Pieni kilpailumatematiikan opas

Matematiikkakilpailujen tehtävät ovat usein sellaisilta alkeismatematiikan aloilta, joista koulukurssissa puhutaan vähän tai ei ollenkaan. Tähän koosteeseen on kerätty joitakin perusasioita todistamisesta, epäyhtälöistä, lukuteoriasta, algebrasta, geometriasta ja kombinatoriikasta. Esitys on tiivistä, joten lukijan ei tule lannistua, vaikka kaikki ei avaudukaan ensimmäisellä tai toisella lukukerralla!

1 Todistamisesta

Kilpailutehtävät ovat lähes poikkeuksetta sen luontoisia, että niiden ratkaisu joko on itsessään *todistus* tai siihen olennaisesti liittyy todistus. Todistus voi olla *suora* tai *epäsuora*. Suoran todistuksen osat ovat 1) *oletus*, joka esittelee tehtävässä tunnetuiksi ja tosiksi tiedetyt asiat, 2) päättelyaskeleet, jotka johtavat viimein 3) *väitökseen*, eli tehtävässä todistettavaksi vaadittuun asiaan. Epäsuorassa todistuksessa oletukseksi otetaan alkuperäisen väitöksen vastakohta eli *vastaoletus*, ja päättelyaskeleet johtavat asiaintilaan, joka on ristiriidassa joko alkuperäisen oletuksen tai muiden tunnettujen totuuksien kanssa.

Psykologisesti ymmärrettävää on kirjoitustapa, jossa lähdetään liikkeelle väitteestä, esim. jostain todistettavasta kaavasta tai ratkaistavasta yhtälöstä, ja sitä muotoillaan, kunnes saadaan tunnettu tulos – esimerkiksi oikeaksi todistettavasta yhtälöstä johdetaan identtinen yhtälö $0 = 0$ – tai esim. $x = 15$ -tyyppinen vastaus. (Usein askelten väliin sijoitetaan vielä implikaatio- eli $\Rightarrow$-merkkejä.) Tämä on kuitenkin periaatteessa virheellinen menetelmä, ellei jokainen päättelyaskel ole käännettävissä. Kun todistettavaksi tarkoitetun väittämän totuus on lähtökohtaisesti epävarmaa, siitä seuraavat mahdollisesti todetkin asiat eivät todista alkuperäistä asiaa todeksi. Pitäisi siis olla mahdollista panna askeleiden väliin $\Leftarrow$- tai $\Leftrightarrow$-merkit.

Induktiotodistus eli *täydellinen induktio* tähtää sellaisten väittämien todistamiseen, jotka koskevat mielivaltaista kokonaislukua n, kuten esimerkiksi

$$1 + a + a^2 + \ldots + a^n = \frac{1 - a^{n+1}}{1 - a}.$$

Induktiotodistus on *kaksivaiheinen*. Ensin todennetaan, että väite pätee pienimmällä tehtävässä mielekkäällä kokonaisluvun arvolla n (kuten esimerkissä tapauksessa $n = 0$, jolloin todistettava yhtälö on $1 = 1$). Toisessa vaiheessa *oletetaan*, että väite pätee, kun n:llä on mielivaltainen arvo k ja *nojautuen* tähän oletukseen päätellään, että väite pätee myös, kun $n = k + 1$. (Jos

$$1 + a + a^2 + \ldots + a^k = \frac{1 - a^{k+1}}{1 - a},$$

niin

$$1 + a + a^2 + \ldots + a^{k+1} = \frac{1 - a^{k+1}}{1 - a} + a^{k+1} = \frac{1 - a^{k+2}}{1 - a};$$

ensimmäinen yhtäsuuruuden merkki perustui induktio-oletukseen.) – Joissakin tapauksissa induktio saattaa esim. kulkea erikseen parittomien arvojen ja parillisten arvojen kautta;

silloin ensimmäinen vaihe saattaisi olla väitteen todentaminen, kun $n = 0$ ja kun $n = 1$, ja toinen vaihe se, että oletetaan väite todeksi, kun $n = 2k - 1$ ja todistetaan, että tämän oletuksen perusteella väite on tosi myös, kun $n = 2k + 1$ sekä oletetaan, että väite on tosi, kun $n = 2k$ ja todistetaan, että tällöin väite on tosi myös, kun $n = 2k + 2$.

2 Epäyhtälöistä

Erittäin tavallinen kilpailutehtävätyyppi on epäyhtälötehtävä. Siinä pyritään yleensä osoittamaan, että jokin epäyhtälö on voimassa kaikilla tai ainakin suurella joukolla yhden tai useamman muuttujan arvoja. Epäyhtälötehtävien ratkaisuissa käytetään usein hyväksi tiettyjä perusepäyhtälötyyppejä. Niiden oletetaan olevan ratkaisijoille tuttuja.

2.1. Triviaaleja epäyhtälöitä. Suuri osa epäyhtälöistä perustuu viime kädessä totuuksiin $x^2 \geq 0$ kaikilla x ja $x^2 = 0$ vain, kun $x = 0$. Esimerkiksi *aritmeettisen* ja *geometrisen keskiarvon* välinen epäyhtälö

$$\sqrt{ab} \leq \frac{a+b}{2}, \tag{1}$$

kun $0 \leq a$ ja $0 \leq b$, seuraa sanotusta relaatiosta, kun $x = \sqrt{a} - \sqrt{b}$; nähdään myös, että yhtäsuuruus (1):ssä pätee aina ja vain, kun $a = b$.

Esimerkki. Jos a, b ja c ovat reaalilukuja, niin

$$a^2 + b^2 + c^2 \geq ab + bc + ca.$$

Todistus. Koska

$$0 \leq (a-b)^2 + (b-c)^2 + (c-a)^2,$$

niin

$$2ab + 2bc + 2ca \leq 2a^2 + 2b^2 + 2c^2.$$

Esimerkki. Jos a ja b ovat positiivisia reaalilukuja, niin

$$\frac{a}{b} + \frac{b}{a} \geq 2,$$

ja yhtäsuuruus pätee vain, jos $a = b$.

Todistus.

$$\frac{a}{b} + \frac{b}{a} - 2 = \left(\sqrt{\frac{a}{b}} - \sqrt{\frac{b}{a}}\right)^2 \geq 0.$$

Esimerkki. Jos a, b ja c ovat positiivisia, niin

$$\frac{1}{a}+\frac{1}{b}+\frac{1}{c}\geq\frac{9}{a+b+c}.$$

Todistus. Koska

$$a(b-c)^2+b(c-a)^2+c(a-b)^2\geq 0,$$

niin

$$ab^2+ac^2+ba^2+bc^2+ca^2+cb^2\geq 6abc$$

eli

$$ab^2+ac^2+ba^2+bc^2+ca^2+cb^2+3abc\geq 9abc.$$

Vasen puoli sievenee tuloksi $(bc+ca+ab)(a+b+c)$, joten haluttuun epäyhtälöön päästään, kun molemmat puolet jaetaan $abc(a+b+c)$:llä

Epäyhtälötehtävissä on usein hyödyllistä käyttää hyväksi *symmetriaa*, joka sallii olettaa, että yhtälössä esiintyvät luvut ovat jo valmiiksi suuruusjärjestyksessä. Symmetriaan vedotessa tulee kuitenkin olla huolellinen.

Esimerkki. Luvut a, b ja c on valittu väliltä $(0,\,1)$. Osoita, että luvuista $a(1-b)$, $b(1-c)$ ja $c(1-a)$ ainakin yksi on $\leq\frac{1}{4}$.

Todistus. Tässä ei vallitse täydellinen symmetria, ts. ei ole sallittua olettaa, että esim. $a\leq b\leq c$. Kuitenkin voidaan olettaa, että esim. a on luvuista pienin. Koska $(b-\frac{1}{2})^2\geq 0$, niin

$$\frac{1}{4}\geq -b^2+b=b(1-b)\geq a(1-b).$$

Triviaali totuus on myös, että positiivinen murtoluku pienenee, kun nimittäjä kasvaa.

Esimerkki. Jos a, b ja c ovat positiivisia, niin

$$\frac{1}{a+b}+\frac{1}{b+c}+\frac{1}{c+a}>\frac{3}{a+b+c}.$$

Todistus. Lasketaan yhteen epäyhtälöt

$$\frac{1}{a+b}>\frac{1}{a+b+c},$$
$$\frac{1}{b+c}>\frac{1}{a+b+c},$$
$$\frac{1}{c+a}>\frac{1}{a+b+c}.$$

2.2. Yleinen aritmeettis-geometrinen epäyhtälö. Epäyhtälön (1) yleistyksen todistamiseksi oletetaan, että x_1, x_2 ... on jono positiivisia lukuja. Merkitään

$$A_n=\frac{x_1+x_2+\cdots+x_n}{n},\qquad G_n=\sqrt[n]{x_1x_2\cdot\ldots\cdot x_n}.$$

Epäyhtälön $G_n\leq A_n$ todistamiseksi todistetaan ensin

Apulause. *Jos a ja b ovat positiivisia lukuja, niin*

$$(n-1)a^n + b^n \geq na^{n-1}b$$

kaikilla $n = 1, 2, \ldots$

Todistus. Induktio: väite on tosi, kun $n = 1$. Oletetaan, että se tosi, kun $n = k$. Silloin

$$\begin{aligned} ka^{k+1} + b^{k+1} &\geq ka^k b - ab^k + a^{k+1} + b^{k+1} \\ &= (k+1)a^k b + a^{k+1} + b^{k+1} - ab^k - a^k b \\ &= (k+1)a^k b + (a-b)(a^k - b^k) \geq (k+1)a^k b. \end{aligned}$$

Yhtäsuuruus pätee vain, kun $a = b$.

Lause. *Aina on voimassa $A_n \geq G_n$. Lisäksi $A_n = G_n$ vain jos $x_1 = x_2 = \ldots = x_n$.*

Todistus. Induktio jälleen: $A_2 \geq G_2$. Jos $A_{n-1} \geq G_{n-1}$, niin

$$\begin{aligned} nA_n &= (n-1)A_{n-1} + x_n \geq (n-1)(G_{n-1}^{1/n})^n + (x_n^{1/n})^n \\ &\geq n\left(G_{n-1}^{1/n}\right)^{n-1} x_n^{1/n} = n(x_1 x_2 \cdot \ldots \cdot x_n)^{1/n} = nG_n. \end{aligned}$$

Yhtäsuuruutta koskeva väite todistuu samoin induktiolla.

Palautetaan mieleen summan merkitseminen $\sum$-merkillä: jos x_1, x_2, $\ldots x_n$ ovat lukuja, niin summaa $x_1 + x_2 + \cdots + x_n$ merkitään lyhyesti

$$\sum_{k=1}^{n} x_k.$$

Esimerkki. Olkoot $a_1, a_2, \ldots, a_n$ ja $b_1, b_2, \ldots, b_n$ samat positiiviset luvut kirjoitettuina eri järjestykseen. Osoita, että

$$\sum_{i=1}^{n} \frac{a_n}{b_n} \geq n.$$

Ratkaisu.

$$1 = \left(\frac{a_1}{b_1}\frac{a_2}{b_2} \cdot \ldots \cdot \frac{a_n}{b_n}\right)^{\frac{1}{n}} \leq \frac{1}{n}\left(\frac{a_1}{b_1} + \frac{a_2}{b_2} + \cdots + \frac{a_n}{b_n}\right).$$

2.3 Cauchyn – Schwarzin epäyhtälö. *Jos $a_1, a_2, \ldots, a_n$ ja $b_1, b_2, \ldots, b_n$ ovat reaalilukuja, niin*

$$\left(\sum_{i=1}^{n} a_i b_i\right)^2 \leq \sum_{i=1}^{n} a_i^2 \sum_{i=1}^{n} b_i^2.$$

Todistus. Käytetään hyödyksi toisen asteen polynomien tunnettua ominaisuutta. Koska kaikilla x pätee

$$0 \leq \sum_{i=1}^{n}(a_i x - b_i)^2 = \left(\sum_{i=1}^{n} a_i^2\right) x^2 - 2\left(\sum_{i=1}^{n} a_i b_i\right) x + \sum_{i=1}^{n} b_i^2,$$

on oltava

$$4\left(\sum_{i=1}^{n} a_i b_i\right)^2 - 4\sum_{i=1}^{n} a_i^2 \sum_{i=1}^{n} b_i^2 \leq 0.$$

Cauchyn – Schwarzin epäyhtälön yhtäsuuruusehto saadaan tiedosta, jonka mukaan toisen asteen yhtälöllä on tasan yksi nollakohta jos ja vain jos sen diskriminantti on tasan nolla. Yhtäsuuruus epäyhtälössä toteutuu, jos on olemassa sellainen x, että $a_i x - b_i = 0$ kaikilla $i = 1, 2, \ldots, n$.

Esimerkki.

$$\frac{1}{\sqrt{n}} \sum_{i=1}^{n} a_i \leq \sqrt{\sum_{i=1}^{n} a_i^2}.$$

Ratkaisu. Sovelletaan Cauchyn – Schwarzin epäyhtälöä niin, että $b_1 = b_2 = \ldots = b_n = 1$.

2.4. Muita epäyhtälöitä. Tärkeä epäyhtälö on jokseenkin suoraan itseisarvon määritelmästä seuraava *kolmioepäyhtälö*

$$||x| - |y|| \leq |x + y| \leq |x| + |y|$$

ja siitä induktiolla seuraava yleistys

$$\sum_{i=1}^{n} x_i \leq \left|\sum_{i=1}^{n} x_i\right| \leq \sum_{i=1}^{n} |x_i|.$$

Toisinaan on hyötyä induktiolla todistettavasta *Bernoullin epäyhtälöstä*

$$1 + nx \leq (1 + x)^n,$$

joka on voimassa, kaikilla $x > -1$ ja kaikilla positiivisilla kokonaisluvuilla n.

Todistus. Jos $1 + nx \leq (1 + x)^n$, niin

$$1 + (n + 1)x \leq 1 + (n + 1)x + nx^2 = (1 + x)(1 + nx) \leq (1 + x)(1 + x)^n = (1 + x)^{n+1}.$$

Toisinaan epäyhtälötehtävän ratkaisemisessa voidaan käyttää *suuruusjärjestysepäyhtälöä.* Sen mukaan kahden äärellisen jonon $(a_1, a_2, \ldots, a_n)$ ja $(b_1, b_2, \ldots, b_n)$ termien tulojen summa $a_1b_1 + a_2b_2 + \cdots + a_nb_n$ on suurin, kun jonojen termit ovat samassa järjestyksessä, siis $a_i < a_j$ silloin ja vain silloin, kun $b_i < b_j$. Vastaavasti summa on pienin, kun jonot ovat käänteisessä järjestyksessä. Suuruusjärjestysepäyhtälö perustuu seuraavaan yksinkertaiseen havaintoon: jos $a_i < a_j$ ja verrataan alkuperäistä summaa (olkoon se S summaan, jossa b_i ja b_j on vaihdettu keskenään (olkoon se S'), niin $S' - S = a_ib_j + a_jb_i - a_ib_i - a_jb_j = (a_j - a_i)(b_i - b_j)$. Jos olisi $b_j < b_i$, niin vaihto kasvattaisi summaa; vaihtoja voitaisiin tehdä niin kauan kuin jonot eivät olisi samassa suuruusjärjestyksessä.

3 Lukuteoriaa

Matematiikkakilpailuissa esitetään usein melko alkeellisin keinoin ratkeavia *lukuteorian* (tai kuten englantilaiset hiukan vaatimattomammin sanovat, *aritmetiikan*) tehtäviä. Seuraavassa esitetään se tietovarasto, jonka voi katsoa kuuluvan matematiikkakilpailijan yleissivistykseen.

3.1 Jaollisuus. Lukuteoriassa tarkastellaan yleensä luonnollisia lukuja 1, 2, 3, ... ja kokonaislukuja ..., −2, −1, 0, 1, 2, ... Kokonaisluku q on *jaollinen* kokonaisluvulla p, merkittynä $p|q$, jos on olemassa kokonaisluku n siten, että $q = np$. Tällöin sanotaan myös, että p on q:n *tekijä*.

3.2 Suurin yhteinen tekijä. Kokonaislukujen a ja b *suurin yhteinen tekijä* d on se (yksikäsitteinen) luonnollinen luku d, jolle pätee $d|a$ ja $d|b$ sekä jos $c|a$ ja $c|b$, niin $c \leq d$. Merkitään $d = \text{s.y.t.}(a, b) = (a, b)$. Selvästi aina $1 \leq (a, b)$.

Lause. *Jos* $(a, b) = d$, *niin* $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Todistus. Merkitään $c = \left(\frac{a}{d}, \frac{b}{d}\right)$. Silloin $1 \leq c$. Toisaalta, koska c on lukujen $\frac{a}{d}$ ja $\frac{b}{d}$ tekijä, on olemassa luonnolliset luvut m ja n siten, että $\frac{a}{d} = mc$, $\frac{b}{d} = nc$ eli $a = m(cd)$, $b = n(cd)$. Siis cd on sekä a:n että b:n tekijä, joten $cd < d$. Siis $c \leq 1$.

Useamman kuin kahden luvun $a_1, a_2, \ldots, a_n$ suurin yhteinen tekijä

$$(a_1, a_2, \ldots, a_n)$$

määritellään palautuskaavan

$$(a_1, a_2, \ldots, a_n) = ((a_1, a_2, \ldots, a_{n-1}), a_n)$$

avulla.

3.3 Jakoyhtälö. *Kaikilla kokonaisluvuilla* a *ja* b, $b > 0$, *on olemassa sellaiset kokonaisluvut* q *ja* r, *missä* $0 \leq r < b$, *että*

$$a = qb + r.$$

Todistus. Olkoon r_0 pienin ei-negatiivinen luku, joka on muotoa $a - qb$, missä q on kokonaisluku. Oletetaan, että $r_0 > b$. Mutta silloin olisi myös $a - (q + 1)b = r_0 - b$ ei-negatiivinen kokonaisluku, vastoin oletusta.

Lause. *Jos* $a = qb + r$, *niin* $(a, b) = (b, r)$.

Todistus. Luku (a, b) on b:n tekijä. Koska (a, b) on a:n ja b:n tekijä, se on myös r:n tekijä. Siis $(a, b) \leq (b, r)$. Täsmälleen samoin päätellään, että $(b, r) \leq (a, b)$.

3.4 Eukleideen algoritmi. Olkoon $b > 0$. Jakoyhtälöä ja sitä seurannutta lausetta toistuvasti käyttämällä voidaan aina määrittää a:n ja b:n suurin yhteinen tekijä (a, b): On olemassa q_1 ja $r_1 < b$ siten, että $a = q_1 b + r_1$. Jos $r_1 > 0$, on olemassa q_2 ja $r_2 < r_1$ siten, että $b = q_2 r_1 + r_2$. Jatkamalla näin saadaan jonot lukuja q_k, r_k, missä aina $r_{k-2} = q_k r_{k-1} + r_k$ ja $r_1 > r_2 > \ldots > r_k > \ldots \geq 0$. Jollakin indeksin k arvolla on silloin varmasti $r_{k-1} > 0$, $r_k = 0$. Kohdan 3.3 tuloksen perusteella on nyt $(r_{k-2},\, r_{k-1}) = (r_{k-3}, r_{k-2}) = \ldots = (b, r_1) = (a, b)$. Lisäksi (jakoyhtälö!) $(r_{k-2},\, r_{k-1}) = r_{k-1}$, joten $(a,\, b)$ on edelliseen prosessiin sisältyvän jakoketjun viimeinen nollasta eroava jakojäännös.

3.5 Diofantoksen yhtälön $ax + by = d$ (eräs) ratkaisu. Jos a, b ja d ovat kokonaislukuja, niin tehtävää, jossa on määritettävä ehdon

$$ax + by = d$$

toteuttavat *kokonaisluvut* x ja y, sanotaan *ensimmäisen asteen Diofantoksen yhtälöksi*. Oletetaan, että $d = (a, b)$. Tehtävä saadaan ratkaistuksi, kun luetaan Eukleideen algoritmissa esiintyvät jakoyhtälöt lopusta alkuun:

$$\begin{aligned} d = r_{k-1} &= r_{k-3} - q_{k-1} r_{k-2} = r_{k-3} - (r_{k-4} - q_{k-2} r_{k-3}) q_{k-1} \\ &= (1 + q_{k-1} q_{k-2}) r_{k-2} - q_{k-2} r_k r_{k-3} = \ldots = (\text{ kok.luku })a + (\text{ kok.luku })b \\ &= ax + by. \end{aligned}$$

Lause. *Jos* $(d,\, a) = 1$ *ja* $d|ab$, *niin* $d|b$.

Todistus. Edellä sanotun perusteella on olemassa sellaiset kokonaisluvut x ja y, että $dx + ay = 1$. Siis $(db)x + (ab)y = b$. Luku d on tekijänä molemmissa vasemman puolen yhteenlaskettavissa, joten se on tekijänä myös oikealla puolella.

Lause. *Jos* $(a, b) = d$ *ja* $c|a$, $c|b$, *niin* $c|d$.

Todistus. Väite seuraa yhtälön $ax + by = d$ toteuttavien lukujen x ja y olemassaolosta ja siitä, että $c|(ax + by)$.

3.6 Alkuluvut. Positiivinen luku p on *alkuluku,* jos siitä, että $c|p$ seuraa, että $|c| = p$ tai $|c| = 1$. Positiivinen luku, joka ei ole alkuluku, on *yhdistetty luku*. Yhdistetyllä luvulla on muita tekijöitä kuin se itse tai 1. Yleensä sovitaan, että 1 ei ole sen paremmin alkuluku kuin yhdistetty lukukaan.

Lause. *Jokainen kokonaisluku* $n > 1$ *on jaollinen jollakin alkuluvulla.*

Todistus. 2 on alkuluku ja siis jaollinen alkuluvulla. Induktio-oletus: jokainen $k \leq n$ on jaollinen alkuluvulla. Luku $n+1$ on joko alkuluku tai yhdistetty luku. Jos se on yhdistetty luku, on $n + 1 = pq$, missä $p < n$. Oletuksen nojalla p on jaollinen alkuluvulla, joten niin on myös $n + 1$.

Lause. *Jokainen kokonaisluku* $n > 1$ *on alkuluku tai alkulukujen tulo.*

Todistus. Luku 2 on alkuluku. Jos jokainen $k \leq n$ on alkuluku tai alkulukujen tulo ja $n + 1$ ei ole alkuluku, niin $n + 1 = pq$, missä p ja q ovat alkulukuja tai alkulukujen tuloja.

Alkutekijöiden etsimistä helpottaa seuraava tulos.

Lause. *Jos n on yhdistetty luku, niin sillä on tekijä, joka on $\leq \sqrt{n}$.*

Todistus. $n = pq$, missä $1 < p < n$ ja $1 < q < n$. Jos sekä p että q olisivat $> \sqrt{n}$, jouduttaisiin ristiriitaan $pq > n$.

Samanlaisella induktiopäättelyllä, kuin mikä tehtiin edellä alkuluvulla jaollisuuden yhteydessä, voidaan todistaa vielä alkutekijöihin jaon yksikäsitteisyys.

Lause. *Kokonaisluvun esitys alkulukujen tulona on yksikäsitteinen, lukuun ottamatta tekijöiden järjestystä.*

Tuloesityksen perusteella saadaan uusi keino lukujen m ja n suurimman yhteisen tekijän (m, n) laskemiseksi: jos

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}, \tag{1}$$

ja

$$n = p_1^{\beta_1} p_2^{\beta_2} \cdot \ldots \cdot p_k^{\beta_k}, \tag{2}$$

missä $\alpha_i \geq 0$ ja $\beta_i \geq 0$ kaikilla $i = 1, 2, \ldots, k$, niin

$$(m, n) = p_1^{\gamma_1} p_2^{\gamma_2} \cdot \ldots \cdot p_k^{\gamma_k},$$

missä $\gamma_i = \min\{\alpha_i, \beta_i\}$.

3.7 Pienin yhteinen monikerta. Lukujen m ja n *pienin yhteinen monikerta* (eli *pienin yhteinen jaettava*) p.y.j.(m, n) on positiivinen luku a, jolle on voimassa

$m|a$ ja $n|a$ ja

jos b on positiivinen ja $m|b$, $n|b$, niin $a < b$.

Merkitään $a = \text{p.y.j.}(m, n) = [m, n]$. Jos m ja n ovat kuten kaavoissa (1) ja (2), niin

$$[m, n] = p_1^{\delta_1} p_2^{\delta_2} \cdot \ldots \cdot p_k^{\delta_k},$$

missä $\delta_i = \max\{\alpha_i, \beta_i\}$. (Miksi?) Koska $\gamma_i + \delta_i = \alpha_i + \beta_i$, on

$$(m, n)[m, n] = mn.$$

3.8 Alkulukujen määrä. Lause. *Alkulukuja on äärettömän paljon.*

Todistus. Tehdään vastaoletus: alkulukujen joukko on äärellinen joukko

$$\{p_1, p_2, \ldots, p_k\}.$$

Olkoon $n = p_1 p_2 \cdot \ldots \cdot p_k + 1$. Kohdan 3.6 lauseen perusteella luvulla n on alkutekijä p, joka on eräs luvuista p_i, $i = 1, 2, \ldots, k$. Koska $p|n$ ja p on tekijänä myös luvussa $p_1 p_2 \cdot \ldots \cdot p_k$, joudutaan ristiriitaan $p|1$.

Kaikki alkuluvut voi tuottaa ns. *Eratostheneen seulalla*: kirjoitetaan kaikki luonnolliset luvut jonoon, pyyhitään ensin pois kahdella jaolliset 4, 6, 8, ..., sitten kolmella jaolliset (6), 9, (12), 15,..., sitten viidellä jaolliset (10), (15), (20), 25, (30), 35, ...jne. Jäljelle jäävät alkuluvut ja vain ne.

3.9 Diofantoksen yhtälöt jälleen. Lause. *Yhtälöllä*

$$ax + by = c$$

on kokonaislukuratkaisu x, y silloin ja vain silloin, kun $(a, b)|c$.

Todistus. Jos yhtälöllä on ratkaisu, niin $(a, b)|c$. Oletetaan, että $(a, b)|c$ ja merkitään $(a, b) = d$. Silloin $c = md$, missä m on kokonaisluku. Yhtälöllä $ax + by = d$ on kohdan 3.5 mukaan ratkaisu x', y'. Selvästi $x = mx'$, $y = my'$ on alkuperäisen yhtälön ratkaisu.

Tarkastellaan vielä Diofantoksen yhtälöä $ax + by = c$, missä $\dfrac{c}{(a, b)}$ on kokonaisluku (ja yhtälöllä on siis ratkaisu). Olkoon $a' = \dfrac{a}{(a, b)}$, $b' = \dfrac{b}{(a, b)}$ ja $c' = \dfrac{c}{(a, b)}$. Tällöin yhtälöt $ax + by = c$ ja $a'x + b'y = c'$ ovat yhtäpitävät, joten niillä on samat ratkaisut. Koska $(a', b') = 1$ (kohta 3.2), voidaan rajoittua tutkimaan sellaisia yhtälöitä $ax + by = c$, joissa $(a, b) = 1$.

Lause. *Olkoon $(a, b) = 1$, $ab \neq 0$ ja $ax_0 + by_0 = c$. Silloin yhtälön $ax + by = c$ kaikki ratkaisut ovat*

$$x = x_0 + bt, \quad y = y_0 - at,$$

missä t saa kaikki kokonaislukuarvot.

Todistus.

$$a(x_0 + bt) + b(y_0 - at) = ax_0 + by_0 = c.$$

Jos toisaalta $ax+by = c$, niin $a(x-x_0)+b(y-y_0) = 0$. Siis $b|(a(x-x_0))$, ja koska $(a, b) = 1$, niin $b|(x-x_0)$. Siis $x-x_0 = bt$ jollakin kokonaisluvulla t. Samoin nähdään, että $y-y_0 = at'$ jollakin kokonaisluvulla t'. Mutta koska $0 = ax+by-c = ax_0+abt+by_0+bat'-c = ab(t+t')$ ja $ab \neq 0$, on $t = -t'$, ja lause on todistettu.

3.10 Kongruenssit. Olkoon c positiivinen kokonaisluku. Lukujen a ja b sanotaan olevan *kongruentteja modulo c*, jos $c|(b - a)$ eli jos $a = b + kc$ jollakin kokonaisluvulla k. Tällöin merkitään $a \equiv b \bmod c$ (tai jos epäselvyyden vaaraa ei ole, vain $a \equiv b$). Jos a on mielivaltainen kokonaisluku ja c on positiivinen kokonaisluku, on aina olemassa ehdon $0 \leq r < c$ täyttävä luku r siten, että $a \equiv r \bmod c$. Tämä seuraa jakoyhtälöstä. Relaatiota $a \equiv b \bmod c$ sanotaan *kongruenssiksi*.

Kongruenssit ovat erittäin käyttökelpoisia jaollisuuteen liittyvissä tehtävissä. Tämä perustuu siihen, että kongruenssi käyttäytyy tavallisten laskutoimitusten suhteen lähes samoin kuin tavallinen yhtäsuuruus.

Oletetaan, että $a \equiv b \bmod m$ ja $c \equiv d \bmod m$. Silloin on voimassa

$$a + c \equiv b + d \bmod m$$
$$ac \equiv bd \bmod m$$

ja

$$a^k \equiv b^k \bmod m$$

kaikilla positiivisilla kokonaisluvuilla k.

Todistetaan esimerkiksi keskimmäinen relaatio: Oletuksesta seuraa, että $a = b + em$ ja $c = d + fm$, missä e ja f ovat kokonaislukuja. Siis

$$ac = (b + em)(d + fm) = bd + (efm + bf + ed)m = bd + gm,$$

missä g on kokonaisluku.

Jakolaskun suhteen kongruensseille pätee seuraavaa: jos $ac \equiv bc \bmod m$ ja $(c, m) = 1$, niin $a \equiv b \bmod m$.

Todistus: Olkoon $ac - bc = km$. Koska $(a - b)c$ on jaollinen m:llä ja $(c, m) = 1$, on $a - b$ jaollinen m:llä eli $a \equiv b \bmod m$.

Yleisemmin: Jos $ac \equiv bc \bmod m$ ja $(c, m) = d$, niin $a \equiv b \bmod \frac{m}{d}$.

Kongruenssien avulla saadaan helposti muutamia *jaollisuustarkistimia*. Koska on voimassa $10 \equiv 1 \bmod 3$ ja $\bmod\ 9$, niin

$$a_k 10^k + a_{k-1} 10^{k-1} + \ldots + a_1 10^1 + a_0 \equiv a_k + a_{k-1} + \cdots + a_1 + a_0 \bmod 3$$

ja $\bmod\ 9$. Tästä seuraa erityisesti, että luku on jaollinen kolmella tai yhdeksällä silloin ja vain silloin, kun sen kymmenjärjestelmäesityksen numeroiden summa on jaollinen 3:lla tai 9:llä.

Koska $10 \equiv -1 \bmod 11$, päätellään samoin, että luku n on jaollinen 11:llä jos ja vain jos luku, joka saadaan kun n:n kymmenjärjestelmäesityksen ensimmäisestä numerosta vähennetään toinen, lisätään kolmas jne. on jaollinen 11:llä.

3.11 Kongruenssiyhtälön ratkaisu. Sanomme, että x on kongruenssiyhtälön $ax \equiv b \bmod m$ *varsinainen ratkaisu*, jos $ax \equiv b$ ja $0 \leq x < m$.

Lause. *Jos $(a, m)|b$, niin yhtälöllä $ax \equiv b \bmod m$ on (a, m) kappaletta varsinaisia ratkaisuja. Jos (a, m) ei ole b:n tekijä, yhtälöllä ei ole ratkaisuja.*

Todistus. Etsitään x ja y siten, että $ax - b = my$ eli $ax - my = b$. Jos (a, m) ei ole tekijänä luvussa b, tällaisia lukuja ei ole (kohta 3.10). Jos $(a, m)|b$, merkitään $(a, m) = d$. Olkoon x_0, y_0 se yhtälön $\frac{a}{d}x - \frac{m}{d}y = \frac{b}{d}$ ratkaisu, jolle x_0 on ei-negatiivinen ja pienin mahdollinen. Silloin $x_0 < \frac{m}{d}$ ja x_0, $x_0 + \frac{m}{d}$, $x_0 + 2\frac{m}{d}$, $\ldots$, $x_0 + (d-1)\frac{m}{d}$ ovat varsinaisia ratkaisuja.

Fermat'n (pieni) lause on monesti käyttökelpoinen jaollisuustehtävissä. *Olkoon p alkuluku ja a kokonaisluku, jolle pätee $(a, p) = 1$. Silloin*

$$a^{p-1} \equiv 1 \bmod p.$$

Todistus. Oletetaan ensin, että a on positiivinen ja todistetaan, että p on luvun $a^p - a = a(a^{p-1} - 1)$ tekijä; koska $(a, p) = 1$, p on tällöin myös luvun $a^{p-1} - 1$ tekijä. Jos $a = 1$ niin $a^p - a = 0$ ja varmasti $p|(a^p - a)$. Olkoon $a \geq 1$ ja $p|(a^p - a)$. Tarkastellaan lukuja $k!\binom{p}{k} = p(p-1)\dots(p-k+1)$. Nyt $p|k!\binom{p}{k}$, mutta jos $k < p$, niin p ei ole tekijänä luvussa $k!$. Siis $p|\binom{p}{k}$, joten p jakaa luvun

$$(a+1)^p - a^p - 1 = \sum_{k=1}^{p-1} \binom{p}{k} a^k = (a+1)^p - (a+1) - (a^p - a).$$

Induktioaskel on näin otettu. Negatiivisia a:n arvoja koskeva tulos seuraa parittomilla p:n arvoilla suoraan tästä; jos taas $p = 2$, on $a^p - a = a(a-1)$; tämä on jaollinen kahdella koska a tai $a - 1$ on parillinen.

Jos $(a, p) = 1$ ja p on alkuluku, voidaan kongruenssiyhtälö $ax \equiv b \bmod p$ ratkaista Fermat'n lauseen avulla:

$$x \equiv a^{p-1}x \equiv a^{p-2}(ax) = a^{p-2}b \bmod p.$$

3.12 Eulerin funktio ja lause. Olkoon $\phi(n)$ niiden lukujen a, $1 \leq a < n$ lukumäärä, joille pätee $(a, n) = 1$. Täten esimerkiksi $\phi(1) = 1$, $\phi(2) = 1$, $\phi(3) = 2$, $\phi(4) = 2$ ja $\phi(5) = 4$. Positiivisten kokonaislukujen joukossa määritelty funktio ϕ on *Eulerin funktio*.

Lause. *Jos* $(a, n) = 1$, *niin* $a^{\phi(n)} = 1 \bmod n$.

Todistus. Olkoot $1 = r_1 < r_2 < \ldots < r_{\phi(n)} = n - 1$ ehdon $(r_i, n) = 1$ toteuttavat luvut. Olkoon $ar_i = q_i \bmod n$, $0 \leq q_i < n$. Jos $q_i \equiv q_j$, on $ar_j \equiv ar_i \bmod n$ ja kohdan 3.10 perusteella $r_i \equiv r_j$ eli $r_i = r_j$. Tämän vuoksi

$$\{q_1, q_2, \ldots, q_{\phi(n)}\} = \{r_1, r_2, \ldots r_{\phi(n)}\}.$$

Siis myös

$$r_1 r_2 \cdot \ldots \cdot r_{\phi(n)} \equiv (ar_1)(ar_2)\dots(ar_{\phi(n)}) \equiv a^{\phi(n)} r_1 r_2 \dots r_{\phi(n)} \bmod n.$$

Koska $(r_1 r_2 \dots r_{\phi(n)}, n) = 1$, saadaan edellä esitetyn kongruenssien jakolaskuominaisuuden perusteella $1 \equiv a^{\phi(n)} \bmod n$.

Jos n on alkuluku, on $\phi(n) = n - 1$, ja Eulerin lause antaa Fermat'n lauseen (joka siis on tullut tässä uudelleen ja eri tavalla todistetuksi).

Eulerin lausetta voidaan käyttää lineaaristen kongruenssien ratkaisemiseen samoin kuin Fermat'n pientä lausetta: jos $(a, n) = 1$, niin kongruenssilla $ax \equiv b \bmod n$ on ratkaisu $x = ba^{\phi(n)-1}$.

3.13 Kiinalainen jäännöslause. Jos $a_1, a_2, \ldots, a_n$ ovat kokonaislukuja, jotka ovat pareittain yhteistekijättömiä ($(a_i, a_j) = 1$, kun $i \neq j$), jos $a = \prod_{i=1}^{n} a_i$ ja jos $b_1, b_2, \ldots, b_n$ ovat mielivaltaisia kokonaislukuja, niin on olemassa (ja modulo a vain yksi) luku x, jolle on pätevät yhtälöt

$$x \equiv b_i \bmod a_i, \quad i = 1, 2, \ldots, n.$$

3.14 Pythagoraan luvut. Kokonaislukukolmikon (x, y, z) jäsenet ovat *Pythagoraan lukuja*, jos

$$x^2 + y^2 = z^2.$$

Tunnetuimpia esimerkkejä Pythagoraan luvuista ovat lukukolmikot $(3a, 4a, 5a)$ ja $(5a, 12a, 13a)$.

Pythagoraan lukuja voidaan tuottaa äärettömän monta kaavojen

$$x = (m^2 - n^2)p, \quad y = 2mnp, \quad z = (m^2 + n^2)p, \tag{1}$$

missä m, n ja p ovat kokonaislukuja, avulla. Kaikki Pythagoraan luvut ovat toisaalta muotoa (1).

4 Algebraa

Kilpailutehtäviä luokiteltaessa epäyhtälötehtävät luetaan algebraan. Tässä luvussa luetellut lauseet ja käsitteen kattavat suunnilleen sen, mitä muissa algebrallisissa kilpatehtävissä edellytetään. Ns. algebrallisia struktuureja, jotka ovat nykyaikaisen algebran keskeisiä tutkimuskohteita, kilpatehtävissä ei juuri käsitellä.

4.1 Hyödyllisiä identiteettejä. Kaavojen manipuloinnissa tavallisimmin hyödyksi käytettäviä identiteettejä ovat binomin potenssikaavojen ohessa mm.

$$a^2 - b^2 = (a - b)(a + b),$$
$$a^2 + b^2 + c^2 + 2(ab + bc + ca) = (a + b + c)^2,$$
$$a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1})$$
$$a^3 + b^3 + c^3 - 3abc = (a + b + c)(a^2 + b^2 + c^2 - bc - ca - ab)$$
$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2.$$

Seuraavat summaidentiteetit tulevat myös aika ajoin käyttöön:

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}, \qquad \sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6},$$
$$\sum_{k=1}^{n} k^3 = \frac{n^2(n+1)^2}{4}, \qquad \sum_{k=1}^{n} k(k+1) = \frac{n(n+1)(n+2)}{3},$$
$$\sum_{k=1}^{n} k(k+1)(k+2) = \frac{n(n+1)(n+2)(n+3)}{4},$$
$$\sum_{k=1}^{n} \frac{1}{k(k+1)} = 1 - \frac{1}{n+1}, \qquad \sum_{k=0}^{n} (a + bk) = \frac{(n+1)(2a+bn)}{2},$$
$$\sum_{k=0}^{n} aq^k = \frac{a(1-q^{n+1})}{1-q}, \quad (q \neq 1).$$

4.2 Polynomit. Olkoot a_0, a_1, ..., a_n kiinteitä lukuja. Muuttujan x funktio p,

$$p(x) = a_0 + a_1 x + \cdots + a_n x^n,$$

on (yhden muuttujan) polynomi. Jos $a_n \neq 0$, niin p:n *aste* on n, $n = \deg p$. Luvut a_i ovat polynomin p *kertoimet*, jos ne ovat kaikki kokonaislukuja, rationaalilukuja, reaalilukuja tai kompleksilukuja, puhutaan vastaavasti kokonaiskertoimisesta, rationaalikertoimisesta, reaalikertoimisesta tai kompleksikertoimisesta polynomista.

Jos $p(r) = 0$, niin r on p:n *nollakohta* tai *juuri*. Jos polynomin aste on $\leq n$, mutta sen nollakohtien lukumäärä on $> n$, niin polynomi on identtisesti nolla eli *nollapolynomi*. Tästä seuraa, että jos kahdella polynomilla on sama arvo useammassa pisteessä kuin polynomeista asteluvultaan suuremman asteluku, niin molemmat polynomit ovat identtisesti samat.

Toisen asteen reaalikertoimisella polynomilla $p(x) = ax^2 + bx + c$, $a \neq 0$, on tasan kaksi reaalista nollakohtaa, jos sen *diskriminantti* $\Delta = b^2 - 4ac$ on positiivinen. Jos $\Delta = 0$, p:llä on tasan yksi reaalinen nollakohta. Jos $\Delta < 0$, p:llä ei ole reaalisia nollakohtia, mutta kylläkin kaksi kompleksista nollakohtaa. Nollakohtien lausekkeet ovat

$$r_{1,2} = \frac{1}{2a}(-b \pm \sqrt{\Delta}).$$

Toisen asteen polynomi voidaan täydentää neliöksi:

$$ax^2 + bx + c = a\left[\left(x + \frac{b}{2a}\right)^2 - \frac{\Delta}{4a^2}\right];$$

tästä nähdään mm., että tapauksessa $\Delta < 0$ p ja a ovat aina samanmerkkiset.

Jos u ja v ovat polynomeja ja $\deg u \geq 1$, niin on olemassa polynomit q ja r, $\deg r < \deg u$, siten, että

$$v(x) = q(x)u(x) + r(x). \tag{1}$$

Polynomit q ja r voidaan määrittää jakolaskualgoritmilla jakokulmassa. Jos u ja v ovat rationaali- tai reaalikertoimisia, niin q ja r ovat samaa lajia. Jos u ja v ovat kokonaislukukertoimisia ja u:n korkeinta astetta olevan termin kerroin on 1, niin myös q ja r ovat kokonaislukukertoimisia. Jos $r = 0$, niin v on jaollinen u:lla.

Polynomi h on polynomien u ja v *suurin yhteinen tekijä*, jos u ja v ovat molemmat jaollisia h:lla ja h on jaollinen jokaisella polynomilla, jolla u ja v ovat jaollisia. Jos h_1 ja h_2 ovat u:n ja v:n suurimpia yhteisiä tekijöitä, niin $h_2 = ch_1$, missä c on vakio. Suurin yhteinen tekijä löydetään soveltamalla *Eukleideen algoritmia*.

Kun jakoyhtälöä (1) sovelletaan polynomiin $v(x) = x - a$, saadaan

$$u(x) = (x - a)q(x) + u(a).$$

Jos a on u:n juuri, niin u on jaollinen $(x - a)$:lla.

Jos

$$p(x) = (x-a)^m q(x)$$

ja $q(a) \neq 0$, niin a on p:n m-kertainen juuri. Polynomin juurten kertalukujen summa on enintään polynomin aste.

Polynomi p on *jaoton*, jos siitä, että $p(x) = u(x)v(x)$ seuraa, että joko u tai v on vakio eli nollannen asteen polynomi. Polynomi saattaa olla esim. rationaalikertoimisena jaoton, mutta reaalikertoimisena jaollinen jne. ($p(x) = x^2 - 2$ on rationaalikertoimisena jaoton, koska $\sqrt{2}$ on irrationaaliluku, muttei reaalikertoimisena: $p(x) = (x-\sqrt{2})(x+\sqrt{2})$.)

Jokainen vähintään astetta 1 oleva reaalikertoiminen polynomi voidaan kirjoittaa jaottomien polynomien tulona; esitys on yksikäsitteinen, paitsi tekijöiden järjestystä ja sitä, että tekijät voidaan kertoa vakioilla.

Jos

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

on kokonaiskertoiminen polynomi ja jos rationaaliluku $\frac{s}{q}$, missä s:n ja q:n suurin yhteinen tekijä on 1, on p:n juuri, niin s on a_0:n tekijä ja q on a_n:n tekijä.

Jos r_1 ja r_2 ovat polynomin $x^2 + ax + b$ nollakohdat, niin $r_1 + r_2 = -a$ ja $r_1 r_2 = b$. Yleisemmin, jos $r_1, r_2, \ldots, r_n$ ovat polynomin

$$p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

juuret (useampikertaiset juuret lueteltuna kertalukunsa osoittaman määrän kertoja) ja jos S_i on summa, jonka yhteenlaskettavina ovat kaikki mahdolliset i:stä luvuista $r_1, \ldots, r_n$ muodostetut tulot, niin $S_1 = -a_{n-1}$, $S_2 = a_{n-2}, \ldots, S_i = (-1)^i a_{n-i}$, $S_n = (-1)^n a_0$. (S_i:t ovat n:n muuttujan *symmetrisiä polynomeja*.

Jos $x_1, x_2, \ldots, x_n$ ovat keskenään eri lukuja ja $y_1, y_2, \ldots, y_n$ mielivaltaisia lukuja, on olemassa yksikäsitteinen enintään astetta $n-1$ oleva polynomi p, jolle pätee $p(x_1) = y_1$, $p(x_2) = y_2, \ldots, p(x_n) = y_n$. p löydetään käyttämällä *Lagrangen interpolaatiokaavaa*: merkitään

$$g(x) = (x-x_1)(x-x_2)\cdot \ldots \cdot (x-x_n)$$

ja

$$g'(x_1) = (x_1-x_2)(x_1-x_3)\cdot \ldots \cdot (x_1-x_n),$$
$$g'(x_2) = (x_2-x_1)(x_2-x_3)\cdot \ldots \cdot (x_2-x_n)$$

jne. Silloin

$$p(x) = \frac{g(x)y_1}{(x-x_1)g'(x_1)} + \frac{g(x)y_2}{(x-x_2)g'(x_2)} + \cdots + \frac{g(x)y_n}{(x-x_n)g'(x_n)}.$$

4.3 Kompleksiluvut. Kompleksiluvut ovat muotoa $z = x+iy$, missä $x = \Re z$ ja $y = \Im z$ ovat reaalilukuja ja $i^2 = -1$. Kertolasku:

$$zw = (x+iy)(u+iv) = xu - yv + i(xv + yu).$$

Jakolasku:

$$\frac{z}{w} = \frac{x+iy}{u+iv} = \frac{xu+yv+i(-xv+yu)}{u^2+v^2}.$$

Kompleksiluvun $z = x + iy$ *liittoluku* eli *kompleksikonjugaatti* on kompleksiluku $\overline{z} = \overline{x+iy} = x - iy$. Pätee

$$\overline{z+w} = \overline{z} + \overline{w},$$
$$\overline{zw} = \overline{z}\,\overline{w}$$
$$\overline{az} = a\overline{z}, \quad a \in \mathbf{R}.$$

Kompleksiluvun z reaali- ja imaginaariosat voidaan lausua z:n ja $\overline{z}$:n avulla:

$$x = \Re z = \frac{1}{2}(z+\overline{z}) \qquad y = \Im z = \frac{1}{2i}(z-\overline{z}).$$

Kompleksiluvun $z = x + iy$ *itseisarvo* $|z|$ on ei-negatiivinen luku

$$|z| = \sqrt{z\overline{z}} = \sqrt{x^2+y^2}.$$

Itseisarvolle pätee $|zw| = |z||w|$, josta $|z^n| = |z|^n$, ja $|z+w| \le |z| + |w|$.

Jos $z = x + iy$ samastetaan xy-tason pisteen $P = (x, y)$ kanssa, voidaan kirjoittaa $x = |z|\cos\phi$, $y = |z|\sin\phi$, missä ϕ on
x-akselin ja suoran OP välinen kulma. Siis

$$z = |z|(\cos\phi + i\sin\phi) = |z|e^{i\phi}.$$

Tässä on käytetty *Eulerin kaavaa*

$$\cos\phi + i\sin\phi = e^{i\phi}.$$

– Kulmaa ϕ sanotaan z:n *argumentiksi*, $\phi = \arg z$.

Kompleksiluvun esitys itseisarvon ja argumentin avulla johtaa kaavoihin

$$zw = |z||w|e^{i(\arg z + \arg w)},$$
$$\frac{z}{w} = \frac{|z|}{|w|}e^{i(\arg z - \arg w)},$$
$$z^n = |z|^n e^{in\arg z}.$$

Viimeinen kaava pätee kaikilla eksponenteilla n, ja mahdollistaa siten esim. juurien ottamisen kompleksiluvuista.

Algebran peruslause. Jokaisella kompleksilukukertoimisella polynomilla p, jonka aste on ≥ 1, on ainakin yksi kompleksinen nollakohta.

Jos reaalikertoimisella polynomilla p on kompleksinen juuri z, on myös $0 = \overline{p(z)} = p(\overline{z})$. Reaalikertoimisen polynomin kompleksijuuren ohella sen liittoluku on myös juuri. Koska

$$(x-z)(x-\overline{z}) = x^2 - 2x\Re z + |z|^2,$$

nähdään, että reaalikertoiminen polynomi voidaan aina esittää ensimmäistä tai toista astetta olevien jaottomien polynomien tulona.

Yhtälön $z^n = 1$ juuret eli *n:nnet yksikköjuuret* ovat luvut 1, $e^{i2\pi/n}$, $e^{i4\pi/n}$, $\ldots$, $e^{i2(n-1)\pi/n}$.

4.4 Kolmannen ja neljännen asteen yhtälöt. Kolmannen ja neljännen asteen yhtälöiden ratkaisukaavoja ei yleensä tarvita kilpailutehtävien ratkaisuissa. Kaavojen johto esitetään tässä lyhyesti esimerkkinä algebrallisista tekniikoista.

Kolmannen asteen yhtälö $x^3 + ax^2 + bx + c = 0$ voidaan sijoituksella $x = y - \frac{a}{3}$ saada muotoon $y^3 + py + q = 0$. Kun tähän sijoitetaan $u + v = y$, tullaan yhtälöön

$$u^3 + v^3 + (3uv + p)(u + v) + q = 0.$$

Valitaan u ja v niin, että $3uv = -p$. Tällöin u tulee toteuttamaan yhtälön

$$u^3 - \frac{p^3}{27u^3} - q = 0.$$

Tämä on muuttujan $t = u^3$ toisen asteen yhtälö. Kun tämä yhtälö ratkaistaan ja tehdyt sijoitukset puretaan, saadaan alkuperäisen kolmannen asteen yhtälön ratkaisukaavat, *Cardanon kaavat*.

Yleisestä neljännen asteen yhtälöstä voidaan samoin hävittää kolmannen asteen termi. Tarpeen on ratkaista yhtälö

$$x^4 + ax^2 + bx + c = 0 \tag{2}$$

eli

$$\left(x^2 + \frac{a}{2}\right)^2 = -bx - c + \frac{a^2}{4}.$$

Jos x on (2):n ratkaisu ja y mielivaltainen, niin

$$\left(x^2 + \frac{a}{2} + y\right)^2 = -bx - c + \frac{a^2}{4} + 2y\left(x^2 + \frac{a}{2}\right) + y^2 \tag{3}$$

Pyritään valitsemaan y niin, että yhtälön (3) oikea puoli olisi myös täydellinen neliö. Tämä saadaan aikaan valitsemalla oikean puolen x:n toisen asteen polynomin diskriminantti on nolla. Diskriminantin nollaehto on kolmannen asteen yhtälö y:lle. Kun se ratkaistaan ja tulos sijoitetaan (3):een, saadaan kahden neliön yhtäsuuruus. Kun siitä otetaan neliöjuuri, jää jäljelle x:n toisen asteen yhtälö, josta x voidaan ratkaista.

4.5. Funktionaaliyhtälöt. Melko tavallinen kilpailutehtävätyyppi on *funktionaaliyhtälö*. Siinä etsitään yhden tai useamman muuttujan funktiota, joka toteuttaa joitain ehtoja, yleensä jonkin tai joitakin yhtälöitä jotka ovat voimassa kaikilla muttujan tai muuttujien arvoilla.

Funktionaaliyhtälötehtävän ratkaisuun ei ole yhtä aina toimivaa reseptiä, mutta usein pääsee alkuun sijoittamalla ehtoyhtälöön joitakin helppoja muuttujanarvoja.

Esimerkki. Etsi kaikki rationaalilukujen joukossa määritellyt funktiot f, joille $f(x+y) = f(x) + f(y)$ kaikilla rationaaliluvuilla x ja y (*Cauchyn funktionaaliyhtälö*).

Ratkaisu. Sijoitetaan ehtoyhtälöön $y = 0$. Saadaan $f(x) = f(x+0) = f(x) + f(0)$. Tästä seuraa $f(0) = 0$. Olkoon a mikä tahansa rationaaliluku. Sijoitetaan ehtoyhtälöön $x = y = a$. Saadaan $f(2a) = f(a+a) = f(a) + f(a) = 2f(a)$. Osoitetaan induktiolla, että $f(na) = nf(a)$ kaikilla positiivisilla kokonaisluvuilla n. Asia on jo todettu, kun $n = 1$ ja $n = 2$. Oletetaan, että asia on tosi, kun $n = k$. Silloin $f((k+1)a) = f(ka + a) = f(ka) + f(a) = kf(a) + f(a) = (k+1)f(a)$. Osoitetaan, että $f(n) = nf(a)$ kaikilla negatiivisilla kokonaisluvuilla n. Olkoon n negatiivinen kokonaisluku. Silloin $-n$ on positiivinen kokonaisluku ja $0 = f(0) = f(na + (-n)a) = f(na) + f((-n)a) = f(na) + (-n)f(a)$. Siis $f(n) = -(-n)f(a) = nf(a)$. Sijoitetaan $a = 1$. Saadaan $f(n) = nf(1)$. Olkoon sitten $a = \dfrac{1}{n}$. Nyt $f(1) = f\left(n \cdot \dfrac{1}{n}\right) = nf\left(\dfrac{1}{n}\right)$. Tästä ratkaistaan $f\left(\dfrac{1}{n}\right) = \dfrac{1}{n}f(1)$. Olkoon sitten $\dfrac{p}{q}$ mielivaltainen rationaaliluku. Edellä saatuja tuloksia yhdistelemällä saadaan $f\left(\frac{p}{q}\right) = f\left(p \cdot \dfrac{1}{q}\right) = pf\left(\dfrac{1}{q}\right) = \dfrac{p}{q}f(1)$. Funktion f on oltava muotoa $f(x) = xf(1)$ kaikilla rationaaliluvuilla x. Arvoa $f(1)$ ei ole rajoitettu, joten voidaan kirjoittaa $f(x) = bx$ kaikilla x, missä b on mikä hyvänsä rationaaliluku.

Funktionaaliyhtälötehtävän ratkaisuun kuluu olennaisesti saadun ratkaisun oikeellisuuden tarkastaminen. Ehtoyhtälöstä voidaan yleensä johtaa ratkaisun välttämättä toteuttavia ehtoja. Aina ei ole selvää, että nämä ehdot ovat riittäviä. Siksi on aina tarkistettava, että saatu funktionaliyhtälön ratkaisu myös toteuttaa alkuperäisen yhtälön. Esimerkin tapauksessa asia on selvä: jos $f(x) = bx$, niin $f(x+y) = b(x+y) = bx + by = f(x) + f(y)$.

5 Tasogeometriaa

Matematiikkaolympialaisten kuuden tehtävän joukossa on säännönmukaisesti ainakin yksi ja usein kaksikin tasogeometrian tehtävää. Tehtävät ratkeavat yleensä ainakin "perinteisen" geometrian keinoin, mutta usein voi käyttää myös analyyttistä geometriaa, vektoreita tai kompleksilukuja. Hyödyllistä saattaa olla myös ajatella tilannetta geometrisena kuvauksena: siirtona, kiertona kiinteän pisteen ympäri, peilauksena suoran yli tai homotetiakuvauksena. – Tässä luvussa asiat esitellään lähinnä luetteloiden, puuttumatta todistuksiin. Tarkemmin asiaan on syytä perehtyä jonkin vanhemman, ennen 1970-lukua julkaistuun geometrian oppikirjaan, teokseen Lehtinen, Merikoski, Tossavainen: Johdatus tasogeometriaan tai matematiikan olympiavalmennussivujen materiaaleihin.

Geometrisen tehtävän geometrisessa ratkaisussa tarvittaviin työkaluihin kuuluvat geometriset peruskäsitteet ('yhdensuuntaisuus', 'keskinormaali', 'kehäkulma', kuvion sisään ja ympäri piirretty kuvio jne.), lauseet yhdensuuntaisista suorista, kolmioiden yhtenevyys- ja yhdenmuotoisuuslauseet ("sks", "ssk", "ksk", "kks", "sss"; "kk"), tasakylkisten kolmioiden perusominaisuudet, suunnikkaiden, suorakulmioiden ja vinoneliöiden perusominaisuudet; lause puoliympyrän sisältämästä kehäkulmasta (*Thaleen lause*), *Pythagoraan lause*, suorakulmaisen kolmion sivujen suhteet (trigonometriset funktiot) jne.; tärkeimmät geometriset kuvaukset (*symmetria* pisteen ja suoran suhteen, *siirto* ja *kierto*, *homotetia*). Perusvälineitä ovat myös mm. seuraavan luettelon tulokset.

5.1. Yhdensuuntaiset ja kohtisuorat. Kulmat, joiden vastinkyljet ovat kohtisuo-

rassa toisiaan vastaan, ovat yhtä suuret: jos $\angle ABC$ ja $\angle DEF$ ovat joko molemmat teräviä tai molemmat tylppiä ja jos $AB \perp DE$ ja $BC \perp EF$, niin $\angle ABC = \angle DEF$.

Jos neljä suoraa ℓ_1, ℓ_2, ℓ_3 ja ℓ_4 ovat yhdensuuntaisia, ja suorien ℓ_1 ja ℓ_2 jostakin suorasta erottama jana on yhtä pitkä kuin suorien ℓ_3 ja ℓ_4 tästä suorasta erottama jana, niin pari ℓ_1, ℓ_2 erottaa jokaisesta suorasta yhtä pitkän janan kuin pari ℓ_3, ℓ_4.

Puolisuunnikkaan $ABCD$ ei-yhdensuuntaisten sivujen BC ja AD keskipisteet yhdistävän janalla EF on seuraavat ominaisuudet:

(a) $EF \parallel AB$;

(b) $|EF| = \frac{1}{2}(|AB| + |CD|)$;

(c) EF puolittaa jokaisen janan, jonka toinen päätepiste on AB:llä ja toinen CD:llä.

Koska kolmio ABC on puolisuunnikkaan $ABCD$ surkastuma, ominaisuudet (a), (b) ja (c) koskevat myös kolmion sivujen keskipisteiden yhdysjanaa.

5.2. Kolmioiden osat. Kolmion mediaanien, korkeusjanojen ja kulman puolittajien leikkauspisteet:

(a) kolmion kolme keskijanaa leikkaavat toisensa samassa pisteessä (kolmion *painopisteessä*), ja tämä piste jakaa jokaisen keskijanan suhteessa $2 : 1$;

(b) kolmion kulmien puolittajat leikkaavat toisensa samassa pisteessä, joka on yhtä etäällä kolmion sivuista;

(c) kolmion korkeusjanat leikkaavat toisensa samassa pisteessä (kolmion *ortokeskuksessa*).

Kolmion kulman vieruskulma on kolmion kahden muun kulman summa. Kolmion pidempää sivua vastassa oleva kulma on suurempi kuin lyhempää sivua vastassa oleva kulma.

Suorakulmaisen kolmion hypotenuusaa vastaan piirretty keskijana on puolet hypotenuusasta; jos kolmiossa jokin keskijana on puolet hypotenuusasta, niin kolmio on suorakulmainen.

Kolmion ABC kulman C puolittaja jakaa vastaisen sivun $AB = c$ viereisten sivujen suhteessa: $\frac{a}{b} = \frac{a'}{b'}$.

Suorakulmaisen kolmion metriset ominaisuudet: jos c on kolmion hypotenuusa, a ja b sen kateetit, h hypotenuusaa vastaava korkeusjana ja a', b' kateettien projektiot hypotenuusalle, niin (a) $h^2 = ab$; (b) $a^2 = a'c$; (c) $b^2 = b'c$; (d) $a^2 + b^2 = c^2$; (e) $h = \frac{ab}{c}$.

Pythagoraan lauseelle (d) sukua on

Suunnikaslause. Suunnikkaan sivujen a ja b neliöiden summa on sama kuin lävistäjien d_1 ja d_2 neliöiden summa: ${d_1}^2 + {d_2}^2 = 2a^2 + 2b^2$.

Merkitään kolmion ABC kärjessä A olevaa kulmaa myös A:lla ja kolmion kulmaa A vastassa oleva sivua a:lla (vastaavasti B, C, b, c).

Kosinilause.

$$a^2 = b^2 + c^2 - 2bc\cos A.$$

Sinilause.

$$\frac{a}{\sin A} = \frac{b}{\sin B} = \frac{c}{\sin C} = 2R,$$

missä R on kolmion ympäri piirretyn ympyrän säde.

Kolmion muodon ja sen sivujen pituuksien a, b ja c välinen yhteys: jos c on pisin sivu, niin (a) kolmio on teräväkulmainen, jos $c^2 < a^2 + b^2$; (b) kolmio on suorakulmainen, jos $c^2 = a^2 + b^2$; (c) kolmio on tylppäkulmainen, jos $c^2 > a^2 + b^2$.

Ns. kolmion merkillisiä pisteitä koskevat tulokset ovat kaikki erikoistapauksia seuraavasta lauseesta.

Cevan lause. Kolmion ABC kärjistä vastakkaisten sivujen pisteisiin D, E ja F piirretyt janat leikkaavat samassa pisteessä silloin ja vain silloin, kun

$$\frac{AD}{BD} \cdot \frac{BE}{CE} \cdot \frac{CF}{AF} = 1.$$

Hengeltään samanlainen on

Menelaoksen lause. Olkoot X, Y ja Z pisteitä kolmion ABC sivuilla BC, CA ja AB tai niiden jatkeilla. Jos suorilla AB, BC ja CA on kullakin määritelty positiivinen suunta ja $[PQ]$ tarkoittaa suoran pisteiden P ja Q etäisyyttä varustettuna + tai −-merkillä sen mukaan, onko Q P:n oikealla vai vasemmalla puolella, niin

$$\frac{[BX]}{[CX]} \cdot \frac{[CY]}{[AY]} \cdot \frac{[AZ]}{[BZ]} = -1$$

silloin ja vain silloin, kun X, Y ja Z ovat samalla suoralla.

5.3. Ympyrä. Ympyrän tangentin ominaisuudet: (a) sivuamispisteeseen piirretty säde on kohtisuorassa tangenttia vastaan; (b) ympyrän ulkopuolisesta pisteestä ympyrälle piirretyissä tangenteissa yhteisen pisteen ja sivuamispisteiden yhdysjanat ovat yhtä pitkät ja tangenttien ja pisteen ympyrän keskipisteeseen yhdistävän suoran väliset kulmat yhtä suuret.

Yllättävän usein matematiikkakilpailutehtävän ratkaisu perustuu seuraavaan *kehäkulmalauseeseen*: (a) ympyrän keskuskulma ja sen erottama kaari ovat yhtä suuret; (b) ympyrän kehäkulma on puolet vastaavasta kaaresta, ja siten samaa kaarta vastaavat kehäkulmat ovat yhtä suuret; (c) tangenttikulma on puolet vastaavasta kaaresta.

Kolmiot ja ympyrät: (a) jokaisen kolmion ympäri voidaan piirtää ympyrä: sen keskipiste on kolmion sivujen keskinormaalien leikkauspiste; (b) jokaisen kolmion sisään voidaan piirtää ympyrä: sen keskipiste on kolmion kulmien puolittajien leikkauspiste.

Nelikulmiot ja ympyrät: (a) nelikulmion ympäri voidaan piirtää ympyrä silloin ja vain silloin, kun nelikulmion vastakkaisten kulmien summa on 180° ($\alpha + \beta = 180°$) tällöin nelikulmiota sanotaan *jännenelikulmioksi*; (b) nelikulmion sisään voidaan piirtää ympyrä silloin ja vain silloin, kun sen vastakkaisten sivujen pituuksien summa on sama ($a + c = b + d$).

Metrisiä relaatioita ympyrässä: (a) jos ympyrän jänteet AB ja CD leikkaavat pisteessä M, niin $|AM| \cdot |BM| = |CM| \cdot |DM|$; tulon yhteinen arvo on pisteen M *potenssi* ympyrän suhteen; (b) jos MAB ja MCD ovat ympyrän sekantteja, niin $|AM| \cdot |BM| = |CM| \cdot |DM|$; (c) jos MAB on ympyrän sekantti ja MC ympyrän tangentti, niin $|AM| \cdot |BM| = |CM|^2$.

5.4. Pinta-alat. Yhdenmuotoisten kuvioiden pinta-alojen suhde on yhdenmuotoisuussuhteen neliö.

Kolmion ABC ala S voidaan laskea kaavoista (a) $S = \frac{1}{2}ah$, missä h on sivua a vastaava korkeus; (b) $S = \frac{1}{2}ab\sin C$; (c) $S = \frac{abc}{4R}$, missä R on kolmion ympäri piirretyn ympyrän säde; (d) $S = pr$, missä $p = \frac{1}{2}(a+b+c)$ ja r on kolmion sisään piirretyn ympyrän säde ja (e) $S = \sqrt{p(p-a)(p-b)(p-c)}$ (*Heronin kaava*).

Jos ympyrän säde on R, niin sektorin ala on $S = \frac{1}{2}R^2\alpha$, missä α on sektorin keskuskulma radiaaneissa.

Ympyrän segmentin ala on $S = \frac{1}{2}R^2(\alpha - \sin\alpha)$.

6 Kombinatoriikkaa

Kombinatorisiksi luokitellaan usein melkein kaikki sellaiset kilpailutehtävät, jotka eivät ole selvästi algebraa, geometriaa tai lukuteoriaa. Kombinatorisessa tehtävässä on usein tavalla tai toisella kyse jonkin joukon lukumäärästä, esimerkiksi eri tavoista tehdä jokin asia, vaikkapa jonkin ruudukon värittäminen tietyin säännöin. Kombinatorinen tehtävä voi myös olla vaikkapa kysymys siitä, onko tietyin säännöin pelattavassa pelissä jollakin pelaajalla mahdollisuus voittaa riippumatta siitä, miten vastustajat pelaavat.

6.1. Laatikkoperiaate. Tavallisin matematiikkakilpailutehtävien kombinatorinen työkalu on *kyyhkyslakkaperiaate* eli *(Dirichlet'n) laatikkoperiaate*. Sen yksinkertaisin muoto on seuraava:

> Jos $n+1$ esinettä sijoitetaan umpimähkään n:ään lokeroon, niin ainakin yhteen lokeroon tulee ainakin kaksi esinettä.

Hiukan kehittyneempi versio laatikkoperiaatteesta on seuraava:

> Jos $kn+1$ esinettä sijoitetaan umpimähkään n:ään lokeroon, niin ainakin yhteen lokeroon tulee ainakin $k+1$ esinettä.

Laatikkoperiaate on tehokas tilanteissa, joissa pyritään osoittamaan, että jokin asia on olemassa. Se ei anna tarkempaa tietoa siitä, mikä kyseinen olio on.

Valaistaan laatikkoperiaatteen käyttöä kolmella esimerkillä:

Esimerkki. Olkoon S neliö, jonka sivun pituus on 2. Todista, että jos P_1, P_2, P_3, P_4 ja P_5 ovat S:n sisäpisteitä, niin ainakin yksi janoista P_iP_j, $i \neq j$, on pituudeltaan enintään $\sqrt{2}$.

Ratkaisu. Jaetaan S sivujen suuntaisilla janoilla neljäksi yhtä suureksi neliöksi. Viidestä pisteestä kaksi on välttämättä samassa pikkuneliössä. Näiden pisteiden etäisyys on enintään sama kuin pikkuneliön lävistäjän pituus eli $\sqrt{2}$.

Esimerkki. Olkoon annettuna 1001 positiivista kokonaislukua, kukin ≤ 2000. Osoita, että ainakin yksi luvuista on tekijänä jossakin muussa.

Ratkaisu. Olkoot luvut $x_i = 2^{n_i} y_i$, $i = 1, , 2, \ldots, , 1001$, missä y_i on pariton kokonaisluku ja $n_i \geq 0$. Olkoon $M = \{y_i \mid i = 1, 2, \ldots 1001\}$. Jokainen M:n alkio on pariton ja ≤ 2000. Tällaisia lukuja on enintään 1000 erilaista. Siis $y_i = y_j$ joillakin $i \neq j$. Jos $n_i \leq n_j$, niin x_i on x_j:n tekijä; jos $n_i \geq n_j$, niin x_j on x_i:n tekijä.

Esimerkki. On annettu kymmenen kaksinumeroisen kokonaisluvun joukko. Osoita, että joukolla on kaksi erillistä osajoukkoa, joiden alkioilla on sama summa.

Ratkaisu. Kymmenalkioisella joukolla on $2^{10} - 1 = 1023$ erilaista epätyhjää osajoukkoa. Jokaisessa on enintään 10 lukua, ja näistä kukin on enintään 99, joten minkään osajoukon alkioiden summa ei ole suurempi kuin 1000. On olemassa (useitakin) osajoukkopareja, joiden alkioilla on sama summa. Jos kahdesta tällaisesta osajoukosta poistetaan niiden mahdolliset yhteiset alkiot, saadaan tehtävässä vaaditut kaksi erillistä osajoukkoa. (Tehtävä on kansainvälisistä matematiikkaolympialaisista vuodelta 1972.)

6.2. Summan ja erotuksen periaate. Kombinatoriikassa lasketaan yleensä joitakin ehtoja täyttävien olioiden lukumääriä. Tärkeä työkalu on *summan ja erotuksen periaate*. Jos äärellisen joukon A alkioiden lukumäärää merkitään $|A|$:lla, niin ilmeisesti

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Induktiolla voidaan todistaa yleisemmin

$$|A_1 \cup A_2 \cup \ldots \cup A_n| = \sum_{i=1}^{n} |A_i| - \sum_{i<j} |A_i \cap A_j|$$
$$+ \sum_{i<j<k} |A_i \cap A_j \cap A_k| - \ldots + (-1)^n |A_1 \cap A_2 \cap \ldots \cap A_n|.$$

Esimerkki. Olkoon X joukko, jonka alkioina ovat kaikki kirjaimista a, b, c ja d muodostetut n-kirjaimiset sanat. Monessako sanassa $w \in X$ esiintyvät kaikki kirjaimet a, b, c ja d?

Ratkaisu. Olkoon $A = \{w \in X \mid$ a ei esiinny w:ssä$\}$. Määritellään joukot B, C ja D vastaavasti. Tällöin $|A| = |B| = |C| = |D| = 3^n$, $|A \cap B| = |A \cap C| = \ldots = 2^n$ ja $|A \cap B \cap C| = |A \cap B \cap D| = \ldots = 1$. Summan ja erotuksen periaate antaa kysytyksi lukumääräksi

$$|X \setminus (A \cup B \cup C \cup D)| = 4^n - 4 \cdot 3^n + 6 \cdot 2^n - 4.$$

6.3 Kombinaatiot, variaatiot ja permutaatiot. Olkoon $|X| = n$, $X = \{x_1, x_2, \ldots, x_n\}$. Joukon X *k-variaatio* on X:n k:n eri alkion muodostama järjestetty jono $(x_{i_1}, x_{i_2}, \ldots, x_{i_k})$. Joukon X *k-kombinaatio* on X:n k:n eri alkion muodostama (järjestämätön) joukko $\{x_{i_1}, xi_2, \ldots, x_{i_k}\}$. (Huomaa, että jos $a \neq b$, niin $(a, b) \neq (b, a)$, mutta $\{a, b\} = \{b, a\} = \{a, a, b, b, a\} = \ldots$.)

Lause. *Kun $|X| = n$, niin joukolla X on*

$$n(n-1)(n-2) \cdot \ldots \cdot (n-k+1) = \frac{n!}{(n-k)!}$$

k-variaatiota.

Todistus. k-variaatiossa $(x_{i_1}, x_{i_2}, \ldots x_{i_k})$ voidaan x_{i_1} valita n:llä tavalla, x_{i_2} $n-1$:llä tavalla jne.

Kun $|X| = n$, niin X:n n-variaatioita kutsutaan *permutaatioksi*. X:llä on $n!$ eri permutaatiota. Permutaatiot kuvaavat tapoja luetella kaikki X:n alkiot; ne vastaavat myös joukon X *bijektioita* eli kääntäen yksikäsitteisiä kuvauksia itselleen.

Lause. *Kun $|X| = n$, niin X:llä on*

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

k-kombinaatiota.

Todistus. Väite seuraa heti edellisestä lauseesta, sillä jokaisesta k-kombinaatiosta saadaan järjestämällä $k!$ eri k-variaatiota.

Jos tulo $(a+b)^n$ kirjoitetaan muotoa $c_{nk}a^k b^{n-k}$ olevien termien summaksi, niin $c_{nk} = \binom{n}{k}$, sillä eri tapoja valita n:stä tulon tekijästä ne k, joista termiin $a^k b^{n-k}$ tulevat a:t, on yhtä monta kuin n-alkioisen joukon k-kombinaatioita. Näin tulee perustelluksi *binomikaava*

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$

6.4 Sijoittelut. Tarkastellaan joukkoja $X = \{x_1, x_2, \ldots, x_n\}$ ja $Y = \{y_1, y_2, \ldots, y_m\}$. Ajatellaan alkioita x_i esineinä ja alkioita y_j lokeroina, joihin näitä esineitä yritetään sijoittaa. Kysytään, monellako eri tavalla tämä voidaan tehdä. Tämä kysymys voidaan esittää eri muunnelmina.

A. Haluamme tietää jokaisesta alkiosta, missä lokerossa se on. Tällöin vastaus on tietysti $m \cdot m \cdot \ldots \cdot m = m^n$.

B. Olemme kiinnostuneita vain siitä, miten monta alkiota kussakin lokerossa on. Merkitään lokerossa y_j olevien esineiden lukumäärää n_j:llä. Kysymme nyt, miten monta eri jonoa $(n_1, n_2, \ldots, n_m)$ on sellaista, joille

$$\sum_{j=1}^{m} n_j = n.$$

Tällaisia jonoja kutsutaan joukon Y *n-jakaumiksi*. Esimerkiksi kun $n = 2$ ja $m = 3$, n-jakaumia on 6.

Lause. *Kun $|Y| = m$, niin Y:n n-jakaumien lukumäärä on*

$$\binom{n+m-1}{n}.$$

Todistus. Ajatellaan lokerikkoa, jossa on vierekkäin $n+m-1$ lokeroa. Jos näistä lokeroista valitaan mitkä tahansa $m-1$ kappaletta, ja ensimmäisen valitun lokeron vasemmalle puolelle jää n_1 lokeroa, ensimmäisen ja toisen väliin n_2 lokeroa jne., niin $n_1+n_2+\cdots+n_m = n$. Jokainen eri $(m-1)$:n lokeron valinta johtaa eri n-jakaumaan, ja jokaista n-jakaumaa vastaa yksikäsitteinen $(m-1)$:n "väliseinälokeron" valinta. n-jakaumia on siis yhtä paljon kuin $(n+m-1)$:n alkion $(m-1)$-kombinaatioita, eli

$$\binom{n+m-1}{m-1} = \binom{n+m-1}{n}$$

kappaletta.

C. Ollaan kiinnostuneita vain siitä, mitkä X:n alkiot ovat samassa lokerossa, ei siitä, mikä lokero tämä on. Nyt kyseessä ovat n:n alkion *ositukset*. Jos $p(n,\, m)$ on n-alkioisen joukon m-ositusten lukumäärä, niin on voimassa helposti induktiolla todistettava palautuskaava

$$p(n,\, m) = mp(n-1,\, m) + p(n-1,\, m-1).$$

D. Jos sekä alkiot että lokerot jätetään nimeämättä, niin kysymys on siitä, kuinka monella tavalla lukumäärä n voidaan esittää summana

$$n = n_1 + n_1 + \cdots + n_m,$$

missä jokainen n_i on kokonaisluku ja > 0. Tällaista esitystä kutsutaan n:n *partitioksi*; lukujen n_i järjestykseen ei kiinnitetä huomiota. Esimerkiksi luvulla 5 on 7 partitiota: $5 = 4+1 = 3+2 = 3+1+1 = 2+1+1+1 = 1+1+1+1+1 = 2+2+1$. Kysymys partitioiden lukumäärästä yleisessä tapauksessa on melko hankala, eikä siihen puututa tässä lähemmin.

6.5. Differenssiyhtälöt. Palautuskaava määrittelee lukujonon (a_n) siten, että jonon ensimmäiset k $(k \geq 1)$ lukua annetaan sellaisinaan, ja jonon loput luvut määritellään kaavalla

$$a_n = f(a_{n-1},\, a_{n-2},\, \ldots,\, a_{n-k+1},\, n).$$

Eräs usein esiintyvä erikoistapaus on muotoa

$$C_0a_n + C_1a_{n-1} + \cdots + C_ra_{n-r} = f(n) \qquad \text{(Y)}$$

oleva palautuskaava. Jos lukujonon $a_0,\, a_1,\, a_2,\, \ldots$ termit toteuttavat yhtälön (Y) ja jonon $b_0,\, b_1,\, b_2,\, \ldots$ termit toteuttavat vastaavan *homogeenisen yhtälön*

$$C_0a_n + C_1a_{n-1} + \cdots + C_ra_{n-r} = 0, \qquad \text{(HY)}$$

niin jonon $a_0+b_0,\, a_1+b_1,\, \ldots$ termit toteuttavat myöskin yhtälön (Y). Tästä seuraa, että yhtälön (Y) kaikki ratkaisut saadaan, jos yhtälön (HY) mielivaltaiseen ratkaisuun lisätään mikä hyvänsä yhtälön (Y) yksittäinen ratkaisu.

Yhtälön (HY) ratkaisemiseksi kokeillaan yritettä $a_n = A\alpha^n$. Kun tämä sijoitetaan yhtälöön, nähdään, että jos

$$C_0\alpha^r + C_1\alpha^{r-1} + \cdots + C_r = 0, \tag{KY}$$

niin yrite on (HY):n ratkaisu. Yhtälö (KY) on (HY):n *karakteristinen yhtälö*. Jos karakteristisella yhtälöllä on r kappaletta eri suuria reaalijuuria α_1, α_2, …, α_r, niin jokainen summa

$$a_n = A_1\alpha_1^n + A_2\alpha_2^n + \cdots + A_r\alpha_r^n$$

on (HY):n ratkaisu. Jos karakteristisella yhtälöllä on kompleksijuuria tai moninkertaisia juuria, niin homogeeniyhtälön yleinen ratkaisu saadaan hiukan eri muodossa.

Esimerkki. *Fibonaccin luvut* määritellään palautuskaavoilla $a_0 = a_1 = 1$, $a_{n+1} = a_n + a_{n-1}$. Karakteristinen yhtälö on $\alpha^2 - \alpha - 1 = 0$, ja sen juuret ovat

$$\frac{1 \pm \sqrt{5}}{2}.$$

jonon luvut ovat siis muotoa

$$a_n = A_1\left(\frac{1+\sqrt{5}}{2}\right)^2 + A_2\left(\frac{1-\sqrt{5}}{2}\right)^n.$$

Kertoimet A_1 ja A_2 määrittyvät ehdoista $a_0 = a_1 = 1$; saadaan

$$A_1 = \frac{1}{\sqrt{5}}\frac{1+\sqrt{5}}{2}, \qquad A_2 = -\frac{1}{\sqrt{5}}\frac{1-\sqrt{5}}{2}.$$