

802328A LUKUTEORIAN PERUSTEET OSA

II

BASICS OF NUMBER THEORY PART II

Tapani Matala-aho

MATEMATIIKKA/LUTK/OULUN YLIOPISTO

SYKSY 2016

## Sisältö

<b>1</b>	<b>KERTOMAT, BINOMIKERTOIMET</b>	<b>2</b>
1.0.1	Kertoma/Factorial . . . . .	2
1.1	Palautuskaava, Pascalin kolmio . . . . .	4
1.2	Binomisarja, Binomikehitelmä . . . . .	6
<b>2</b>	<b><math>p</math>-valuaatio</b>	<b>7</b>
<b>3</b>	<b>Rationaaliluvun jaollisuus (mod <math>n</math>)</b>	<b>11</b>
3.1	Perusteita . . . . .	11
3.2	Rengas $\mathbb{Q}_n$ . . . . .	15
3.3	Sovelluksia . . . . .	18
3.3.1	Wilsonin lause . . . . .	19
3.3.2	Euler-Fermat . . . . .	20
3.3.3	Euler-Fermat'n todistus . . . . .	21
3.4	Wolstenholmen lause . . . . .	23
3.5	$(p - 1)!$ ja $a^{p-1} \pmod{p^2}$ /EI kokeeseen . . . . .	28
<b>4</b>	<b>Polynomien kongruenssi</b>	<b>31</b>
4.1	Sovelluksia lukujen kongruensseihin . . . . .	37
4.1.1	Lucasin binomikerroinlause . . . . .	37
4.1.2	Lucasin binomikerroinlauseen todistus . . . . .	37
<b>5</b>	<b>Summausmenetelmiä</b>	<b>39</b>
5.1	Polynomialgebran sovelluksia . . . . .	39
5.2	Teleskoopit . . . . .	40

# 1 KERTOMAT, BINOMIKERTOIMET

## 1.0.1 Kertoma/Factorial

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

**Määritelmä 1.**

$$0! = 1, \quad (1.1)$$

$$n! = (n - 1)! \cdot n, \quad \forall n \in \mathbb{Z}^+. \quad (1.2)$$

Yleisesti tapauksessa  $n \geq 1$  kirjoitetaan löyhästi

$$n! = 1 \cdot 2 \cdot 3 \cdots (n - 1) \cdot n, \quad (1.3)$$

missä  $\cdots$  on eräänlainen lyhennysmerkintä tarkasta määritelmästä (1.2).

Kertoman yleistys, Pochhammerin symboli  $(a)_n$ , saadaan seuraavasti.

**Määritelmä 2.** Olkoon  $a \in \mathbb{C}$ . Tällöin

$$(a)_0 = 1, \quad (1.4)$$

$$(a)_n = (a)_{n-1} \cdot (a + n - 1), \quad \forall n \in \mathbb{Z}^+. \quad (1.5)$$

Nytkin tapauksessa  $n \geq 1$  kirjoitetaan

$$(a)_n = a \cdot (a + 1) \cdots (a + n - 2) \cdot (a + n - 1). \quad (1.6)$$

Erityisesti

$$(1)_n = n!. \quad (1.7)$$

**Määritelmä 3.** Olkoot  $a \in \mathbb{C}$  ja  $k \in \mathbb{N}$ . Tällöin luvut

$$\binom{a}{k} = \frac{(a - k + 1)_k}{k!} \quad (1.8)$$

ovat binomikertoimia " $a$  yli  $k:n$ ".

### Huomautus 1.

Aikaisempi Määritelmä ja Määritelmä 3 ovat ekvivalentit eli

$$\binom{a}{k} = \frac{(a-k+1)_k}{k!} = (-1)^k \frac{(-a)_k}{k!}. \quad (1.9)$$

Binomikertoimen Määritelmä 3 esitetään usein (epätarkemmin) muodossa

**Määritelmä 4.** Olkoot  $a \in \mathbb{C}$  ja  $k \in \mathbb{N}$ . Tällöin luvut

$$\binom{a}{k} = \begin{cases} 1, & \text{jos } k = 0; \\ \frac{(a-k+1)(a-k+2)\cdots(a-1)a}{k!}, & \text{jos } k \in \mathbb{Z}^+ \end{cases} \quad (1.10)$$

ovat binomikertoimia " $a$  yli  $k:n$ ".

Perustelu. Olkoon aluksi  $k = 0$ . Tällöin

$$\binom{a}{k} = \binom{a}{0} = \frac{(a+1)_0}{0!} = 1 \quad \forall a \in \mathbb{C}. \quad (1.11)$$

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

$$\binom{a}{k} = \frac{(a-k+1)_k}{k!} = \frac{(a-k+1)(a-k+2)\cdots(a-1)a}{k!} \quad \forall a \in \mathbb{C}. \quad (1.12)$$

Kuten yleensäkin niin seuraavassakin käytetään enimmäkseen tätä esitystä.

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

$$\begin{aligned} \binom{n}{k} &= \frac{(n-k+1)(n-k+2)\cdots(n-1)n}{k!} = \\ &= \frac{(n-k)!(n-k+1)(n-k+2)\cdots(n-1)n}{k!(n-k)!}, \end{aligned} \quad (1.13)$$

joten

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} \quad \forall 0 \leq k \leq n. \quad (1.14)$$

Jos  $k \geq n + 1$ , niin

$$\binom{n}{k} = (-1)^k \frac{(-n) \cdots (-n + j) \cdots (-n + k - 1)}{k!}, \quad (1.15)$$

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

$$\binom{n}{k} = 0 \quad \forall k \geq n + 1. \quad (1.16)$$

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

$$\begin{aligned} \binom{-n}{k} &= (-1)^k \frac{n(n+1) \cdots (n+k-1)}{k!} = \\ &= (-1)^k \frac{(n+k-1)!}{k!(n-1)!}, \end{aligned} \quad (1.17)$$

joten

$$\binom{-n}{k} = (-1)^k \binom{n+k-1}{k} \quad \forall k \geq 0. \quad (1.18)$$

## 1.1 Palautuskaava, Pascalin kolmio

**Lause 1.** Olkoon  $a \in \mathbb{C}$ . Tällöin

$$\binom{a+1}{k+1} = \binom{a}{k+1} + \binom{a}{k} \quad \forall k \in \mathbb{N}. \quad (1.19)$$

Erikoistapauksena saadaan Pascalin kolmion sääntö

**Lause 2.**

$$\binom{n+1}{k+1} = \binom{n}{k+1} + \binom{n}{k} \quad \forall k, n \in \mathbb{N}. \quad (1.20)$$

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

$$\begin{aligned} \binom{a}{k+1} + \binom{a}{k} &= \\ \frac{a(a-1) \cdots (a-(k+1)+1)}{(k+1)!} + \frac{a(a-1) \cdots (a-k+1)}{k!} &= \end{aligned}$$

$$\begin{aligned} & \frac{a(a-1)\cdots(a-k+1)(a-k)}{k!(k+1)} + \frac{a(a-1)\cdots(a-k+1)}{k!} = \\ & \frac{a(a-1)\cdots(a-k+1)}{k!} \left( \frac{a-k}{k+1} + 1 \right) = \\ & \frac{(a+1)(a+1-1)\cdots(a+1-(k+1)+1)}{(k+1)!} = \binom{a+1}{k+1}. \end{aligned} \quad (1.21)$$

Siis saatiin väitteen vasen puoli.  $\square$

Pascalin kolmion säännöllä voidaan todistaa

**Lause 3.**

$$\binom{n}{k} \in \mathbb{Z}^+ \quad \forall \quad 0 \leq k \leq n \in \mathbb{N}. \quad (1.22)$$

Todistus. Induktio  $n$ :n suhteen.

Aluksi  $n = 0, 1$ .

$$\binom{0}{0} = \binom{1}{0} = \binom{1}{1} = 1. \quad (1.23)$$

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

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

$$\binom{l+1}{k+1} = \binom{l}{k+1} + \binom{l}{k} \quad \forall \quad 1 \leq k+1 \leq l, \quad (1.24)$$

missä induktio-oletuksen nojalla oikea puoli  $\in \mathbb{Z}^+$ , joten

$$\binom{l+1}{k+1} \in \mathbb{Z}^+ \quad \forall \quad 1 \leq k+1 \leq l. \quad (1.25)$$

Lisäksi

$$\binom{l+1}{l+1} = \binom{l+1}{0} = 1. \quad \square \quad (1.26)$$

Tuloksen (1.22) nojalla

$$\frac{(n-k+1)(n-k+2)\cdots(n-1)n}{k!} \in \mathbb{Z}^+, \quad (1.27)$$

joten

$$k! \mid (n-k+1)(n-k+2)\cdots(n-1)n, \quad (1.28)$$

mistä saadaan.

**Lause 4.**

$$k! \mid (m+1)(m+2)\cdots(m+k) \quad \forall k, m \in \mathbb{N}. \quad (1.29)$$

Edelleen

**Lause 5.** Olkoon  $p \in \mathbb{P}$ , tällöin

$$p \mid \binom{p}{k} \quad \forall 1 \leq k \leq p-1. \quad (1.30)$$

Todistus. Tuloksen (1.28) nojalla

$$k! \mid (p-k+1)(p-k+2)\cdots(p-1)p, \quad (1.31)$$

Koska  $p \perp k!$ , niin (1.31) johtaa relaatioon

$$k! \mid (p-k+1)\cdots(p-1) = l \cdot k!, \quad (1.32)$$

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

$$\binom{p}{k} = \frac{(p-k+1)(p-k+2)\cdots(p-1)p}{k!} = \quad (1.33)$$

$$l \cdot p \equiv 0 \pmod{p}. \quad \square \quad (1.34)$$

## 1.2 Binomisarja, Binomikehitelmä

Sarjaa

$$(1+t)^a = \sum_{k=0}^{\infty} \binom{a}{k} t^k, \quad a \in \mathbb{C} \quad (1.35)$$

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

$$(1+t)^n = \sum_{k=0}^n \binom{n}{k} t^k. \quad (1.36)$$

Asetetaan  $t = A/B$ , jolloin yhtälöstä (1.36) saadaan Binomikehitelmä:

$$(A + B)^n = \sum_{k=0}^n \binom{n}{k} A^k B^{n-k} = \quad (1.37)$$

$$\sum_{\substack{k+l=n \\ 0 \leq k, l \leq n}} \frac{n!}{k!l!} A^k B^l. \quad (1.38)$$

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

$$\frac{1}{1-x} = \sum_{k=0}^{\infty} x^k. \quad (1.39)$$

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

$$\frac{1}{(1-x)^n} = \sum_{k=0}^{\infty} \binom{n+k-1}{k} x^k \quad (1.40)$$

identiteetin (1.18) nojalla.

## 2 $p$ -valuaatio

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

**Määritelmä 5.** Olkoot  $p \in \mathbb{P}$ ,  $k \in \mathbb{Z} \setminus \{0\}$ ,  $r \in \mathbb{N}$  ja

$$p^r \parallel k. \quad (2.1)$$

Tällöin asetetaan

$$v_p(k) = r. \quad (2.2)$$

Kertaa vielä, että

$$p^r \parallel k \Leftrightarrow k = p^r c, \quad p \nmid c \in \mathbb{Z} \setminus \{0\}. \quad (2.3)$$



**Lause 6.** Laskusääntöjä. Olkoon  $p \in \mathbb{P}$  ja  $n, m \in \mathbb{Z} \setminus \{0\}$ , tällöin

$$v_p(1) = 0; \quad (2.4)$$

$$v_p(n) \geq 0; \quad (2.5)$$

$$v_p(nm) = v_p(n) + v_p(m); \quad (2.6)$$

$$v_p(n!) = v_p(1) + v_p(2) + \dots + v_p(n), \quad n \geq 1; \quad (2.7)$$

$$n = \prod_{p|n} p^{v_p(n)} = \prod_{p \leq n} p^{v_p(n)} = \prod_{p \in \mathbb{P}} p^{v_p(n)}, \quad n \geq 1. \quad (2.8)$$

**Määritelmä 6.** Olkoot  $p \in \mathbb{P}$ ,  $k \in \mathbb{Z} \setminus \{0\}$ ,  $l \in \mathbb{Z}^+$ . Asetetaan tällöin

$$w_{p^l}(k) = 1 \quad \text{jos} \quad p^l | k; \quad (2.9)$$

$$w_{p^l}(k) = 0 \quad \text{jos} \quad p^l \nmid k. \quad (2.10)$$

**Lause 7.** Olkoot  $p \in \mathbb{P}$ ,  $k \in \mathbb{Z} \setminus \{0\}$ ,  $r \in \mathbb{N}$  ja  $v_p(k) = r$ . Tällöin

$$v_p(k) = \sum_{i=1}^r w_{p^i}(k) = \sum_{i=1}^{\infty} w_{p^i}(k). \quad (2.11)$$

**Lause 8.** Olkoot  $n \in \mathbb{Z}^+$  ja

$$A_p = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor, \quad p \in \mathbb{P}. \quad (2.12)$$

Tällöin

$$v_p(n!) = A_p. \quad (2.13)$$

$$p^{A_p} \parallel n! \quad \forall p | n!. \quad (2.14)$$

$$n! = \prod_{p \leq n} p^{A_p}. \quad (2.15)$$

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

Todistus. I osan tuloksen (4.26) nojalla välillä  $[1, n]$  olevien luvulla  $p^i$  jaollisten lukujen lkm=

$$\#\{k \in \mathbb{Z}^+ \mid 1 \leq k \leq n, p^i | k\} = \left\lfloor \frac{n}{p^i} \right\rfloor. \quad (2.16)$$

Toisaalta

$$\#\{k \in \mathbb{Z}^+ \mid 1 \leq k \leq n, p^i | k\} = w_{p^i}(1) + w_{p^i}(2) + \dots + w_{p^i}(n). \quad (2.17)$$

Esimerkiksi

$$1, \dots, 1 \cdot p, \dots, 2 \cdot p, \dots, p \cdot p, \dots, \left\lfloor \frac{n}{p} \right\rfloor \cdot p, \dots, n \quad (2.18)$$

missä pätee

$$w_p(1) = w_p(2) = \dots = w_p(p-1) = w_p(p+1) = \dots = 0 \quad (2.19)$$

$$w_p(p) = w_p(2p) = \dots = w_p\left(\left\lfloor \frac{n}{p} \right\rfloor p\right) = 1. \quad (2.20)$$

Olkoon

$$p^r \leq n < p^{r+1}, \quad \Rightarrow \quad \left\lfloor \frac{n}{p^{r+1}} \right\rfloor = 0. \quad (2.21)$$

Siten

$$w_p(1) + w_p(2) + \dots + w_p(n) = \left\lfloor \frac{n}{p} \right\rfloor; \quad (2.22)$$

$$w_{p^2}(1) + w_{p^2}(2) + \dots + w_{p^2}(n) = \left\lfloor \frac{n}{p^2} \right\rfloor; \quad (2.23)$$

...

$$w_{p^r}(1) + w_{p^r}(2) + \dots + w_{p^r}(n) = \left\lfloor \frac{n}{p^r} \right\rfloor, \quad (2.24)$$

Lasketaan yhtälöt (2.22–2.24) puolittain yhteen, jolloin saadaan

$$v_p(1) + v_p(2) + \dots + v_p(n) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \dots + \left\lfloor \frac{n}{p^r} \right\rfloor. \quad (2.25)$$

Siten

$$v_p(n!) = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor = A_p, \quad p \in \mathbb{P}. \quad (2.26)$$

Edelleen

$$n! = \prod_{p \leq n} p^{v_p(n!)}. \quad \square \quad (2.27)$$

**Huomautus 2.** Alkuluvulle  $p$  pätee

$$p|n! \Leftrightarrow p \leq n. \quad (2.28)$$

**Esimerkki 1.**

$v_2(11!)$ :

$k$	1	2	3	4	5	6	7	8	9	10	11	$\Sigma$
$w_{2^1}(k)$	0	1	0	1	0	1	0	1	0	1	0	5
$w_{2^2}(k)$	0	0	0	1	0	0	0	1	0	0	0	2
$w_{2^3}(k)$	0	0	0	0	0	0	0	1	0	0	0	1
$v_2(k)$	0	1	0	2	0	1	0	3	0	1	0	8

Toisaalta,  $2^3 \leq 11 < 2^4$ , joten  $r = 3$  ja

$$v_2(11!) = \sum_{i=1}^{\infty} \left\lfloor \frac{11}{2^i} \right\rfloor = \left\lfloor \frac{11}{2^1} \right\rfloor + \left\lfloor \frac{11}{2^2} \right\rfloor + \left\lfloor \frac{11}{2^3} \right\rfloor = 5 + 2 + 1 = 8.$$

Lauseen 4.3 todistus/2. tapa:

Kertomien alkutekijäkehitysten nojalla

$$\frac{n!}{k!(n-k)!} = \prod_{p \leq n} p^{B_p}, \quad (2.29)$$

missä

$$B_p = \sum_{i=1}^{\infty} \left[ \frac{n}{p^i} \right] - \left[ \frac{k}{p^i} \right] - \left[ \frac{n-k}{p^i} \right]. \quad (2.30)$$

Tuloksen (??)

$$\lfloor a \rfloor + \lfloor b \rfloor \leq \lfloor a + b \rfloor \quad (2.31)$$

avulla saadaan

$$\left\lfloor \frac{k}{p^i} \right\rfloor + \left\lfloor \frac{n-k}{p^i} \right\rfloor \leq \left\lfloor \frac{k}{p^i} + \frac{n-k}{p^i} \right\rfloor = \left\lfloor \frac{n}{p^i} \right\rfloor. \quad (2.32)$$

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

$$\prod_{p \leq n} p^{B_p} \in \mathbb{Z}^+, \quad (2.33)$$

joka identiteetin (2.29) kanssa todistaa, että

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

### 3 Rationaaliluvun jaollisuus (mod n)

#### 3.1 Perusteita

**Määritelmä 7.** Rationaaliluku  $A = a/b \in \mathbb{Q}^*$  on supistetussa muodossa/reduced form, kun  $a \perp b$ . Edelleen,  $\text{den}(A) = b$  on  $A$ :n nimittäjä/denominator.

**Määritelmä 8.** Olkoon  $p \in \mathbb{P}$ ,  $a, b \in \mathbb{Z}$ , ja  $a \perp b \neq 0$ . Silloin asetetaan

$$p \mid_{\mathbb{Q}} \frac{a}{b} \iff p \mid_{\mathbb{Z}} a \quad (3.1)$$

ja sanotaan, että  $p$  jakaa rationaaliluvun  $a/b$ .

**Huomautus 3.** Käytetään myös merkintää

$$p \left| \frac{a}{b} \right. . \quad (3.2)$$

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

$$\frac{a}{b} = p^r \frac{c}{d}, \quad c \in \mathbb{Z}, d \in \mathbb{Z}^+, c \perp d, p \nmid cd, r \in \mathbb{Z}. \quad (3.3)$$

Tällöin saadaan

**Lause 9.**

$$p \left| \frac{a}{b} \right. \Leftrightarrow r \geq 1. \quad (3.4)$$

**Määritelmä 9.** Olkoon  $p \in \mathbb{P}$ ,  $a, b \in \mathbb{Z}$  ja  $a \perp b \neq 0$ . Silloin asetetaan

$$\frac{a}{b} \equiv 0 \pmod{p} \Leftrightarrow p \left| \frac{a}{b} \right. \quad (3.5)$$

**Esimerkki 2.**

$$5 \left| \frac{20}{3} \right. \Leftrightarrow \frac{20}{3} \equiv 0 \pmod{5}. \quad (3.6)$$

**Esimerkki 3.**

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} = \frac{50}{4!} \equiv 0 \pmod{5}. \quad (3.7)$$

Laajennetaan Määritelmä 8 vapaasti valittavalle modulukselle  $n \in \mathbb{Z}_{\geq 2}$ .

**Määritelmä 10.** Olkoon  $n \in \mathbb{Z}_{\geq 2}$ ,  $a, b \in \mathbb{Z}$ , ja  $a \perp b \neq 0$ . Silloin asetetaan

$$n \left| \frac{a}{b} \right. \Leftrightarrow n \left| \frac{a}{b} \right. \Leftrightarrow n \left| a \right. \quad (3.8)$$

ja sanotaan, että  $n$  jakaa rationaaliluvun  $a/b$ .

**Huomautus 4.**

$$n \left| \frac{a}{b} \right. \Rightarrow n \perp b. \quad (3.9)$$

**Lause 10.**

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

$$\frac{a}{b} = \pm p_1^{r_1} \cdots p_k^{r_k} \cdot q_1^{v_1} \cdots q_l^{v_l}; \quad (3.10)$$

$$p_i, q_j \in \mathbb{P} \quad r_i \in \mathbb{Z}^+, \quad v_i \in \mathbb{Z}^-, \quad (3.11)$$

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

$$n = p_1^{s_1} \cdots p_k^{s_k}, \quad s_i \in \mathbb{N}, \quad (3.12)$$

ja

$$0 \leq s_i \leq r_i \quad \forall i = 1, \dots, k, \quad (3.13)$$

niin

$$n \mid_{\mathbb{Q}} \frac{a}{b}. \quad (3.14)$$

**Määritelmä 11.** Olkoon  $n \in \mathbb{Z}_{\geq 2}$  annettu ja  $a/b, c/d \in \mathbb{Q}$ . Jos

$$n \mid_{\mathbb{Q}} \frac{a}{b} - \frac{c}{d}, \quad (3.15)$$

niin asetetaan

$$\frac{a}{b} \equiv \frac{c}{d} \pmod{n} \quad (3.16)$$

ja sanotaan, että luvut  $a/b$  ja  $c/d$  ovat kongruenteja  $(\text{mod } n)$ .

**Huomautus 5.**

$$\frac{a}{b} \equiv 0 \pmod{n} \quad \Leftrightarrow \quad a \equiv 0 \pmod{n}, \quad b \perp n. \quad (3.17)$$

**Lause 11.** Olkoot  $n \in \mathbb{Z}_{\geq 2}$  ja  $a/b, c/d \in \mathbb{Q}$  sekä polynomi  $P(x) \in \mathbb{Q}[x]$ . Tällöin,

jos

$$\frac{a}{b} \equiv \frac{c}{d} \pmod{n}, \quad (3.18)$$

niin

$$P\left(\frac{a}{b}\right) \equiv P\left(\frac{c}{d}\right) \pmod{n}, \quad (3.19)$$

mikäli kongruenssi (3.19) on määritelty.

**Lause 12.** Olkoot  $n \in \mathbb{Z}_{\geq 2}$  ja  $a/b, c/d \in \mathbb{Q}$  sekä rationaalifunktio  $R(x) \in \mathbb{Q}(x)$ .

Tällöin, jos

$$\frac{a}{b} \equiv \frac{c}{d} \pmod{n}, \quad (3.20)$$

niin

$$R\left(\frac{a}{b}\right) \equiv R\left(\frac{c}{d}\right) \pmod{n}, \quad (3.21)$$

mikäli kongruenssi (3.21) on määritelty.

**Esimerkki 4.**

$$\frac{20}{3} = 2^2 \cdot 5^1 \cdot 3^{-1} \equiv 0 \pmod{2 \cdot 5}; \quad (3.22)$$

$$\frac{20}{3} \equiv 0 \pmod{20}, \quad (3.23)$$

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

**Esimerkki 5.**

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} = \frac{50}{4!} \equiv 0 \pmod{5^2}. \quad (3.24)$$

**Esimerkki 6.**

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} \equiv \frac{25}{7} \pmod{5^3}. \quad (3.25)$$

**Esimerkki 7.** Olkoon  $p \in \mathbb{P}, p \neq 5$ , tällöin

$$\frac{1}{p+5} \equiv \frac{1}{5} \pmod{p}. \quad (3.26)$$

Huomaa, että kongruenssi (3.26) ei ole määritelty  $\pmod{5}$ .

**Esimerkki 8.** Olkoon  $p \in \mathbb{P}$ , tällöin

$$(2p-1)(2p-2) \cdots (p+2)(p+1) \equiv$$

$$(p-1)(p-2) \cdots 2 \cdot 1 = (p-1)! \pmod{p}, \quad (3.27)$$

joten

$$\binom{2p}{p} = 2 \frac{(2p-1)(2p-2) \cdots (p+2)(p+1)}{(p-1)!} \equiv 2 \pmod{p}. \quad (3.28)$$

**Lause 13.** Kongruenssi  $\equiv \pmod{n}$  on ekvivalenssirelaatio joukossa

$$\left\{ \frac{c}{d} \in \mathbb{Q} \mid d \perp n \right\}.$$

### 3.2 Rengas $\mathbb{Q}_n$

**Määritelmä 12.** Olkoot  $n \in \mathbb{Z}_{\geq 2}$  ja  $a/b \in \mathbb{Q}$  annettu ja  $n \perp b$ . Tällöin

$$\overline{a/b} = \left\{ \frac{c}{d} \in \mathbb{Q} \mid \frac{c}{d} \equiv \frac{a}{b} \pmod{n} \right\} \quad (3.29)$$

on edustajan  $a/b$  määräämä jakojäännösluokka  $\pmod{n}$  ja

$$\mathbb{Q}_n = \{ \overline{a/b} \mid a/b \in \mathbb{Q}, n \perp b \}. \quad (3.30)$$

Asetetaan vielä laskutoimitukset (binary operations)

$$\begin{cases} \bar{x} + \bar{y} = \overline{x + y}, \\ \bar{x} \cdot \bar{y} = \overline{xy} \end{cases} \quad (3.31)$$

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

**Lause 14.**

a) Laskutoimitukset

$$\begin{cases} + : \mathbb{Q}_n \times \mathbb{Q}_n \rightarrow \mathbb{Q}_n, \end{cases} \quad (3.32)$$

ovat hyvinmääritellyjä (well defined) eli binäärioperaatiot ovat funktioita.

b). Nolla-alkio (zero) on

$$\bar{0} = \left\{ \frac{ln}{d} \mid l, d \in \mathbb{Z}, d \perp n \right\} \quad (3.33)$$

ja vasta-alkio

$$-\bar{x} = \overline{-x} \quad \forall \quad \bar{x} \in \mathbb{Q}_n. \quad (3.34)$$



c). Ykkösalkio (unity)

$$\bar{1} = \left\{ \frac{d + ln}{d} \mid l, d \in \mathbb{Z}, \quad d \perp n \right\} \quad (3.35)$$

ja käänteisalkio (inverse)

$$\bar{x}^{-1} = \overline{x^{-1}} \quad \forall \quad \bar{x}, \overline{x^{-1}} \in \mathbb{Q}_n. \quad (3.36)$$

d) Kolmikko  $(\mathbb{Q}_n, +, \cdot)$  muodostaa ykkösellisen kommutatiivisen renkaan.

**Lause 15.** Olkoon  $n \in \mathbb{Z}_{\geq 2}$ . Tällöin kuvaus

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

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

on rengasisomorfia eli

$$\mathbb{Q}_n \cong \mathbb{Z}_n. \quad (3.37)$$

Todistusta EI kysytä kokeessa.

Todistus: Laskemalla saadaan

1)

$$\begin{aligned} F\left(\frac{\bar{a}}{\bar{b}} + \frac{\bar{c}}{\bar{d}}\right) &= F\left(\frac{\overline{ad + bc}}{\bar{bd}}\right) = \\ \overline{ad + bc} (\bar{bd})^{-1} &= (\bar{a}\bar{d} + \bar{b}\bar{c}) (\bar{b})^{-1} (\bar{d})^{-1} = \\ \bar{a} (\bar{b})^{-1} + \bar{c} (\bar{d})^{-1} &= \end{aligned}$$

$$F\left(\frac{\bar{a}}{\bar{b}}\right) + F\left(\frac{\bar{c}}{\bar{d}}\right), \quad (3.38)$$

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

2)

$$F\left(\frac{\bar{a}}{\bar{b}} \cdot \frac{\bar{c}}{\bar{d}}\right) = F\left(\frac{\overline{ac}}{\bar{bd}}\right) =$$

$$\begin{aligned} \overline{ac} (\overline{bd})^{-1} &= \overline{a} (\overline{b})^{-1} \overline{c} (\overline{d})^{-1} = \\ &F \left( \frac{\overline{a}}{\overline{b}} \right) F \left( \frac{\overline{c}}{\overline{d}} \right). \end{aligned} \quad (3.39)$$

3)

$$F(\overline{1}) = F \left( \frac{\overline{1}}{\overline{1}} \right) = \overline{1} (\overline{1})^{-1} = \overline{1}. \quad (3.40)$$

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

4) Asetetaan nyt

$$F \left( \frac{\overline{a}}{\overline{b}} \right) = \overline{0}, \quad (3.41)$$

missä  $b \perp n$ , joten

$$\overline{a} (\overline{b})^{-1} = \overline{0}. \quad (3.42)$$

Kerrotaan 3.42 puolittain alkiolla  $\overline{b}$ , jolloin saadaan

$$\begin{aligned} \overline{a} (\overline{b})^{-1} \overline{b} &= \overline{0} \cdot \overline{b} \Rightarrow \overline{a} = \overline{0} \\ &\Rightarrow a \equiv 0 \pmod{n} \Rightarrow \frac{\overline{a}}{\overline{b}} = \overline{0}. \end{aligned} \quad (3.43)$$

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

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

$$F \left( \frac{\overline{a}}{\overline{b}} \right) = F \left( \frac{\overline{k}}{\overline{1}} \right) = \overline{k} (\overline{1})^{-1} = \overline{k}. \quad (3.44)$$

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

Kohtien 4) ja 5) nojalla

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

on bijektio ja edelleen rengasisomorfia.  $\square$

Siten  $\mathbb{Q}_n$  ja  $\mathbb{Z}_n$  voidaan samaistaa/can be identified, jolloin merkitään

$$\mathbb{Q}_n \ni \overline{a/b} = \overline{a}(\overline{b})^{-1} \in \mathbb{Z}_n. \quad (3.45)$$

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

$$\frac{2}{3} \equiv \frac{2 + l \cdot 7}{3} \pmod{7} \quad \forall l \in \mathbb{Z}. \quad (3.46)$$

Valitaan  $l = 4$ , jolloin

$$\frac{2}{3} \equiv \frac{2 + 4 \cdot 7}{3} = 10 \equiv 3 \pmod{7}. \quad (3.47)$$

Täten

$$\overline{2/3} = \overline{3}. \quad (3.48)$$

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

$$\overline{2} \cdot \overline{3}^{-1} = \overline{2} \cdot \overline{5} = \overline{10} = \overline{3}. \quad (3.49)$$

### 3.3 Sovelluksia

**Lemma 1.** Olkoon  $G$  ryhmä ja  $a \in G$ . Tällöin kuvaukset

$$\iota : G \rightarrow G, \quad \iota(x) = x^{-1} \quad (3.50)$$

ja

$$\tau : G \rightarrow G, \quad \tau(x) = ax \quad (3.51)$$

ovat bijektioita.

Todistus. Kohta (3.50): Asetetaan

$$\iota(x_1) = \iota(x_2) \Leftrightarrow x_1^{-1} = x_2^{-1}, \quad (3.52)$$

josta saadaan  $x_1 = x_2$ . Siten  $\iota$  on injektio.

Olkoon sitten  $y \in G$  annettu. Valitaan nyt  $x = y^{-1}$ , jolloin

$$\iota(x) = \iota(y^{-1}) = (y^{-1})^{-1} = y. \quad (3.53)$$

Täten  $\iota$  on surjektio ja edelleen bijektio. □

**Seuraus 1.** Olkoon

$$H = \{a_1, \dots, a_m\} \quad (3.54)$$

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

$$\{a_1^{-1}, \dots, a_m^{-1}\} = \{a_1, \dots, a_m\}. \quad (3.55)$$

Edelleen, olkoon  $a \in H$  annettu. Tällöin  $\tau(H) = H$  eli

$$\{a \cdot a_1, \dots, a \cdot a_m\} = \{a_1, \dots, a_m\}. \quad (3.56)$$

### 3.3.1 Wilsonin lause

**Lause 16.** WILSONIN LAUSE: Olkoon  $p \in \mathbb{P}$ . Tällöin

$$(p-1)! \equiv -1 \pmod{p}. \quad (3.57)$$

**Esimerkki 9.** Olkoon  $H = \mathbb{Z}_{11}^*$ , missä

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

$$6^{-1} = 2, 7^{-1} = 8, 8^{-1} = 7, 9^{-1} = 5, 10^{-1} = 10. \quad (3.58)$$

Siten

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

$$1 \cdot 2 \cdot 2^{-1} \cdot 3 \cdot 3^{-1} \cdot 5 \cdot 5^{-1} \cdot 7 \cdot 7^{-1} \cdot 10 = -1. \quad (3.59)$$

**Lause 17.** Olkoon  $p \in \mathbb{P}_{\geq 3}$ . Tällöin

$$1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{p-1} \equiv 0 \pmod{p}. \quad (3.60)$$

Todistus. Lemman 3.50 nojalla  $\iota(\mathbb{Z}_p^*) = \mathbb{Z}_p^*$  eli

$$\{\bar{1}^{-1}, \dots, \overline{p-1}^{-1}\} = \{\bar{1}, \dots, \overline{p-1}\}. \quad (3.61)$$

Täten

$$\sum_{a=1}^{p-1} \bar{a}^{-1} = \sum_{b=1}^{p-1} \bar{b}, \quad (3.62)$$

Seuraavassa käytetään samaistusta (3.45).

Yhtälön V.P. (vasen puoli)=

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

$$\bar{1} + \overline{1/2} + \dots + \overline{1/(p-1)} = \overline{1 + 1/2 + \dots + 1/(p-1)}. \quad (3.63)$$

Toisaalta Yhtälön O.P. (oikea puoli)=

$$\bar{1} + \dots + \overline{p-1} = \overline{1 + 2 + \dots + p-1} = \overline{p(p-1)/2} = \bar{0}, \quad (3.64)$$

missä  $p|p(p-1)/2$ , sillä  $p \geq 3$ . Ekvivalenssiluokkien (3.63) ja (3.64) identtisyydestä seuraa edustajien välinen kongruenssi (3.60).  $\square$

### 3.3.2 Euler-Fermat

**Lause 18.** Olkoot  $a \in \mathbb{Z}$ ,  $m \in \mathbb{Z}_{\geq 2}$  annettu ja  $a \perp m$ . Tällöin

$$a^{\varphi(m)} \equiv 1 \pmod{m}. \quad (3.65)$$

Seurauksena saadaan

**Lause 19.** FERMAT'N PIKKULAUSE: Olkoot  $a \in \mathbb{Z}$ ,  $p \in \mathbb{P}$  annettu ja  $p \nmid a$ .

Tällöin

$$a^{p-1} \equiv 1 \pmod{p}. \quad (3.66)$$

### 3.3.3 Euler-Fermat'n todistus

Todistus. Asetetaan  $\tau(\bar{x}) = \bar{a} \cdot \bar{x}$ . Koska  $\bar{a} \in \mathbb{Z}_m^*$ , niin Lemman 3.50 nojalla  $\tau(\mathbb{Z}_m^*) = \mathbb{Z}_m^*$  eli

$$\{\bar{a} \cdot \bar{a}_1, \dots, \bar{a} \cdot \overline{a_{\varphi(m)}}\} = \{\bar{a}_1, \dots, \overline{a_{\varphi(m)}}\}. \quad (3.67)$$

Siten

$$\bar{a} \cdot \bar{a}_1 \cdots \bar{a} \cdot \overline{a_{\varphi(m)}} = \bar{a}_1 \cdots \overline{a_{\varphi(m)}} \Leftrightarrow \quad (3.68)$$

$$\bar{a}^{\varphi(m)} \bar{a}_1 \cdots \overline{a_{\varphi(m)}} = \bar{a}_1 \cdots \overline{a_{\varphi(m)}}, \quad (3.69)$$

josta

$$\overline{a^{\varphi(m)}} = \bar{1}. \quad \square \quad (3.70)$$

Todistetaan seuraavaksi eräs Wilsonin lauseen yleistys.

**Lause 20.** Olkoot  $p \in \mathbb{P}_{\geq 3}$  ja  $r \in \mathbb{Z}^+$ . Tällöin

$$\prod_{k=1, p \nmid k}^{p^r-1} k \equiv -1 \pmod{p^r}. \quad (3.71)$$

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

$$\bar{a} = \bar{a}^{-1} \Leftrightarrow \bar{a}^2 = \bar{1}. \quad (3.72)$$

Siten

$$\overline{a^2 - 1} = \bar{0}, \quad (3.73)$$

josta

$$(a-1)(a+1) = l \cdot p^r, \quad (3.74)$$

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

$$p|a-1 \quad \text{tai} \quad p|a+1. \quad (3.75)$$

Jos

$$p|a - 1 \quad \text{ja} \quad p|a + 1, \quad (3.76)$$

niin

$$p|2a \Rightarrow p|a. \quad (3.77)$$

Mutta  $a \perp p$ , joten joudutaan ristiriitaan.

Tarkastellaan siis tapaukset

$$1.) \quad p|a - 1 \quad \text{ja} \quad p \nmid a + 1 \quad (3.78)$$

ja

$$2.) \quad p \nmid a - 1 \quad \text{ja} \quad p|a + 1. \quad (3.79)$$

Tapaus 1. Yhtälön (3.74) nojalla

$$p^r|a - 1 \Rightarrow \bar{a} = \bar{1}. \quad (3.80)$$

Tapaus 2. Yhtälön (3.74) nojalla

$$p^r|a + 1 \Rightarrow \bar{a} = -\bar{1}. \quad (3.81)$$

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

Edelleen

$$\mathbb{Z}_{p^r}^* = \{\bar{1}, -\bar{1}\} \cup B, \quad (3.82)$$

missä joukon

$$B = \{\bar{b}_1, \dots, \bar{b}_m\}, \quad m = \varphi(p^r) - 2, \quad (3.83)$$

alkioille pätee

$$\bar{b}_i^{-1} \neq \bar{b}_i, \quad i = 1, \dots, m. \quad (3.84)$$

Täten

$$B = \{\bar{c}_1, \dots, \bar{c}_{m/2}, \bar{c}_1^{-1}, \dots, \bar{c}_{m/2}^{-1}\} \quad (3.85)$$

ja siten

$$\prod_{\bar{a} \in \mathbb{Z}_p^*} \bar{a} = \bar{1}(-\bar{1})\bar{c}_1 \bar{c}_1^{-1} \cdots \bar{c}_{m/2} \bar{c}_{m/2}^{-1} = -\bar{1}. \quad \square \quad (3.86)$$

**Esimerkki 10.**  $3^2 = p^r$ . Jolloin

$$1 \cdot 2 \cdot 4 \cdot 5 \cdot 7 \cdot 8 \equiv -1 \pmod{3^2}. \quad (3.87)$$

### 3.4 Wolstenholmen lause

**Lause 21.** WOLSTENHOLMEN LAUSE: Olkoon  $p \in \mathbb{P}_{\geq 5}$ . Tällöin

$$1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{p-1} \equiv 0 \pmod{p^2}. \quad (3.88)$$

(Tätä todistusta EI kysytä kokeessa.)

Todistus, I tapa:

Tarkastellaan polynomia

$$G(x) = (x-1)(x-2)\cdots(x-(p-1)) \in \mathbb{Z}[x]. \quad (3.89)$$

Aukaistaan tulo, jolloin

$$\begin{aligned} G(x) &= x^{p-1} - W_{p-2}x^{p-2} + W_{p-3}x^{p-3} - \dots \\ &\quad + W_2x^2 - W_1x + W_0, \end{aligned} \quad (3.90)$$

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

$$\begin{aligned} x(x-1)(x-2)\cdots(x-(p-1)) &= \\ x^p - W_{p-2}x^{p-1} + W_{p-3}x^{p-2} - W_{p-4}x^{p-3} + \dots \\ &\quad + W_2x^3 - W_1x^2 + W_0x, \end{aligned} \quad (3.91)$$



johon sijoitetaan  $x = y - 1$  ja siten

$$\begin{aligned}
& (y-1)(y-2)\cdots(y-(p-1))(y-p) = (y-1)^p \\
& -W_{p-2}(y-1)^{p-1} + W_{p-3}(y-1)^{p-2} - W_{p-4}(y-1)^{p-3} + \dots \\
& +W_2(y-1)^3 - W_1(y-1)^2 + W_0(y-1).
\end{aligned} \tag{3.92}$$

Yhtälössä (3.92) V.P.=

$$\begin{aligned}
(y-p)G(y) &= (y-p)(y^{p-1} - W_{p-2}y^{p-2} + W_{p-3}y^{p-3} - \dots \\
& +W_2y^2 - W_1y + W_0) = \\
& y^p - (p + W_{p-2})y^{p-1} + (pW_{p-2} + W_{p-3})y^{p-2} \\
& - (pW_{p-3} + W_{p-4})y^{p-3} + \dots \\
& - (pW_2 + W_1)y^2 + (pW_1 + W_0)y - pW_0.
\end{aligned} \tag{3.93}$$

Toisaalta yhtälön (3.92) O.P.=

$$\begin{aligned}
y^p &- \left( \binom{p}{1} + W_{p-2} \right) y^{p-1} + \left( \binom{p}{2} + W_{p-2} \binom{p-1}{1} + W_{p-3} \right) y^{p-2} \\
&- \left( \binom{p}{3} + W_{p-2} \binom{p-1}{2} + W_{p-3} \binom{p-2}{1} + W_{p-4} \right) y^{p-3} \\
&+ \dots + \left( \binom{p}{p-1} + W_{p-2} \binom{p-1}{p-2} + \dots + W_1 \binom{2}{1} + W_0 \right) y \\
&- (1 + W_{p-2} + \dots + W_1 + W_0).
\end{aligned} \tag{3.94}$$

Verrataan seuraavaksi vastinpotenssien kertoimia yhtälöissä (3.93) ja (3.94), jolloin

$$y^p : \quad 1 = 1, \tag{3.95}$$

$$y^{p-1} : \quad p + W_{p-2} = \binom{p}{1} + W_{p-2}, \quad (3.96)$$

$$y^{p-2} : \quad pW_{p-2} + W_{p-3} = \binom{p}{2} + W_{p-2} \binom{p-1}{1} + W_{p-3}, \quad (3.97)$$

$$y^{p-3} : \quad pW_{p-3} + W_{p-4} = \binom{p}{3} + W_{p-2} \binom{p-1}{2} + W_{p-3} \binom{p-2}{1} + W_{p-4}, \quad (3.98)$$

...

$$y^1 : \quad pW_1 + W_0 = \binom{p}{p-1} + W_{p-2} \binom{p-1}{p-2} + \dots + W_1 \binom{2}{1} + W_0, \quad (3.99)$$

$$y^0 : \quad pW_0 = 1 + W_{p-2} + \dots + W_1 + W_0. \quad (3.100)$$

Kaksi ensimmäistä ovat triviaali-identiteettejä mutta seuraavista saadaan palautuskaavat:

$$W_{p-2} = \binom{p}{2}, \quad (3.101)$$

$$2W_{p-3} = \binom{p}{3} + \binom{p-1}{2} W_{p-2}, \quad (3.102)$$

$$3W_{p-4} = \binom{p}{4} + \binom{p-1}{3} W_{p-2} + \binom{p-2}{2} W_{p-3}, \dots \quad (3.103)$$

$$(p-2)W_1 = \binom{p}{p-1} + \binom{p-1}{p-2} W_{p-2} + \dots + \binom{3}{2} W_2, \quad (3.104)$$

$$(p-1)W_0 = 1 + W_{p-2} + \dots + W_1. \quad (3.105)$$

Huomaa, että nämä yhtälöt ovat muotoa

$$jW_{p-j-1} = \binom{p}{j+1} + \dots \quad \forall \quad 1 \leq j \leq p-1. \quad (3.106)$$

Käytetään tulosta (1.30), jolloin

$$p \mid \binom{p}{2} \quad (3.107)$$

ja siten

$$j = 1. \quad p \mid W_{p-2}. \quad (3.108)$$

Seuraavaksi

$$p \mid \binom{p}{3} \quad \text{ja} \quad p \mid W_{p-2}, \quad (3.109)$$

joten

$$j = 2. \quad p \mid W_{p-3}. \quad (3.110)$$

Edelleen

$$p \mid \binom{p}{4}, \quad p \mid W_{p-2} \quad \text{ja} \quad p \mid W_{p-3}, \quad (3.111)$$

joten

$$j = 3. \quad p \mid W_{p-4}. \quad (3.112)$$

...

$$j = p-2. \quad p \mid W_1. \quad (3.113)$$

Siten

$$p \mid W_1, W_2, \dots, W_{p-2}, \quad (3.114)$$

josta tuloksen (3.105) kanssa seuraa

$$j = p-1. \quad (p-1)W_0 \equiv 1 \pmod{p} \quad (3.115)$$

eli

$$W_0 \equiv -1 \pmod{p}. \quad (3.116)$$

Mutta

$$W_0 = (p-1)!, \quad (3.117)$$

joten saadaan II todistus Wilsonin lauseelle.

Sijoitetaan nyt  $x = p$  yhtälöön

$$G(x) = \prod_{j=1}^{p-1} (x-j) = \sum_{i=0}^{p-1} (-1)^i W_i x^i, \quad W_{p-1} = 1, \quad (3.118)$$

josta saadaan

$$W_1 = W_2 p - W_3 p^2 - \dots + p^{p-2}. \quad (3.119)$$

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

$$p^2|W_1. \quad (3.120)$$

Toisaalta

$$\begin{aligned} W_1 &= \sum_{j=1}^{p-1} \prod_{i=1, i \neq j}^{p-1} i = \\ &= 2 \cdot 3 \cdots (p-1) + 1 \cdot 3 \cdot 4 \cdots (p-1) + \dots \\ &+ 1 \cdot 2 \cdots (p-3) \cdot (p-1) + 1 \cdot 2 \cdots (p-2) = \\ &= (p-1)! \left( 1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{p-1} \right). \end{aligned} \quad (3.121)$$

Siten

$$p^2 \left| 1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{p-1} \right. \quad \square \quad (3.122)$$

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

$$a \equiv j \pmod{p}, \quad (3.123)$$

jollakin  $j = 1, 2, \dots, p-1$ . Sijoitetaan  $x = a$  yhtälöön (3.118), jolloin

$$a^{p-1} - W_{p-2}a^{p-2} + W_{p-3}a^{p-3} - \dots + W_2a^2 - W_1a + W_0 \equiv 0 \pmod{p}, \quad (3.124)$$

missä

$$W_{p-2}, \dots, W_1 \equiv 0 \pmod{p}. \quad (3.125)$$

Siten

$$a^{p-1} \equiv -W_0 \equiv -(p-1)! \equiv 1 \pmod{p}. \quad \square \quad (3.126)$$

### 3.5 $(p-1)!$ ja $a^{p-1} \pmod{p^2}$ /EI kokeeseen

Tiedetään, että

$$(p-1)! \equiv -1 \pmod{p^2}, \quad (3.127)$$

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

$$a^{p-1} \equiv 1 \pmod{p^2}, \quad (3.128)$$

kun  $p = 1093, 3511, \dots$ . Mutta yleisellä tasolla kohtien (3.127) ja (3.128) jakojäännöksen  $\pmod{p^2}$  käyttäytymistä ei tunneta.

Ehdon (3.128) tutkiminen on ollut tärkeää liittyen Fermat'n suuren lauseen todistusyrityksiin, sillä jos  $p \in \mathbb{P}_{\geq 3}$  ja

$$2^{p-1} \not\equiv 1 \pmod{p^2}, \quad (3.129)$$

niin

$$x^p + y^p \neq z^p \quad \forall \quad x, y, z \in \mathbb{Z}^+. \quad (3.130)$$

Tosin Andre Wiles [Annals of Mathematics 141 (1994)] on todistanut, että (3.130) pätee ilman lisäoletusta (3.129). Wilesin todistus perustuu mm. elliptisten käyrien ominaisuuksiin.

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

$$2^{p-1} - 1 = l \cdot p, \quad (3.131)$$

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

$$q_p(2) = \frac{2^{p-1} - 1}{p} \in \mathbb{Z}. \quad (3.132)$$

**Lause 22.** Olkoon  $p \in \mathbb{P}_{\geq 3}$ . Tällöin

$$q_p(2) = \frac{2^{p-1} - 1}{p} \equiv 1 + \frac{1}{3} + \frac{1}{5} + \dots + \frac{1}{p-2} \pmod{p}. \quad (3.133)$$

Huomaa, että (3.133) on yhtäpitävää ehdon

$$2^{p-1} \equiv 1 + p \left( 1 + \frac{1}{3} + \frac{1}{5} + \dots + \frac{1}{p-2} \right) \pmod{p^2} \quad (3.134)$$

kanssa.

Todistus. Aluksi binomikaavalla saadaan

$$2^p = \sum_{i=0}^p \binom{p}{i} = 2 + \sum_{i=1}^{p-1} \binom{p}{i}, \quad (3.135)$$

jossa tuloksen (1.30) nojalla

$$\binom{p}{i} = ph_i, \quad (3.136)$$

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

$$\begin{aligned} h_i &= \frac{(p-1)(p-2)\cdots(p-i+1)}{i!} \equiv \\ & \frac{(-1)^{i-1}(i-1)!}{i!} = \frac{(-1)^{i-1}}{i} \pmod{p} \end{aligned} \quad (3.137)$$

eli

$$h_i = \frac{(-1)^{i-1}}{i} + m_i p, \quad (3.138)$$

jollakin  $m_i = a/b \in \mathbb{Q}$ ,  $p \nmid b$ .

Siten (3.136) ja (3.138) antavat

$$\binom{p}{i} = p \left( \frac{(-1)^{i-1}}{i} + m_i p \right) \equiv (-1)^{i-1} \frac{p}{i} \pmod{p^2}. \quad (3.139)$$

Yhtälöiden (3.135) ja (3.139) nojalla

$$2^p \equiv 2 + p \left( 1 - \frac{1}{2} + \frac{1}{3} - \dots + \frac{1}{p-2} - \frac{1}{p-1} \right) \pmod{p^2}. \quad (3.140)$$

Toisaalta

$$\begin{aligned} & 1 - \frac{1}{2} + \frac{1}{3} - \dots + \frac{1}{p-2} - \frac{1}{p-1} = \\ & \quad 2 \left( 1 + \frac{1}{3} + \frac{1}{5} + \dots + \frac{1}{p-2} \right) \\ & \quad - \left( 1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{p-2} + \frac{1}{p-1} \right) \\ & \equiv 2 \left( 1 + \frac{1}{3} + \frac{1}{5} + \dots + \frac{1}{p-2} \right) \pmod{p^2} \end{aligned} \quad (3.141)$$

tuloksen (3.88) nojalla.

Yhdistämällä (3.140) ja (3.141) saadaan

$$2^p \equiv 2 + 2p \left( 1 + \frac{1}{3} + \frac{1}{5} + \dots + \frac{1}{p-2} \right) \pmod{p^2}, \quad (3.142)$$

missä  $p \nmid 2$ , joten (3.134) seuraa.  $\square$

**Esimerkki 11.** Olkoon  $p = 7$ . Nyt

$$2^{p-1} = 2^6 = 1 + 63 = 1 + 7 \cdot 9 \equiv \quad (3.143)$$

$$1 + 7 \left( 1 + \frac{1}{3} + \frac{1}{5} \right) \pmod{7^2}. \quad (3.144)$$

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

## 4 Polynomien kongruenssi

**Määritelmä 13.** 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

$$P(x) \equiv Q(x) \pmod{n} \Leftrightarrow$$

$$p_k \equiv q_k \pmod{n} \quad \forall k = 0, 1, \dots, n. \quad (4.1)$$

Seuraavassa käytetään jakojäännösluokkia  $\bar{a} \in \mathbb{Z}_n$ . Huomaa, että kun  $p \in \mathbb{P}$ , niin  $\mathbb{Z}_p$  on kunta.

**Määritelmä 14.** Olkoon  $n \in \mathbb{Z}_{\geq 2}$  ja  $a(x) = a_0 + a_1x + \dots + a_dx^d \in \mathbb{Z}[x]$ . Kuvaus

$$r_n(a_0 + a_1x + \dots + a_dx^d) = \bar{a}_0 + \bar{a}_1x + \dots + \bar{a}_dx^d \quad (4.2)$$

$$r_n : \mathbb{Z}[x] \rightarrow \mathbb{Z}_n[x], \quad r_n(a(x)) = \bar{a}(x),$$

on reduktio  $\pmod{n}$ .

**Lause 23.** Reduktio

$$r_n : \mathbb{Z}[x] \rightarrow \mathbb{Z}_n[x], \quad r_n(a(x)) = \bar{a}(x),$$

on rengasmorfismi.

**Lause 24.**

$$\bar{a}_0 + \dots + \bar{a}_dx^d = \bar{b}_0 + \dots + \bar{b}_dx^d \Leftrightarrow \quad (4.3)$$

$$a_0 + \dots + a_dx^d \equiv b_0 + \dots + b_dx^d \pmod{n} \quad (4.4)$$



**Lause 25.** WOLSTENHOLMEN LAUSE: Olkoon  $p \in \mathbb{P}_{\geq 5}$ . Tällöin

$$1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{p-1} \equiv 0 \pmod{p^2}. \quad (4.5)$$

II Todistus. Tämä todistus nojautuu Fermat'n pikkulauseeseen 19.

Tarkastellaan polynomeja

$$G(x) = (x-1)(x-2)\cdots(x-(p-1)) \in \mathbb{Z}[x]; \quad (4.6)$$

$$F(x) = x^{p-1} - 1 \in \mathbb{Z}[x] \quad (4.7)$$

ja niiden reduktioita  $\pmod{p}$

$$\overline{G}(x), \overline{F}(x) \in \mathbb{Z}_p[x]. \quad (4.8)$$

Välittömästi Fermat'n pikkulauseeseen 19 nojalla

$$\overline{F}(\overline{j}) \stackrel{19}{\equiv} \overline{0}, \quad \forall j = 1, 2, \dots, p-1. \quad (4.9)$$

Täten  $\overline{F}(x)$  jakaantuu polynomirenkaassa  $\mathbb{Z}_p[x]$  tekijöihin seuraavasti

$$\overline{F}(x) = (x - \overline{1})(x - \overline{2})\cdots(x - \overline{p-1}) = \overline{G}(x) \quad (4.10)$$

polynomialgebran tulosten nojalla (Katso: Merkintöjä ja algebrallisia rakenteita).

Kirjoitetaan  $G(x)$  auki polynomiksi

$$G(x) = \prod_{j=1}^{p-1} (x-j) = \sum_{i=0}^{p-1} (-1)^i W_i x^i = \quad (4.11)$$

$$x^{p-1} - W_{p-2}x^{p-2} + W_{p-3}x^{p-3} - \dots + W_2x^2 - W_1x + W_0, \quad W_{p-1} = 1.$$

Tuloksen (4.10) nojalla

$$x^{p-1} - W_{p-2}x^{p-2} + W_{p-3}x^{p-3} - \dots$$

$$+W_2x^2 - W_1x + W_0 \equiv x^{p-1} - 1 \pmod{p}. \quad (4.12)$$

eli

$$W_k \equiv 0 \pmod{p}, \quad k = 1, 2, \dots, p-2, \quad W_0 \equiv -1 \pmod{p}. \quad (4.13)$$

Siirrytään takaisin polynomirenkaaseen  $\mathbb{Z}[x]$  ja aukaistaan (4.11):

$$(x-1)(x-2)\cdots(x-(p-2))(x-(p-1)) = \quad (4.14)$$

$$x^{p-1} - W_{p-2}x^{p-2} + W_{p-3}x^{p-3} - \dots + W_2x^2 - W_1x + (p-1)!.$$

Sijoitetaan  $x = p$  yhtälöön (4.14), jolloin

$$(p-1)! = p^{p-1} - W_{p-2}p^{p-2} + W_{p-3}p^{p-3} - \dots + W_2p^2 - W_1p + (p-1)!. \quad (4.15)$$

Tällöin saadaan

$$W_1 = W_2p - W_3p^2 + \dots - W_{p-2}p^{p-3} + p^{p-2}. \quad (4.16)$$

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

$$p^2|W_1. \quad (4.17)$$

Toisaalta

$$\begin{aligned} W_1 &= \sum_{j=1}^{p-1} \prod_{i=1, i \neq j}^{p-1} i = \\ &= 2 \cdot 3 \cdots (p-1) + 1 \cdot 3 \cdot 4 \cdots (p-1) + \dots \\ &+ 1 \cdot 2 \cdots (p-3) \cdot (p-1) + 1 \cdot 2 \cdots (p-2) = \\ &(p-1)! \left( 1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{p-1} \right). \end{aligned} \quad (4.18)$$

Siten

$$p^2 \left| 1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{p-1} \right. \quad \square \quad (4.19)$$

**Esimerkki 12.** $p = 5$ .

$$\begin{aligned}
G(x) &= \prod_{j=1}^4 (x - j) = \\
&= x^4 - W_3x^3 + W_2x^2 - W_1x + W_0, \\
W_3 &= 4 + 3 + 2 + 1, \\
W_2 &= 3 \cdot 4 + 2 \cdot 4 + 1 \cdot 4 + 2 \cdot 3 + 1 \cdot 3 + 1 \cdot 2, \\
W_1 &= 2 \cdot 3 \cdot 4 + 1 \cdot 3 \cdot 4 + 1 \cdot 2 \cdot 4 + 1 \cdot 2 \cdot 3, \\
W_0 &= 4!.
\end{aligned} \tag{4.20}$$

ja

$$\begin{aligned}
W_1 = 50 &= 4! \left(1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4}\right), \quad 5^2 \perp 4! \\
&\Rightarrow 5^2 \parallel \left(1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4}\right). \tag{4.21}
\end{aligned}$$

**Esimerkki 13.** Tapauksessa  $p = 3$  lauseen väite ei päde kuten nähdään seuraavasta:

$$\begin{aligned}
G(x) &= \prod_{j=1}^2 (x - j) = x^2 - W_1x + W_0 = x^2 - 3x + 2, \\
W_1 = 3 &= 2! \left(1 + \frac{1}{2}\right), \quad \Rightarrow \quad 3 \parallel \left(1 + \frac{1}{2}\right). \tag{4.22}
\end{aligned}$$

Terävöitetään Esimerkin 8 tulosta.

**Esimerkki 14.**Olkoon  $p \in \mathbb{P}_{p \geq 5}$ , tällöin

$$\binom{2p}{p} = 2 \frac{(2p-1)(2p-2) \cdots (p+2)(p+1)}{(p-1)!} \equiv 2 \pmod{p^3}. \tag{4.23}$$

Todistus. Kerrataan aluksi, että  $W_1 = v_1 p^2$  ja  $W_k = v_k p$ , missä  $v_k \in \mathbb{Z}$  aina, kun  $k = 1, \dots, k-2$ . Sijoitetaan nyt  $x = 2p$  yhtälöön (4.14), jolloin

$$\begin{aligned}
(2p-1)(2p-2)\cdots(p+2)(p+1) &= \\
(2p)^{p-1} - W_{p-2}(2p)^{p-2} + \dots + W_2(2p)^2 - W_1 2p + (p-1)! &= \\
(2p)^{p-1} - v_{p-2}(2)^{p-2} p^{p-1} + \dots + v_2(2)^2 p^3 - v_1 2p^3 + (p-1)! &\equiv \\
(p-1)! \pmod{p^3}. &\quad \square \quad (4.24)
\end{aligned}$$

**Lause 26.** Olkoon  $p \in \mathbb{P}$ , tällöin

$$(x+1)^p \equiv x^p + 1 \pmod{p}. \quad (4.25)$$

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

Todistus. Binomisarjan ja Lauseen 4.5 nojalla

$$(x+1)^p = \sum_{k=0}^p \binom{p}{k} x^k \equiv \quad (4.26)$$

$$x^p + 0 \cdot x^{p-1} + 0 \cdot x^{p-2} + \dots + 0 \cdot x + 1 = x^p + 1 \pmod{p}. \quad \square$$

**Lause 27.** Olkoot  $n \in \mathbb{Z}_{\geq 2}$  ja  $f(x), g(x), h(x) \in \mathbb{Q}[x]$  ja

$$g(x) \equiv h(x) \pmod{n}. \quad (4.27)$$

Tällöin

$$f(g(x)) \equiv f(h(x)) \pmod{n}. \quad (4.28)$$

**Lause 28.** Olkoot  $p \in \mathbb{P}$  ja  $r \in \mathbb{N}$ . Tällöin

$$(x+1)^{p^r} \equiv x^{p^r} + 1 \pmod{p}. \quad (4.29)$$

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

Todistus. Induktiolla.  $r = 1$ .  $\Leftrightarrow$  Lause 26.

Induktioaskeleessa lasketaan V.P.=

$$(x + 1)^{p^{r+1}} = ((x + 1)^{p^r})^p \equiv (x^{p^r} + 1)^p \quad (4.30)$$

$$\equiv (x^{p^r})^p + 1 = x^{p^{r+1}} + 1 \pmod{p} \quad (4.31)$$

=O.P. Kohdassa (4.30) sovellettiin induktio-oletusta ja Lausetta 27 sekä kohdassa (4.30) Lausetta 26.  $\square$

Seurauksena saadaan

**Lause 29.** Olkoot  $p \in \mathbb{P}$  ja  $r \in \mathbb{Z}^+$ . Tällöin

$$\binom{p^r}{k} \equiv 0 \pmod{p} \quad \forall k = 1, \dots, p^r - 1. \quad (4.32)$$

Lause 28 voidaan yleistää kahdenmuuttujan polynomeille.

**Lause 30.** Olkoot  $p \in \mathbb{P}$  ja  $r \in \mathbb{N}$ . Tällöin

$$(x + y)^{p^r} \equiv x^{p^r} + y^{p^r} \pmod{p} \quad (4.33)$$

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

Ja edelleen useanmuuttujan tapaukseen.

**Lause 31.** Olkoot  $p \in \mathbb{P}$  ja  $r \in \mathbb{N}$ . Tällöin

$$(x_1 + \dots + x_m)^{p^r} \equiv x_1^{p^r} + \dots + x_m^{p^r} \pmod{p} \quad (4.34)$$

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

## 4.1 Sovelluksia lukujen kongruensseihin

**Määritelmä 15.** Olkoon  $p \in \mathbb{P}$  ja

$$A = \frac{a}{b} = p^r \frac{c}{d}, \quad p \nmid cd. \quad (4.35)$$

Tällöin asetetaan

$$v_p(A) = r, \quad (4.36)$$

joka on luvun  $A$  eksponentiaalinen  $p$ -valuaatio.

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

Sovelletaan Lausetta 31 antamalle muuttujille rationaalilukuarvot.

**Lause 32.** Olkoot  $p \in \mathbb{P}$ ,  $r \in \mathbb{N}$  ja  $A_i \in \mathbb{Q}$ ,  $v_p(A_i) \geq 0$  aina, kun  $i = 1, \dots, m$ .

Tällöin

$$(A_1 + \dots + A_m)^{p^r} \equiv A_1^{p^r} + \dots + A_m^{p^r} \pmod{p}. \quad (4.37)$$

Huomaa, että (4.37) on Pikku-Fermat'n yleistys.

### 4.1.1 Lucasin binomikerroinlause

**Lause 33.** Olkoot  $p \in \mathbb{P}$ ,  $n, k \in \mathbb{N}$  sekä

$$n = \sum_{i \geq 0} n_i p^i, \quad k = \sum_{i \geq 0} k_i p^i, \quad 0 \leq k_i, n_i \leq p-1. \quad (4.38)$$

Tällöin

$$\binom{n}{k} \equiv \prod_{i \geq 0} \binom{n_i}{k_i} \pmod{p}. \quad (4.39)$$

### 4.1.2 Lucasin binomikerroinlauseen todistus

**Huomautus 6.** Olkoot  $p \in \mathbb{P}$  ja  $n \in \mathbb{N}$ . Tiedetään, että  $p$ -kantakehitelmä

$$n = \sum_{i \geq 0} n_i p^i, \quad 0 \leq n_i \leq p-1 \quad (4.40)$$

on yksikäsitteinen.

Lauseen 33 Todistus: Aluksi huomataan, että

$$(1+x)^n = (1+x)^{n_0}(1+x)^{pn_1}(1+x)^{p^2n_2} \dots \equiv (1+x)^{n_0}(1+x^p)^{n_1}(1+x^{p^2})^{n_2} \dots \pmod{p} \quad (4.41)$$

Lauseen 28 nojalla. Sama binomikehitelmillä

$$\begin{aligned} \sum_{k=0}^n \binom{n}{k} x^k &\equiv \\ \sum_{i_0=0}^{n_0} \binom{n_0}{i_0} x^{i_0} \sum_{i_1=0}^{n_1} \binom{n_1}{i_1} x^{pi_1} \sum_{i_2=0}^{n_2} \binom{n_2}{i_2} x^{p^2i_2} \dots &= \\ \sum_{i_0=0}^{p-1} \binom{n_0}{i_0} x^{i_0} \sum_{i_1=0}^{p-1} \binom{n_1}{i_1} x^{pi_1} \sum_{i_2=0}^{p-1} \binom{n_2}{i_2} x^{p^2i_2} \dots &= \\ \sum_{0 \leq j} \sum_{0 \leq i_j \leq p-1} \binom{n_0}{i_0} \binom{n_1}{i_1} \binom{n_2}{i_2} \dots x^{i_0+i_1p+i_2p^2+\dots} & \\ &\pmod{p}. \end{aligned} \quad (4.42)$$

Tutkitaan V.P. polynomien termiä  $x^k$  ja sen O.P. polynomien vastintermiä  $x^{i_0+i_1p+i_2p^2+\dots}$ , joka saadaan, kun

$$k = k_0 + k_1p + k_2p^2 + \dots = i_0 + i_1p + i_2p^2 + \dots \quad (4.43)$$

Luvun  $k$  yksikäsitteisen  $p$ -kantaesityksen nojalla havaitaan, että  $i_0 = k_0$ ,  $i_1 = k_1, \dots$ . Täten vertaamalla kongruenssin (4.42) V.P. ja O.P. termejä  $x^k$ , saadaan kongruenssi

$$\binom{n}{k} \equiv \prod_{i \geq 0} \binom{n_i}{k_i} \pmod{p}. \quad \square \quad (4.44)$$

**Esimerkki 15.**  $p = 7$ ,  $n = 11 = 4 + 1 \cdot 7$ ,  $k = 5 = 5 + 0 \cdot 7$ , joten

$$\binom{11}{5} \equiv \binom{n_0}{k_0} \binom{n_1}{k_1} = \binom{4}{5} \binom{1}{0} = 0 \cdot 1 = 0 \pmod{7}. \quad (4.45)$$

**Esimerkki 16.**

$$\binom{3^{100} + 2 \cdot 3^{10} + 2}{3^{10} + 2} \equiv 2 \pmod{3} \quad (4.46)$$

## 5 Summausmenetelmiä

### 5.1 Polynomialalgebran sovelluksia

**Esimerkki 17.**

Lähdetään identiteetistä

$$(1+x)^n(1+x)^m = (1+x)^{n+m}, \quad (5.1)$$

joka kirjoitetaan muotoon

$$\sum_{j=0}^n \binom{n}{j} x^j \sum_{l=0}^m \binom{m}{l} x^l = \sum_{k=0}^{n+m} \binom{n+m}{k} x^k. \quad (5.2)$$

Nyt Caychyn kertosäännöllä

$$\sum_{k=0}^{n+m} \left( \sum_{j+l=k} \binom{n}{j} \binom{m}{l} \right) x^k = \sum_{k=0}^{n+m} \binom{n+m}{k} x^k, \quad (5.3)$$

josta

$$\sum_{j+l=k, 0 \leq j, l \leq k} \binom{n}{j} \binom{m}{l} = \binom{n+m}{k} \quad (5.4)$$

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

$$\sum_{j=0}^m \binom{n}{j} \binom{m}{m-j} = \binom{2m}{m} \quad (5.5)$$

eli

$$\sum_{j=0}^m \binom{m}{j}^2 = \binom{2m}{m}. \quad (5.6)$$



## 5.2 Teleskoopit

Teleskooppisumma

$$\sum_{i=0}^n (a_{i+1} - a_i) = a_{n+1} - a_0 \quad (5.7)$$

ja teleskooppitulo

$$\prod_{i=0}^n \frac{a_{i+1}}{a_i} = \frac{a_{n+1}}{a_0} \quad (5.8)$$

soveltuvat hyvin muunmuassa seuraavantyyppisten tulosten johtamiseen.

$$\sum_{k=0}^n k = \frac{n(n+1)}{2} \quad (5.9)$$

$$\sum_{k=0}^n k^2 = \frac{n(n+1)(2n+1)}{6} \quad (5.10)$$

$$\sum_{k=0}^n k^3 = \left( \frac{n(n+1)}{2} \right)^2 \quad (5.11)$$

$$\sum_{k=0}^n (2k+1) = (n+1)^2 \quad (5.12)$$

Johdetaan (5.12) valitsemalla  $a_k = k^2$  ja lähtemällä identiteetistä

$$a_{k+1} - a_k = (k+1)^2 - k^2 = 2k+1. \quad (5.13)$$

Otetaan summat (5.13) molemminpuolin, jolloin

$$\sum_{k=0}^n (2k+1) = \sum_{k=0}^n (a_{k+1} - a_k) = a_{n+1} - a_0 = (n+1)^2. \quad \square \quad (5.14)$$

Edelleen

$$2 \sum_{k=0}^n k + \sum_{k=0}^n 1 = (n+1)^2, \quad (5.15)$$

josta saadaan (5.9).

Valitsemalla  $a_k = k^3$  ja teleskopoimalla identiteettiä

$$a_{k+1} - a_k = (k+1)^3 - k^3 = 3k^2 + 3k + 1 \quad (5.16)$$

päästään tulokseen (5.10). JNE.