja

$$1(x) = 1 + 0 \cdot x + 0 \cdot x^2 + \ldots \tag{5.5}$$

on ykkösalkio.

Olkoon $R = K$ kunta. Tällöin polynomirengas $K[x]$ on kokonaisalue, jossa pätee Jakoalgoritmi:
Olkoon $a(x), b(x) \in K[x]$, $a(x)b(x) \neq 0(x)$ ja $\deg b(x) \leq \deg a(x)$. Tällöin $\exists\, q(x), r(x) \in K[x]$ s.e.

$$[(J.A.)] a(x) = q(x)b(x) + r(x), \quad \deg r(x) < \deg b(x). \tag{5.6}$$

Seuraus:

$$p(\alpha) = 0,\ \alpha \in K \Leftrightarrow (x - \alpha) \underset{K[x]}{|}\ p(x). \tag{5.7}$$

Kokonaisalueen $D = K[x]$ yksikköryhmä on K^*. Joten polynomien $a(x)$ ja $b(x)$ suurin yhteinen tekijä $d(x) = \text{s.y.t.}(a(x), b(x))$ voidaan valita pääpolynomiksi. Eukleideen algoritmin nojalla saadaan, että on olemassa sellaiset polynomit $s(x), t(x) \in K[x]$, että

$$d(x) = s(x)a(x) + t(x)b(x). \tag{5.8}$$

6 Rationaaliluvun jaollisuus (mod n)

6.1 Perusteita

Olkoon $p \in \mathbb{P}$. Jokaisella $a/b \in \mathbb{Q}^*$ on yksikäsitteinen esitys

$$\frac{a}{b} = p^r \frac{c}{d}, \quad c \in \mathbb{Z},\ d \in \mathbb{Z}^+,\ c \perp d,\ p \nmid cd,\ r \in \mathbb{Z}. \tag{6.1}$$

Asetetaan nyt

Määritelmä 6.1. Rationaaliluku a/b (osoittaja) on p:llä jaollinen eli

$$p \left| \frac{a}{b} \right. \quad \Leftrightarrow \quad r \geq 1. \tag{6.2}$$

Edelleen

$$\frac{a}{b} \equiv 0 \pmod{p} \quad \Leftrightarrow \quad p \left| \frac{a}{b} \right. \tag{6.3}$$

ESIM.

$$5 \left| \frac{20}{3} \right. \quad \Leftrightarrow \frac{20}{3} \equiv 0 \pmod{5}. \tag{6.4}$$

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} = \frac{50}{4!} \equiv 0 \pmod{5}. \tag{6.5}$$

Olkoon $p \in \mathbb{P}$, tällöin

$$(2p-1)(2p-2)\cdots(p+2)(p+1) \equiv (p-1)(p-2)\cdots 2 \cdot 1 = (p-1)! \pmod{p}, \tag{6.6}$$

joten

$$\binom{2p}{p} \equiv 2 \pmod{p}. \tag{6.7}$$

Laajennetaan Määritelmä 6.1 vapaastivalittavalle modulukselle $n \in \mathbb{Z}_{\geq 2}$.

Määritelmä 6.2. Olkoon $n \in \mathbb{Z}_{\geq 2}$ annettu ja olkoon rationaaliluvun $a/b \in \mathbb{Q}^*$ alkutekijäesitys

$$\frac{a}{b} = \pm p_1^{r_1} \cdots p_k^{r_k} \cdot q_1^{v_1} \cdots q_l^{v_l}; \quad p_i, q_j \in \mathbb{P} \quad r_i \in \mathbb{Z}^+,\ v_i \in \mathbb{Z}^-, \tag{6.8}$$

missä $q_j \notin \{p_1, ..., p_k\}$. Jos

$$n = p_1^{s_1} \cdots p_k^{s_k}, \quad s_i \in \mathbb{N}, \quad 0 \leq s_i \leq r_i \quad \forall i = 1, ..., k, \tag{6.9}$$

niin

$$n \left| \frac{a}{b} \right. \tag{6.10}$$

ja sanotaan, että n jakaa rationaaliluvun a/b (osoittajan).

HUOM: Jos, $n|a/b$, niin $n \perp b$.

Määritelmä 6.3. Olkoon $n \in \mathbb{Z}_{\geq 2}$ annettu ja $a/b, c/d \in \mathbb{Q}$. Jos

$$n \left| \frac{a}{b} - \frac{c}{d} \right., \tag{6.11}$$

niin

$$\frac{a}{b} \equiv \frac{c}{d} \pmod{n} \tag{6.12}$$

ja sanotaan, että luvut a/b ja c/d ovat kongruentteja (mod n).

Esim.

$$\frac{20}{3} = 2^2 \cdot 5^1 \cdot 3^{-1} \equiv 0 \pmod{2 \cdot 5}. \tag{6.13}$$

$$\frac{20}{3} \equiv 0 \pmod{20}, \tag{6.14}$$

missä $p_1 = 2, p_2 = 5, q_1 = 3$ ja $r_1 = 2, r_2 = 1, v_1 = -1$.

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} = \frac{50}{4!} \equiv 0 \pmod{5^2}. \tag{6.15}$$

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} \equiv \frac{25}{7} \pmod{5^3}. \tag{6.16}$$

Lause 6.1. *Kongruenssi $\equiv$ (mod n) on ekvivalenssirelaatio joukossa $\mathbb{Q}$.*

Määritelmä 6.4. Olkoot $n \in \mathbb{Z}_{\geq 2}$ ja $a/b \in \mathbb{Q}$ annettu ja $n \perp b$. Tällöin

$$\overline{a/b} = \{\frac{c}{d} \in \mathbb{Q} |\ \frac{c}{d} \equiv \frac{a}{b} \pmod{n}\} \tag{6.17}$$

on edustajan a/b määräämä jakojäännösluokka (mod n) ja

$$\mathbb{Q}_n = \{\overline{a/b} |\ a/b \in \mathbb{Q},\ n \perp b\}. \tag{6.18}$$

Asetetaan vielä laskutoimitukset (binary operations)

$$\begin{cases} \overline{x} + \overline{y} = \overline{x+y}, \\ \overline{x} \cdot \overline{y} = \overline{xy} \end{cases} \tag{6.19}$$

aina, kun $\overline{x}, \overline{y} \in \mathbb{Q}_n$.

Lause 6.2. *a) Laskutoimitukset*

$$\begin{cases} + : \mathbb{Q}_n \times \mathbb{Q}_n \to \mathbb{Q}_n, \end{cases} \tag{6.20}$$

ovat hyvinmääriteltyjä (well defined) eli binäärioperaatiot ovat funktioita.

b). Nolla-alkio (zero) on

$$\overline{0} = \frac{\overline{na}}{b} \quad \forall a, b, \quad b \perp n \tag{6.21}$$

ja vasta-alkio

$$-\overline{x} = \overline{-x} \quad \forall \quad \overline{x} \in \mathbb{Q}_n. \tag{6.22}$$

c). Ykkösalkio (unity)

$$\overline{1} = \frac{\overline{b+ln}}{b} \quad \forall l, b, \quad b \perp n \tag{6.23}$$

ja käänteisalkio (inverse)

$$\overline{x}^{-1} = \overline{x^{-1}} \quad \forall \quad \overline{x},\ \overline{x^{-1}} \in \mathbb{Q}_n. \tag{6.24}$$

Lause 6.3. *Olkoon $n \in \mathbb{Z}_{\geq 2}$. Tällöin kuvaus*

$$F(\overline{a/b}) = \overline{a}(\overline{b})^{-1} \tag{6.25}$$

$$F : \mathbb{Q}_n \to \mathbb{Z}_n \tag{6.26}$$

on rengasisomorfia eli $\mathbb{Q}_n \cong \mathbb{Z}_n$.

Todistus: Laskemalla saadaan

1)

$$F\left(\frac{\overline{a}}{b} + \frac{\overline{c}}{d}\right) = F\left(\frac{\overline{ad+bc}}{bd}\right) =$$
$$\overline{ad+bc}(\overline{bd})^{-1} = (\overline{a}\overline{d} + \overline{b}\overline{c})(\overline{b})^{-1}(\overline{d})^{-1} =$$
$$\overline{a}(\overline{b})^{-1} + \overline{c}(\overline{d})^{-1} =$$
$$F\left(\frac{\overline{a}}{b}\right) + F\left(\frac{\overline{c}}{d}\right), \tag{6.27}$$

joten F on ryhmien $(\mathbb{Q}_n, +)$ ja $(\mathbb{Z}_n, +)$ välinen homomorfia.

2)

$$F\left(\frac{\overline{a}}{b} \cdot \frac{\overline{c}}{d}\right) = F\left(\frac{\overline{ac}}{\overline{bd}}\right) =$$
$$\overline{ac}(\overline{bd})^{-1} = \overline{a}(\overline{b})^{-1}\overline{c}(\overline{d})^{-1} =$$
$$F\left(\frac{\overline{a}}{b}\right) F\left(\frac{\overline{c}}{d}\right). \tag{6.28}$$

3)

$$F\left(\overline{1}\right) = F\left(\frac{\overline{1}}{1}\right) = \overline{1}(\overline{1})^{-1} = \overline{1}. \tag{6.29}$$

Kohtien 1),2) ja 3) nojalla $F : \mathbb{Q}_n \to \mathbb{Z}_n$ on rengasmorfismi.

4) Asetetaan nyt

$$F\left(\frac{\overline{a}}{b}\right) = \overline{0}, \tag{6.30}$$

joten

$$\overline{a}(\overline{b})^{-1} = \overline{0}. \tag{6.31}$$

Kerrotaan 6.31 puolittain alkiolla $\overline{b}$, jolloin saadaan

$$\overline{a}(\overline{b})^{-1}\overline{b} = \overline{0} \cdot \overline{b} \quad \Rightarrow \quad \overline{a} = \overline{0}. \tag{6.32}$$

Siten $F : \mathbb{Q}_n \to \mathbb{Z}_n$ on injektio.

5) Olkoon vielä $\overline{k} \in \mathbb{Z}_n$. Tällöin, jos valitaan $a = k, b = 1$, niin

$$F\left(\frac{\overline{a}}{\overline{b}}\right) = F\left(\frac{\overline{k}}{\overline{1}}\right) = \overline{k}(\overline{1})^{-1} = \overline{k}. \tag{6.33}$$

Siispä $F : \mathbb{Q}_n \to \mathbb{Z}_n$ on surjektio.

Kohtien 4) ja 5) nojalla

$$F : \mathbb{Q}_n \to \mathbb{Z}_n$$

on bijektio ja edelleen rengasisomorfia. □

Siten $\mathbb{Q}_n$ ja $\mathbb{Z}_n$ voidaan samaistaa, jolloin merkitään

$$\mathbb{Q}_n \ni \overline{a/b} = \overline{a}\overline{b}^{-1} \in \mathbb{Z}_n. \tag{6.34}$$

ESIM: Lasketaan $\overline{2/3}$ renkaassa $\mathbb{Q}_7$. Aluksi saadaan

$$\frac{2}{3} \equiv \frac{2 + l \cdot 7}{3} \pmod 7 \quad \forall l \in \mathbb{Z}. \tag{6.35}$$

Valitaan $l = 4$, jolloin

$$\frac{2}{3} \equiv \frac{2 + 4 \cdot 7}{3} = 10 \equiv 3 \pmod 7. \tag{6.36}$$

Täten

$$\overline{2/3} = \overline{3}. \tag{6.37}$$

Toisaalta $\mathbb{Z}_7$:ssa.

$$\overline{2} \cdot \overline{3}^{-1} = \overline{2} \cdot \overline{5} = \overline{10} = \overline{3}. \tag{6.38}$$

Lemma 6.1. *Olkoon G ryhmä ja $a \in G$. Tällöin kuvaukset*

$$\iota : G \to G, \qquad \iota(x) = x^{-1} \tag{6.39}$$

ja

$$\tau : G \to G, \qquad \tau(x) = ax \tag{6.40}$$

ovat bijektioita.

Todistus: Asetetaan

$$\iota(x_1) = \iota(x_2) \Leftrightarrow x_1^{-1} = x_2^{-1}, \tag{6.41}$$

josta saadaan $x_1 = x_2$. Siten ι on injektio.
Olkoon sitten $y \in G$ annettu. Valitaan nyt $x = y^{-1}$, jolloin

$$\iota(x) = \iota(y^{-1}) = (y^{-1})^{-1} = y. \tag{6.42}$$

Täten ι on surjektio ja edelleen bijektio. □

Seuraus: Olkoon

$$H = \{a_1, ..., a_m\} \tag{6.43}$$

äärellinen ryhmä. Tällöin $\iota(H) = H$ eli

$$\{a_1^{-1}, ..., a_m^{-1}\} = \{a_1, ..., a_m\}. \tag{6.44}$$

ESIM: Olkoon $H = \mathrm{Z}_{11}^*$, missä

$$1^{-1} = 1,\ 2^{-1} = 6,\ 3^{-1} = 4,,\ 4^{-1} = 3,\ 5^{-1} = 9,$$

$$6^{-1} = 2,\ 7^{-1} = 8,\ 8^{-1} = 7,\ 9^{-1} = 5,\ 10^{-1} = 10. \tag{6.45}$$

Tällöin

$$1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 =$$

$$1 \cdot 2 \cdot 2^{-1} \cdot 3 \cdot 3^{-1} \cdot 5 \cdot 5^{-1} \cdot 7 \cdot 7^{-1} \cdot 10 = -1. \tag{6.46}$$

Lause 6.4. *WILSONIN LAUSE: Olkoon $p \in \mathbb{P}$. Tällöin*

$$(p-1)! \equiv -1 \ (mod\ p). \tag{6.47}$$

Lause 6.5. *Olkoot $p \in \mathbb{P}_{\geq 3}$. Tällöin*

$$1 + \frac{1}{2} + \frac{1}{3} + ... + \frac{1}{p-1} \equiv 0 \ (mod\ p). \tag{6.48}$$

Todistus. Lemman 6.1 nojalla $\iota(\mathbb{Z}_p^*) = \mathbb{Z}_p^*$ eli

$$\{\overline{1}^{-1}, ..., \overline{p-1}^{-1}\} = \{\overline{1}, ..., \overline{p-1}\}. \tag{6.49}$$

Täten

$$\sum_{a=1}^{p-1} \overline{a}^{-1} = \sum_{b=1}^{p-1} \overline{b}, \tag{6.50}$$

Seuraavassa käytetään samaistusta (6.34). Yhtälön V.P. (vasen puoli)=

$$1/\overline{1} + 1/\overline{2} + ... + 1/\overline{p-1} =$$

$$\overline{1} + \overline{1/2} + ... + \overline{1/(p-1)} = \overline{1 + 1/2 + ... + 1/(p-1)}. \tag{6.51}$$

Toisaalta Yhtälön O.P. (oikea puoli)=

$$\overline{1} + ... + \overline{p-1} = \overline{1 + 2 + ... + p - 1} = \overline{p(p-1)/2} = \overline{0}, \tag{6.52}$$

missä $p | p(p-1)/2$, sillä $p \geq 3$. Ekvivalenssiluokkien (6.51) ja (6.52) identtisyydestä seuraa edustajien välinen kongruenssi (6.48). □

Lause 6.6. *EULER-FERMAT: Olkoot $a \in \mathbb{Z}$, $m \in \mathbb{Z}_{\geq 2}$ annettu ja $a \perp m$. Tällöin*

$$a^{\varphi(m)} \equiv 1 \quad (mod\ m). \tag{6.53}$$

Todistus. Asetetaan $\tau(\overline{x}) = \overline{a} \cdot \overline{x}$. Koska $\overline{a} \in \mathbb{Z}_m^*$, niin Lemman 6.1 nojalla $\tau(\mathbb{Z}_m^*) = \mathbb{Z}_m^*$ eli

$$\{\overline{a} \cdot \overline{a}_1, ..., \overline{a} \cdot \overline{a_{\varphi(m)}}\} = \{\overline{a}_1, ..., \overline{a_{\varphi(m)}}\}. \tag{6.54}$$

Siten

$$\overline{a} \cdot \overline{a}_1 \cdots \overline{a} \cdot \overline{a_{\varphi(m)}} = \overline{a}_1 \cdots \overline{a}_{\varphi(m)} \tag{6.55}$$

eli

$$\overline{a}^{\varphi(m)} \overline{a}_1 \cdots \overline{a}_{\varphi(m)} = \overline{a}_1 \cdots \overline{a_{\varphi(m)}}, \tag{6.56}$$

josta

$$\overline{a^{\varphi(m)}} = \overline{1}. \qquad \square \tag{6.57}$$

SEURAUS:

Lause 6.7. *FERMAT'N PIKKULAUSE: Olkoot $a \in \mathbb{Z}$, $p \in \mathbb{P}$ annettu ja $p \nmid a$. Tällöin*

$$a^{p-1} \equiv 1 \pmod{p}. \tag{6.58}$$

Todistetaan seuraavaksi eräs Wilsonin lauseen yleistys.

Lause 6.8. *Olkoot $p \in \mathbb{P}_{\geq 3}$ ja $r \in \mathbb{Z}^+$. Tällöin*

$$\prod_{k=1, p \nmid k}^{p^r - 1} k \equiv -1 \ (mod\ p^r). \tag{6.59}$$

Todistus. Olkoon $\overline{a} \in \mathbb{Z}_{p^r}^*$ oma käänteisalkionsa eli

$$\overline{a} = \overline{a}^{-1} \Leftrightarrow \overline{a}^2 = \overline{1}. \tag{6.60}$$

Siten

$$\overline{a^2 - 1} = \overline{0}, \tag{6.61}$$

josta

$$(a-1)(a+1) = l \cdot p^r, \tag{6.62}$$

jollakin $l \in \mathbb{Z}$. Välttämättä

$$p|a-1 \quad \text{tai} \quad p|a+1. \tag{6.63}$$

Jos

$$p|a-1 \quad \text{ja} \quad p|a+1, \tag{6.64}$$

niin

$$p|2a \Rightarrow p|a. \tag{6.65}$$

Mutta $a \perp p$, joten joudutaan ristiriitaan. Tarkastellaan siis tapaukset

$$1.) \qquad p|a-1 \quad \text{ja} \quad p \nmid a+1 \tag{6.66}$$

ja

$$2.) \qquad p \not| a-1 \quad \text{ja} \quad p|a+1. \tag{6.67}$$

Tapaus 1. Yhtälön (6.62) nojalla

$$p^r|a-1 \Rightarrow \overline{a} = \overline{1}. \tag{6.68}$$

Tapaus 2. Yhtälön (6.62) nojalla

$$p^r|a+1 \Rightarrow \overline{a} = -\overline{1}. \tag{6.69}$$

Siten $\overline{a} \in \mathbb{Z}_{p^r}^*$ on oma käänteisalkionsa täsmälleen silloin, kun $\overline{a} = \pm\overline{1}$. Edelleen

$$\mathbb{Z}_{p^r}^* = \{\overline{1}, -\overline{1}\} \cup B, \tag{6.70}$$

missä joukon

$$B = \{\overline{b_1}, ..., \overline{b_m},\ m = \varphi(p^r) - 2\} \tag{6.71}$$

alkioille pätee

$$\overline{b_i}^{-1} \neq \overline{b_i}, \quad i = 1, ..., m. \tag{6.72}$$

Täten

$$B = \{\overline{c_1}, ..., \overline{c_{m/2}}, \overline{c_1}^{-1}, ..., \overline{c_{m/2}}^{-1}\} \tag{6.73}$$

ja siten

$$\prod_{\overline{a} \in \mathbb{Z}_{p^r}^*} \overline{a} = \overline{1}(-\overline{1})\overline{c_1 c_1}^{-1} \cdots \overline{c_{m/2} c_{m/2}}^{-1} = -\overline{1}. \quad \square \tag{6.74}$$

ESIM: $3^2 = p^r$. Jolloin

$$1 \cdot 2 \cdot 4 \cdot 5 \cdot 7 \cdot 8 \equiv -1 \pmod{3^2}. \tag{6.75}$$

6.2 Wolstenholmen lause

Lause 6.9. *WOLSTENHOLMEN LAUSE: Olkoon $p \in \mathbb{P}_{\geq 5}$. Tällöin*

$$1 + \frac{1}{2} + \frac{1}{3} + ... + \frac{1}{p-1} \equiv 0 \ (mod\ p^2). \tag{6.76}$$

Todistus. Tarkastellaan polynomia

$$G(x) = (x-1)(x-2)\cdots(x-(p-1)) \in \mathbb{Z}[x]. \tag{6.77}$$

Aukaistaan tulo, jolloin

$$G(x) = x^{p-1} - W_{p-2}x^{p-2} + W_{p-3}x^{p-3} - ... + W_2x^2 - W_1x + W_0, \tag{6.78}$$

missä $W_i \in \mathbb{Z}$. Välittömästi saadaan

$$x(x-1)(x-2)\cdots(x-(p-1)) =$$

$$x^p - W_{p-2}x^{p-1} + W_{p-3}x^{p-2} - W_{p-4}x^{p-3} + ... + W_2x^3 - W_1x^2 + W_0x, \tag{6.79}$$

johon sijoitetaan $x = y - 1$ ja siten

$$(y-1)(y-2)\cdots(y-(p-1))(y-p) =$$

$$(y-1)^p - W_{p-2}(y-1)^{p-1} + W_{p-3}(y-1)^{p-2} - W_{p-4}(y-1)^{p-3} + ...$$

$$+W_2(y-1)^3 - W_1(y-1)^2 + W_0(y-1). \tag{6.80}$$

Yhtälössä (6.80) V.P.=

$$(y-p)G(y) = (y-p)(y^{p-1} - W_{p-2}y^{p-2} + W_{p-3}y^{p-3} - ... + W_2y^2 - W_1y + W_0) =$$

$$y^p - (p + W_{p-2})y^{p-1} + (pW_{p-2} + W_{p-3})y^{p-2} - (pW_{p-3} + W_{p-4})y^{p-3}$$
$$+... - (pW_2 + W_1)y^2 + (pW_1 + W_0)y - pW_0. \tag{6.81}$$

Toisaalta yhtälön (6.80) O.P.=

$$y^p - (\binom{p}{1} + W_{p-2})y^{p-1} + (\binom{p}{2} + W_{p-2}\binom{p-1}{1} + W_{p-3})y^{p-2}$$
$$-(\binom{p}{3} + W_{p-2}\binom{p-1}{2} + W_{p-3}\binom{p-2}{1} + W_{p-4})y^{p-3}$$
$$+... + (\binom{p}{p-1} + W_{p-2}\binom{p-1}{p-2} + ... + W_1\binom{2}{1} + W_0)y$$
$$-(1 + W_{p-2} + ... + W_1 + W_0). \tag{6.82}$$

Verrataan seuraavaksi vastinpotenssien kertoimia yhtälöissä (6.81) ja (6.82), jolloin

$$y^p : \quad 1 = 1, \tag{6.83}$$
$$y^{p-1} : \ p + W_{p-2} = \binom{p}{1} + W_{p-2}, \tag{6.84}$$
$$y^{p-2} : \ pW_{p-2} + W_{p-3} = \binom{p}{2} + W_{p-2}\binom{p-1}{1} + W_{p-3}, \tag{6.85}$$
$$y^{p-3} : \ pW_{p-3} + W_{p-4} = \binom{p}{3} + W_{p-2}\binom{p-1}{2} + W_{p-3}\binom{p-2}{1} + W_{p-4}, ... \tag{6.86}$$
$$y^1 : \ pW_1 + W_0 = \binom{p}{p-1} + W_{p-2}\binom{p-1}{p-2} + ... + W_1\binom{2}{1} + W_0, \tag{6.87}$$
$$y^0 : \ pW_0 = 1 + W_{p-2} + ... + W_1 + W_0. \tag{6.88}$$

Kaksi ensimmäistä ovat triviaali-identiteettejä mutta seuraavista saadaan palautuskaavat:

$$W_{p-2} = \binom{p}{2}, \tag{6.89}$$
$$2W_{p-3} = \binom{p}{3} + \binom{p-1}{2}W_{p-2}, \tag{6.90}$$

$$3W_{p-4} = \binom{p}{4} + \binom{p-1}{3}W_{p-2} + \binom{p-2}{2}W_{p-3}, ... \tag{6.91}$$

$$(p-2)W_1 = \binom{p}{p-1} + \binom{p-1}{p-2}W_{p-2} + ... + \binom{3}{2}W_2, \tag{6.92}$$

$$(p-1)W_0 = 1 + W_{p-2} + ... + W_1. \tag{6.93}$$

Huomaa, että nämä yhtälöt ovat muotoa

$$jW_{p-j-1} = \binom{p}{j+1} + ... \quad \forall \quad 1 \leq j \leq p-1. \tag{6.94}$$

Käytetään tulosta (4.26), jolloin

$$p|\binom{p}{2} \tag{6.95}$$

ja siten

$$j = 1. \qquad p|W_{p-2}. \tag{6.96}$$

Seuraavaksi

$$p|\binom{p}{3} \quad \text{ja} \quad p|W_{p-2}, \tag{6.97}$$

joten

$$j = 2. \qquad p|W_{p-3}. \tag{6.98}$$

Edelleen

$$p|\binom{p}{4}, \quad p|W_{p-2} \quad \text{ja} \quad p|W_{p-3}, \tag{6.99}$$

joten

$$j = 3. \qquad p|W_{p-4}. \tag{6.100}$$

...

$$j = p-2. \qquad p|W_1. \tag{6.101}$$

Siten

$$p|W_1, W_2, ..., W_{p-2}, \tag{6.102}$$

josta

$$j = p-1. \qquad (p-1)W_0 \equiv 1 \pmod{p} \tag{6.103}$$

eli

$$W_0 \equiv -1 \pmod{p}. \tag{6.104}$$

Mutta

$$W_0 = (p-1)!, \tag{6.105}$$

joten saadaan II todistus Wilsonin lauseelle.

Sijoitetaan nyt $x = p$ yhtälöön

$$G(x) = \prod_{j=1}^{p-1}(x-j) = \sum_{i=0}^{p-1}(-1)^i W_i x^i, \quad W_{p-1} = 1, \tag{6.106}$$

josta saadaan

$$W_1 = W_2 p - W_3 p^2 - ... + p^{p-2}. \tag{6.107}$$

Koska $p|W_2$ ja $p \geq 5$, niin

$$p^2 | W_1. \tag{6.108}$$

Toisaalta

$$W_1 = \sum_{j=1}^{p-1} \prod_{i=1, i\neq j}^{p-1} i =$$

$$2 \cdot 3 \cdots (p-1) + 1 \cdot 3 \cdot 4 \cdots (p-1) + ... + 1 \cdot 2 \cdots (p-3) \cdot (p-1) + 1 \cdot 2 \cdots (p-2) =$$

$$(p-1)! \left(1 + \frac{1}{2} + \frac{1}{3} + ... + \frac{1}{p-1}\right). \tag{6.109}$$

Siten

$$p^2 \left| 1 + \frac{1}{2} + \frac{1}{3} + ... + \frac{1}{p-1} \right. \quad \square \tag{6.110}$$

II todistus Fermat'n pikkulauseelle. Olkoot $p \in \mathbb{P}$, $a \in \mathbb{Z}$ ja $p \nmid a$. Tällöin

$$a \equiv j \pmod{p}, \tag{6.111}$$

jollakin $j = 1, 2, ..., p-1$. Sijoitetaan $x = a$ yhtälöön (6.106), jolloin

$$a^{p-1} - W_{p-2} a^{p-2} + W_{p-3} a^{p-3} - ... + W_2 a^2 - W_1 a + W_0 \equiv 0 \pmod{p}, \tag{6.112}$$

missä

$$W_{p-2}, ..., W_1 \equiv 0 \pmod{p}. \tag{6.113}$$

Siten

$$a^{p-1} \equiv -W_0 \equiv -(p-1)! \equiv 1 \pmod{p}. \quad \square \tag{6.114}$$

6.3 $(p-1)!$ ja a^{p-1} (mod p^2)

Tiedetään, että

$$(p-1)! \equiv -1 \pmod{p^2}, \tag{6.115}$$

kun $p = 5, 13, 563, ...$ (Wilsonin alkulukuja) ja

$$a^{p-1} \equiv 1 \pmod{p^2}, \tag{6.116}$$

kun $p = 1093, 3511, ...$ Mutta yleisellä tasolla kohtien (6.115) ja (6.116) jakojäännöksien (mod p^2) käyttäytymistä ei tunneta.
Ehdon (6.116) tutkiminen on ollut tärkeää liittyen Fermat'n suuren lauseen todistusyrityksiin, sillä jos $p \in \mathbb{P}_{\geq 3}$ ja

$$2^{p-1} \not\equiv 1 \pmod{p^2}, \tag{6.117}$$

niin

$$x^p + y^p \neq z^p \quad \forall \quad x, y, z \in \mathbb{Z}^+. \tag{6.118}$$

Tosin Andre Wiles [Annals of Mathematics 141 (1994)] on todistanut, että (6.118) pätee ilman lisäoletusta (6.117). Wilesin todistus perustuu mm. elliptisten käyrien ominaisuuksiin.

Olkoon $p \in \mathbb{P}_{\geq 3}$, tällöin Pikku Fermat'n nojalla tiedetään, että

$$2^{p-1} - 1 = l \cdot p, \tag{6.119}$$

jollakin $l \in \mathbb{Z}$, joten on luonnollista tutkia Fermat'n osamääriä

$$q_p(2) = \frac{2^{p-1} - 1}{p} \in \mathbb{Z}. \tag{6.120}$$

Lause 6.10. *Olkoon $p \in \mathbb{P}_{\geq 3}$. Tällöin*

$$q_p(2) = \frac{2^{p-1} - 1}{p} \equiv 1 + \frac{1}{3} + \frac{1}{5} + ... + \frac{1}{p-2} \pmod{p} \tag{6.121}$$

Huomaa, että (6.121) on yhtäpitävää ehdon

$$2^{p-1} \equiv 1 + p\left(1 + \frac{1}{3} + \frac{1}{5} + ... + \frac{1}{p-2}\right) \pmod{p^2} \tag{6.122}$$

kanssa.

Todistus. Aluksi binomikaavalla saadaan

$$2^p = \sum_{i=0}^{p} \binom{p}{i} = 2 + \sum_{i=1}^{p-1} \binom{p}{i}, \tag{6.123}$$

jossa tuloksen (4.26) nojalla

$$\binom{p}{i} = ph_i, \tag{6.124}$$

jollakin $h_i \in \mathbb{Z}$ aina, kun $i = 1, ..., p-1$. Edelleen

$$h_i = \frac{(p-1)(p-2)\cdots(p-i+1)}{i!} \equiv \frac{(-1)^{i-1}(i-1)!}{i!} = \frac{(-1)^{i-1}}{i} \pmod{p} \tag{6.125}$$

eli

$$h_i = \frac{(-1)^{i-1}}{i} + m_i p, \tag{6.126}$$

jollakin $m_i \in \mathbb{Z}$. Siten (6.124) ja (6.126) antavat

$$\binom{p}{i} = p\left(\frac{(-1)^{i-1}}{i} + m_i p\right) \equiv (-1)^{i-1}\frac{p}{i} \pmod{p^2}. \tag{6.127}$$

Yhtälöiden (6.123) ja (6.127) nojalla

$$2^p \equiv 2 + p\left(1 - \frac{1}{2} + \frac{1}{3} - ... + \frac{1}{p-2} - \frac{1}{p-1}\right) \pmod{p^2}. \tag{6.128}$$

Toisaalta

$$1 - \frac{1}{2} + \frac{1}{3} - ... + \frac{1}{p-2} - \frac{1}{p-1} =$$
$$2\left(1 + \frac{1}{3} + \frac{1}{5} - ... + \frac{1}{p-2}\right)$$
$$-\left(1 + \frac{1}{2} + \frac{1}{3} + ... + \frac{1}{p-2} + \frac{1}{p-1}\right)$$
$$\equiv 2\left(1 + \frac{1}{3} + \frac{1}{5} - ... + \frac{1}{p-2}\right) \pmod{p^2} \tag{6.129}$$

tuloksen (6.76) nojalla. Yhdistämällä (6.128) ja (6.129) saadaan

$$2^p \equiv 2 + 2p\left(1 + \frac{1}{3} + \frac{1}{5} - ... + \frac{1}{p-2}\right) \pmod{p^2}, \tag{6.130}$$

missä $p \perp 2$, joten (6.122) seuraa. □

ESIM: Olkoon $p = 7$. Nyt

$$2^{p-1} = 2^6 = 1 + 63 = 1 + 7 \cdot 9 \equiv 1 + 7\left(1 + \frac{1}{3} + \frac{1}{5}\right) \pmod{7^2}. \tag{6.131}$$

Huomaa, että $1/3 = 5$ ja $1/5 = 3 \pmod 7$.

7 Lisää polynomialgebraa

7.1 Symmetriset peruspolynomit

Tutkitaan polynomi-identiteettiä

$$F(x) = \prod_{k=1}^{n}(x - x_k) = \sum_{i=0}^{n}(-1)^{n-i}A_i x^i. \tag{7.1}$$

0. Sijoittamalla $x = 0$, saadaan vakiotermeistä identiteetti

$$F(0) = (-1)^n \prod_{j=1}^{n} x_j = (-1)^n A_0,$$

joten

$$A_0 = \prod_{j=1}^{n} x_j. \qquad (7.2)$$

(Tulolla (7.2) määritellään Normi, kts. Lukuteoria.)

1. Lasketaan derivaatat yhtälössä (7.1) puolittain, jolloin

$$D\prod_{k=1}^{n}(x - x_k) =$$

$$1\cdot(x-x_2)\cdots(x-x_n)+(x-x_1)\cdot(x-x_3)\cdots(x-x_n)+...+(x-x_1)(x-x_2)\cdots(x-x_{n-1}), \qquad (7.3)$$

josta kohdassa $x = 0$ saadaan

$$DF(0) = (-1)^{n-1}(x_2x_3\cdots x_n + x_1x_3\cdots x_n + ... + x_1x_2\cdots x_{n-1}). \qquad (7.4)$$

Toisaalta

$$DF(0) = (-1)^{n-1}A_1$$

ja siten

$$A_1 = \sum_{j=1}^{n}\prod_{i=1,i\neq j}^{n} x_i. \qquad (7.5)$$

n-1. Myös

$$A_{n-1} = \sum_{j=1}^{n} x_j \qquad (7.6)$$

on usein tarpeen (ja sen avulla määritellään Jälki(=Trace).) Yleisesti saadaan

$$A_{n-k} = \sum_{1\leq j_1<j_2<...<j_k\leq n} x_{j_1}x_{j_2}\cdots x_{j_k}, \qquad (7.7)$$

joilla on yhteys

$$A_{n-k} = s_k(x_1, ...x_n) \qquad (7.8)$$

symmetrisiin peruspolynomeihin s_k (elementary symmetric polynomials).

ESIM: a) $n = 4$.

$$(x - x_1)(x - x_2)(x - x_3)(x - x_4) = x^4 - (x_1 + x_2 + x_3 + x_4)x^3+$$

$$(x_1x_2+x_1x_3+x_1x_4+x_2x_3+x_2x_4+x_3x_4)x^2-(x_1x_2x_3+x_1x_3x_4+x_2x_3x_4)x+x_1x_2x_3x_4. \qquad (7.9)$$

b) Wolstenholmen lauseen todistuksessa tarkasteltiin polynomia

$$G(x) = \prod_{j=1}^{p-1}(x-j) = \sum_{i=0}^{p-1}(-1)^i W_i x^i, \quad W_{p-1} = 1,$$

missä kohtien (7.2), (7.5) ja (7.6) nojalla

$$W_0 = \prod_{j=1}^{p-1} j = (p-1)!,$$

$$W_1 = 2\cdot 3\cdots(p-1)+1\cdot 3\cdot 4\cdots(p-1)+...+1\cdot 2\cdots(p-3)\cdot(p-1)+1\cdot 2\cdots(p-2)$$

ja

$$W_{p-2} = 1+2+...+p-1 = \binom{p}{2}.$$

7.2 Polynomien kongruenssi

Määritelmä 7.1. Olkoot $n \in \mathbb{Z}_{\geq 2}$ ja

$$P(x) = \sum_{k=0}^{n} p_k x^k \in \mathbb{Q}[x],$$

$$Q(x) = \sum_{k=0}^{n} q_k x^k \in \mathbb{Q}[x],$$

jolloin asetetaan

$$P(x) \equiv Q(x) \pmod{n} \quad \Leftrightarrow \quad p_k \equiv q_k \pmod{n} \qquad \forall k = 0, 1, ..., n.$$

Lause 7.1. *Olkoon $p \in \mathbb{P}$, tällöin*

$$(x+1)^p \equiv x^p + 1 \quad (mod\ p). \qquad (7.10)$$

polynomirenkaassa $\mathbb{Q}[x]$.

Todistus. Binomisarjan ja Lauseen 4.5 nojalla

$$(x+1)^p = \sum_{k=0}^{p} \binom{p}{k} x^k \equiv x^p + 0 \cdot x^{p-1} + 0 \cdot x^{p-2} + ... + 0 \cdot x + 1 = x^p + 1 \pmod{p}. \quad \square$$

Lause 7.2. *Olkoot $n \in \mathbb{Z}_{\geq 2}$ ja $f(x), g(x), h(x) \in \mathbb{Q}[x]$ ja*

$$g(x) \equiv h(x) \quad (mod\ n). \qquad (7.11)$$

Tällöin

$$f(g(x)) \equiv f(h(x)) \quad (mod\ n). \qquad (7.12)$$

Lause 7.3. *Olkoot $p \in \mathbb{P}$ ja $r \in \mathbb{N}$. Tällöin*

$$(x+1)^{p^r} \equiv x^{p^r} + 1 \quad (mod\ p). \qquad (7.13)$$

polynomirenkaassa $\mathbb{Q}[x]$.

Todistus. Induktiolla. $r = 1$. $\Leftrightarrow$ Lause 7.1.

Induktioaskeleessa lasketaan V.P.=

$$(x+1)^{p^{r+1}} = ((x+1)^{p^r})^p \equiv (x^{p^r} + 1)^p \qquad (7.14)$$

$$\equiv (x^{p^r})^p + 1 = x^{p^{r+1}} + 1 \pmod{p} \qquad (7.15)$$

=O.P. Kohdassa (7.14) sovellettiin Lausetta 7.2 ja kohdassa (7.15) Lausetta 7.1.

$\square$

Seurauksena saadaan

Lause 7.4. *Olkoot $p \in \mathbb{P}$ ja $r \in \mathbb{Z}^+$. Tällöin*

$$\binom{p^r}{k} \equiv 0 \quad (mod\ p) \quad \forall\ k = 1, ..., p^r - 1. \qquad (7.16)$$

Lause 7.3 voidaan yleistää kahdenmuuttujan polynomeille.

Lause 7.5. *Olkoot $p \in \mathbb{P}$ ja $r \in \mathbb{N}$. Tällöin*

$$(x+y)^{p^r} \equiv x^{p^r} + y^{p^r} \quad (mod\ p) \qquad (7.17)$$

polynomirenkaassa $\mathbb{Q}[x, y]$.

Ja edelleen useanmuuttujan tapaukseen.

Lause 7.6. *Olkoot $p \in \mathbb{P}$ ja $r \in \mathbb{N}$. Tällöin*

$$(x_1 + ... + x_m)^{p^r} \equiv x_1^{p^r} + ... + x_m^{p^r} \quad (mod\ p) \qquad (7.18)$$

polynomirenkaassa $\mathbb{Q}[x_1, ..., x_m]$.

7.3 Sovelluksia lukujen kongruensseihin

Sovelletaan Lausetta 7.6 antamalle muuttujille rationaalilukuarvot.

Rationaaliluku $a/b \in \mathbb{Q}^*$ on supistetussa muodossa, kun $a \perp b$.

Määritelmä 7.2. Olkoon $p \in \mathbb{P}$ ja

$$A = \frac{a}{b} = p^r \frac{c}{d}, \quad p \not| cd.$$

Tällöin $v_p(A) = r$ on eksponentiaalinen valuaatio ja $\text{den}(a/b) = b$ on A:n nimittäjä.

Siten, jos $v_p(A) \geq 0$, niin $p \perp b$ ja jos $p|A$, niin $p \perp b$.

Lause 7.7. *Olkoot $p \in \mathbb{P}$, $r \in \mathbb{N}$ ja $A_i \in \mathbb{Q}$, $v_p(A_i) \geq 0$ aina, kun $i = 1, ..., m$. Tällöin*

$$(A_1 + ... + A_m)^{p^r} \equiv A_1^{p^r} + ... + A_m^{p^r} \quad (mod\ p). \qquad (7.19)$$

Huomaa, että (7.19) on PikkuFermat'n yleistys.

Olkoot $p \in \mathbb{P}$ ja $n \in \mathbb{N}$. Tiedetään, että p-kantakehitelmä

$$n = \sum_{i \geq 0} n_i p^i, \quad 0 \leq n_i \leq p - 1$$

on yksikäsitteinen.

Lause 7.8. *LUCASIN (BINOMIKERROIN)LAUSE. Olkoot $p \in \mathbb{P}$, $n, k \in \mathbb{N}$ sekä*

$$n = \sum_{i \geq 0} n_i p^i, \quad k = \sum_{i \geq 0} k_i p^i, \quad 0 \leq k_i, n_i \leq p - 1. \qquad (7.20)$$

Tällöin

$$\binom{n}{k} \equiv \prod_{i\geq 0} \binom{n_i}{k_i} \quad (mod\ p). \qquad (7.21)$$

Todistus. Aluksi huomataan, että

$$(1+x)^n = (1+x)^{n_0}(1+x)^{pn_1}(1+x)^{p^2n_2}\cdots \equiv (1+x)^{n_0}(1+x^p)^{n_1}(1+x^{p^2})^{n_2}\cdots \pmod{p} \qquad (7.22)$$

Lauseen 7.3 nojalla. Sama binomikehitelmillä

$$\sum_{k=0}^{n}\binom{n}{k}x^k \equiv \sum_{i_0=0}^{n_0}\binom{n_0}{i_0}x^{i_0}\sum_{i_1=0}^{n_1}\binom{n_1}{i_1}x^{pi_1}\sum_{i_2=0}^{n_2}\binom{n_2}{i_2}x^{p^2i_2} =$$

$$\sum_{i_0=0}^{p-1}\binom{n_0}{i_0}x^{i_0}\sum_{i_1=0}^{p-1}\binom{n_1}{i_1}x^{pi_1}\sum_{i_2=0}^{p-1}\binom{n_2}{i_2}x^{p^2i_2} =$$

$$\sum_{0\leq j}\sum_{0\leq i_j\leq p-1}\binom{n_0}{i_0}\binom{n_1}{i_1}\binom{n_2}{i_2}\cdots x^{i_0+i_1p+i_2p^2+\ldots} \pmod{p}. \qquad (7.23)$$

Luvun k yksikäsitteisen p-kantaesityksen nojalla havaitaan, että O.P. termi x^k saadaan täsmälleen, silloin kun $i_0 = k_0$, $i_1 = k_1$,... . Täten vertaamalla kongruenssin (7.23) V.P. ja O.P. termejä x^k, saadaan kongruenssi

$$\binom{n}{k}x^k \equiv \prod_{i\geq 0}\binom{n_i}{k_i}x^k \pmod{p}. \qquad (7.24) \quad \square$$

Esim: $p = 7$, $n = 11 = 4 + 1\cdot 7$, $k = 5 = 5 + 0\cdot 7$, joten

$$\binom{11}{5} \equiv \binom{n_0}{k_0}\binom{n_1}{k_1} = \binom{4}{5}\binom{1}{0} = 0\cdot 1 = 0 \pmod{7}. \qquad (7.25)$$

8 Summausmenetelmiä

8.1 Polynomialgebran sovelluksia

ESIM: Lähdetään identiteetistä

$$(1+x)^n(1+x)^m = (1+x)^{n+m},$$

josta

$$\sum_{j=0}^{n} \binom{n}{j} x^j \sum_{l=0}^{m} \binom{m}{l} x^l = \sum_{k=0}^{n+m} \binom{n+m}{k} x^k.$$

Caychyn kertosäännöllä

$$\sum_{k=0}^{n+m} \left(\sum_{j+l=k} \binom{n}{j} \binom{m}{l} \right) x^k = \sum_{k=0}^{n+m} \binom{n+m}{k} x^k,$$

josta

$$\sum_{j+l=k, 0 \le j,l \le k} \binom{n}{j} \binom{m}{l} = \binom{n+m}{k} \qquad (8.1)$$

Edelleen, asettamalla $n = m = k$, saadaan

$$\sum_{j=0}^{m} \binom{n}{j} \binom{m}{m-j} = \binom{2m}{m} \quad \sum_{j=0}^{m} \binom{m}{j}^2 = \binom{2m}{m}. \qquad (8.2)$$

8.2 Teleskoopit

Teleskooppisumma

$$\sum_{i=0}^{n} (a_{i+1} - a_i) = a_{n+1} - a_0 \qquad (8.3)$$

ja teleskooppitulo

$$\prod_{i=0}^{n} \frac{a_{i+1}}{a_i} = \frac{a_{n+1}}{a_0} \qquad (8.4)$$

soveltuvat hyvin muunmuassa seuraavantyyppisten tulosten johtamiseen.

$$\sum_{k=0}^{n} k = \frac{n(n+1)}{2} \qquad (8.5)$$

$$\sum_{k=0}^{n} k^2 = \frac{n(n+1)(2n+1)}{6} \qquad (8.6)$$

$$\sum_{k=0}^{n} k^3 = \left(\frac{n(n+1)}{2} \right)^2 \qquad (8.7)$$

$$\sum_{k=0}^{n}(2k+1) = (n+1)^2 \qquad (8.8)$$

Johdetaan (8.8) valitsemalla $a_k = k^2$ ja lähtemällä identiteetistä

$$a_{k+1} - a_k = (k+1)^2 - k^2 = 2k + 1. \qquad (8.9)$$

Otetaan summat (8.9) molemminpuolin, jolloin

$$\sum_{k=0}^{n}(2k+1) = \sum_{k=0}^{n}(a_{k+1} - a_k) = a_{n+1} - a_0 = (n+1)^2.$$

Johdetaan vielä

$$\sum_{j=0}^{\infty}\frac{j-1}{j!} = 0 \qquad (8.10)$$

lähtemällä erotuksesta

$$\frac{1}{k!} - \frac{1}{(k+1)!} = \frac{k}{(k+1)!}. \qquad (8.11)$$

Summataan (8.11) puolittain, jolloin saadaan

$$\sum_{k=0}^{n}\left(\frac{1}{k!} - \frac{1}{(k+1)!}\right) = \sum_{k=0}^{n}\frac{k}{(k+1)!}. \qquad (8.12)$$

Yhtälön (8.12)vasemmanpuolen summassa on teleskooppi ja siten

$$\sum_{k=0}^{n}\frac{k}{(k+1)!} = 1 - \frac{1}{(n+1)!}, \qquad (8.13)$$

josta raja-arvona saadaan

$$\sum_{k=0}^{\infty}\frac{k}{(k+1)!} = 1 \qquad (8.14)$$

eli (8.10).

9 Fibonaccin ja Lucasin luvut

9.1 Rekursio ja Binet'n kaava

Määritelmä 9.1. Luvut $f_0 = 0$, $f_1 = 1$ ja palautuskaava (eli rekursio)

$$f_{n+2} = f_{n+1} + f_n, \quad n \in \mathbb{N}, \qquad (9.1)$$

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

$$l_{n+2} = l_{n+1} + l_n, \quad n \in \mathbb{N}, \qquad (9.2)$$

muodostavat Lucasin luvut.

Siten Fibonaccin lukuja ovat

$$f_0 = 0, f_1 = 1, f_2 = 1, f_3 = 2, f_4 = 3, f_5 = 5, f_6 = 8, f_7 = 13, ... \qquad (9.3)$$

ja Lucasin lukuja ovat

$$l_0 = 2, l_1 = 1, l_2 = 3, l_3 = 4, l_4 = 7, l_5 = 11, l_6 = 18, l_7 = 29, ... \qquad (9.4)$$

Ratkaistaan rekursio

$$v_{n+2} = v_{n+1} + v_n, \quad n \in \mathbb{N}, \qquad (9.5)$$

yritteellä

$$v_n = x^n, \quad x \in \mathbb{C}^*. \qquad (9.6)$$

Rekursiosta (9.5) saadaan

$$x^{n+2} = x^{n+1} + x^n \quad \Leftrightarrow \quad x^2 - x - 1 = 0, \qquad (9.7)$$

jonka ratkaisut ovat

$$\alpha = \frac{1+\sqrt{5}}{2}, \quad \beta = \frac{1-\sqrt{5}}{2}. \qquad (9.8)$$

Lause 9.1. *Olkoot $a, b \in \mathbb{C}$. Tällöin*

$$F_n = a\alpha^n + b\beta^n \qquad (9.9)$$

on rekursion (9.5) ratkaisu.

Todistus. Suoraan laskemalla saadaan

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

$$a\alpha^{n+1} + b\beta^{n+1} + a\alpha^n + b\beta^n = F_{n+1} + F_n. \quad \square \qquad (9.10)$$

Siten Fibonaccin luvut ovat muotoa

$$f_n = a\alpha^n + b\beta^n \qquad (9.11)$$

mistä saadaan

$$f_0 = a\alpha^0 + b\beta^0, \quad f_1 = a\alpha^1 + b\beta^1. \qquad (9.12)$$

Sijoitetaan alkuarvot $f_0 = 0$ ja $f_1 = 1$ yhtälöön (9.12), josta

$$a + b = 0, \quad a\frac{1+\sqrt{5}}{2} + b\frac{1-\sqrt{5}}{2} = 1 \qquad (9.13)$$

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

Lause 9.2. *Fibonaccin ja Lucasin luvut voidaan esittää Binet'n kaavoilla*

$$f_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right), \qquad (9.14)$$

$$l_n = \left(\frac{1+\sqrt{5}}{2}\right)^n + \left(\frac{1-\sqrt{5}}{2}\right)^n. \qquad (9.15)$$

HUOM: Rekursioilla saadaan tarkat arvot nopeasti (laskennallinen kompleksisuus), mutta eksplisiittisistä esityksistä (9.14) ja (9.15) saadaan likiarvo nopeasti.

Lause 9.3.

$$f_{2k} = \left\lfloor \frac{\alpha^{2k}}{\sqrt{5}} \right\rfloor \quad \forall k \in \mathbb{N}, \qquad (9.16)$$

$$f_{2k+1} = \left\lceil \frac{\alpha^{2k+1}}{\sqrt{5}} \right\rceil \quad \forall k \in \mathbb{N}. \qquad (9.17)$$

Todistus. Aluksi haetaan likiarvot. Koska

$$\alpha = \frac{1+\sqrt{5}}{2} = 1.6180..., \qquad (9.18)$$

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

$$\beta = \frac{1-\sqrt{5}}{2} = 1 - \alpha = -0.6180.... \qquad (9.19)$$

Siten

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

Tarkemmin laskareissa.

9.2 Matriisiesitys

Olkoon

$$\mathbb{F} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} f_2 & f_1 \\ f_1 & f_0 \end{pmatrix}. \qquad (9.20)$$

Lasketaan potensseja

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

$$\mathbb{F}^3 = \begin{pmatrix} 3 & 2 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} f_4 & f_3 \\ f_3 & f_2 \end{pmatrix}. \qquad (9.21), ...$$

Jolloin huomataan, että alkioiksi tulee Fibonaccin lukuja. Sovitaan vielä, että $f_{-1} = 1$, sillä tällöin pätee

$$f_1 = f_0 + f_{-1}. \qquad (9.22)$$

Nyt

$$\mathbb{F}^0 = \mathbb{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} f_1 & f_0 \\ f_0 & f_{-1} \end{pmatrix}. \qquad (9.23)$$

Lause 9.4. *Olkoon*

$$\mathbb{F}_n = \mathbb{F}^n \quad n \in \mathbb{N}. \qquad (9.24)$$

Tällöin

$$\mathbb{F}_n = \begin{pmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{pmatrix}. \qquad (9.25)$$

Todistus. Induktiolla. Tapaukset $n = 0$ ja $n = 1$ kohdista (9.20) ja (9.23).

Induktio-oletus: Identiteetti (9.24) pätee, kun $n = k$.

Induktioaskel; Lasketaan

$$\mathbb{F}_{k+1} = \mathbb{F}_1\mathbb{F}_k = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} f_{k+1} & f_k \\ f_k & f_{k-1} \end{pmatrix} =$$

$$\begin{pmatrix} f_{k+1} + f_k & f_k + f_{k-1} \\ f_{k+1} & f_k \end{pmatrix} = \begin{pmatrix} f_{k+2} & f_{k+1} \\ f_{k+1} & f_k \end{pmatrix} = \mathbb{F}_{k+1}. \qquad (9.26) \quad \square$$

Lause 9.5. *Olkoot $n, m \in \mathbb{N}$, tällöin*

$$f_{n+m+1} = f_{n+1}f_{m+1} + f_nf_m, \qquad (9.27)$$

$$f_{2m+1} = f_{m+1}^2 + f_m^2, \qquad (9.28)$$

$$f_{2m} = f_m(f_{m+1} + f_{m-1}). \qquad (9.29)$$

Todistus. Sovelletaan identiteettiä

$$\mathbb{F}_{n+m} = \mathbb{F}_{n+m} = \mathbb{F}^{n+m} = \mathbb{F}^n\mathbb{F}^m = \mathbb{F}_n\mathbb{F}_m, \qquad (9.30)$$

jolloin

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

$$\begin{pmatrix} f_{n+1}f_{m+1} + f_n f_m & f_{n+1}f_m + f_n f_{m-1} \\ f_n f_{m+1} + f_{n-1}f_m & f_n f_m + f_{n-1}f_{m-1} \end{pmatrix}. \qquad (9.31)$$

Vertaamalla matriisien (9.31) alkioita saadaan (9.27), josta edelleen saadaan (9.28) ja (9.29). □

Lause 9.6. *Olkoon $n \in \mathbb{N}$, tällöin*

$$f_{n+1}f_{n-1} - f_n^2 = (-1)^n. \qquad (9.32)$$

Todistus. Otetaan determinantit tuloksesta (9.24), jolloin

$$\begin{vmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{vmatrix} = \begin{vmatrix} 1 & 1 \\ 1 & 0 \end{vmatrix}^n. \qquad (9.33) \quad \square$$

Lause 9.7. *Olkoon $n \in \mathbb{N}$, tällöin lukujen f_{n+2} ja f_{n+1} Eukleideen algoritmin pituus on n. Edelleen*

$$syt(f_{n+1}, f_n) = 1. \qquad (9.34)$$

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

$$r_n = \text{syt}(a, b) = 1. \qquad (9.35) \quad \square$$

Edelleen saadaan

$$r_n = s_n a + t_n b \quad \Leftrightarrow \quad 1 = s_n f_{n+2} + t_n f_{n+1}, \qquad (9.36)$$

missä s_n ja t_n saadaan palautuskaavoista

$$s_{k+2} = s_k - q_{k+1} s_{k+1} = s_k - s_{k+1}, \qquad (9.37)$$

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

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

$$1 = (-3) \cdot 13 + 5 \cdot 8 = f_5 f_6 - f_4 f_7. \qquad (9.38)$$

Lause 9.8. *Olkoon $a, b \in \mathbb{Z}^+$ annettu, tällöin Eukleideen algoritmin pituudelle n pätee*

$$n \leq \log a / \log((1 + \sqrt{5})/2)). \qquad (9.39)$$

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

$$r_n \geq 1 = f_2,$$

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

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

Edelleen induktiolla saadaan

$$r_{n-h} \geq f_{h+2} \quad \forall \quad h = 0, 1, ..., n \qquad (9.40)$$

ja siten

$$a = r_0 \geq f_{n+2} \geq ((1 + \sqrt{5})/2)^n. \qquad (9.41)$$

Epäyhtälön (9.41) todistus laskareissa. □

9.3 Generoiva sarja

Olkoon

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

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

$$F(z) = \sum_{n=0}^{\infty} f_{n+2} z^{n+2} + f_1 z + f_0. \qquad (9.42)$$

Seuraavaksi käytetään rekursiota (9.1), jolloin

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

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

$$z(F(z) - f_0) + z^2 F(z) + z. \qquad (9.43)$$

Yhtälöstä (9.43) saadaan ratkaisu

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

Lause 9.9. *Sarjalla*

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

on esitys rationaalifunktiona

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

Määritelmä 9.2. Sarja

$$F(z) = \sum_{k=0}^{\infty} f_k z^k \qquad (9.44)$$

on Fibonaccin lukujen generoiva sarja ja funktio

$$F(z) = \frac{z}{1 - z - z^2} \qquad (9.45)$$

on Fibonaccin lukujen generoiva funktio.

Määritelmä 9.3. Polynomi

$$K(x) = K_f(x) = x^2 - x - 1$$

on rekursion (9.1) karakteristinen polynomi.

Huomaa, että

$$K_f(x) = (x - \alpha)(x - \beta), \qquad (9.46)$$

joten

$$F(z) = \frac{1/z}{(1/z)^2 - 1/z - 1} = \frac{1/z}{K(1/z)} =$$
$$\frac{1/z}{(1/z - \alpha)(1/z - \beta)} = \frac{z}{(1 - \alpha z)(1 - \beta z)}. \qquad (9.47)$$

Jaetaan (9.47) osamurtoihin ja käytetään geometrisen sarjan summakaavaa, jolloin

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

$$\sum_{k=0}^{\infty} \frac{1}{\sqrt{5}} \left(\alpha^k - \beta^k\right) z^k = \sum_{k=0}^{\infty} f_k z^k. \qquad (9.48)$$

Vertaamalla sarjojen kertoimia saadaan jälleen Binet'n esitys (9.14).

9.4 Laajennus negatiivisiin indekseihin

Sallitaan Fibonaccin lukujen palautuskaavassa

$$f_{k+2} = f_{k+1} + f_k \qquad (9.49)$$

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

$$f_1 = f_0 + f_{-1} \Rightarrow f_{-1} = 1, \qquad (9.50)$$

$$f_0 = f_{-1} + f_{-2} \Rightarrow f_{-2} = -1, \qquad (9.51)$$

$$f_{-1} = f_{-2} + f_{-3} \Rightarrow f_{-3} = 2, ... \qquad (9.52)$$

Sijoitetaan $k = -n$ rekursioon (9.49), jolloin

$$f_{-n} = -f_{-(n-1)} + f_{-(n-2)}. \qquad (9.53)$$

Lause 9.10.

$$f_{-n} = (-1)^{n+1} f_n \quad \forall\ n \in \mathbb{N}. \qquad (9.54)$$

Todistus. Induktiolla käyttäen rekursiota (9.53).

Äskeisen tuloksen nojalla Lause 9.4 laajenee myös negatiiviselle puolelle.

Lause 9.11. *Olkoon*

$$\mathbb{F} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

ja

$$\mathbb{F}_n = \mathbb{F}^n \quad n \in \mathbb{Z}. \qquad (9.55)$$

Tällöin

$$\mathbb{F}_n = \begin{pmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{pmatrix}. \qquad (9.57)$$

Todistus. $n \geq 0$ kts. Lause 9.4.

$n \leq 0$.

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

$$\mathbb{F}^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \qquad (9.58)$$

ja toisaalta

$$\mathbb{F}_{-1} = \begin{pmatrix} f_0 & f_{-1} \\ f_{-1} & f_{-2} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}. \qquad (9.59)$$

Laskareissa loput.

Edelleen Lauseet 9.5 ja 9.6 laaajenevat negatiivisiin indekseihin.

Lause 9.12. *Olkoot $n, m \in \mathbb{Z}$, tällöin*

$$f_{n+m+1} = f_{n+1}f_{m+1} + f_n f_m, \qquad (9.60)$$

$$f_{2m+1} = f_{m+1}^2 + f_m^2, \qquad (9.61)$$

$$f_{2m} = f_m(f_{m+1} + f_{m-1}). \qquad (9.62)$$

Huomaa, että (9.60) on yhtäpitävä kaavan

$$f_{n+m} = f_{n+1}f_m + f_n f_{m-1} \qquad (9.63)$$

kanssa.

Lause 9.13. *Olkoon $n \in \mathbb{Z}$, tällöin*

$$f_{n+1}f_{n-1} - f_n^2 = (-1)^n. \qquad (9.64)$$

Lause 9.14. *Olkoot $n, r, N, M \in \mathbb{Z}$, tällöin*

$$f_n | f_{rn}, \qquad (9.65)$$

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

$$(f_M, f_N) = f_d \qquad (9.66)$$

ja jos $M \perp N$, niin

$$f_M f_N | f_{MN}. \qquad (9.67)$$

Todistus. Kohta (9.65). Relaatiosta (9.62) saadaan

$$f_{2n} = f_n(f_{n+1} + f_{n-1}), \qquad (9.68)$$

joten saadaan induktion alkuaskel

$$f_n | f_{2n}. \qquad (9.69)$$

Sijoitetaan $m = rn$ yhtälöön (9.63), jolloin

$$f_{(r+1)n} = f_{n+1} f_{rn} + f_n f_{rn-1}, \qquad (9.70)$$

jonka avulla saadaan induktioaskel ja siten (9.65) 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 (9.66). Nyt $M = dm$ ja $N = dk$, joillakin $m, k \in \mathbb{Z}$. siten kohdan (9.65) nojalla

$$f_d | f_M, \quad f_d | f_N. \qquad (9.71)$$

Lauseen 3.4 nojalla on olemassa sellaiset $r, s \in \mathbb{Z}$, että

$$d = rN + sM,$$

joten jälleen kaavan (9.63) nojalla

$$f_d = f_{rN+sM} = f_{rN+1} f_{sM} + f_{rN} f_{sM-1}. \qquad (9.72)$$

Jos, nyt

$$c | f_M, \quad c | f_N, \qquad (9.73)$$

niin kohdan (9.65) nojalla

$$c | f_{sM}, \quad c | f_{rN}. \qquad (9.74)$$

Täten kohdan (9.72) nojalla saadaan

$$c|f_d. \qquad (9.75)$$

Kohdan (9.71) nojalla f_d on yhteinen tekijä ja kohdan (9.75) nojalla suurin tekijä.

□

Kohta (9.67) laskarit.

9.5 f_n (mod k)

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

ESIM:

$$(f_n) \equiv (0,1,1,0,1,1,0,1,1,...) \pmod 2. \qquad (9.76)$$

$$(f_n) \equiv (0,1,1,2,0,2,2,1,0,1,1,...) \pmod 3. \qquad (9.77)$$

$$(f_n) \equiv (0,1,1,2,3,0,3,3,1,4,0,4,4,3,2,0,2,2,4,1,0,1,1,...) \pmod 5. \qquad (9.78)$$

$$(f_n) \equiv (0,1,1,2,3,5,8,3,1,4,5,9,4,3,7,0,3,3...) \pmod{10}, \qquad (9.79)$$

$$f_{15} = f_{30} = f_{45} = f_{60} \equiv 0,\ f_{61} = f_{62} \equiv 1 \pmod{10}. \qquad (9.80)$$

Siten

$$f_{3+l} \equiv f_l \pmod 2, \quad \forall\ l \in \mathbb{N}. \qquad (9.81)$$

$$f_{8+l} \equiv f_l \pmod 3, \quad \forall\ l \in \mathbb{N}. \qquad (9.82)$$

$$f_{20+l} \equiv f_l \pmod 5, \quad \forall\ l \in \mathbb{N}. \qquad (9.83)$$

$$f_{60+l} \equiv f_l \pmod{10}, \quad \forall\ l \in \mathbb{N}. \qquad (9.84)$$

Määritelmä 9.4. Jonon (a_l) jakso on luku $J = J_a \in \mathbb{Z}^+$, jolle pätee

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

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

Tarkastellaan jonoa $(\overline{f}_n) \subseteq \mathbb{Z}_k = \{\overline{0}, ..., \overline{k-1}\}$ ja olkoon $J_f = J_f(k)$.
ESIM:

$$MJ_f(2) = 3,\ MJ_f(3) = 8,\ MJ_f(5) = 20,\ MJ_f(10) = 60. \qquad (9.85)$$

Koska

$$\#\mathbb{Z}_k^2 = \#\{(\overline{a}, \overline{b}) |\ \overline{a}, \overline{b} \in \mathbb{Z}_k\} = k^2, \qquad (9.86)$$

niin joukossa

$$\{(\overline{f}_l, \overline{f}_{l+1}) |\ l = 0, 1, ..., k^2\} \qquad (9.87)$$

on sellaiset alkiot, että

$$(\overline{f}_l, \overline{f}_{l+1}) = (\overline{f}_h, \overline{f}_{h+1}) \qquad (9.88)$$

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

$$\overline{f}_{l+J} = \overline{f}_l, \quad \overline{f}_{l+J+1} = \overline{f}_{l+1} \qquad (9.89)$$

ja siten rekursion nojalla

$$\overline{f}_{n+J} = \overline{f}_n \quad \forall\ n \in \mathbb{N}, \qquad (9.90)$$

missä $1 \leq J \leq k^2$.
Esim: $J_f(10) = 60 < 10^2$.

9.6 f_n (mod p)

Binet'n kaavan (9.14) avulla

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

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

$$\frac{1}{2^n\sqrt{5}}\left(\binom{n}{0}\cdot 0+\binom{n}{1}\cdot 2\sqrt{5}+\binom{n}{2}\cdot 0+\binom{n}{3}\cdot 2\sqrt{5}^3+...\right), \qquad (9.91)$$

josta

$$2^{n-1}f_n=\sum_{j=0}^{\lfloor\frac{n-1}{2}\rfloor}\binom{n}{2j+1}5^j. \qquad (9.92)$$

Lause 9.15. *Olkoon* $p\in\mathbb{P}_{\geq 7}$.

1.) Jos,

$$5^{\frac{p-1}{2}}\equiv 1 \pmod{p}, \qquad (9.93)$$

niin

$$f_{p-1}\equiv 0 \pmod{p} \quad ja \quad MJ_f(p)\leq p-1. \qquad (9.94)$$

2.) Jos,

$$5^{\frac{p-1}{2}}\equiv -1 \pmod{p}, \qquad (9.95)$$

niin

$$f_{p+1}\equiv 0 \pmod{p} \quad ja \quad MJ_f(p)\leq 2p+2. \qquad (9.96)$$

Myöhemmin neliöjäännösteorian avulla osoitetaan, että

1.) (9.93) $\Leftrightarrow p=5m\pm 1$.

2.) (9.95) $\Leftrightarrow p=5m\pm 2$.

Todistus. Yhtälöstä (9.92) saadaan

$$2^{p-1}f_p=\sum_{j=0}^{\frac{p-1}{2}}\binom{p}{2j+1}5^j=\binom{p}{1}+\binom{p}{3}5+...+\binom{p}{p}5^{\frac{p-1}{2}}, \qquad (9.97)$$

josta Lauseiden 4.5 ja 6.7 nojalla

$$f_p\equiv 5^{\frac{p-1}{2}} \pmod{p}. \qquad (9.98)$$

Edelleen asettamalla $n=p+1$ yhtälöön (9.92) saadaan

$$2^p f_{p+1}=\sum_{j=0}^{\lfloor\frac{p}{2}\rfloor}\binom{p+1}{2j+1}5^j=\binom{p+1}{1}+\binom{p+1}{3}5+...+\binom{p+1}{p}5^{\frac{p-1}{2}}. \qquad (9.99)$$

Tässä

$$\binom{p+1}{3} = \frac{(p+1)p(p-1)}{3 \cdot 2} \equiv 0 \pmod{p} \qquad (9.100)$$

ja yleisemminkin pätee

$$\binom{p+1}{k} \equiv 0 \pmod{p} \quad \forall\ 2 \leq k \leq p-1. \qquad (9.101)$$

Siten yhtälön (9.99) nojalla

$$2f_{p+1} \equiv 1 + 5^{\frac{p-1}{2}} \pmod{p}. \qquad (9.102)$$

Merkitään $a = 5^{\frac{p-1}{2}}$, jolloin $a^2 \equiv 1 \pmod{p}$. Nyt Lauseen 6.8 todistuksen nojalla $a \equiv \pm 1 \pmod{p}$.

1.) Olkoon $a \equiv 1 \pmod{p}$. Tällöin yhtälöiden (9.98) ja (9.102) nojalla

$$f_p \equiv 1, \quad f_{p+1} \equiv 1 \pmod{p}. \qquad (9.103)$$

Täten, ensin rekursion avulla

$$f_{p-1} \equiv 0 \pmod{p} \qquad (9.104)$$

ja edelleen rekursion nojalla

$$f_{p-1+l} \equiv f_l \pmod{p} \quad \forall l \in \mathbb{N}, \qquad (9.105)$$

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

2.) Olkoon $a \equiv -1 \pmod{p}$. Tällöin yhtälöiden (9.98) ja (9.102) nojalla

$$f_p \equiv -1, \quad f_{p+1} \equiv 0 = f_0 \pmod{p}. \qquad (9.106)$$

Täten

$$f_{p+2} \equiv -1 = -f_1 \pmod{p}, \qquad (9.107)$$

$$f_{p+3} \equiv -1 = -f_2 \pmod{p} \qquad (9.108)$$

ja edelleen

$$f_{2p+1} \equiv -f_p \equiv 1 \pmod{p} \qquad (9.109)$$

sekä

$$f_{2p+2} \equiv -f_{p+1} \equiv 0, \pmod{p} \qquad (9.110)$$

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

ESIM: 1.) $p = 11$ ja

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

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

$p = 29$ ja

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

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

2.) $p = 7$ ja

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

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

10 Lucasin jonot

10.1 Rekursio ja ratkaisu yritteellä

Jono (w_n) on ei-triviaali, jos ainakin yksi alkio $w_n \neq 0$.

Määritelmä 10.1. Olkoot $r, s \in \mathbb{C}, s \neq 0$. Ei-triviaalia jonoa (w_n), joka toteuttaa palautuskaavan

$$w_{n+2} = rw_{n+1} + sw_n, \quad n \in \mathbb{N} \qquad (10.1)$$

sanotaan Lucasin jonoksi.

Ratkaistaan rekursio (10.1) yritteellä

$$w_n = x^n, \quad x \in \mathbb{C}^*. \qquad (10.2)$$

Kuten pykälässä 9. rekursiosta (10.1) saadaan

$$x^2 - rx - s = 0, \qquad (10.3)$$

jonka ratkaisut ovat

$$\alpha = \frac{r + \sqrt{r^2 + 4s}}{2}, \quad \beta = \frac{r - \sqrt{r^2 + 4s}}{2}. \qquad (10.4)$$

Määritelmä 10.2. Polynomi

$$K(x) = K_w(x) = x^2 - rx - s = (x - \alpha)(x - \beta) \qquad (10.5)$$

on rekursion (10.1) karakteristinen polynomi.

Lause 10.1. *Olkoot $a, b \in \mathbb{C}$. Tällöin*

$$w_n = a\alpha^n + b\beta^n \qquad (10.6)$$

on rekursion (10.1) ratkaisu.

1.) Olkoon $r^2+4s \neq 0$, tällöin $\alpha \neq \beta$. Siten rekursion (10.1) kaikki ratkaisut ovat muotoa (10.4), joillakin $a, b \in \mathbb{C}$, jotka riippuvat jonon (w_n) alkuarvoista w_0, w_1. Olkoot erityisesti

$$F_n = \frac{1}{\alpha - \beta}\left(\alpha^n - \beta^n\right), \qquad (10.7)$$

jota sanotaan Fibonaccin muodoksi ja

$$L_n = \alpha^n + \beta^n, \qquad (10.8)$$

jota sanotaan Lucasin muodoksi. Huomaa, että $\alpha\beta = -s$, $\alpha + \beta = r$, $\alpha - \beta = \sqrt{r^2+4s}$ ja $F_0 = 0$, $F_1 = 1$, $F_2 = r$, $L_0 = 2$, $L_1 = r$, $L_2 = r^2 + 2s$.

Lause 10.2.

$$L_n = \frac{F_{2n}}{F_n}. \qquad (10.9)$$

Todistus. Suoraan laskemalla

$$\frac{F_{2n}}{F_n} = \frac{\alpha^{2n} - \beta^{2n}}{\alpha^n - \beta^n} = \alpha^n + \beta^n = L_n. \qquad (10.10) \quad \square$$

ESIM:Rekursion

$$w_{n+2} = w_{n+1} - w_n \qquad (10.11)$$

karakteristinen polynomi on

$$K_w(x) = x^2 - x + 1 = (x - \alpha)(x - \beta), \qquad (10.12)$$

missä

$$\alpha = \frac{1 + i\sqrt{3}}{2}, \quad \beta = \frac{1 - i\sqrt{3}}{2}. \qquad (10.13)$$

Siten rekursion (10.11) yleinen ratkaisu on muotoa (10.6).

a). Olkoot alkuarvot $w_0 = 2$ ja $w_1 = 2$, tällöin

$$w_n = \frac{3 - i\sqrt{3}}{3}\left(\frac{1 + i\sqrt{3}}{2}\right)^n + \frac{3 + i\sqrt{3}}{3}\left(\frac{1 - i\sqrt{3}}{2}\right)^n. \qquad (10.14)$$

Toisaalta rekursiota (10.11) käyttäen saadaan

$$w_2 = 0,\ w_3 = -2,\ w_4 = -2,\ w_5 = 0,\ w_6 = 2,\ w_7 = 2, ...$$

ja siten jono (w_n) on jaksollinen!

2.) Tapaus $r^2 + 4s = 0$ eli $\alpha = \beta$. Tällöin lineaariyhdisteellä (10.6) ei saada kaikkia ratkaisuja. Siis tarvitaan toisenlainen ratkaisuyrite, joka löytyy luonnollisella tavalla generoivan sarjan avulla. Olkoon

$$W(z) = \sum_{k=0}^{\infty} w_k z^k$$

ja menetellään kuten kohdassa (9.42) eli saadaan

$$W(z) = \sum_{n=0}^{\infty} w_{n+2} z^{n+2} + w_1 z + w_0 =$$

$$z \sum_{n=0}^{\infty} r w_{n+1} z^{n+1} + z^2 \sum_{n=0}^{\infty} s w_n z^n + w_1 z + w_0 =$$

$$z \sum_{k=1}^{\infty} r w_k z^k + z^2 \sum_{k=0}^{\infty} s w_k z^k + w_1 z + w_0 =$$

$$rz(W(z) - w_0) + sz^2 W(z) + w_1 z + w_0. \qquad (10.15)$$

Yhtälöstä (10.15) saadaan ratkaisu

$$W(z) = \frac{(w_1 - r w_0)z + w_0}{1 - rz - sz^2}.$$

Määritelmä 10.3. Sarja

$$W(z) = \sum_{k=0}^{\infty} w_k z^k \qquad (10.16)$$

on lukujonon (w_k) generoiva sarja ja funktio

$$W(z) = \frac{(w_1 - r w_0)z + w_0}{1 - rz - sz^2}. \qquad (10.17)$$

on lukujonon (w_k) generoiva funktio.

Muokataan nimittäjää karakteristisen polynomin avulla seuraavasti

$$1 - rz - sz^2 = z^2((1/z)^2 - r/z - s) = z^2K(1/z) =$$

$$z^2(1/z - \alpha)(1/z - \beta) = (1 - \alpha z)(1 - \beta z) \qquad (10.18)$$

ja jaetaan (10.18) osamurtoihin.

II.) Tapaus $\alpha = \beta$. Nyt

$$W(z) = \frac{(w_1 - rw_0)z + w_0}{(1 - \alpha z)^2} = \frac{E}{1 - \alpha z} + \frac{F}{(1 - \alpha z)^2}, \qquad (10.19)$$

missä

$$E + F = w_0, \quad E\alpha = rw_0 - w_1. \qquad (10.20)$$

Siten

$$W(z) = E\sum_{k=0}^{\infty} \alpha^k z^k + F\sum_{k=0}^{\infty}(k+1)\alpha^k z^k = \sum_{k=0}^{\infty} w_k z^k, \qquad (10.21)$$

joten

$$w_k = (E + F)\alpha^k + Fk\alpha^k. \qquad (10.22)$$

Tulos (10.22) antaa perustelun toiselle ratkaisuyritteelle

$$w_k = kx^k. \qquad (10.23)$$

ESIM:Rekursion

$$w_{n+2} = 4w_{n+1} - 4w_n \qquad (10.24)$$

tapauksessa $r^2 + 4s = 0$ eli $\alpha = \beta$. Nyt $\alpha = -2$, joten

$$w_k = a\alpha^k + bk\alpha^k. \qquad (10.25)$$

Olkoot nyt $w_0 = 1$ ja $w_1 = -1$, jolloin saadaan $a = 1$ ja $b = -1/2$ ja siten

$$w_k = (-2)^k - k\frac{1}{2}(-2)^k. \qquad (10.26)$$

HUOM: 1. VÄLIKOE TÄHÄN ASTI!!

10.2 Matriisiesitys

Työn alla...

11 Formaaleista potenssisarjoista

Olkoon R ykkösellinen rengas. Muodollista summaa

$$A(T) = \sum_{k=0}^{\infty} a_k T^k, \qquad a_k \in R \quad \forall\ k \in \mathbb{N},$$

sanotaan formaaliksi potenssisarjaksi. Olkoon

$$R[[T]] = \{A(T) = \sum_{k=0}^{\infty} a_k T^k |\ a_k \in R \quad \forall\ k \in \mathbb{N}\}$$

R-kertoimisten formaalien potenssisarjojen (formal power series) joukko, missä asetetaan yhtäsuuruus, summa ja tulo seuraavasti.

Määritelmä 11.1. Olkoot

$$A(T) = \sum_{k=0}^{\infty} a_k T^k, \quad B(T) = \sum_{k=0}^{\infty} b_k T^k \in R[[T]].$$

Tällöin

$$A(T) = B(T) \Leftrightarrow \forall k(a_k = b_k); \qquad (11.1)$$

$$A(T) + B(T) = \sum_{k \geqslant 0} (a_k + b_k) T^k; \qquad (11.2)$$

$$A(T)B(T) = \sum_{k \geqslant 0} c_k T^k, \qquad (11.3)$$

missä

$$c_k = \sum_{i=0}^{k} a_i b_{k-i} = \sum_{i+j=k} a_i b_j, \qquad (11.4)$$

joka on Cauchyn kertosääntö.

Merkitään vielä

$$a_k T^k = 0 \cdot T^0 + 0 \cdot T + 0 \cdot T^2 + \ldots + a_k T^k + 0 \cdot T^{k+1} + \ldots.$$

Voidaan osoittaa, että $R[[T]]$ on ykkösellinen rengas, missä
$0(T) = 0 + 0 \cdot T + 0 \cdot T^2 + \ldots$ on nolla-alkio ja

$1(T) = 1 + 0 \cdot T + 0 \cdot T^2 + \ldots$ on ykkösalkio.

HUOM: a). Formaaleilla sarjoilla tutkitaan esimerkiksi rekursiojonojen algebrallisia ominaisuuksia. Formaali sarja EI ole funktio ja siksi symbolisen muuttujan paikalle ei saa asettaa renkaan alkiota. Toisaalta, jos ensin tutkitaan sarjan suppeneminen pisteessä $r \in R$, niin tällöin saadaan funktio, joka kuvaa alkion r alkioksi $A(r) \in R$.

b) Polynomit ovat formaalien sarjojen osajoukko eli $R[T] \subseteq R[[T]]$. Koska polynomi on äärellinen summa, niin muuttujan paikalle voi sijoittaa renkaan alkion.

Olkoon seuraavassa $R = K$ kunta.

Määritelmä 11.2. Olkoon

$$A(T) = a_h T^h + a_{h+1} T^{h+1} + \ldots, \quad a_h \neq 0, \qquad (11.5)$$

tällöin sarjan $A(T)$ kertaluku (order) $\mathrm{ord}A(T) = h$.

Välittömästi saadaan, että

$$\mathrm{ord}(AB) = \mathrm{ord}(A) + \mathrm{ord}(B), \qquad (11.6)$$

$$\mathrm{ord}(A) = 0 \quad \Leftrightarrow \quad a_0 \neq 0. \qquad (11.7)$$

Lause 11.1. *Olkoon $A(T) \in K[[T]]$ ja ord$(A) = 0$. Tällöin on olemassa sellainen $B(T) \in K[[T]]$, että*

$$A(T)B(T) = 1. \qquad (11.8)$$

Toisaalta, jos (11.8) pätee joillekin $A(T), B(T) \in K[[T]]$, niin

$$ord(A) = ord(B) = 0. \qquad (11.9)$$

Merkitään

$$B(T) = \frac{1}{A(T)},$$

mikäli (11.8) toteutuu ja sanotaan, että $1/A(T)$ on sarjan $A(T)$ käänteissarja (inverse series).

Lauseen 3.1 todistus. Olkoon $\mathrm{ord}(A) = 0$ ja

$$A(T) = a_0 + a_1T + a_2T^2 + ... \in K[[T]], \quad a_0 \neq 0. \qquad (11.10)$$

Merkitään

$$B(T) = b_0 + b_1T + b_2T^2 + ..., \qquad (11.11)$$

jolloin yhtälöstä (11.8) saadaan

$$a_0b_0 = 1 \Rightarrow b_0 = \frac{1}{a_0} \in K \qquad (11.12)$$

$$a_0b_1 + a_1b_0 = 0 \Rightarrow b_1 = -\frac{1}{a_0}a_1b_0 = -\frac{a_1}{a_0^2} \in K, \qquad (11.13)$$

...

$$a_0b_n + a_1b_{n-1} + ... + a_nb_0 = 0 \Rightarrow$$

$$b_n = -\frac{1}{a_0}(a_1b_{n-1} + ... + a_nb_0), \qquad (11.14)$$

josta saadaan $b_n \in K$ laskettua. Siten $B(T) \in K[[T]]$ ja (11.8) toteutuu. □

ESIM: Olkoot

$$A(T) = \sum_{k=0}^{\infty} T^k, \quad B(T) = 1 - T \in K[[T]].$$

Tällöin

$$A(T)B(T) = (1 - T)(1 + T + T^2 + T^3 + \dots) =$$

$$1 \cdot 1 + (1 \cdot 1 + (-1) \cdot 1)T + (1 \cdot 1 + (-1) \cdot 1)T^2 + \cdots = 1 \qquad (11.15)$$

ja siten

$$\frac{1}{1 - T} = \sum_{k=0}^{\infty} T^k. \qquad (11.16)$$

Määritelmä 11.3. Sarjojen

$$A(T) = \sum_{k=0}^{\infty} a_kT^k, \quad B(T) = \sum_{k=0}^{\infty} b_kT^k \in R[[T]]$$

yhdistetty sarja on

$$(A \circ B)(T) = A(B(T)) = \sum_{k=0}^{\infty} a_k (B(T))^k. \qquad (11.17)$$

ESIM: a) Olkoot

$$A(T) = B(T) = \sum_{k=0}^{\infty} T^k,$$

tällöin

$$(A \circ B)(T) = A(B(T)) = \sum_{k=0}^{\infty} (B(T))^k =$$

$$\sum_{k=0}^{\infty} (1 + T + T^2 + \dots)^k =$$

$$1 + (1 + T + T^2 + \dots) + (1 + T + T^2 + \dots)^2 + \cdots =$$

$$1 + 1 + 1 + \cdots + (1 + 1 + 1 + \dots)T + (1 + 1 + 1 + \dots)T^2 + \dots, \qquad (11.18)$$

jonka kertoimet eivät suppene. Toisaalta tässä $A(T) = B(T) = 1/(1-T)$, jolloin

$$(A \circ B)(T) = A(B(T)) = \frac{1-T}{-T} = \frac{-1}{T} + 1. \qquad (11.19)$$

Nyt tuloksena ei ole potenssisarja (vaan Laurentin sarja). Siten yhdistetty sarja ei aina ole olemassa.

Muodollista summaa

$$L(T) = \sum_{k=-\infty}^{\infty} l_k T^k, \quad l_k \in R, \quad \forall\ k \in \mathbb{Z}$$

sanotaan formaaliksi Laurentin sarjaksi. Olkoon

$$R((T)) = \{L(T) = \sum_{k=-\infty}^{\infty} l_k T^k |\ l_k \in R \quad \forall\ k \in \mathbb{Z}\}$$

R-kertoimisten formaalien Laurentin sarjojen joukko, missä asetetaan yhtäsuuruus, summa ja yhdiste kuten formaaleilla potenssisarjoilla. Asetetaan vielä

$$\frac{T^k}{T^l} = T^{k-l} \quad \forall \quad k, l \in \mathbb{Z}, \qquad (11.20)$$

jolloin tulo saadaan seuraavasti

$$L(T)K(T) = \sum_k d_k T^k, \qquad (11.21)$$

missä

$$d_k = \sum_{i+j=k} l_i k_j, \qquad (11.22)$$

joka yleistää Cauchyn kertosäännön (11.4). Tärkeitä formaaleja sarjoja ovat

Geometrinen sarja

$$\sum_{k=0}^{\infty} T^k$$

Binomisarja,

$$BIN_a(T) = \sum_{k=0}^{\infty} \binom{a}{k} T^k$$

Eksponenttisarja

$$EXP(T) = \sum_{k=0}^{\infty} \frac{1}{k!} T^k$$

Sinisarja

$$SIN(T) = \sum_{k=0}^{\infty} \frac{(-1)^k}{(2k+1)!} T^{2k+1}$$

Kosinisarja

$$COS(T) = \sum_{k=0}^{\infty} \frac{(-1)^k}{(2k)!} T^{2k}$$

Logaritmisarja

$$LOG(T) = \sum_{k=1}^{\infty} \frac{(-1)^{k+1}}{k} T^k$$

Tangenttisarja

$$TAN(T) = \frac{SIN(T)}{COS(T)}$$

Toisinaan tarvitaan useammanmuuttujan sarjoja, jolloin esimerkiksi kahdenmuuttujan tapauksessa Caychyn kertosääntö on

$$A(T)B(S) = \sum_{k=0}^{\infty} a_k T^k \sum_{l=0}^{\infty} b_l S^l =$$

$$\sum_{n=0}^{\infty} \sum_{k+l=n} a_k b_l T^k S^l. \qquad (11.23)$$

Lause 11.2.

$$EXP(T+S) = EXP(T)EXP(S), \qquad (11.24)$$

$$EXP(-T) = \frac{1}{EXP(T)}, \qquad (11.25)$$

$$EXP(mT) = EXP(T)^m, \quad m \in \mathbb{Z} \qquad (11.26)$$

Todistus. Lähdetään määritelmästä ja käytetään ensin Binomikaavaa (4.27) ja sitten Caychyn kertosääntöä (11.23), jolloin

$$EXP(T+S) = \sum_{n=0}^{\infty} \frac{(T+S)^n}{n!} = \sum_{n=0}^{\infty} \frac{1}{n!} \sum_{k+l=n} \binom{n}{k} T^k S^l =$$

$$\sum_{n=0}^{\infty} \sum_{k+l=n} \frac{T^k}{k!} \frac{S^l}{l!} = \sum_{k=0}^{\infty} \frac{T^k}{k!} \sum_{l=0}^{\infty} \frac{S^l}{l!} = EXP(T)EXP(S). \qquad (11.27) \quad \square$$

Lause 11.3. *Olkoon $m \in \mathbb{Z} \setminus \{0\}$. Tällöin*

$$(BIN_{1/m}(T))^m = 1 + T. \qquad (11.28)$$

Voidaan siis merkitä

$$(1+T)^{1/m} = BIN_{1/m}(T) = \sum_{k=0}^{\infty} \binom{1/m}{k} T^k.$$

12 Bernoullin luvut

12.1 Generoiva funktio ja sarja

Bernoullin luvut voidaan määritellä generoivan funktion avulla seuraavasti.

Määritelmä 12.1. Asetetaan

$$\frac{T}{EXP(T)-1} = \sum_{n=0}^{\infty} \frac{B_n}{n!} T^n, \qquad (12.1)$$

missä luvut B_n ovat Bernoullin lukuja.

Siten Bernoullin luvut saadaan generoivan funktion

$$\frac{T}{EXP(T)-1}$$

sarjakehitelmän kertoimista. Toisaalta yhtälön (12.1) sarja on Bernoullin lukujen generoiva sarja. Merkitään

$$S = \frac{1}{2!}T + \frac{1}{3!}T^2 + \frac{1}{4!}T^3 + \ldots,$$

jolloin yhtälön (11.1) nojalla

$$\frac{T}{EXP(T)-1} = \frac{T}{1 + \frac{1}{1!}T + \frac{1}{2!}T^2 + \frac{1}{3!}T^3 + \frac{1}{4!}T^4 + \cdots - 1} =$$

$$\frac{1}{1 + \frac{1}{2!}T + \frac{1}{3!}T^2 + \frac{1}{4!}T^3 + \ldots} = \frac{1}{1+S} = 1 - S + S^2 - S^3 + S^4 + \ldots. \qquad (12.2)$$

Nyt esimerkiksi

$$S^2 = \left(\frac{1}{2!}T + \frac{1}{3!}T^2 + \ldots\right)^2 = T^2\left(\frac{1}{2} + \frac{1}{6}T + \ldots\right)^2 = \frac{1}{4}T^2 + \frac{1}{6}T^3 + \ldots, \qquad (12.3)$$

joten kohdasta (12.2) saadaan

$$\frac{1}{1+S} = 1 - \frac{1}{2}T - \frac{1}{6}T^2 - \frac{1}{24}T^3 - \cdots + \frac{1}{4}T^2 + \frac{1}{6}T^3 + \cdots - \frac{1}{8}T^3 + \cdots =$$

$$1 - \frac{1}{2}T + \frac{1}{12}T^2 + 0 \cdot T^3 - \cdots = \frac{B_0}{0!}T^0 + \frac{B_1}{1!}T^1 + \frac{B_2}{2!}T^2 + \ldots. \qquad (12.4)$$

Täten

$$B_0 = 1, \quad B_1 = -\frac{1}{2}, \quad B_2 = \frac{1}{6}, \quad B_3 = 0, \quad B_4 = -\frac{1}{30}, \quad B_5 = 0, \quad B_6 = \frac{1}{42}, \ldots. \qquad (12.5)$$

(Tämä menetelmä on käytännössä suhteellisen nopea.)

Lause 12.1. *Olkoon $k \in \mathbb{Z}^+$. Tällöin*

$$B_{2k+1} = 0. \qquad (12.6)$$

Todistus. Merkitään

$$G(T) = \frac{T}{EXP(T)-1} + \frac{T}{2} = \frac{T}{2}\frac{EXP(T)+1}{EXP(T)-1} = \sum_{n=0}^{\infty} g_n T^n, \qquad (12.7)$$

jolloin

$$G(-T) = \frac{-T}{2}\frac{EXP(-T)+1}{EXP(-T)-1} = \frac{-T}{2}\frac{1/EXP(T)+1}{1/EXP(T)-1} = \frac{T}{2}\frac{EXP(T)+1}{EXP(T)-1} = G(T). \qquad (12.8)$$

Yhtälön (12.8) nojalla $G(T)$ on parillinen eli

$$g_{2k+1} = 0 \quad \forall \quad k \in \mathbb{N} \qquad (12.9)$$

ja yhtälön (12.7) nojalla

$$G(T) = \sum_{n=0}^{\infty} \frac{B_n}{n!} T^n + \frac{T}{2}, \qquad (12.10)$$

joten saadaan väite. □

12.2 Palautuskaava

Johdetaan seuraavaksi tärkeä Bernoullin lukujen palautuskaava. Merkitään ensin

$$e^T = \sum_{n=0}^{\infty} \frac{1}{n!} T^n$$

ja

$$B(T) = \sum_{n=0}^{\infty} \frac{B_n}{n!} T^n.$$

Nyt määrittely-yhtälön (12.1) nojalla

$$T = (e^T - 1)B(T), \qquad (12.11)$$

eli

$$T = \sum_{l=1}^{\infty} \frac{1}{l!} T^l \sum_{k=0}^{\infty} \frac{B_k}{k!} T^k. \qquad (12.12)$$

Verrataan vastinpotenssien kertoimia, jolloin saadaan aluksi

$$T^1 : \qquad 1 = \frac{1}{1!}\frac{B_0}{0!} \quad \Rightarrow \quad B_0 = 1. \qquad (12.13)$$

Yleisemmin Caychyn kertosäännöllä saadaan

$$0 = \sum_{l+k=n, l\geq 1} \frac{1}{l!}\frac{B_k}{k!}, \qquad (12.14)$$

missä $0 \leq k \leq n-1$. Lavennetaan vielä $n!$:lla, jolloin palautuskaava saa seuraavan implisiittisen muodon.

Lause 12.2. *Olkoon $n \in \mathbb{Z}_{\geq 2}$. Tällöin*

$$\sum_{k=0}^{n-1} \binom{n}{k} B_k = 0. \qquad (12.15)$$

Edelleen (12.15) voidaan esittää yhtäpitävästi eksplisiittisessä muodossa

$$B_m = \frac{-1}{m+1}\left(\binom{m+1}{0}B_0 + \binom{m+1}{1}B_1 + ... + \binom{m+1}{m-1}B_{m-1}\right)$$
$$\forall\ m \in \mathbb{Z}^+, \quad B_0 = 1. \qquad (12.16)$$

Välittömästi nähdään, että

$$B_m \in \mathbb{Q} \quad \forall\ m \in \mathbb{N}. \qquad (12.17)$$

12.3 Potenssisummia

Johdetaan seuraavassa potenssisummalle

$$S_m(n) = 1^m + 2^m + ... + n^m, \quad m \in \mathbb{N}, \quad n \in \mathbb{Z}^+, \qquad (12.18)$$

lauseke Bernoullin lukujen avulla. Nyt

$$e^{0\cdot T} + e^{1\cdot T} + ... + e^{n\cdot T} =$$

$$1 + \sum_{m=1}^{\infty} 0^m \frac{T^m}{m!} + 1 + \sum_{m=1}^{\infty} 1^m \frac{T^m}{m!} + ... + 1 + \sum_{m=1}^{\infty} n^m \frac{T^m}{m!} =$$

$$n + 1 + \sum_{m=1}^{\infty} S_m(n) \frac{T^m}{m!} \qquad (12.19)$$

ja toisaalta

$$e^{0\cdot T} + e^{1\cdot T} + ... + e^{n\cdot T} = \sum_{l=0}^{n} e^{lT} = \sum_{l=0}^{n} \left(e^T\right)^l = \frac{e^{(n+1)T} - 1}{e^T - 1}. \qquad (12.20)$$

Yhdistetään tulokset (12.19) ja (12.20), jolloin

$$n + 1 + \sum_{m=1}^{\infty} S_m(n) \frac{T^m}{m!} = \frac{e^{(n+1)T} - 1}{e^T - 1} =$$

$$\frac{T}{e^T - 1} \frac{e^{(n+1)T} - 1}{T} = B(T) \sum_{l=1}^{\infty} \frac{(n+1)^l}{l!} T^{l-1} =$$

$$\sum_{k=0}^{\infty} \frac{B_k}{k!} T^k \sum_{h=0}^{\infty} \frac{(n+1)^{h+1}}{(h+1)!} T^h. \qquad (12.21)$$

Vertaamalla identiteetin (12.21) kertoimia, saadaan

$$S_m(n) = m! \sum_{k+h=m} \frac{B_k}{k!} \frac{(n+1)^{h+1}}{(h+1)!},$$

jonka nojalla pätee

Lause 12.3.

$$S_m(n) = \frac{1}{m+1} \sum_{k=0}^{m} \binom{m+1}{k} B_k \ (n+1)^{m+1-k}. \qquad (12.22)$$

Tulkitaan lausekkeet $S_m(n)$ polynomeiksi muuttujan n suhteen. Yhtälön (12.22) nojalla $S_m(n) \in \mathbb{Q}[n]$.

ESIM:

$$S_1(n) = 1 + 2 + ... + n = \frac{n(n+1)}{2} \qquad (12.23)$$

$$S_2(n) = 1^2 + 2^2 + ... + n^2 = \frac{n(n+1)(2n+1)}{6} \qquad (12.24)$$

$$S_3(n) = 1^3 + 2^3 + ... + n^3 = \frac{n^2(n+1)^2}{4} \qquad (12.25)$$

$$S_4(n) = 1^4 + 2^4 + ... + n^4 = \frac{n(n+1)(2n+1)(3n^2+3n-1)}{30} \qquad (12.26)$$

Esimerkin nojalla pätee mm. seuraavat jaollisuusrelaatiot

$$n(n+1) \underset{\mathbb{Q}[n]}{|} S_m(n) \quad m = 1, ..., 4 \qquad (12.27)$$

ja

$$2n+1 \underset{\mathbb{Q}[n]}{|} S_m(n) \quad m = 2, 4. \qquad (12.28)$$

Todistetaan seuraavat pari relaatiota yleiselle indeksille.

Lause 12.4.

$$n+1 \underset{\mathbb{Q}[n]}{|} S_m(n) \quad \forall\ m \in \mathbb{Z}^+, \qquad (12.29)$$

$$(n+1)^2 \underset{\mathbb{Q}[n]}{|} S_m(n) \quad \forall\ m \in 2\mathbb{Z}^+ + 1. \qquad (12.30)$$

Todistus. Suoraan tuloksesta (12.22) seuraa $S_m(n) = R_m(n+1)$, missä

$$R_m(x) = r_{m+1}x^{m+1} + ... + r_1 x, \quad r_1 = \frac{1}{m+1}\binom{m+1}{m}B_m = B_m. \qquad (12.31)$$

Siten

$$x | R_m(x) \quad \forall\ m \in \mathbb{Z}^+ \qquad (12.32)$$

ja lisäksi

$$x^2 | R_{2j+1}(x) \quad \forall\ j \in \mathbb{Z}^+, \qquad (12.33)$$

sillä tässä $r_1 = B_{2j+1} = 0$. □

12.4 Bernoullin polynomit

Lause 12.5. *Olkoon*

$$\frac{Te^{xT}}{EXP(T)-1} = \sum_{n=0}^{\infty} \frac{B_n(x)}{n!} T^n, \qquad (12.34)$$

tällöin

$$B_n(x) = \sum_{k=0}^{n} \binom{n}{k} B_k x^{n-k}. \qquad (12.35)$$

Todistus. Kehitetään sarjaksi yhtälön (12.34) V.P.=

$$B(T)e^{xT} = \sum_{k=0}^{\infty} \frac{B_k}{k!} T^k \sum_{l=0}^{\infty} \frac{x^l}{l!} T^l =$$

$$\sum_{n=0}^{\infty} \left(\sum_{k+l=n} \frac{B_k}{k!} \frac{x^l}{l!} \right) T^n. \qquad (12.36)$$

Verrataan sarjan (12.36) ja yhtälön (12.34) O.P. sarjan vastinkertoimia, jolloin

$$\frac{B_n(x)}{n!} = \sum_{k=0}^{n} \frac{B_k}{k!} \frac{x^{n-k}}{(n-k)!},$$

joka kerrotaan puolittain $n!$:lla. □

Määritelmä 12.2. Polynomit

$$B_n(x) = \sum_{k=0}^{n} \binom{n}{k} B_k x^{n-k}$$

ovat Bernoullin polynomeja.

ESIM:

$$B_0(x) = B_0 = 1, \quad B_1(x) = B_0 x + B_1 = x - 1/2, ...$$

13 p-valuaatio

Tarkastellaan alkuluvun p esiintymistä rationaaliluvussa $A = a/b$.

Määritelmä 13.1. Olkoon $p \in \mathbb{P}$ ja

$$A = \frac{a}{b} = p^r \frac{c}{d} \neq 0, \quad p \nmid cd. \qquad (13.1)$$

Tällöin asetetaan

$$v_p(A) = r, \quad A \neq 0.$$

Asetetaan lisäksi

$$v_p(0) = \infty,$$

missä symboli ∞ toteuttaa laskusäännöt

$$\infty + \infty = \infty, \quad \infty + c = \infty \quad \forall c \in \mathbb{C}, \quad k < \infty \quad \forall k \in \mathbb{R}. \qquad (13.2)$$

Usein lukua $v_P(A)$ kutsutaan eksponentiaaliseksi valuaatioksi tai p-adiseksi valuaatioksi (jonka avulla voidaan määritellä p-adinen itseisarvo).

Lause 13.1. *Laskusääntöjä. Olkoon $k \in \mathbb{Z}$, tällöin*

$$v_p(k) \geq 0. \qquad (13.3)$$

Olkoot $A, B \in \mathbb{Q}$, tällöin

$$v_p(AB) = v_p(A) + v_p(B), \qquad (13.4)$$

$$v_p(1/B) = -v_p(B), \qquad (13.5)$$

$$v_p(A/B) = v_p(A) - v_p(B), \qquad (13.6)$$

$$v_p(A + B) \geq \min\{v_p(A), v_p(B)\}, \qquad (13.7)$$

jos lisäksi $v_p(A) \neq v_p(B)$, niin

$$v_p(A + B) = \min\{v_p(A), v_p(B)\}. \qquad (13.8)$$

Todistetaan kohdat (13.7) ja 13.8).

Tapaus $AB \neq 0$. Olkoot

$$A = p^r \frac{\alpha}{\beta}, \quad B = p^s \frac{\gamma}{\delta},$$

missä

$$\alpha, \beta, \gamma, \delta \in \mathbb{Z} \setminus \{0\}, \quad \alpha \perp \beta, \gamma \perp \delta, \quad p \not| \alpha\beta\gamma\delta. \qquad (13.9)$$

Oletetaan vaikka, että $r \geq s$. Tällöin

$$A + B = p^s \left(p^{r-s} \frac{\alpha}{\beta} + \frac{\gamma}{\delta} \right) = p^s \frac{\alpha\delta p^{r-s} + \beta\gamma}{\beta\delta}, \qquad (13.10)$$

missä kohdan (13.3) nojalla

$$v_p(\alpha\delta p^{r-s} + \beta\gamma) = t \geq 0 \qquad (13.11)$$

sekä oletuksien (13.9) nojalla

$$v_p(\beta\delta) = 0. \qquad (13.12)$$

Käytetään vielä tulon ja osamäärän tuloksia (13.4) ja (13.6), jolloin

$$v_p(A + B) = v_p(p^s) + v_p(\alpha\delta p^{r-s} + \beta\gamma) - v_p(\beta\delta) = s + t - 0 \geq$$

$$s = \min\{r, s\} = \min\{v_p(A), v_p(B)\}. \qquad (13.13)$$

Täten saatiin kohta (13.7). Kohdassa (13.8) oletetaan lisäksi $r > s$. Tällöin

$$p \not| \alpha\delta p^{r-s} + \beta\gamma \quad \Rightarrow \quad v_p(\alpha\delta p^{r-s} + \beta\gamma) = t = 0. \qquad (13.14)$$

Siten kohdassa (13.13) saadaan yhtäsuuruus

$$v_p(A + B) = s + t - 0 = s = \min\{r, s\} = \min\{v_p(A), v_p(B)\}. \qquad (13.15)$$

Kohdassa (13.7) tarvitaan vielä tapaus $AB = 0$.

a) $A = B = 0$, tällöin

$$v_p(A + B) = v_p(0) = \infty = \min\{v_p(A), v_p(B)\}. \qquad (13.16)$$

a) $A \neq 0, B = 0$, tällöin

$$v_p(A+B) = v_p(A) = \min\{v_p(A), v_p(B)\}. \qquad (13.17) \quad \square$$

Annetaan vielä kohdan (13.8) yleistys

$$v_p(A_1 + ... + A_k) \geq \min_{1 \leq j \leq k} \{v_p(A_i)\}. \qquad (13.18)$$

Määritelmä 13.2. Olkoon $p \in \mathbb{P}$ annettu, tällöin

$$\mathbb{Z}_{(p)} = \{A \in \mathbb{Q} |\ v_p(A) \geq 0\}$$

on p-kokonaislukujen (p-integers) joukko.

Lause 13.2. *Olkoon $p \in \mathbb{P}$, tällöin $\mathbb{Z}_{(p)}$ on kommutatiivinen ykkösellinen rengas, jonka yksikköryhmä on*

$$\mathbb{Z}^*_{(p)} = \{A \in \mathbb{Q} |\ v_p(A) = 0\}.$$

Lause 13.3. *Olkoot $p \in \mathbb{P}$, $k \in \mathbb{Z}^+$ ja $A = p^k/(k+1)$. Tällöin*

$$v_p(A) \geq 0, \qquad (13.19)$$

ja jos $k \geq 2$, niin

$$v_p(A) \geq 1 \qquad (13.20)$$

ja jos $k \geq 3$ ja $p \geq 5$, niin

$$v_p(A/p^2) \geq 0. \qquad (13.21)$$

Todettakoon vielä, että kohdassa (13.19)

$$p^k/(k+1) \in \mathbb{Z}_{(p)}$$

ja kohdassa (13.20)

$$p^k/(k+1) \equiv 0 \pmod{p}.$$

14 Bernoullin lukujen jaollisuudesta

Bernoullin lukuihin liitty useita mielenkiintoisia jaollisuusominaisuuksia. Tutkitaan seuraavassa Bernoullin lukujen nimittäjien jaollisuutta.

Lause 14.1. *Olkoon $p \in \mathbb{P}$, tällöin*

$$pB_m \in \mathbb{Z}_{(p)} \quad \forall m \in \mathbb{N}. \qquad (14.1)$$

Todistus. Induktiolla, jolloin aluksi

$$B_0 = 1 \quad \Rightarrow \quad pB_0 = p \in \mathbb{Z}_{(p)} \quad \forall p \in \mathbb{P}.$$

Relaation

$$\binom{m+1}{k} = \frac{m+1}{m+1-k}\binom{m}{k} \qquad (14.2)$$

ja tuloksen (12.22) nojalla

$$S_m(p-1) = \sum_{k=0}^{m} \binom{m}{k} \frac{B_k p^{m+1-k}}{m+1-k} =$$

$$\binom{m}{0}\frac{B_0 p^{m+1}}{m+1} + ... + \binom{m}{m-2}\frac{B_{m-2}p^3}{3} + \binom{m}{m-1}\frac{B_{m-1}p^2}{2} + B_m p. \qquad (14.3)$$

Yhtälön (14.3) termeille pätee

$$S_m(p-1) \in \mathbb{Z} \quad \Rightarrow \quad v_p(S_m(p-1)) \geq 0,$$

$$\binom{m}{k} \in \mathbb{Z} \quad \Rightarrow \quad v_p\binom{m}{k} \geq 0$$

$$\text{Lause 13.3} \quad \Rightarrow \quad v_p\left(\frac{p^m}{m+1}\right), ..., v_p\left(\frac{p}{2}\right) \geq 0$$

$$\text{Induktio-oletus} \quad \Rightarrow \quad v_p(pB_{m-k}) \geq 0 \quad \forall \quad k = 1, ..., m.$$

Täten

$$v_p(pB_m) = v_p\left(S_m(p-1) - \binom{m}{0}pB_0\frac{p^m}{m+1} - ...\right.$$
$$\left. -\binom{m}{m-2}pB_{m-2}\frac{p^2}{3} - \binom{m}{m-1}pB_{m-1}\frac{p}{2}\right) \geq$$

$$\min_{1\le j\le k}\{v_p(S_m(p-1)), v_p(pB_{m-k})v_p\binom{m}{m-k}v_p\left(\frac{p^k}{k+1}\right)\} \ge 0. \quad \square \qquad (14.4)$$

ESIM.

$$2B_2 = 2\frac{1}{6} = \frac{1}{3} \in \mathbb{Z}_{(2)},$$

$$3B_2 = 3\frac{1}{6} = \frac{1}{2} \in \mathbb{Z}_{(3)},$$

$$pB_2 = p\frac{1}{6} = \frac{p}{6} \in \mathbb{Z}_{(p)} \quad \forall p \in \mathbb{P}_{\ge 5}.$$

Merkitään nyt

$$B_m = \frac{N_m}{D_m}, \quad N_m \in \mathbb{Z}, \quad D_m \in \mathbb{Z}^+, \quad N_m \perp D_m.$$

Siten tulos

$$pB_m \in \mathbb{Z}_{(p)} \quad \forall p \in \mathbb{P}$$

tarkoittaa, että

$$0 \le v_p(D_m) \le 1 \quad \forall \quad p \in \mathbb{P} \qquad (14.5)$$

Joten ei ole sellaista alkulukua p, että

$$p^2 | D_m. \qquad (14.6)$$

Määritelmä 14.1. Luku $k \in \mathbb{Z}$ on neliövapaa (square free), jos ehdosta

$$a^2 | k \quad \text{ja} \quad a \in \mathbb{Z}^+$$

seuraa, että $a = 1$.

Tuloksen (14.6) nojalla saadaan

Lause 14.2. *Bernoullin lukujen nimittäjät D_m ovat neliövapaita.*

Lause 14.3. *Olkoon $m = 2l \in 2\mathbb{Z}^+$ ja $p \in \mathbb{P}$, tällöin*

$$pB_{2l} \equiv S_{2l}(p-1) \pmod{p}. \qquad (14.7)$$

Todistus. Tapaus $m = 2$ laskareissa. Olkoon nyt $m \geq 4$. Tällöin $B_{m-1} = 0$, joten yhtälön (14.3) nojalla

$$S_m(p-1) = \binom{m}{0} pB_0 \frac{p^m}{m+1} + ... + \binom{m}{m-2} pB_{m-2} \frac{p^2}{3} + pB_m. \qquad (14.8)$$

Lauseen 14.1 nojalla

$$pB_{m-k} \in \mathbb{Z}_{(p)} \quad \forall \quad 2 \leq k \leq m$$

ja tuloksen (13.20) nojalla

$$v_p\left(\frac{p^k}{k+1}\right) \geq 1 \quad \forall \quad 2 \leq k \leq m,$$

joten

$$p \left| \binom{m}{m-k} pB_{m-k} \frac{p^k}{k+1} \right. \quad \forall \quad 2 \leq k \leq m. \qquad (14.9)$$

Täten yhtälöstä (14.8) saadaan

$$S_m(p-1) \equiv pB_m \pmod{p}. \qquad (14.10) \quad \square$$

Lause 14.4. *Olkoon $m \in \mathbb{Z}^+$ ja $p \in \mathbb{P}$. Tällöin*

$$p-1|m \quad \Rightarrow \quad S_m(p-1) \equiv -1 \pmod{p}, \qquad (14.11)$$

$$p-1 \not| m \quad \Rightarrow \quad S_m(p-1) \equiv 0 \pmod{p}. \qquad (14.12)$$

Todistetaan kohta (14.11). Olkoon siis $m = a(p-1)$, jollakin $a \in \mathbb{Z}$. Fermat'n pikkulauseella saadaan

$$S_m(p-1) = 1^m + 2^m + ... + (p-1)^m =$$

$$\left(1^{p-1}\right)^a + \left(2^{p-1}\right)^a + ... + \left((p-1)^{p-1}\right)^a \equiv$$

$$1^a + 1^a + ... + 1^a = p - 1 \equiv -1 \pmod{p}. \quad \square$$

Tapaus (14.12) sivuutetaan.

Yhdistämällä Lauseet 14.3 ja 14.4 saadaan

Lause 14.5. *Olkoot $m \in 2\mathbb{Z}^+$ ja $p \in \mathbb{P}$. Tällöin*

$$p-1|m \quad \Rightarrow \quad pB_m \equiv -1 \pmod{p}, \qquad (14.13)$$

$$p-1 \not| m \quad \Rightarrow \quad pB_m \equiv 0 \pmod{p}. \qquad (14.14)$$

Seuraava tulos selvittää Bernoullin lukujen nimittäjien olemuksen.

Lause 14.6. *Olkoon $l \in \mathbb{Z}^+$. Tällöin*

$$B_{2l} = A_{2l} - \sum_{q-1|2l, q\in\mathbb{P}} \frac{1}{q}, \qquad (14.15)$$

jollakin $A_{2l} \in \mathbb{Z}$.

Todistus. Olkoon

$$R_{2l} = \{q \in \mathbb{P} |\ q-1|2l\} = \{q_1, ..., q_r\}$$

ja merkitään

$$A_{2l} = B_{2l} + \sum_{q\in R_{2l}} \frac{1}{q}$$

ja todistetaan, että rationaaliluku A_{2l} on kokonainen.

a) Jos $p \in \mathbb{P} \setminus R_{2l}$, niin tuloksen (14.14) nojalla

$$pB_{2l} \equiv 0 \pmod{p}.$$

Siten

$$v_p(pB_{2l}) \geq 1 \quad \Rightarrow \quad v_p(p) + v_p(B_{2l}) \geq 1,$$

joten

$$v_p(B_{2l}) \geq 0. \qquad (14.16)$$

Edelleen

$$v_p(A_{2l}) \geq \min_{1\leq j\leq r} \{v_p(B_{2l}), v_p\left(\frac{1}{q_j}\right)\} \geq 0. \qquad (14.17)$$

b) Jos $p = q \in R_{2l}$, niin tuloksen (14.15) nojalla

$$qB_{2l} \equiv -1 \pmod{q} \qquad (14.18)$$

eli $qB_{2l} = -1 + hq$, jollakin $h \in \mathbb{Z}$. Siten

$$v_q(q) + v_q(B_{2l}) = v_q(-1 + hq) = 0,$$

joten

$$v_q(B_{2l}) = -1. \qquad (14.19)$$

Tuloksen (14.19) nojalla

$$D_{2l} = qC_{2l}, \quad C_{2l} \in \mathbb{Z}, \quad q \not| C_{2l}$$

Toisaalta tuloksesta (14.18) tulee

$$q\frac{N_{2l}}{D_{2l}} + 1 = \frac{N_{2l}}{C_{2l}} + 1 =$$

$$\frac{N_{2l} + C_{2l}}{C_{2l}} \equiv 0 \pmod{q}, \qquad (14.20)$$

josta saadaan

$$q|N_{2l} + C_{2l} = qL, \quad L \in \mathbb{Z}. \qquad (14.21)$$

Käyttämällä tulosta (14.21) lasketaan

$$B_{2l} + \frac{1}{q} = \frac{N_{2l}}{D_{2l}} + \frac{1}{q} = \frac{1}{q}\frac{N_{2l} + C_{2l}}{C_{2l}} = \frac{L}{C_{2l}}, \qquad (14.22)$$

missä $L \in \mathbb{Z}, \quad q \not| C_{2l}$. Niinpä

$$v_p(B_{2l} + \frac{1}{q}) \geq 0. \qquad (14.23)$$

Valitaan vaikka $p = q_1$, jolloin

$$v_p(A_{2l}) \geq \min_{2 \leq j \leq r} \{v_{q_1}(B_{2l} + \frac{1}{q_1}), v_p\left(\frac{1}{q_j}\right)\} \geq 0. \qquad (14.24)$$

Kohtien a) ja b) nojalla

$$v_p(A_{2l}) \geq 0 \quad \forall \quad p \in \mathbb{P}. \qquad (14.25)$$

Täten vihdoin $A_{2l} \in \mathbb{Z}$. $\square$

Äskeisten tulosten nojalla nimittäjän käyttäytyminen tunnetaan siis hyvin. Valitettavasti osoittajista ei tiedetä läheskään yhtä paljon, mikä seuraavan Kummerin tuloksen valossa olisi ratkaisevaa Fermat'n suuren lauseen tutkimuksessa.

Määritelmä 14.2. Alkuluku $p \in \mathbb{P}_{p\geq 3}$ on säännöllinen (regular), jos

1) $p = 3$ tai

2) $p \geq 5$ ja pätee

$$p \not| N_2 N_4 \cdots N_{p-3}.$$

Muutoin p on epäsäännöllinen (irregular).

Lause 14.7. *Olkoon $p \in \mathbb{P}_{p\geq 3}$ säännöllinen, tällöin*

$$x^p + y^p \neq z^p \quad \forall \quad x, y, z \in \mathbb{Z}^+. \qquad (14.26)$$

Mainittakoon, että Andrew Wiles [Annals of Mathematics 141 (1995)] on todistanut Fermat'n väitteen (14.26) kaikille parittomille alkuluvuille. Wilesin todistus perustuu mm. elliptisten käyrien ominaisuuksiin.

15 Eulerin luvut

Eulerin luvut liittyvät läheisesti Bernoullin lukuihin ja ovat algebrallisen lukuteorian kalustoa sekä esiintyvät myös kombinatoriikan kysymyksissä.

15.1 Generoiva funktio ja sarja

Eulerin luvut voidaan määritellä generoivan funktion avulla vastaavasti kuten Bernoullin luvutkin

Määritelmä 15.1. Asetetaan

$$\frac{2e^T}{e^{2T}+1} = \sum_{n=0}^{\infty} \frac{E_n}{n!} T^n, \qquad (15.1)$$

missä luvut E_n ovat Eulerin lukuja.

Aukaisemalla sarjakehitelmä voidaan Eulerin lukuja määrätä kuten Bernoullin lukujakin, jolloin

$$E_0 = 1, \quad E_1 = 0, \quad E_2 = -1, \quad E_3 = 0, \quad E_4 = 5, \quad E_5 = 0, \quad E_6 = -61, ... \qquad (15.2)$$

Huomaa, että generoiva funktio

$$EU(T) = \frac{2e^T}{e^{2T}+1} = \frac{2}{e^T + e^{-T}} \qquad (15.3)$$

on parillinen, joten välittömästi pätee

Lause 15.1. *Olkoon $k \in \mathbb{N}$. Tällöin*

$$E_{2k+1} = 0. \qquad (15.4)$$

15.2 Palautuskaava

Johdetaan seuraavaksi tärkeä Eulerin lukujen palautuskaava. Lähtemällä määrittelyyhtälöstä (15.1), saadaan

$$2 = (e^T + e^{-T}) EU(T), \qquad (15.5)$$

eli

$$2 = \sum_{l=0}^{\infty} \frac{2}{(2l)!} T^{2l} \sum_{k=0}^{\infty} \frac{E_{2k}}{(2k)!} T^{2k}. \qquad (15.6)$$

Verrataan vastinpotenssien kertoimia, jolloin saadaan aluksi

$$T^0: \qquad 2 = \frac{2}{0!}\frac{E_0}{0!} \quad \Rightarrow \quad E_0 = 1. \qquad (15.7)$$

Yleisemmin Caychyn kertosäännöllä saadaan

$$0 = 2 \sum_{l+k=n} \frac{E_{2k}}{(2l)!(2k)!}. \qquad (15.8)$$

Lavennetaan vielä $(2n)!$:lla, jolloin palautuskaava saa seuraavan implisiittisen muodon.

Lause 15.2. *Olkoon $n \in \mathbb{Z}^+$. Tällöin*

$$\sum_{k=0}^{n} \binom{2n}{2k} E_{2k} = 0. \qquad (15.9)$$

16 Sarjakehitelmiä

(EI tule 2. välikokeeseen.) Työn alla..

17 Riemannin zetafunktio

(EI tule 2. välikokeeseen.) Työn alla..

18 Stirlingin luvut

18.1 Määritelmä ja rekursio

Stirlingin lukuihin törmätään erityisesti kombinatorisissa kysymyksissä ja lukuteoriaan ne liittyvät läheisesti seuraavan polynomin

$$P(x) = x(x-1)\cdots(x-n+1) = (-1)^n(-x)_n = x^n + ... + (-1)^n(n-1)!x \qquad (18.1)$$

kertoimien kautta. Polynomi (18.1) esintyi jo Wolstenholmen lauseen yhteydessä ja silloin havaittiin, että kertoimet voidaan esittää lukujen $1, 2, ..., n-1$ symmetristen peruspolynomien avulla.

Määritelmä 18.1. Olkoon $n \in \mathbb{N}$. Asetetaan

$$x(x-1)\cdots(x-n+1) = \sum_{k=0}^{n} s_1(n,k)x^k, \qquad (18.2)$$

missä luvut $s_1(n,k)$ ovat 1. lajin Stirlingin lukuja, ja

$$x^n = \sum_{k=0}^{n} S_2(n,k)x(x-1)\cdots(x-k+1), \qquad (18.3)$$

missä luvut $S_2(n,k)$ ovat 2. lajin Stirlingin lukuja.

Käytetään merkintöjä

$$\delta_{kl} = \begin{cases} 1, & \text{jos} \quad k = l, \\ 0, & \text{jos} \quad k \neq l \end{cases}$$

ja

$$H_n = 1 + \frac{1}{2} + \frac{1}{3} + ... + \frac{1}{n} \quad n \in \mathbb{Z}^+,$$

jotka ovat harmoonisia lukuja. Sovitaan vielä, että

$$s_1(n,-1) = 0, \quad s_1(n,m) = 0 \quad \forall\, n,m \in \mathbb{N}, \quad n < m,$$

$$S_2(n,-1) = 0, \quad S_2(n,m) = 0 \quad \forall\, n,m \in \mathbb{N} \quad n < m. \qquad (18.4)$$

Lause 18.1. *Ensimmäisen lajin Stirlingin luvuille pätee* $s_1(0,0) = 1$, *sekä palautuskaava*

$$s_1(n,m) = s_1(n-1,m-1) - (n-1)s_1(n-1,m) \quad \forall\, n \in \mathbb{Z}^+, \quad 0 \leq m \leq n. \qquad (18.5)$$

Todistus. Käytetään aluksi määritelmää muodossa

$$(-1)^n(-x)_n = \sum_{k=0}^{n} s_1(n,k)x^k. \qquad (18.6)$$

Tällöin tapauksessa $n = 0$ yhtälö (18.6) antaa

$$s_1(0,0)x^0 = (-1)^0(-x)_0 = 1 \quad \Rightarrow \quad s_1(0,0) = 1.$$

Tapauksessa $n \geq 1$ edetään seuraavasti

$$\sum_{m=0}^{n} s_1(n,m)x^m = x(x-1)\cdots(x-n+2)(x-n+1) =$$

$$x \cdot x(x-1)\cdots(x-n+2) - (n-1)x(x-1)\cdots(x-n+2) =$$

$$x\sum_{l=0}^{n-1} s_1(n-1,l)x^l - (n-1)\sum_{m=0}^{n-1} s_1(n-1,m)x^m =$$

$$\sum_{m=1}^{n} s_1(n-1,m-1)x^m - (n-1)\sum_{m=0}^{n-1} s_1(n-1,m)x^m =$$

$$\sum_{m=1}^{n-1}(s_1(n-1,m-1) - (n-1)s_1(n-1,m))x^m +$$

$$s_1(n-1,n-1)x^n - (n-1)s_1(n-1,m))x^0. \qquad (18.7)$$

Verrataan yhtälön (18.7) vastinpotenssien kertoimia, jolloin tapauksissa $1 \leq m \leq n-1$ saadaan palautuskaava (18.5). Kun $m = 0$, niin käyttämällä sopimusta (18.4) yhtälöstä (18.7) saadaan

$$s_1(n,0) = -(n-1)s_1(n-1,0) = s_1(n-1,-1) - (n-1)s_1(n-1,0)$$

eli palautuskaava (18.5) toteutuu. Vastaavasti, kun $m = n$, niin yhtälöstä (18.7) saadaan

$$s_1(n,n) = s_1(n-1,n-1) = s_1(n-1,n-1) - (n-1)s_1(n-1,n), \qquad (18.8)$$

missä jälleen käytettiin sopimusta ((18.4). Siten palautuskaava (18.5) toteutuu nytkin. □

SEURAUKSIA:

$$s_1(n,0) = \delta_{n,0}, \quad s_1(n,n) = 1,$$

$$s_1(n,1) = (-1)^{n-1}(n-1)!,$$

$$s_1(n,2) = (-1)^n(n-1)!H_{n-1},$$

$$s_1(n,n-1) = -\binom{n}{2}. \qquad (18.9)$$

Lause 18.2. *Toisen lajin Stirlingin luvuille pätee* $S_2(0,0) = 1$, *sekä palautuskaava*

$$S_2(n,m) = S_2(n-1,m-1)+mS_2(n-1,m) \quad \forall\, n \in \mathbb{Z}^+, \quad 0 \leq m \leq n. \tag{18.10}$$

Edelleen

$$S_2(n,m) = \frac{1}{m!}\sum_{i=0}^{m}(-1)^i\binom{m}{i}(m-i)^n =$$

$$\frac{(-1)^m}{m!}\sum_{k=0}^{m}(-1)^k\binom{m}{k}k^n. \tag{18.11}$$

SEURAUKSIA:

$$S_2(n,0) = \delta_{n,0}, \quad S_2(n,n) = 1, \quad S_2(n,1) = 1,$$

$$S_2(n,2) = 2^{n-1} - 1, \quad S_2(n,n-1) = \binom{n}{2}. \tag{18.12}$$

18.2 Matriisiyhteys

Määrittely-yhtälöiden ja rekursioiden nojalla Stirlingin 1. ja 2. lajin luvut ovat tietynlaisessa duaalisessa yhteydessä, joka nähdään seuraavasta matriisiesityksestä. Muodostetaan Stirlingin luvuista luonnollisella tavalla matriisit merkitsemällä

$$M_1(n) = (s_1(i,j))_{i,j=0,\ldots,n}, \quad M_2(n) = (S_2(i,j))_{i,j=0,\ldots,n},$$

jotka ovat $(n+1) \times (n+1)$ neliömatriiseja. Olkoon vielä $I_{n+1} = (\delta_{ij})_{i,j=0,\ldots,n}$ identiteettimatriisi.

ESIM:

$$M_1(4)M_2(4) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & -1 & 1 & 0 & 0 \\ 0 & 2 & -3 & 1 & 0 \\ 0 & -6 & 11 & -6 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 3 & 1 & 0 \\ 0 & 1 & 7 & 6 & 1 \end{pmatrix} = I_5. \tag{18.13}$$

Yleistetään tulos (18.13).

Lause 18.3. *Olkoon $n \in \mathbb{N}$, tällöin*

$$M_1(n)M_2(n) = M_2(n)M_1(n) = I_{n+1}. \qquad (18.14)$$

Todistus. Määritelmän 18.1 mukaan

$$x^h = \sum_{k=0}^{h} S_2(h,k)x(x-1)\cdots(x-k+1) =$$

$$\sum_{k=0}^{h} S_2(h,k) \sum_{m=0}^{k} s_1(k,m)x^m =$$

$$\sum_{m=0}^{k} \left(\sum_{k=0}^{h} S_2(h,k)s_1(k,m) \right) x^m. \qquad (18.15)$$

Verrataan vastinpotenssien kertoimia, joten

$$\sum_{k=0}^{h} S_2(h,k)s_1(k,m) = \delta_{hm}. \qquad (18.16)$$

Toisaalta, olkoon

$$(c_{hm}) = M_2(n)M_1(n) = (S_2(h,l)(s_1(k,m)), \qquad (18.17)$$

jolloin matriisitulon alkioille pätee

$$c_{hm} = \sum_{k=0}^{n} S_2(h,k)s_1(k,m). \qquad (18.18)$$

Koska $S_2(h,k) = 0$, kun $k > h$, niin soveltamalla tulosta (18.16) saadaan

$$c_{hm} = \sum_{k=0}^{h} S_2(h,k)s_1(k,m) = \delta_{hm} \qquad (18.19)$$

eli $c_{hh} = 1$ ja $c_{hm} = 0$ aina, kun $h \neq m$. Niinpä saadaan tulos

$$M_2(n)M_1(n) = I_{n+1}. \qquad (18.20)$$

Edelleen, (kts. Lineaarialgebra) tuloksen (18.20) nojalla pätee myös

$$M_1(n)M_2(n) = I_{n+1}. \quad \square \qquad (18.21)$$

ESIM: a). Kerrataanpa vielä polynomialgebraan liittyvä Lineaarialgebran tulos. Olkoon K kunta. Tällöin polynomijoukko $K[x]$ muodostaa lineaariavaruuden, jossa vektorit (=polynomit)

$$x^0, x^1, x^2, ..., x^m, \quad m \in \mathbb{N}, \qquad (18.22)$$

ovat lineaarisesti vapaita kunnan K yli.

b). Vastaavasti Pochammerin polynomit

$$(x)_0, (x)_1, ..., (x)_m, \quad m \in \mathbb{N}, \qquad (18.23)$$

muodostavat lineaarisesti riippumattoman joukon kunnan K yli.

Todistetaan tämä. Asetetaan lineaarikombinaatio nollaksi eli

$$r_0(x)_0 + r_1(x)_1 + ... + r_m(x)_m =$$

$$r_0 \cdot 1 + r_1 x + r_2 x(x+1)... + r_m x(x+1)\cdots(x+m-1) = 0, \quad r_i \in K. \qquad (18.24)$$

Kohdassa $x = 0$ saadaan

$$r_0 \cdot 1 + r_1 \cdot 0 + ... + r_m \cdot 0 = 0 \quad \Rightarrow \quad r_0 = 0. \qquad (18.25)$$

Siten yhtälö (18.24) lyhentyy muotoon

$$r_1 x + r_2 x(x+1)... + r_m x(x+1)\cdots(x+m-1) = 0. \qquad (18.26)$$

Yhtälö (18.26) on siis polynomi-identiteetti

$$x(r_1 + r_2(x+1)... + r_m(x+1)\cdots(x+m-1)) = 0, \qquad (18.27)$$

jonka toinen tekijä on nollapolynomi eli vääjäämättä

$$r_1 + r_2(x+1)... + r_m(x+1)\cdots(x+m-1) = 0. \qquad (18.28)$$

Sijoitetaan $x = -1$ yhtälöön (18.28), jolloin saadaan $r_1 = 0$. Edetään sitten induktiolla. □

HUOM: Esim. b) tulosta (18.23) voitaisiin käyttää äskeisen lauseen tuloksen (18.21) todistamiseen.

18.3 Yhteys Wolstenholmeen

Wolstenholmen lauseen todistuksessa (6.23) käytettiin polynomia

$$G(x) = (x-1)(x-2)\cdots(x-(p-1)) =$$

$$x^{p-1} - W_{p-2}x^{p-2} + W_{p-3}x^{p-3} - ... + W_2x^2 - W_1x + W_0, \quad p \in \mathbb{P}_{p\geq 3}.$$

Siten 1. lajin Stirlingin lukujen määritelmän nojalla

$$\sum_{k=0}^{p} s_1(p,k)x^k = x(x-1)(x-2)\cdots(x-(p-1)) = xG(x) =$$

$$x^p - W_{p-2}x^{p-1} + W_{p-3}x^{p-2} - W_{p-4}x^{p-3} + ... + W_2x^3 - W_1x^2 + W_0x. \qquad (18.29)$$

Relaation (18.29) perusteella

$$s_1(p,k) = (-1)^{k-1}W_{k-1}, \quad k = 1, ..., p \qquad (18.30)$$

joten välittömästi Lauseen 6.9 todistuksen perusteella pätee

Lause 18.4. *Olkoon $p \in \mathbb{P}_{p\geq 3}$. Tällöin*

$$s_1(p,k) \equiv 0 \pmod{p} \quad \forall\ 2 \leq k \leq p-1, \qquad (18.31)$$

$$s_1(p,2) \equiv 0 \pmod{p^2} \quad p \geq 5, \qquad (18.32)$$

$$s_1(p,1) \equiv -1 \pmod{p}. \qquad (18.33)$$

19 Osamääräkunta

Tarkennetaan hieman rationaalilukujen ja rationaalifunktioiden käsitteitä ja sitä kautta niillä operointia.

Määritelmä 19.1. Olkoon D kokonaisalue ja $a, b, c, d \in D$, $bd \neq 0$. Asetetaan relaatio

$$(a,b) \sim (c,d) \quad \Leftrightarrow \quad ad = bc. \qquad (19.1)$$

Lause 19.1. *Relaatio* $\sim$ *on ekvivalenssirelaatio joukossa* $D \times (D \setminus \{0\}) = \mathcal{D}$.

Määritelmä 19.2. Ekvivalenssiluokille

$$[a, b] = \{(c, d) \in \mathcal{D} |\ (c, d) \sim (a, b)\}$$

sovitaan yhteenlasku

$$[a_1, b_1] + [a_2, b_2] = [a_1 b_2 + a_2 b_1, b_1 b_2] \qquad (19.2)$$

ja kertolasku

$$[a_1, b_1][a_2, b_2] = [a_1 a_2, b_1 b_2] \qquad (19.3)$$

aina, kun $(a_1, b_1), (a_2, b_2) \in \mathcal{D}$.

Merkitään vielä

$$a/b = \frac{a}{b} = [a, b] \quad \text{ja} \quad Q(D) = \{a/b |\ (a, b) \in \mathcal{D}\}.$$

Voidaan todistaa, että

Lause 19.2. *Kolmikko* $(Q(D), +, \cdot)$ *on kunta.*

Sanotaan, että $Q(D)$ on D:n osamääräkunta (quotient field, field of fractions). Tällöin pätee rengasisomorfiatulos

$$\{\frac{a}{1} |\ a \in D\} \cong D, \qquad (19.4)$$

jonka nojalla voidaan merkitä $a = a/1$. Edelleen

$$ab^{-1} = \frac{a}{1}\left(\frac{b}{1}\right)^{-1} = \frac{a}{1}\frac{1}{b} = \frac{a}{b} \qquad (19.5)$$

ESIM: a) Olkoon $D = \mathbb{Z}$, joka on kokonaisalue. Tällöin saadaan osamääräkunta $Q(\mathbb{Z})$, jonka avulla rationaalilukujoukko saadaan määriteltyä tarkasti.

Määritelmä 19.3. Rationaalilukujen kunta $\mathbb{Q} = Q(\mathbb{Z})$.

Nyt rationaalilukujen supistamis-

$$\frac{ac}{bc} = \frac{a}{b} \qquad (19.6)$$

ja laventamislaki

$$\frac{a}{b} = \frac{da}{db} \qquad (19.7)$$

seuraa suoraan määritelmästä 19.1.

b.) Olkoon K kunta, jolloin polynomirengas $D = K[x]$ on kokonaisalue.

Määritelmä 19.4. Rationaalifunktioiden kunta $K(x) = Q(K[x])$.

Tällöin pätevät ylläesitetyt supistussäännöt, jolloin mm.

$$\frac{(x^2-1)x}{(x-1)x^2} = \frac{x+1}{x} = 1 + \frac{1}{x}. \qquad (19.8)$$

c.) Olkoon K kunta, jolloin formaalien sarjojen joukko $D = K[[T]]$ on kokonaisalue. Tällöin saadaan osamääräkunta, joka on isomorfinen aikaisemmin määritellyn formaalien Laurentin sarjojen kunnan kanssa eli

Lause 19.3.

$$K((T)) \cong Q(K[[T]]). \qquad (19.9)$$

Näillä rakenteilla on seuraavat suhteet:

$$K[T] \subset K(T) \subset K((T)),$$

$$K[T] \subset K[[T]] \subset K((T)).$$

Määritelmä 19.5. Formaali derivaatta

$$D: \ K((T)) \to K((T))$$

on lineaarinen kuvaus, jolle pätee

$$DT^k = kT^{k-1} \quad \forall \quad k \in \mathbb{Z}. \qquad (19.10)$$

20 Jonojen algebraa

20.1 Määritelmä, lineaariavaruus

Määritelmä 20.1. Olkoon R rengas. Kuvaus

$$\Psi : \mathbb{N} \to R$$

on jono (sequence).

Usein kuvaus Ψ ja sen kuvajoukko $\Psi(\mathbb{N})$ samaistetaan. Merkitään tutummin

$$a_n = \Psi(n) \quad n \in \mathbb{N},$$

jolloin

$$\Psi(\mathbb{N}) = \{a_n |\ n \in \mathbb{N}\}$$

ja merkitään vielä

$$(a_n) = (a_n)_{n=0}^{\infty} = (a_0, a_1, ...) = \Psi(\mathbb{N}).$$

Siten esimerkiksi

$$(a) = (a, a, ...),$$

joka on vakiojono.

Määritelmä 20.2. Olkoot $(a_n), (b_n) \subseteq R$ jonoja ja $r \in R$. Tällöin asetetaan yhtäsuuruus, summa ja skalaarilla kertominen seuraavasti

$$(a_n) = (b_n) \quad \Leftrightarrow \quad a_n = b_n \qquad (20.1)$$

$$(a_n) + (b_n) = (a_n + b_n) \qquad (20.2)$$

$$r(a_n) = (ra_n) \qquad (20.3)$$

kaikilla $n \in \mathbb{N}$.

Lause 20.1. *Olkoon $R = K$ kunta, tällöin*

$$l = \{(a_n) |\ a_n \in K\}$$

on lineaariavaruus kunnan K yli.

ESIM: Lineaariavaruuden l nolla-alkio on

$$(0) = (0, 0, ...).$$

20.2 Erotus/Differenssioperaattorit

Määritelmä 20.3. Olkoon

$$a :\ \mathbb{C} \to \mathbb{C}$$

kuvaus. Tällöin asetetaan

$$(Ea)(x) = a(x + 1) \quad \forall \quad x \in \mathbb{C}, \qquad (20.4)$$

$$(\Delta a)(x) = a(x + 1) - a(x) \quad \forall \quad x \in \mathbb{C}, \qquad (20.5)$$

missä E on nosto-operaattori ja Δ on erotus- eli differenssioperaattori. Olkoon vielä I identiteettioperaattori eli

$$(Ia)(x) = a(x) \quad \forall \quad x \in \mathbb{C}. \qquad (20.6)$$

Kerrataan nyt funktioiden summan ja skalaarilla kertomisen määritelmät.

Määritelmä 20.4. Olkoot C ja D renkaita sekä A ja B kuvauksia : $C \to D$ ja $c \in D$. Tällöin asetetaan

$$(A + B)(z) = A(z) + B(z) \quad \forall \quad z \in C, \qquad (20.7)$$

$$(cA)(z) = cA(z) \quad \forall \quad z \in C. \qquad (20.8)$$

Annetaan kompleksikuvausten joukolle merkintä

$$\mathcal{F} = \{a : \ \mathbb{C} \to \mathbb{C}\},$$

jolloin differenssioperaattorit I, E, Δ ovat funktioita $\mathcal{F} \to \mathcal{F}$. Siten differenssioperaattoreiden summa ja skalaarilla kertominen on Määritelmän 20.4 erikoistapaus. Edelleen pätee

Lause 20.2. *Olkoot $A \in \{I, E, \Delta\}$ Tällöin*

$$A(a + b) = Aa + Ab \qquad (20.9)$$

ja

$$A(ca) = cAa \qquad (20.10)$$

aina, kun $c \in \mathbb{C}$ ja $a, b \in \mathcal{F}$.

Tarvitaan vielä operaattoritulo, joka on itseasiassa operaattoreiden normaali yhdistetty kuvaus seuraavasti

Määritelmä 20.5. Olkoot A ja B operaattoreita, jolloin

$$(A \circ B)a = A(Ba) \quad \forall \quad a \in \mathcal{F} \qquad (20.11)$$

määrää operaattoritulon $AB = A \circ B$. Edelleen

$$A^0 = I, \quad A^{n+1} = A \circ A^n \quad \forall \quad n \in N \qquad (20.12)$$

määrää operaattoripotenssin induktiivisesti.

ESIM: a) Lasketaan aluksi nosto-operaattorin toinen potenssi

$$E^2 a(x) = E(Ea)(x) = Ea(x + 1) = a(x + 2)$$

joten induktiolla

$$E^n a(x) = a(x + n) \quad \forall \quad n \in N. \qquad (20.13)$$

b.) Differenssioperaattorit liittyvät toisiinsa seuraavasti

$$\Delta = E - I, \quad E = \Delta + I. \qquad (20.14)$$

Siirrytään nyt jonojen tarkasteluun ja merkitään

$$a_n = a(x + n),$$

jolloin

$$Ia_n = a_n, \qquad (20.15)$$

$$Ea_n = a_{n+1}, \qquad (20.16)$$

$$\Delta a_n = a_{n+1} - a_n. \qquad (20.17)$$

ESIM:

$$E^2 a_n = a_{n+2},$$

$$\Delta^2 a_n = a_{n+2} - 2a_{n+1} + a_n = E^2 a_n - 2Ea_n + a_n.$$

Yleisemmin pätee

Lause 20.3. *Olkoon $n \in \mathbb{N}$ annettu, tällöin*

$$\Delta^n = (-1)^n \sum_{k=0}^{n} \binom{n}{k} (-E)^k, \qquad (20.18)$$

$$E^n = \sum_{k=0}^{n} \binom{n}{k} \Delta^k. \qquad (20.19)$$

20.3 Rekursioyhtälöitä

Käsitellään seuraavassa hieman ei-vakiokertoimisten ensimmäisen ja toisen kertalukujen differenssi- eli rekursioyhtälöiden ratkaisemista.

Määritelmä 20.6. Olkoot

$$c_i, g : \mathbb{N} \to \mathbb{C}$$

annettu. Tällöin

$$c_1(n)a_{n+1} + c_0(n)a_n = g(n) \qquad (20.20)$$

on 1. kertaluvun ei-homogeeninen lineaarinen rekursioyhtälö,

$$c_1(n)a_{n+1} + c_0(n)a_n = 0 \qquad (20.21)$$

on 1. kertaluvun homogeeninen lineaarinen rekursioyhtälö ja

$$c_2(n)a_{n+2} + c_1(n)a_{n+1} + c_0(n)a_n = 0 \qquad (20.22)$$

on 2. kertaluvun homogeeninen lineaarinen rekursioyhtälö.

Voidaan todistaa, että

Lause 20.4. *Yhtälöllä (20.22) on kaksi lineaarisesti vapaata ratkaisua*

$$(a_n^1), \quad (a_n^2) \subseteq \mathbb{C}$$

ja jokainen yhtälön (20.22) ratkaisu (a_n) *voidaan esittää yksikäsitteisesti muodossa*

$$(a_n) = r(a_n^1) + s(a_n^2), \qquad (20.23)$$

joillakin $r, s \in \mathbb{C}$.

Siis 2. kertaluvun lineaarisen homogeenisen rekursioyhtälön (20.22) ratkaisujoukko

$$\{r(a_n^1) + s(a_n^2) |\ r, s \in \mathbb{C}\} \qquad (20.24)$$

on kompleksilukujonojen 2-dimensioinen aliavaruus. Vastaavasti ensimmäisen kertaluvun homogeenisen yhtälön (20.21) ratkaisujoukko on 1-dimensioinen.

ESIM: $K = \mathbb{C}$. Olkoot

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

jolloin jonot (α^n) ja (β^n) ovat lineaarisesti vapaita/$\mathbb{C}$.

Todistus. Olkoot $t, v \in \mathbb{C}$ ja asetetaan lineaarikombinaatio nollaksi eli

$$t(\alpha^n) + v(\beta^n) = (0). \qquad (20.25)$$

Yhtäpitävästi identiteetin (20.25) kanssa meillä on

$$(t\alpha^n + v\beta^n) = (0) \quad \Leftrightarrow \quad t\alpha^n + v\beta^n = 0 \quad \forall \quad n \in \mathbb{N}. \qquad (20.26)$$

Valitaan nyt $n = 0$ ja $n = 1$, joten

$$t \cdot 1 + v \cdot 1 = 0 \quad \text{ja} \quad t\alpha + v\beta = 0 \quad \Rightarrow \quad t = v = 0. \qquad (20.27) \quad \square$$

Siten rekursion

$$a_{n+2} - a_{n+1} - a_n = 0 \qquad (20.28)$$

ratkaisukannaksi voidaan ottaa

$$\{(\alpha^n), (\beta^n)\}, \qquad (20.29)$$

jolloin jokainen ratkaisu on muotoa

$$(a_n) = (r\alpha^n + s\beta^n), \qquad (20.30)$$

joillakin $r, s \in \mathbb{C}$. Tarkastellaan seuraavaksi 1. kertaluvun rekursioyhtälöitä.

ESIM: a)

$$a_{n+1} - a_n = 0. \qquad (20.31)$$

Ratkaistaan (20.31) tarkastelemalla alimpia indeksin arvoja, jolloin induktiolla

$$a_1 = a_0, \quad a_2 = a_1 = a_0, ..., a_n = a_{n+1} = ... = a_0.$$

Siten yhtälön

$$\Delta a_n = 0 \qquad (20.32)$$

ratkaisu on vakiojono.

ESIM: b.)

$$(n+1)a_{n+1} - a_n = 0. \qquad (20.33)$$

Ratkaistaan (20.33) laskemalla

$$a_1 = \frac{a_0}{1}, \quad a_2 = \frac{a_1}{2} = \frac{a_0}{2!}, ..., \quad a_n = \frac{a_0}{n!}.$$

Siten yhtälön (20.33) ratkaisu saadaan jonon

$$(1/n!) \qquad (20.34)$$

skalaarikertana.

ESIM: c.)

$$a_{n+1} - a_n = \frac{1}{n+1}. \qquad (20.35)$$

Ratkaistaan (20.35) laskemalla

$$a_1 = a_0 + \frac{1}{1}, \quad a_2 = a_1 + \frac{1}{2} = a_0 + 1 + \frac{1}{2}, ..., \quad a_n = a_0 + H_n. \qquad (20.36)$$

ESIM: d.)

$$(n+2)a_{n+2} - (2n+3)a_{n+1} + (n+1)a_n = 0. \qquad (20.37)$$

Käytetään tämän ratkaisuun operaattoritekniikkaa. Aluksi (20.37) on yhtäpitävä yhtälön

$$((n+2)E^2 - (2n+3)E + (n+1))a_n = 0 \qquad (20.38)$$

kanssa. Nyt operaattori jakaantuu, jolloin

$$(E - I)((n+1)E - (n+1))a_n = 0. \qquad (20.39)$$

Merkitään

$$b_n = ((n+1)E - (n+1))a_n, \qquad (20.40)$$

jolloin (20.39) yksinkertaistuu muotoon

$$(E - I)b_n = 0,$$

jonka ratkaisu a) kohdan nojalla on vakio eli

$$b_n = c = vakio. \qquad (20.41)$$

Täten relaatio (20.40) antaa yhtälön

$$((n+1)E - (n+1))a_n = c \quad \Leftrightarrow \quad (n+1)(a_{n+1} - a_n) = c. \qquad (20.42)$$

Kohdan c) nojalla yhtälön (20.42) ratkaisuksi tulee

$$a_n = a_0 + cH_n, \quad a_0, c \in \mathbb{C}. \qquad (20.43)$$

Yhtälö (20.37) voidaan tietenkin ratkaista ilman operaattoritekniikkaa, kunhan huomataan, että (20.37) voidaan kirjoittaa muotoon

$$(n+2)a_{n+2} - (n+2)a_{n+1} - ((n+1)a_{n+1} - (n+1)a_n) = 0. \qquad (20.44)$$

Sitten edetään kuten äsken kohdasta (20.40).
HUOM: Yleisessä tapauksessa 2. kertaluvun yhtälöä ei pysty ratkaisemaan helposti eli ratkaisuille ei löydy kovinkaan nättejä lausekkeita.
e) Usein differenssiyhtälöt ja niiden ratkaisut on tarpeellista muuntaa yhtäpitäviin esityksiin. Tarkastellaan kohdan d) yhtälöä (20.37), johon sijoitetaan

$$b_n = n!a_n \qquad (20.45)$$

ja siten (b_n) toteuttaa yhtälön

$$b_{n+2} - (2n+3)b_{n+1} + (n+1)^2 b_n = 0. \qquad (20.46)$$

21 Irrationaaliluvuista

Määritelmä 21.1. 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.)

ESIM: a)

$$\sqrt{5} \notin \mathbb{Q}. \qquad (21.1)$$

Todistus. Jos, olisi

$$\sqrt{5} = \frac{m}{n} \in \mathbb{Q}, \quad m \perp n, \qquad (21.2)$$

niin

$$5n^2 = m^2 \quad \Rightarrow \quad 5|m^2 \quad \Rightarrow \quad 5|m \qquad (21.3)$$

$$\Rightarrow \quad 5^2|m^2 = 5n^2 \quad \Rightarrow \quad 5|n^2 \quad \Rightarrow \quad 5|n. \qquad (21.4)$$

Selvästi tulokset (21.3) ja (21.4) ovat ristiriidassa valinnan $m \perp n$ kanssa. □

Tämä yleistyy tulokseksi

Lause 21.1. *Olkoon $D \in \mathbb{Z}$ neliövapaa. Tällöin*

$$\sqrt{D} \notin \mathbb{Q}. \qquad (21.5)$$

Todistus laskareissa.

Lause 21.2. *Olkoot $n \in \mathbb{Z}_{\geq 3}$ ja $r \in \mathbb{Q}^+$. Tällöin*

$$\sqrt[n]{1 + r^n} \notin \mathbb{Q}. \qquad (21.6)$$

Todistus, joka perustuu Wilesin tulokseen, laskareissa.

ESIM: b).

$$\frac{\log 2}{\log 3} \notin \mathbb{Q}. \qquad (21.7)$$

Todistus. Jos olisi

$$\frac{\log 2}{\log 3} = \frac{a}{b}, \quad a, b \in \mathbb{Z}^+, \qquad (21.8)$$

niin

$$2^b = 3^a \quad \Rightarrow \quad 2|3^a \quad \Rightarrow \quad 2|3 \qquad (21.9)$$

mikä on mahdotonta. □

ESIM: c).

$$\log 2 \notin \mathbb{Q}. \qquad (21.10)$$

Ei todisteta. Todistus huomattavasti vaikeampi kuin kohdassa b).

Lause 21.3. *Neperin luku e on irrationaalinen.*

Todistus. Tiedetään, että

$$e = \lim_{n\to\infty} \left(1 + \frac{1}{n}\right)^n = \sum_{k=0}^{\infty} \frac{1}{k!}. \qquad (21.11)$$

Olkoon siis vastaoletuksena

$$e = \frac{a}{b} \in \mathbb{Q}, \quad a, b \in \mathbb{Z}^+, \quad a \perp b. \qquad (21.12)$$

Valitaan sellainen kokonaisluku m, että

$$m \in \mathbb{Z}^+, \quad b \leq m \qquad (21.13)$$

ja merkitään

$$A = m! \left(e - \sum_{k=0}^{m} \frac{1}{k!}\right). \qquad (21.14)$$

Aluksi huomataan, että

$$A = \frac{m!a}{b} - m! \sum_{k=0}^{m} \frac{1}{k!} \in \mathbb{Z}. \qquad (21.15)$$

Toisaalta

$$A = m! \sum_{k=m+1}^{\infty} \frac{1}{k!}, \qquad (21.16)$$

joten saadaan arviot

$$0 < A = m!\left(\frac{1}{(m+1)!} + \frac{1}{(m+2)!} + \frac{1}{(m+3)!} + ...\right) =$$

$$\frac{1}{m+1} + \frac{1}{(m+1)(m+2)} + \frac{1}{(m+1)(m+2)(m+3)} + ... =$$

$$\frac{1}{m+1}\left(1 + \frac{1}{m+2} + \frac{1}{(m+2)(m+3)} + ...\right) <$$

$$\frac{1}{m+1}\left(1 + \frac{1}{m+1} + \frac{1}{(m+1)^2} + ...\right) = \frac{1}{m} \leq 1. \qquad (21.17)$$

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

22 Ketjumurtoluvut

Äärellisellä ketjumurtoluvulla (finite continued fraction) tarkoitetaan rationaalilauseketta

$$\cfrac{a_1}{b_1 + \cfrac{a_2}{b_2 + ... \atop + \frac{a_n}{b_n}}},$$

jolle käytetään seuraavia merkintöjä

$$\mathbb{K}_{k=1}^{n}\left(\frac{a_k}{b_k}\right) = \frac{a_1}{b_1 +}\frac{a_2}{b_2 +}...\frac{a_n}{+\, b_n}. \qquad (22.1)$$

Lause 22.1. *Olkoot luvut A_n ja B_n annettu rekursioilla*

$$A_{n+2} = b_{n+2}A_{n+1} + a_{n+2}A_n, \qquad (22.2)$$

$$B_{n+2} = b_{n+2}B_{n+1} + a_{n+2}B_n \qquad (22.3)$$

lähtien alkuarvoista $A_0 = b_0$, $B_0 = 1$, $A_1 = b_0b_1 + a_1$ ja $B_1 = b_1$. Tällöin

$$b_0 + \mathbb{K}_{k=1}^{n}\left(\frac{a_k}{b_k}\right) = \frac{A_n}{B_n} \quad \forall\ n \in \mathbb{N}, \qquad (22.4)$$

kunhan $B_n \neq 0$.

Todistus. Induktiolla.

$n = 0$, jolloin

$$V.P. = b_0 = \frac{b_0}{1} = \frac{A_0}{B_0} = O.P..$$

$n = 1$, jolloin

$$V.P. = b_0 + \frac{a_1}{b_1} = \frac{b_0 b_1 + a_1}{b_1} = \frac{A_1}{B_1} = O.P..$$

Induktio-oletus: Väite pätee, kun $n = 0, 1, ..., l$, jolloin

$$b_0 + \frac{a_1}{b_1 +}\frac{a_2}{b_2 +}...\frac{a_l}{+ b_l} = \frac{A_l}{B_l} = \frac{b_l A_{l-1} + a_l A_{l-2}}{b_l B_{l-1} + a_l B_{l-2}}. \qquad (22.5)$$

Korvataan b_l muuttujalla x ja merkitään

$$K(x) = b_0 + \frac{a_1}{b_1 +}\frac{a_2}{b_2 +}...\frac{a_l}{+ x}, \qquad (22.6)$$

jolle kohdan (22.5) nojalla pätee

$$K(x) = \frac{xA_{l-1} + a_l A_{l-2}}{xB_{l-1} + a_l B_{l-2}}, \qquad (22.7)$$

kunhan $x \neq 0$ ja nimittäjä $\neq 0$. Siten kohdista (22.6) ja (22.7) seuraa

$$K(b_l + \frac{a_{l+1}}{b_{l+1}}) = b_0 + \mathbb{K}_{k=1}^{l+1}\left(\frac{a_k}{b_k}\right) =$$

$$\frac{\left(b_l + \frac{a_{l+1}}{b_{l+1}}\right) A_{l-1} + a_l A_{l-2}}{\left(b_l + \frac{a_{l+1}}{b_{l+1}}\right) B_{l-1} + a_l B_{l-2}} =$$

$$\frac{\frac{a_{l+1}}{b_{l+1}} A_{l-1} + b_l A_{l-1} + a_l A_{l-2}}{\frac{a_{l+1}}{b_{l+1}} B_{l-1} + b_l B_{l-1} + a_l B_{l-2}} =$$

$$\frac{a_{l+1}A_{l-1} + b_{l+1}A_l}{a_{l+1}B_{l-1} + b_{l+1}B_l} = \frac{A_{l+1}}{B_{l+1}}, \qquad (22.8)$$

missä on sovellettu rekursioita (22.2) ja (22.3) pariin otteeseen. Siten induktioaskel on osoitettu ja induktioperiaatteen nojalla väite pätee. □

Määritelmä 22.1. Luku A_n/B_n on äärettömän ketjumurtoluvun

$$b_0 + \mathbb{K}_{k=1}^{\infty}\left(\frac{a_k}{b_k}\right) \qquad (22.9)$$

n. konvergentti. Edelleen ketjumurtoluku (22.9) suppenee, mikäli raja-arvo

$$\lim_{n\to\infty}\frac{A_n}{B_n} \qquad (22.10)$$

on olemassa. Tällöin sanotaan, että äärettömän ketjumurtoluvun (22.9) arvo on raja-arvo (22.10).

Ääretöntä ketjumurtolukua (22.9) voidaan merkitä myös seuraavasti

$$b_0 + \frac{a_1}{b_1 +}\frac{a_2}{b_2 +}... = b_0 + \frac{a_1}{b_1 + \frac{a_2}{b_2 + ...}}.$$

Usein tarkastellaan yksinkertaisia ketjumurtolukuja.

Määritelmä 22.2. Olkoot

$$b_0 \in \mathbb{N}, \quad b_k \in \mathbb{Z}^+, \quad a_k = 1, \quad \forall \quad k \in \mathbb{Z}^+. \qquad (22.11)$$

Tällöin ketjumurtoluku

$$[b_0; b_1, ..., b_n] = b_0 + \mathbb{K}_{k=1}^{n}\left(\frac{1}{b_k}\right) \qquad (22.12)$$

on äärellinen yksinkertainen (simple) ketjumurtoluku ja vastaavasti

$$[b_0; b_1, ...] = b_0 + \mathbb{K}_{k=1}^{\infty}\left(\frac{1}{b_k}\right) \qquad (22.13)$$

on ääretön yksinkertainen ketjumurtoluku.

ESIM: a) Olkoot

$$\beta = \frac{1-\sqrt{5}}{2}, \quad \gamma = -\beta = \frac{\sqrt{5}-1}{2}, \quad 0 < \gamma < 1. \qquad (22.14)$$

Yhtälöstä

$$\beta^2 = 1 + \beta \qquad (22.15)$$

saadaan

$$\beta^3 = \beta + \beta^2 = 1 + 2\beta.$$

Edelleen

$$\beta^4 = 2 + 3\beta$$

ja induktiolla nähdään, että

$$\beta^{n+1} = f_n + f_{n+1}\beta \quad \forall\ n \in \mathbb{N} \qquad (22.16)$$

missä f_n on Fibonaccin luku. Siten

$$\gamma - \frac{f_n}{f_{n+1}} = \frac{\beta^{n+1}}{f_{n+1}} \quad \forall\ n \in \mathbb{N} \qquad (22.17)$$

josta seuraa

$$\left|\gamma - \frac{f_n}{f_{n+1}}\right| \underset{n\to\infty}{\to} 0 \qquad (22.18)$$

eli

$$\gamma = \frac{\sqrt{5}-1}{2} = \lim_{n\to\infty} \frac{f_n}{f_{n+1}}. \qquad (22.19)$$

Merkitään nyt

$$A_n = f_n, \quad B_n = f_{n+1}, \qquad (22.20)$$

jolloin

$$A_0 = 0, \quad B_0 = 1, \quad A_1 = 1, \quad B_1 = 1 \qquad (22.21)$$

ja

$$A_{n+2} = A_{n+1} + A_n, \quad B_{n+2} = B_{n+1} + B_n \quad \forall \quad n \in \mathbb{N}. \qquad (22.22)$$

Olkoot vielä

$$b_0 = 0, \quad a_n = 1, \quad b_n = 1 \quad \forall \quad n \in \mathbb{Z}^+. \qquad (22.23)$$

Lause 22.2. *Valinnoilla (22.20-23) saadaan*

$$b_0 + \mathbb{K}_{k=1}^{n} \left(\frac{a_k}{b_k}\right) = \frac{A_n}{B_n} \quad \forall\ n \in \mathbb{N} \qquad (22.24)$$

ja

$$\gamma = \frac{\sqrt{5}-1}{2} = \lim_{n\to\infty} \frac{A_n}{B_n}. \qquad (22.25)$$

Todistukseen tarvitaan enää rekursioiden (22.22) alkuarvojen tarkistus

$$A_0 = 0 = b_0, \quad B_0 = 1, \quad B_1 = 1 = b_1, \quad A_1 = 1 = b_0 b_1 + a_1 \qquad (22.26)$$

sekä raja-arvo

$$\lim_{n\to\infty} \frac{A_n}{B_n} = \lim_{n\to\infty} \frac{f_n}{f_{n+1}} = \gamma, \qquad (22.27)$$

joka tulee tuloksesta (22.19). □

Huomaa, että tuloksen (22.25) nojalla saatiin laskettua arvo äärettömälle ketjumurtoluvulle

$$\frac{1}{1+\frac{1}{1+\frac{1}{1+\ldots}}} = \frac{\sqrt{5}-1}{2}. \qquad (22.28)$$

Toisin sanoen, ensin määrättiin ketjumurtoluvun (22.28) n. konvergentti $A_n/B_n = f_n/f_{n+1}$ ja laskettiin sen raja-arvo $= \gamma$, joten Määritelmän 22.1 nojalla se on äärettömän ketjumurtoluvun (22.28) arvo.

23 Polynomien nollakohdista

Lause 23.1. *Olkoon K kunta ja $p(x) \in K[x]$, $1 \le \deg p(x)$. Tällöin*

$$p(\alpha) = 0,\ \alpha \in K \qquad \Leftrightarrow \qquad x - \alpha | p(x) \text{ renkaassa } K[x].$$

Määritelmä 23.1. Jos $\alpha \in K$ ja

$$(x-\alpha)^m \| p(x),\ m \in \mathbb{Z}^+,$$

niin $m = m(\alpha)$ on polynomin $p(x)$ nollakohdan α kertaluku. Nollakohtien lukumäärä $n_p$on summa kertaluvuista eli

$$n_p = \#\{\alpha |\ p(\alpha) = 0\} = \sum_{p(\alpha_i)=0} m(\alpha_i).$$

ESIM:

- a) Olkoon $p(x) = (x-1)^3(x+1/2)^5$. Polynomin $p(x)$ nollakohdat ovat $\alpha_1 = 1$ ja $\alpha_2 = -1/2$. Nollakohtien kertaluvut ovat $m(\alpha_1) = 3$ ja $m(\alpha_2) = 5$, ja nollakohtien lukumäärä $n_p = 3 + 5 = 8$.
- b) Olkoon $(x^2+1)(x^2-1) \in \mathbb{R}[x]$. Nyt nollakohtien lukumäärä $n_p = m(-1) + m(1) = 2 < 4 = \deg(p(x))$.

Lause 23.2. *Olkoon K kunta ja $p(x) \in K[x]$. Nyt $n_p \leq \deg p(x)$.*

Lause 23.3. *Olkoon $p(x) \in \mathbb{C}[x]$, tällöin $n_p = deg(p(x))$.*

Seurauksena lauseesta saadaan

Lause 23.4. *Olkoon $q(x), r(x) \in K[x]$, $\deg r(x)$, $\deg q(x) \leq D$, ja olkoot olemassa sellaiset pisteet $b_1, b_2, \ldots b_{D+1}$, että $b_i \neq b_j$, kun $i \neq j$, ja*

$$q(b_i) = r(b_i) \text{ kaikilla } i = 1, 2, \ldots, D+1.$$

Tällöin $q(x) = r(x)$ polynomeina.

Todistetaan Lauseen 23.4 sovelluksena

Lause 23.5. *Olkoon $m \in \mathbb{N}$, tällöin pätee polynomiyhtäsuuruus*

$$B_m(x) = m \sum_{k=0}^{m-1} S_2(m-1,k) \binom{x}{k+1} k! \quad + B_m. \qquad (23.1)$$

Todistus:. Olkoon yhtälön oikealla puolella oleva polynomi $C_m(x)$. Todetaan ensin, että

$$B_0(x) = 1 = 0 + B_0 = C_0(x), \text{ ja}$$
$$B_1(x) = x - 1/2 = S_2(0,0)\binom{x}{1} + B_1 = C_1(x), \qquad (23.2)$$

eli väite pätee kun $m = 0$ tai $m = 1$. Olkoon $m \geq 2$.

Lasketaan nyt erotus

$$\begin{aligned} C_n(x+1) - C_n(x) &= n\sum_{k=0}^{n-1} S_2(n-1,k)k!\left(\binom{x+1}{k+1} - \binom{x}{k+1}\right) \\ &= n\sum_{k=0}^{n-1} S_2(n-1,k)k!\binom{x}{k} \\ &= n\sum_{k=0}^{n-1} S_2(n-1,k)x(x-1)(x-2)\cdots(x-k+1) \\ &= nx^{n-1}. \qquad (23.3) \end{aligned}$$

Lasketaan arvoja $C_m(l)$, kun $l = 0, 1, \ldots, m$.

$$\begin{aligned} C_m(0) &= m\sum_{k=0}^{m-1} S_2(m-1,k)\binom{0}{k+1}k! \quad + B_m = B_m, \\ C_m(1) &= C_m(0) + m0^{m-1} = B_m, \\ C_m(2) &= C_m(1) + m1^{m-1} = B_m + m, \\ &\vdots \\ C_m(l+1) &= C_m(l) + ml^{m-1} \text{ kaikilla } l \geq 0. \qquad (23.4) \end{aligned}$$

Toisaalta myös Bernoullin polynomeille pätee sama palautuskaava (23.4) samoilla alkuarvoilla eli

$$\begin{aligned} B_m(0) &= B_m, \\ B_m(1) &= B_m, \\ B_m(2) &= B_m + m, \\ &\vdots \\ B_m(l+1) &= B_m(l) + ml^{m-1} \text{ kaikilla } l \geq 0. \qquad (23.5) \end{aligned}$$

Siten

$$B_m(l) = C_m(l) \qquad (23.6)$$

kaikilla $l = 0, 1, \ldots, m$ ja $\deg B_m(x), \deg C_m(x) \leq m$. Seurauslauseen nojalla siis $B_m(x) = C_m(x)$ polynomeina. $\square$

24 Antiikin lukuja

24.1 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). Laskuharjoitusten perusteella

$$\mathcal{T}_n = \binom{n+2}{3} \text{ kaikilla } n \in \mathbb{Z}^+.$$

24.2 Pythagoraan luvut

Määritelmä:

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

$$a^2 + b^2 = c^2. \qquad (23.7)$$

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

$$a = 2l + 1 \text{ ja } b = 2k + 1 \Rightarrow$$
$$c^2 = a^2 + b^2 = 2(2l^2 + 2l + 2k^2 + 2k + 1), \text{ ristiriita.}$$

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

$$a^2 = (c - b)(c + b) \qquad (23.8)$$

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

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

$$\Rightarrow c - b = \prod_{j \in J} p_j^{2\alpha_j} = \left(\prod_{j \in J} p_j^{\alpha_j} \right)^2 \text{ ja}$$

$$c + b = \prod_{l \in L} p_l^{2\alpha_l} = \left(\prod_{l \in L} p_l^{\alpha_l} \right)^2, \text{ missä}$$

$$J \cup L = \{1, 2, \ldots, r\} \quad J \cap L = \emptyset.$$

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

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

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

Saadaan siis seuraava

Lause 24.1. *Yhtälön*

$$a^2 + b^2 = c^2$$

primitiiviset ratkaisut saadaan parametrimuodossa

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

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

Esimerkki:

- Olkoon $t = 1$. Annetaan luvulle s parittomia arvoja

$$\begin{array}{ll} s = 3 & 3^2 + 4^2 = 5^2 \\ s = 5 & 5^2 + 12^2 = 13^2 \\ \vdots & \vdots \\ s = 2m + 1 & (2m+1)^2 + (4T_m)^2 = (2m^2 + 2m + 1)^2. \end{array}$$

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

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

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