Matematiikka tutuksi, syksy 2013

Helsingin yliopisto

- 5op, ei kelpaa matematiikan pääaineopiskelijan perusopintoihin
- Kurssi suoritetaan tekemällä *laskuharjoitustehtäviä* ja osallistumalla niiden läpikäyntiin.
- Laskareita yhteensä 6 sarjaa, jokaisessa 6 tehtävää.
- Läpipääsyyn vaaditaan 2/3 tehtävistä tehdyiksi (eli 24 tehtävää), sekä osallistuminen niiden läpikäyntiin
- Kerrataan lukion pitkän matematiikan aiheita, käsitellään joitain yliopistomatematiikan perusasioita
- Tutustutaan matematiikan merkintöihin
- Harjoitellaan todistusmenetelmiä ja todistusta

Viikko-ohjelma:

1. Luvut ja yhtälöt.
2. Joukot ja funktiot.
3. Eksponentti- ja logaritmifunktio. Alkuluvut ja jaollisuus.
4. Induktio ja lukujonot. Verkot.
5. Todennäköisyys ja kombinatoriikka. Rekursio.
6. Logiikka.

Mitä matematiikka on?

Miten yliopistomatematiikka eroaa koulumatematiikasta?

Koulumatematiikka: Keskitytään siihen, miten asioita lasketaan. Opetellaan kaavoja ja laskusääntöjä.
Yliopistomatematiikka: Mietitään, mitkä asiat pitävät paikkansa, ja miksi niiden tiedetään pitävän paikkansa. Opetellaan pohtimaan ja etsimään ratkaisuja ongelmiin. Opetellaan todistamaan väitteitä.

Luvut ja yhtälöt

Luvut

Lähdetään liikkeelle kertaamalla mitä tiedämme luvuista.
Mitä erilaiset luvut kuvaavat ja millaisia ominaisuuksia niillä on?

Luonnolliset luvut $\mathbb{N}$

Luonnolliset luvut $0, 1, 2, 3, 4, 5, \ldots$

- Käytetään merkintää $\mathbb{N}$.
- Käytetään kuvaamaan lukumääriä.
- Luonnolliset luvut ovat järjestyksessä.
  Esim. $1 < 2$, $473 > 28$, $0 \leq n$ millä tahansa luonnollisella luvulla n
- Ei ole suurinta luonnollista lukua.
- Kerto- ja yhteenlasku luonnollisten lukujen kesken tuottaa luonnollisen luvun.

Luonnollisten lukujen määritelmä

Määritelmä

1. Luku 0 on luonnollinen luku.
2. Aina kun n on luonnollinen luku, niin myös $n + 1$ on luonnollinen luku.

Kokonaisluvut $\mathbb{Z}$

Kokonaisluvut $\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots$

- Kokonaisluvut kuvaavat lukumäärien eroja.
  Esim. lämpöasteet $+5°C$ tai $-13°C$. (5 astetta enemmän, 13 vähemmän kuin vedenjäätymislämpötila)
- ovat järjestyksessä.
  Esim. $-3 < -1$ ja $-1 < 2$, tai lyhyemmin $-3 < -1 < 2$.
- Ei ole suurinta eikä pienintä kokonaislukua.
- Kerto- ja yhteenlasku kokonaislukujen kesken tuottaa kokonaisluvun.

Kokonaislukujen määritelmä

Määritelmä

Kokonaislukuja ovat kaikki luvut, jotka voidaan ilmaista kahden luonnollisen luvun erotuksena, eli luvut jotka ovat muotoa $m - n$ joillakin luonnollisilla luvuilla m ja n.

Rationaaliluvut $\mathbb{Q}$

Rationaaliluvut $\frac{m}{n}$, missä m ja n ovat kokonaislukuja, $n \neq 0$.

- Kuvaavat "osia kokonaisista". Esim. puolikas $\frac{1}{2}$, viidesosa $\frac{1}{5}$.
- Ovat järjestyksessä. Esim. $\frac{1}{2} < \frac{5}{3}$.
- Ei ole pienintä eikä suurinta rationaalilukua.
- Ei löydy suuruusjärjestyksessä seuraavaa, kahden rationaaliluvun välissä on aina lisää rationaalilukuja.
- Esitys $\frac{m}{n}$ ei ole yksikäsitteinen. Esim. $\frac{1}{3} = \frac{2}{6}$.
- Rationaalilukujen desimaalikehitelmät ovat päättyviä tai jaksollisia. Esim. $\frac{5}{4} = 1,25$, $\frac{3}{22} = 0,13636\ldots = 0,1\overline{36}$.

Rationaalilukujen määritelmä

Määritelmä

Rationaalilukuja ovat kaikki luvut jotka voidaan ilmaista muodossa $\frac{m}{n}$, missä m ja n ovat kokonaislukuja ja $n \neq 0$.

Rationaalilukujen summa

Kahden rationaaliluvun summa on rationaaliluku.

Todistus.

Olkoot x ja y rationaalilukuja. Määritelmän perusteella tämä tarkoittaa, että on olemassa kokonaisluvut k, l, m ja n, $l \neq 0$, $n \neq 0$, niin että

$$x = \frac{k}{l} \quad \text{ja} \quad y = \frac{m}{n}.$$

Tällöin

$$x + y = \frac{k}{l} + \frac{m}{n} \overset{\text{lavennus}}{=} \frac{nk}{nl} + \frac{ml}{nl} = \frac{nk + ml}{nl}.$$

Koska kokonaislukujen tulo ja summa ovat kokonaislukuja, $nk + ml \in \mathbb{Z}$ ja $nl \in \mathbb{Z}$, ja koska kumpikaan luvuista n ja l ei ollut nolla, $nl \neq 0$ (tulon nollasääntö). Siis luku $x + y$ voidaan ilmaista kahden kokonaisluvun osamääränä, joten se on määritelmän nojalla rationaaliluku. □

Esimerkki

Etsi desimaalikehitelmä luvulle $\frac{5}{3}$.

Ratkaisu. $\frac{5}{3} = 1.666\ldots = 1.\overline{6}$

Etsi murtolukuesitys luvuille 0.03, $0.333\ldots$ sekä $0.1242424\ldots$

Ratkaisu. $0.03 = \frac{3}{100}$.
Merkitään $x = 0.333\ldots$. Tällöin $10x = 3.333\ldots$, joten

$$10x - x = 3.333\ldots - 0.333\ldots = 3.$$

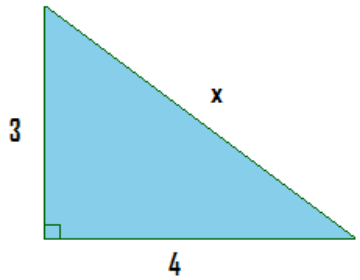
Siis $9x = 3$, eli $0.333\ldots = x = \frac{1}{3}$.
Merkitään seuraavaksi $y = 0.12424\ldots$. Tällöin $10y = 1.2424\ldots$ ja $100y = 124.2424\ldots$, joten

$$100y - 10y = 124.2424\ldots - 1.2424\ldots = 123.$$

Siis $90y = 123$, joten $0.12424\ldots = y = \frac{123}{90} = \frac{41}{30}$.

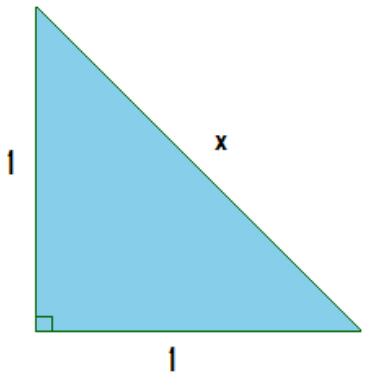
Pituuksista

Pythagoraan lauseen mukaan suorakulmaisen kolmion hypotenuusan pituuden neliö on yhtäsuuri kuin kateettien pituuksien neliöiden summa. Tarkastellaan kolmiota



Hypotenuusalle x pätee siis $x^2 = 4^2 + 3^2 = 25$. Koska $5^2 = 25$, hypotenuusan pituudeksi saadaan $x = 5$.

Entäpä kolmio



Saadaan yhtälö $x^2 = 1^2 + 1^2 = 2$. Ratkaisua ei löydy luonnollisista luvuista, eikä edes rationaaliluvuista. Täytyyhän hypotenuusan pituuden olla jokin luku, merkitään sitä $\sqrt{2}$:lla.

Irrationaaliluvut

$\sqrt{2}$ on esimerkki **irrationaaliluvusta**, eli luvusta joka ei ole rationaaliluku (ts. ei ole muotoa $\frac{m}{n}$). Miten tämä voidaan todistaa?
On huomattavasti helpompi todistaa, että esim. luku $0,1\overline{6}$ on rationaalinen ; riittää vain laskea sille esitys $\frac{1}{6}$.

Reaaliluvut $\mathbb{R}$

Reaaliluvut saadaan rationaaliluvuista lisäämällä niihin kaikki irrationaaliluvut.

- Reaalilukuja voidaan ajatella lukusuorana.
- reaalilukujen desimaalikehitelmät voivat olla päättymättömiä ja jaksottomia (näin on aina irrationaaliluvuilla.)
  Esim. $\sqrt{2} = 1,41421356\ldots$
  $\pi = 3,1415926535897323\ldots$
- Reaaliluvut ovat järjestyksessä.
- Ei ole pienintä eikä suurinta reaalilukua.
- Ei löydy suuruusjärjestyksessä seuraavaa.

Reaalilukujen määritelmä

Määritelmä

Reaalilukuja ovat sellaiset luvut, jotka voidaan ilmaista (mahdollisesti päättymättömänä ja jaksottomana) desimaalikehitelmänä.

Potenssimerkintä ja neliöjuuri

Olkoon n positiivinen kokonaisluku. Reaaliluvulle x käytetään potenssimerkintää

$$x^n = \underbrace{x \cdot x \cdots x}_{n \text{ kpl}}$$

ja mikäli $x \neq 0$, niin myös

$$x^{-n} = \frac{1}{x^n}.$$

Esim. $10^4 = 10 \cdot 10 \cdot 10 \cdot 10 = 10000$ ja $2^{-3} = \frac{1}{2^3} = \frac{1}{2 \cdot 2 \cdot 2} = \frac{1}{8}$.
Lisäksi on sovittu, että $x^0 = 1$ kaikilla $x \neq 0$.
Jokaisella reaaliluvulla $y \geq 0$ on myös olemassa n**:s juuri** eli reaaliluku $x \geq 0$, jolle pätee

$$x^n = y.$$

Tällaista lukua merkitään $x = \sqrt[n]{y}$. Tapauksessa $n = 2$ puhumme neliöjuuresta ja merkitään $x = \sqrt{y}$.

Esim. $\sqrt[3]{27} = 3$ ja $\sqrt{\frac{4}{9}} = \frac{2}{3}$.

Lukujen ominaisuuksia

Millä tahansa reaaliluvuilla a, b, c pätee:

- $a + b = b + a$, $ab = ba$ (vaihdannaisuus)
- $a + (b + c) = (a + b) + c$, $a(bc) = (ab)c$ (liitännäisyys)
- $a(b + c) = ab + ac$ (osittelulaki)
- jokaisella reaaliluvulla a on vastaluku $-a$, jolle pätee $a + (-a) = 0$
- jokaisella nollasta poikkeavalla reaaliluvulla a on käänteisluku $1/a$, jolle pätee $a \cdot (1/a) = 1$. Nollalla ei ole käänteislukua.

Yhtälöiden ominaisuuksia

Millä tahansa reaaliluvuilla a, b, c pätee:

- $a = b \iff a + c = b + c$
- $a = b \iff a - c = b - c$
- $a = b \implies c \cdot a = c \cdot b$
- $a = b \iff c \cdot a = c \cdot b$, mikäli $c \neq 0$
- $a = b \iff a/c = b/c$, mikäli $c \neq 0$
- $a \cdot b = 0 \iff a = 0$ tai $b = 0$ (tulon nollasääntö)

Ensimmäisen ja toisen asteen yhtälöt

Palautetaan lopuksi mieliin 1. ja 2. asteen yhtälöihin ja niiden ratkaisuun liittyvät perusasiat.

Ensimmäisen asteen yhtälö

Yhtälöä, joka on muotoa (tai voidaan saattaa muotoon) $ax + b = 0$, missä a ja b ovat reaalilukuja, sanotaan ensimmäisen asteen yhtälöksi. Mikäli $a \neq 0$, yhtälöllä on varmasti ratkaisu. Tämä löydetään vähentämällä yhtälön molemmilta puolilta b ja jakamalla luvulla a:

$$ax + b = 0 \iff ax = -b \iff x = \frac{-b}{a}.$$

Mikäli $a = 0$, yhtälö saa muodon $b = 0$, jolloin nähdään ettei yhtälön ratkeaminen riipu luvusta x, vaan joko yhtälö toteutuu kaikilla x:n arvoilla (kun $b = 0$) tai ei millään (kun $b \neq 0$).

Esimerkki

Millä muuttujan x arvoilla yhtälö $8x + 17 = 4x - 7$ on tosi?
Ratkaisu.

$$\begin{aligned}
8x + 17 = 4x - 7 \quad &\iff \quad 8x + 17 - 4x = 4x - 7 - 4x \\
&\iff \quad 4x + 17 = -7 \\
&\iff \quad 4x + 17 - 17 = -7 - 17 \\
&\iff \quad 4x = -24 \\
&\iff \quad x = \frac{-24}{4} = -6
\end{aligned}$$

Siis yhtälö on tosi jos ja vain jos $x = -6$, eli -6 on yhtälön ratkaisu ja ainoa sellainen.

Esimerkki

Millä muuttujan x arvoilla yhtälö $2x + 1 = \frac{8x-4}{4}$ on tosi?
Ratkaisu.

$$
\begin{aligned}
2x + 1 = \frac{8x - 4}{4} \quad &\iff \quad 4 \cdot (2x + 1) = 8x - 4 \\
&\iff \quad 8x + 4 = 8x - 4 \\
&\iff \quad 8x + 4 - 8x = 8x - 4 - 8x \\
&\iff \quad 4 = -4
\end{aligned}
$$

Olemme huomanneet, että alkuperäinen yhtälö ratkeaa jos ja vain jos $4 = -4$. Koska $4 \neq -4$, alkuperäisellä yhtälöllä ei ole ratkaisuja.

Esimerkki

Raimo osti luomumyymälästä yhteensä 740g ylihinnoiteltuja luomupähkinöitä ja -taateleita. Pähkinät maksoivat 22e/kg ja taatelit 28e/kg. Raimo maksoi ostoksistaan 17.54e. Kuinka paljon taateleita Raimo osti?

Esimerkki

Ratkaisu. Merkitään muuttujalla x Raimon ostamien taateleiden määrää kiloina. Näin saadaan yhtälö

$$28x + 22(0.740 - x) = 17.54,$$

joka sievenee muotoon $6x - 1.26 = 0$, eli ratkaisuksi saadaan $x = \frac{1.26}{6} = 0.210$. Raimo osti siis noin 210g taateleita.

Esimerkki

Taateleiden ja pähkinöiden lisäksi Raimo osti kuivattuja mansikoita, joista hän antoi kaksi viidesosaa vaimolleen, kuudesosan pojalleen ja jäljelle jääneistä 6 hän syötti naapurin koiralle. Raimo harmistui, sillä hänelle jäi itselleen vain 7 mansikkaa. Kuinka monta mansikoita alunperin oli?

Esimerkki

Ratkaisu. Merkitään mansikoiden kokonaismäärää x. Näin saadaan yhtälö

$$x - \frac{2}{5}x - \frac{1}{6}x - 6 = 7.$$

Tämä sievenee muotoon $\frac{13}{30}x - 13 = 0$, joka toteutuu kun $x = 30$.
Mansikoita oli siis alunperin 30.

Muistikaavat

Seuraavat kaavat on hyvä pitää mielessä mm. korkeampiasteisia yhtälöitä ratkoessa:
Olkoot a ja b reaalilukuja. Tällöin

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

Toisen asteen yhtälö

Toisen asteen yhtälöllä tarkoitetaan yhtälöä, joka on muotoa $ax^2 + bx + c = 0$, missä $a \neq 0$, b ja c ovat reaalilukuja.
Sen ratkeavuus ja ratkaisujen lukumäärä riippuvat sen **diskriminantista** $D = b^2 - 4ac$:

- Jos $D < 0$, niin yhtälöllä ei ole (reaalisia) ratkaisuja.
- Jos $D = 0$, niin yhtälöllä on yksi ratkaisu $x = -\frac{b}{2a}$.
- Jos $D > 0$, niin yhtälöllä on kaksi ratkaisua

$$x = \frac{-b \pm \sqrt{D}}{2a} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Esimerkkejä toisen asteen yhtälöistä

- $x^2 + x + 1 = 0$
  Tarkastellaan diskriminanttia: $D = 1^2 - 4 \cdot 1 \cdot 1 = 1 - 4 = -3 < 0$
  Yhtälöllä ei siis ole ratkaisuja.
- $x^2 - 2x + 1 = 0$
  $D = (-2)^2 - 4 \cdot 1 \cdot 1 = 4 - 4 = 0$
  Yhtälöllä on siis yksi ratkaisu $x = -\frac{b}{2a} = -\frac{-2}{2 \cdot 1} = 1$.
- $x^2 - x - 2 = 0$
  $D = (-1)^2 - 4 \cdot 1 \cdot (-2) = 1 + 8 = 9 > 0$
  Yhtälöllä on siis kaksi ratkaisua

$$x = \frac{-b \pm \sqrt{D}}{2a} = \frac{-(-1) \pm \sqrt{9}}{2 \cdot 1} = \frac{1 \pm 3}{2} \iff x = 2 \text{ tai } x = -1.$$

Esimerkki

Onko toisen asteen yhtälöllä $2x^2 - 8x + 6$ ratkaisuja? Jos on, niin mitkä ne ovat?

Ratkaisu. Tutkitaan yhtälön diskriminanttia. Koska $a = 2$, $b = -8$ ja $c = 6$, diskriminantti on

$$b^2 - 4ac = (-8)^2 - 4 \cdot 2 \cdot 6 = 64 - 48 = 16 > 0,$$

joten yhtälöllä on kaksi ratkaisua:

$$\frac{-b + \sqrt{D}}{2a} = \frac{-(-8) + \sqrt{16}}{2 \cdot 2} = \frac{8 + 4}{4} = 3$$

ja

$$\frac{-b - \sqrt{D}}{2a} = \frac{-(-8) - \sqrt{16}}{2 \cdot 2} = \frac{8 - 4}{4} = 1$$

Esimerkki

Maanviljelijä rakentaa lampaalleen suorakulmion muotoisen 15 neliömetrin aitauksen, jonka pidempi sivu on 2 metriä pidempi kuin lyhyempi sivu. Montako metriä aitaa hän tarvitsee?
Ratkaisu:

Merkitään x:llä aitauksen lyhyemmän sivun pituutta metreissä. Koska aitaus on muodoltaan suorakulmio, jonka pinta-ala on 15 neliömetriä, saadaan yhtälö $x(x+2) = 15$. Tämä voidaan kirjoittaa muodossa $x^2 + 2x - 15 = 0$ ja ratkaista ratkaisukaavalla:

$$x = \frac{-2 + \sqrt{2^2 + 4 \cdot 15}}{2} = \frac{-2 + \sqrt{64}}{2} = \frac{-2 + 8}{2} = 3.$$

Aitaa tarvitaan siis $2x + 2(x+2) = 6 + 10 = 16$ metriä.

Joukot ja funktiot

Joukot

Matematiikassa on pyrkimys määritellä monimutkaiset asiat täsmällisesti yksinkertaisempien asioiden avulla. Tarvitaan jokin lähtökohta, muutama yleisesti hyväksytty ja ymmärretty käsite, joista sitten rakennetaan muut käsitteet. Tarkastelemme seuraavaksi Georg Cantorin 1900-luvun taitteessa luomaa naiivia joukko-oppia.

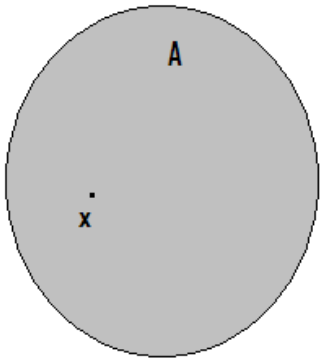
Georg Cantor (1845-1918)

Joukkojen peruskäsitteet

Määrittelemättömät peruskäsitteet ovat:
alkio, **joukko**, ja relaatio **"alkio kuuluu joukkoon"**.
Joukot siis muodostuvat alkioista. Merkitään

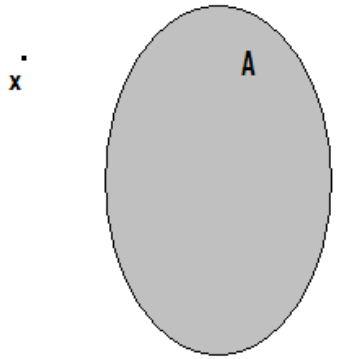
$x \quad \in \quad A$

alkio x kuuluu joukkoon A



$x \quad \notin \quad A$

alkio x ei kuulu joukkoon A



Joukkojen merkinnöistä

Huomattavaa:

- Joukkoja voidaan merkitä mm. seuraavin tavoin:
  $A_1 = \{a, b, c\}$, $A_2 = \{a, b, c, \ldots, h\}$, $A_3 = \{a, b, c, \ldots\}$
  tai käyttämällä alaindeksejä
  $B = \{a_1, a_2, a_3\}$, $C = \{a_1, a_2, \ldots, a_n\}$, $D = \{a_1, a_2, a_3, \ldots\}$
  tai antamalla ehto $E = \{x : x \text{ toteuttaa annetun ehdon}\}$,
  esim. $\{x : x \text{ on positiivinen reaaliluku}\}$ tai $\{x : x \text{ on hedelmä}\}$.
- Jokainen alkio esiintyy vain kerran, esim. $\{a, b, a\} = \{a, b\}$.
- Alkioiden järjestyksellä ei ole väliä, esim. $\{a, b\} = \{b, a\}$.
- Tyhjää joukkoa $\{\}$, jossa ei ole ollenkaan alkioita, merkitään $\emptyset$.

Samat joukot

Joukot ovat samat, jos niissä on täsmälleen samat alkiot.
Siis joukot A ja B ovat samat, merkitään $A = B$, kun pätee

$$x \in A, \text{ jos ja vain jos (lyhennetään joss.) } x \in B.$$

Joukot A ja B voidaan osoittaa samoiksi näyttämällä, että kaikki joukon A alkiot ovat myös joukossa B ja että kaikki joukon B alkiot ovat myös joukossa A.

Lukujoukot

Esimerkiksi juuri tarkastelemamme erilaiset luvut muodostavat lukujoukkoja. Näitä merkitään usein seuraavin symbolein

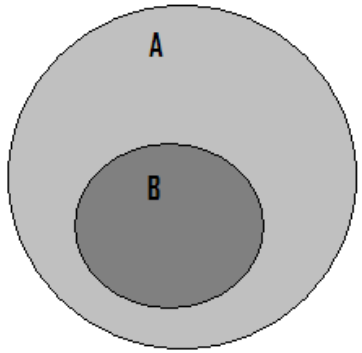
- Luonnolliset luvut $\mathbb{N} = \{0, 1, 2, \ldots\}$ (engl. natural numbers)
- Kokonaisluvut $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ (saksaksi Zahlen)
- Rationaaliluvut $\mathbb{Q} = \{\frac{m}{n} : m, n \in \mathbb{Z}, n \neq 0\}$ (engl. quotient = osamäärä)
- Reaaliluvut $\mathbb{R}$ (engl. real numbers)

Positiivisista (vastaavasti negatiivisista) kokonaisluvuista käytetään usein merkintää $\mathbb{Z}_+$ (vast. $\mathbb{Z}_-$) , ts.

$$\mathbb{Z}_+ = \{1, 2, 3, \ldots\} \quad \text{ja} \quad \mathbb{Z}_- = \{-1, -2, -3, \ldots\}.$$

Osajoukot

Joukko B on joukon A osajoukko, jos jokainen B:n alkio on myös A:n alkio.
Toisin sanoen jos $x \in B$, niin $x \in A$.
Tällöin merkitään $B \subset A$ (joskus $B \subseteq A$).



Esimerkiksi

- $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$.
- Olkoot $A = \{1, 2, 3\}$ ja $B = \{1, 4\}$. Tällöin $A \not\subset B$ ja $B \not\subset A$.
- Tyhjä joukko on jokaisen joukon osajoukko, eli $\emptyset \subset A$ millä tahansa joukolla A.

Huomaa, että $A = B$, jos ja vain jos $A \subset B$ ja $B \subset A$.

Reaalilukuvälit

Olkoot $a, b \in \mathbb{R}$. Merkitään reaalilukuvälejä

- $[a, b] = \{x \in \mathbb{R} : a \leq x \leq b\}$
- $[a, b[= \{x \in \mathbb{R} : a \leq x < b\}$
- $]a, b] = \{x \in \mathbb{R} : a < x \leq b\}$
- $]a, b[= \{x \in \mathbb{R} : a < x < b\}$

Esim. $]-3, \pi] = \{x \in \mathbb{R} : -3 < x \leq \pi\}$ ja $[0, 3] \subset]-3, \pi]$, sillä $\pi > 3$.

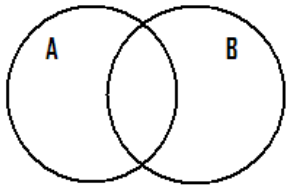
Rajoittamattomia reaalilukuvälejä merkitään vastaavasti:

- $[a, \infty[= \{x \in \mathbb{R} : x \geq a\}$
- $]a, \infty[= \{x \in \mathbb{R} : x > a\}$
- $]\infty, b] = \{x \in \mathbb{R} : x \leq b\}$
- $]\infty, b[= \{x \in \mathbb{R} : x < b\}$

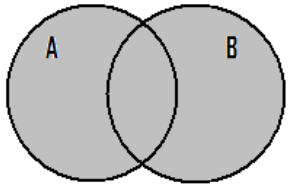
Joukko-operaatiot

Olkoot A ja B joukkoja.

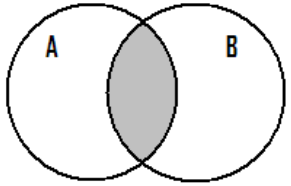
Määritellään



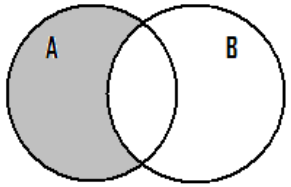
yhdiste $A \cup B = \{x : x \in A \text{ tai } x \in B\}$



leikkaus $A \cap B = \{x : x \in A \text{ ja } x \in B\}$



erotus $A \setminus B = \{x : x \in A \text{ ja } x \notin B\}$



Esimerkki joukko-operaatioiden käytöstä

Olkoon $A = \{1, 2, 3\}$ ja $B = \{3, 4, 5\}$. Nyt

- $A \cup B = \{1, 2, 3, 4, 5\}$
- $A \cap B = \{3\}$
- $A \setminus B = \{1, 2\}$

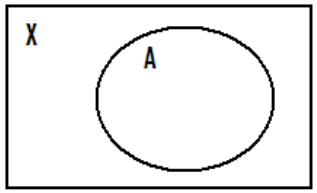
Huomaa, että joukko-operaatioita voidaan tietysti tehdä myös useammille joukoille.

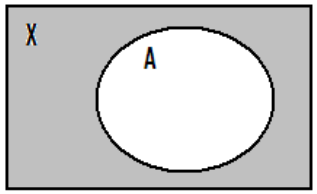
Komplementti

Olkoon X jokin *perusjoukko* ja $A \subset X$.

Määritellään

komplementti $A^{\complement} = \{x \in X : x \notin A\}$





Esimerkki joukko-operaatioiden käytöstä

Olkoon $X = \mathbb{R}$ perusjoukko ja olkoot $A =]-1, 1[$ ja $B = [1, 2[$. Nyt

- $A \cup B =]-1, 2[$
- $A \cap B = \emptyset$
- $A^{\complement} = \{x \in \mathbb{R} : x \leq -1 \text{ tai } x \geq 1\} =]-\infty, -1] \cup [1, \infty[$

Huom. Joukkoa A voidaan merkitä toisella tapaa muistamalla reaaliluvun **itseisarvo**

$$|x| = \begin{cases} x, & \text{jos } x \geq 0 \\ -x, & \text{jos } x < 0. \end{cases}$$

Huomaa, että $|x| \geq 0$ kaikilla $x \in \mathbb{R}$. Nyt voidaan merkitä

$$A =]-1, 1[= \{x \in \mathbb{R} : |x| < 1\}$$

ja toisaalta

$$A^{\complement} = \{x \in \mathbb{R} : |x| \geq 1\}.$$

Joukot alkioina

Joukko voi olla myös alkiona toisessa joukossa. On tärkeää oppia erottamaan alkion ja sen muodostaman joukon ero, samoin kuin relaatioiden $\in$ ("kuuluu") ja $\subset$ ("sisältyy") välinen ero.

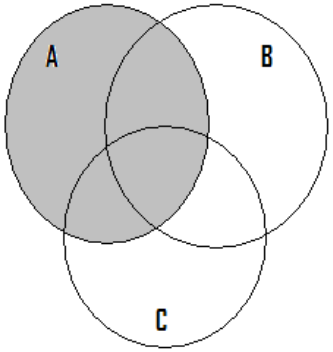
- Olkoon $A = \{1, 2, \{1, 2\}\}$. Nyt $\{1, 2\} \in A$ ja $\{1, 2\} \subset A$. Ei kuitenkaan $A \in A$.
- Onko $\{\emptyset\}$ tyhjä joukko?
  Onko $2 \in \{1, \{1, 2\}\}$?
- Eräs usein esiintyvä joukkojen muodostama joukko on **potenssijoukko**, eli annetun joukon kaikkien osajoukkojen muodostama joukko. Joukon A potenssijoukolle käytetään usein merkintää $\mathcal{P}(A)$. Esim. Joukon $\{1, 2, 3\}$ potenssijoukko on

$$\{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}.$$

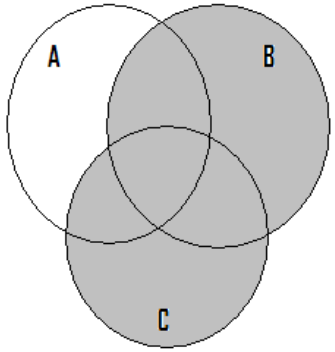
Huom. Jos joukossa on n alkiota, niin sen potenssijoukossa on 2^n alkiota. Kuinka tämä voidaan todistaa?

Osittelulaki

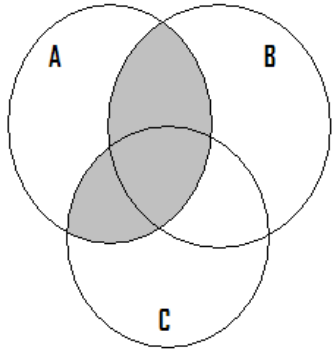
Olkoot A, B ja C joukkoja. Tarkastellaan osittelulakia
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ ensin Venn-diagrammien avulla:



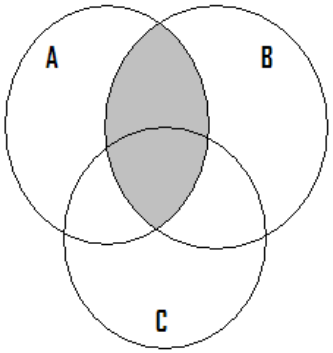
A



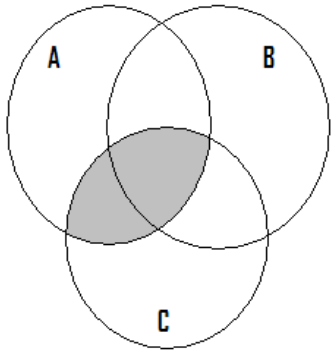
$B \cup C$



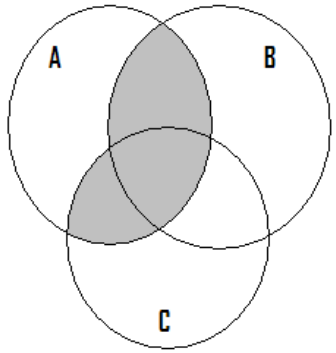
$A \cap (B \cup C)$



$A \cap B$



$A \cap C$



$(A \cap B) \cup (A \cap C)$

Osittelulain todistus

Todistetaan kaava $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

$\boxed{A \cap (B \cup C) \subset (A \cap B) \cup (A \cap C):}$

Olkoon x jokin joukon $A \cap (B \cup C)$ alkio.
Leikkauksen määritelmän mukaan $x \in A$ ja $x \in B \cup C$, josta edelleen yhdisteen määritelmän mukaan $x \in B$ tai $x \in C$:

- Jos $x \in B$, niin $x \in A \cap B \subset (A \cap B) \cup (A \cap C)$.
- Jos $x \in C$, niin $x \in A \cap C \subset (A \cap B) \cup (A \cap C)$.

Siis molemmissa tapauksissa $x \in (A \cap B) \cup (A \cap C)$.

$\boxed{(A \cap B) \cup (A \cap C) \subset A \cap (B \cup C):}$

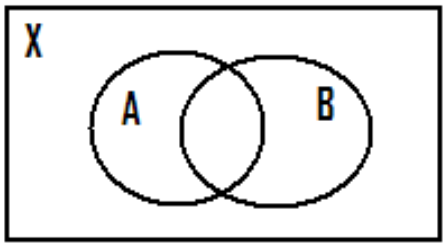
Olkoon x jokin joukon $(A \cap B) \cup (A \cap C)$ alkio.
Yhdisteen määritelmän mukaan $x \in A \cap B$ tai $x \in A \cap C$.

- Jos $x \in A \cap B$, niin $x \in A$ ja $x \in B \subset B \cup C$, eli $x \in A \cap (B \cup C)$.
- Jos $x \in A \cap C$, niin $x \in A$ ja $x \in C \subset B \cup C$, eli $x \in A \cap (B \cup C)$.

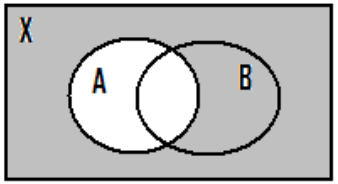
Molemmissa tapauksissa $x \in A \cap (B \cup C)$.

De Morganin laki

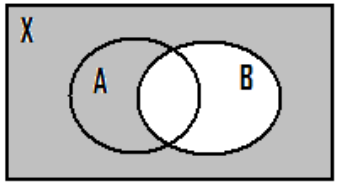
Olkoot A ja B perusjoukon X osajoukkoja.



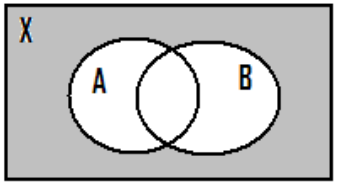
Tarkastellaan De Morganin lakia $(A \cup B)^C = A^C \cap B^C$:



A^C



B^C



$A^C \cap B^C$

De Morganin lain todistus

Olkoon $x \in X$. Nyt $x \in (A \cup B)^{\mathsf{C}}$

$$\iff x \notin A \cup B$$

$$\iff x \notin A \text{ ja } x \notin B$$

$$\iff x \in A^{\mathsf{C}} \text{ ja } x \in B^{\mathsf{C}}$$

$$\iff x \in A^{\mathsf{C}} \cap B^{\mathsf{C}}$$

Siis $(A \cup B)^{\mathsf{C}} = A^{\mathsf{C}} \cap B^{\mathsf{C}}$.

Joukkojen identtisyyksiä

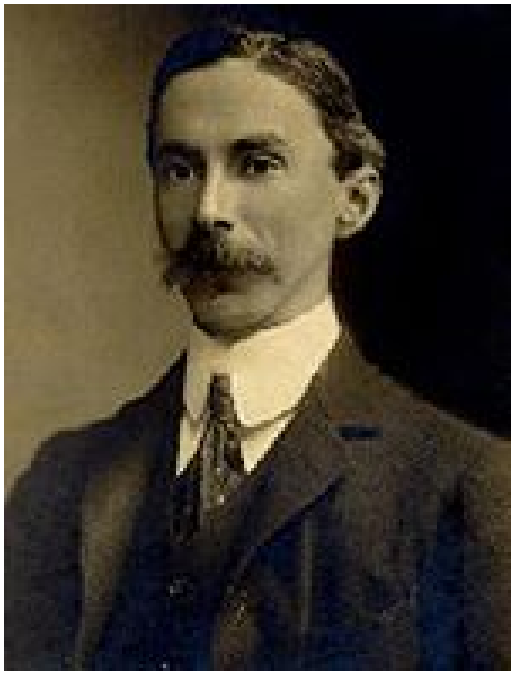
Olkoot A, B ja C perusjoukon X osajoukkoja. Tällöin

- $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ (eli aikaisempi esimerkki)
- $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ (todistus harjoitustehtävänä)
- $(A \cup B)^{\complement} = A^{\complement} \cap B^{\complement}$ (eli äskeinen esimerkki)
- $(A \cap B)^{\complement} = A^{\complement} \cup B^{\complement}$ (myös De Morganin laki)

Russellin paradoksi

Yllä esitettyä joukko-oppia sanotaan naiiviksi, koska sen intuitiivinen ja määrittelemätön joukkokäsite johtaa paradoksiin.

Filosofi Bertrand Russell esitti vuonna 1901 esimerkin:
Olkoon R kaikkien niiden joukkojen joukko, jotka eivät sisällä itseään alkionaan.
Siis: $R = \{A : A \notin A\}$. Onko $R \in R$?
Jos $R \in R$ eli R sisältää itsensä alkionaan, niin R ei toteuta määritelmän ehtoa jolloin $R \notin R$.
Jos taas $R \notin R$ eli R ei sisällä itseään alkionaan, niin toteuttaa määritelmän ehdon jolloin $R \in R$.
Molemmat vaihdoehdot johtivat ristiriitaan.



Bertrand Russell (1872-1970)

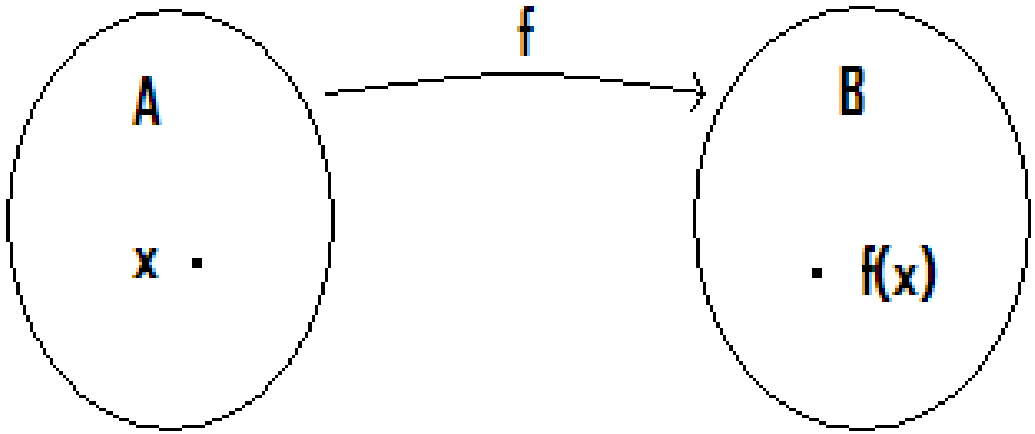
Joukkojen muodostaminen ei siis ole aivan niin vapaata kuin annoimme aluksi ymmärtää. Aksiomaattinen lähestymistapa joukko-oppiin auttaa korjaamaan nämä ongelmat, siinä esimerkiksi itsensä sisältävä "luokka" ei ole joukko.

Funktiot

Funktio on eräs matematiikan tärkeimmistä käsitteistä. Sen voi intuitiivisesti ajatella kuvaavan riippuvuussuhdetta, jossa tarkasteltava suure määräytyy täsmällisesti jostakin muusta suureesta.

Funktion määritelmä

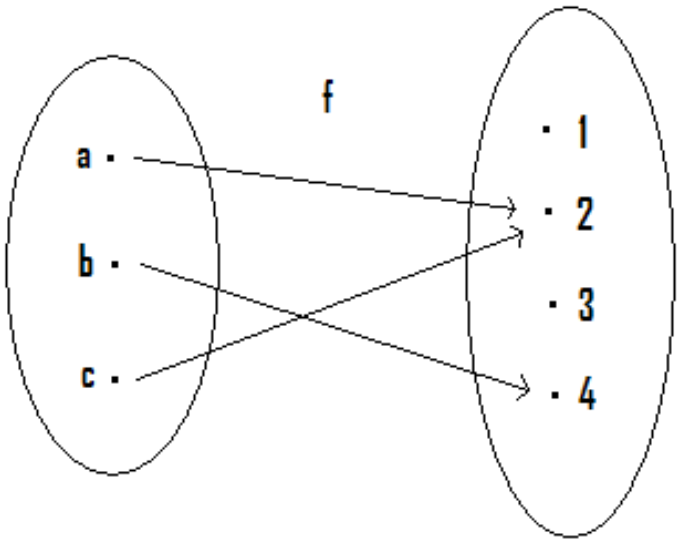
Olkoot A ja B joukkoja.
Funktio eli **kuvaus** f joukolta A joukkoon B, merk. $f : A \to B$, liittää jokaiseen alkioon $x \in A$ täsmälleen yhden alkion $f(x) \in B$.



Sanotaan, että A on f:n **määrittelyjoukko** (tai **lähtöjoukko**) ja B on f:n **maalijoukko**.

Esimerkki funktiosta

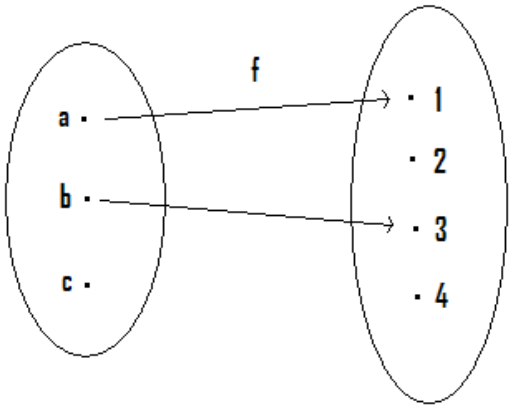
Esim. Olkoon $A = \{a, b, c\}$ ja $B = \{1, 2, 3, 4\}$. Määritellään $f : A \to B$ asettamalla $f(a) = 2$, $f(b) = 4$ ja $f(c) = 2$.
f:n nuolikaavio:



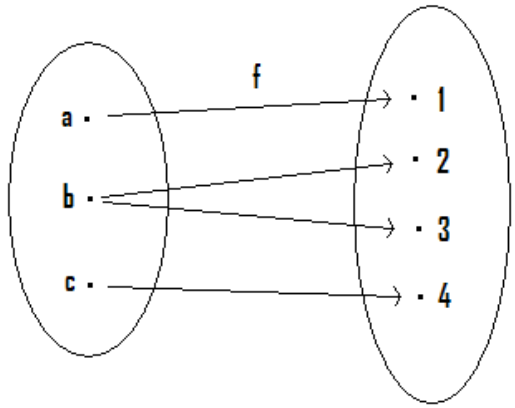
Kuten yllä, kaikkia maalijoukon alkioita ei välttämättä "saavuteta" (mikään A:n alkio ei kuvaudu B:n alkioille 1 tai 3).
Funktion saavuttamat arvot muodostavat sen **arvojoukon**. Yllä arvojoukko $= \{f(a), f(b), f(c)\} = \{2, 4\} \subset \{1, 2, 3, 4\} = B$.

Mikä pielessä?

Mikä on pielessä seuraavissa yrityksissä määritellä funktio $f : \{a, b, c\} \to \{1, 2, 3, 4\}$?



Funktio $f : A \to B$, liittää jokaiseen alkioon $x \in A$ täsmälleen yhden alkion $f(x) \in B$.



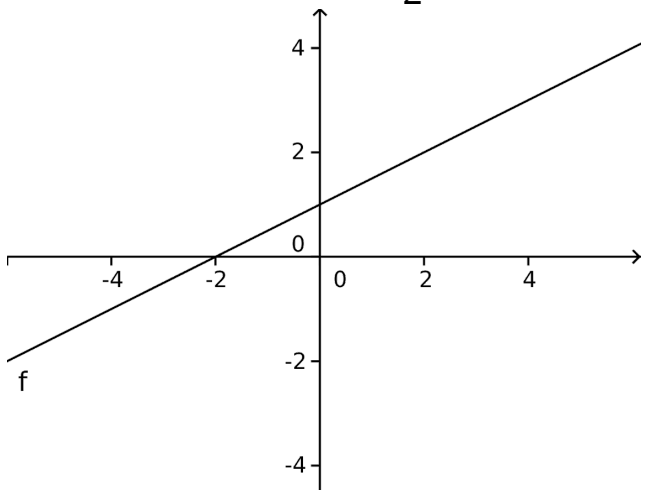
Funktio $f : A \to B$, liittää jokaiseen alkioon $x \in A$ täsmälleen yhden alkion $f(x) \in B$.

Reaalifunktion kuvaaja

Reaalifunktiolla tarkoitetaan funktiota $\mathbb{R} \to \mathbb{R}$ (tai osajoukolta $A \subset \mathbb{R}$ reaaliluvuille).
Niitä on kätevä havainnollistaa kuvaajalla.

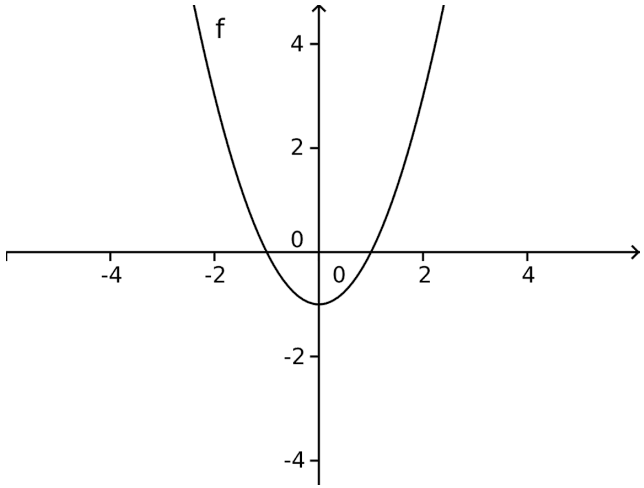
Esimerkkejä funktioiden kuvaajista

$f : \mathbb{R} \to \mathbb{R}, \quad f(x) = \frac{1}{2}x + 1$



f:n kuvaaja on kulmakertoimella $\frac{1}{2}$ nouseva suora.

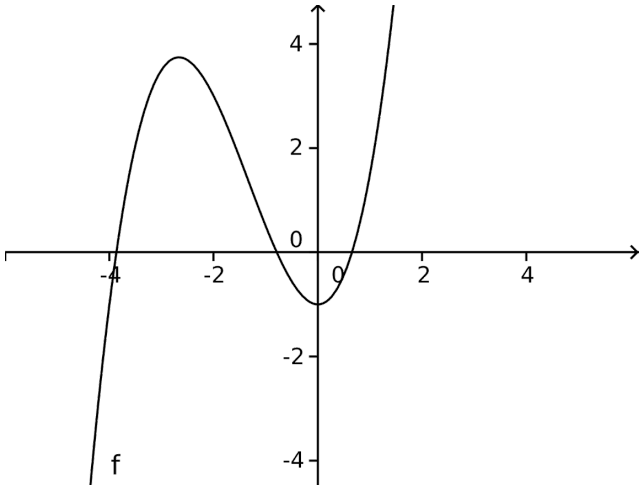
$f : \mathbb{R} \to \mathbb{R}, \quad f(x) = x^2 - 1$



f:n kuvaaja on ylöspäin aukeava paraabeli.

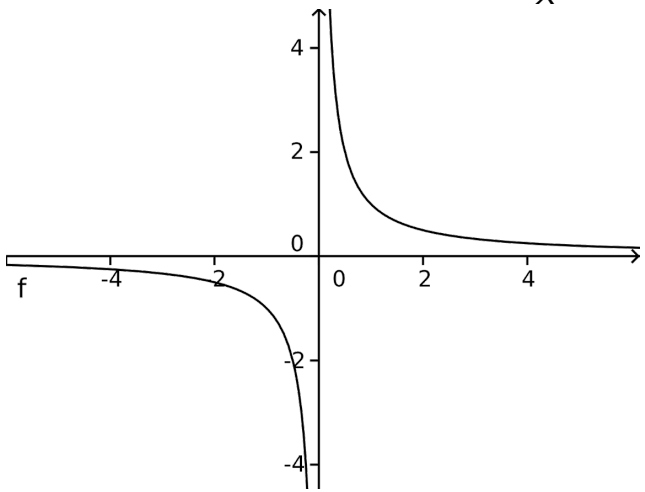
Esimerkkejä funktioiden kuvaajista

$f : \mathbb{R} \to \mathbb{R}, \quad f(x) = \frac{1}{2}x^3 + 2x^2 - 1$



f:n kuvaaja on kolmannen asteen käyrä.

$f : \mathbb{R} \setminus \{0\} \to \mathbb{R}, \quad f(x) = \frac{1}{x}$



f:n arvot kasvavat (vähenevät) rajatta, kun nollaa lähestytään oikealta (vasemmalta).

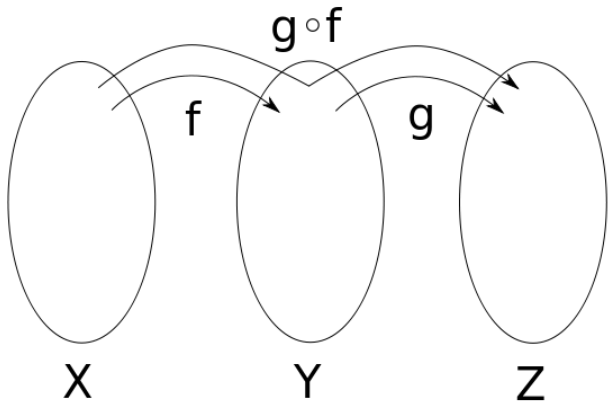
Analyysi

Reaalifunktioista, niiden *derivaatoista* ja *integraaleista* enemmän analyysin kursseilla (esim. Analyysi I ja II, Matemaattisen analyysin kurssi, Analyysin virtuaalinen peruskurssi).

Funktioiden yhdistäminen

Olkoon $f : X \to Y$ ja $g : Y \to Z$.
Määritellään funktioiden f ja g
yhdiste $g \circ f : X \to Z$:

$$(g \circ f)(x) = g(f(x)).$$



Esim. Olkoon $f : \mathbb{R} \setminus \{0\} \to \mathbb{R}, f(x) = \frac{1}{x}$, $g : \mathbb{R} \to \mathbb{R}, g(x) = x^2 + 1$. Nyt

$$(g \circ f)(x) = g(f(x)) = \left(\frac{1}{x}\right)^2 + 1.$$

Lukumääräfunktio

Vilkaisimme aikaisemmin joukon $\{1, 2, 3\}$ potenssijoukkoa, eli sen kaikkien osajoukkojen joukkoa

$$\{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}.$$

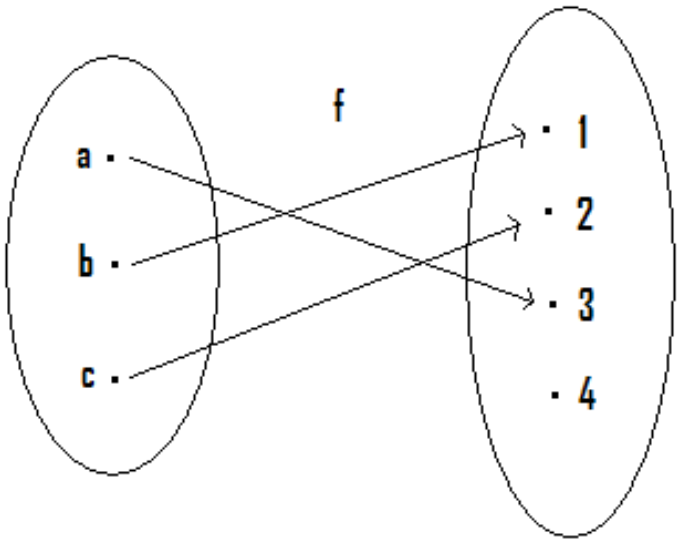
Merkitään tätä joukkoa $\mathcal{P}(\{1, 2, 3\})$:lla ja määritellään funktio $\# : \mathcal{P}(\{1, 2, 3\}) \to \mathbb{N}$, joka liittää jokaiseen näistä osajoukoista sen alkioiden lukumäärän (tarkastelemme tätä käsitettä tarkemmin hetken kuluttua). Siis esim. $\#(\{2\}) = 1$, $\#(\emptyset) = 0$ ja $\#(\{1, 3\}) = 2$. Myös esim.

$$\#(\{1, 2\} \cup \{3\}) = \#(\{1, 2\}) + \#(\{3\}).$$

Tällaiset joukoille määritellyt funktiot, jotka jollain tapaa "mittaavat" joukkojen kokoa, ovat erittäin tärkeitä matemaattisessa analyysissa.

Injektio

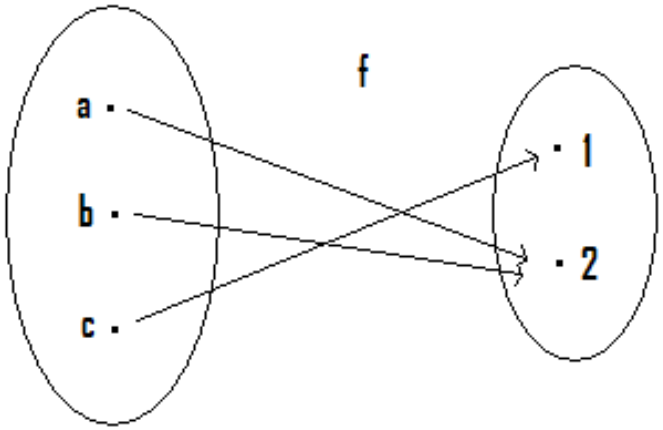
Funktiota sanotaan **injektioksi**, mikäli lähtöjoukon eri alkiot kuvautuvat maalijoukon eri alkioille. Esim.



Funktio f on siis injektio mikäli ehdosta $f(x_1) = f(x_2)$ seuraa, että $x_1 = x_2$.

Surjektio

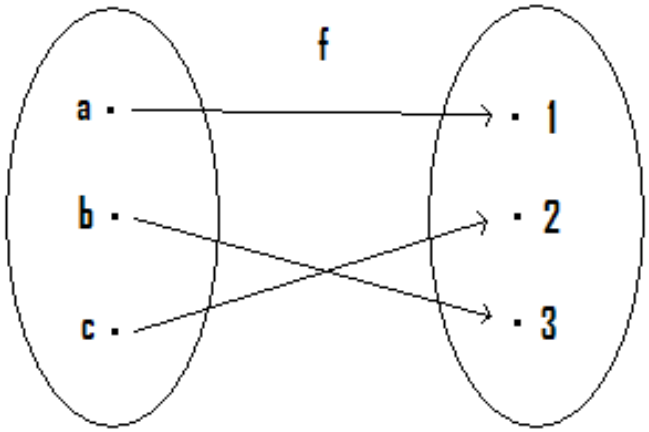
Funktiota sanotaan **surjektioksi**, mikäli sen arvojoukko on koko maalijoukko. Esim.



Funktio $f : A \to B$ on siis surjektio, mikäli jokaista $y \in B$ kohti löytyy $x \in A$, jolle $f(x) = y$.

Bijektio

Funktiota sanotaan **bijektioksi**, mikäli se on sekä injektio että surjektio. Esim.



Esimerkki

Määritellään funktio $f : \mathbb{R} \to \mathbb{R}$, $f(x) = 2x + 1$. Näin määritelty funktio on injektio.

Todistus.

Oletetaan, että $f(x) = f(y)$. Tällöin siis $2x + 1 = 2y + 1$. Nyt

$$\begin{aligned} & 2x + 1 = 2y + 1 && \| -1 \\ \Longrightarrow \quad & 2x = 2y && \| : 2 \\ \Longrightarrow \quad & x = y \end{aligned}$$

Siispä jos $x \neq y$, niin $f(x) \neq f(y)$, eli funktio f on injektio. $\square$

Esimerkki

Osoitetaan, että funktio $f : \mathbb{R} \to \mathbb{R}$, $f(x) = 2x + 1$, on surjektio.

Todistus.

Olkoon $y \in \mathbb{R}$ jokin reaaliluku (maalijoukon alkio). Ratkaistaan yhtälö $f(x) = y$, eli $2x + 1 = y$:

$$\begin{aligned} & 2x + 1 = y && \| -1 \\ \iff & 2x = y - 1 && \| : 2 \\ \iff & x = \tfrac{y-1}{2}. \end{aligned}$$

Siispä millä tahansa reaaliluvulla y pätee: $f\left(\frac{y-1}{2}\right) = y$. Koska $\frac{y-1}{2}$ on reaaliluku ja siten lähtöjoukon alkio, jokaista maalijoukon alkiota kohti on löydetty lähtöjoukon alkio, joka sille kuvautuu. Siispä funktio f on surjektio. □

Esimerkki

Osoitetaan, että funktio $h\colon \mathbb{R} \to \mathbb{R}$, $h(x) = x^2 - 1$, ei ole injektio.

Todistus.

Huomataan, että $h(-1) = (-1)^2 - 1 = 1 - 1 = 0$, ja $h(1) = 1^2 - 1 = 1 - 1 = 0$. Funktio siis kuvaa lähtöjoukosta kaksi eri alkiota -1 ja 1 samalle maalijoukon alkiolle, joten se ei ole injektio. □

Esimerkki

Osoitetaan, että funktio $h\colon \mathbb{R} \to \mathbb{R}$, $h(x) = x^2 - 1$, ei ole surjektio.

Todistus.

Tutkitaan, kuvaako funktio h mitään lukua x luvuksi -2. Tutkitaan siis milloin yhtälö $h(x) = -2$ voisi ratketa.

$$\begin{aligned} & h(x) &= -2 & \\ \iff & x^2 - 1 &= -2 & \quad \| +1 \\ \iff & x^2 &= -1. & \end{aligned}$$

Funktio h siis kuvaa luvun x luvuksi -2 jos ja vain jos x kerrottuna itsellään on -1. Mikään x ei tätä toteuta (minkään reaaliluvun toinen potenssi ei voi olla negatiivinen), joten funktio h ei kuvaa mitään lukua x luvulle -2, eikä se siten ole surjektio. $\square$

Tarkastelemme seuraavaksi erilaisten joukkojen kokoja. Lähdetään siitä, että

- tyhjässä joukossa $\emptyset$ ei ole yhtään alkiota
- joukossa $\{1\}$ on yksi alkio
- joukossa $\{1, 2, \ldots, n\}$ on n alkiota

Kuinka mittaamme muunlaisten joukkojen kokoa? Vastaus: Käytämme apuna bijektioita.

Määritelmä

Joukko A on **äärellinen**, mikäli on olemassa bijektio $A \to \{1, 2, \ldots, n\}$ jollakin $n \in \mathbb{Z}_+$. Joukossa A on tällöin n alkiota, merkitään $\#A = n$.

Joukossa A on siis tarkalleen n alkiota, mikäli jokaista A:n alkiota vastaa täsmälleen yksi luku $1, 2, \ldots, n$. Huom. myös tyhjää joukkoa sanotaan äärelliseksi.

Esimerkki

Osoita, että joukot $A = \{1, 3, 5, 7, 9\}$ ja $B = \{1, 4, 9, 16, 25\}$ ovat yhtä suuret, toisin sanoen etsi bijektio joukolta A joukolle B.

Ratkaisu: Haluttu bijektio saadaan asettamalla kaikilla $m \in A$

$$f : A \to B, \quad f(m) = \left(\frac{m+1}{2}\right)^2.$$

Kuvaus todella on bijektio (tarkista yksityiskohdat).
Entä jos $A = \{1, 3, 5, 7, \ldots\}$ ja $B = \{1, 4, 9, 16, \ldots\}$, ts. molemmissa joukoissa on ääretön määrä alkioita?

Joukkoa, joka ei ole äärellinen sanotaan **äärettömäksi**. Vaikka tarkasteltavat joukot olisivatkin äärettömiä, voidaan niiden kokoja kuitenkin vertailla:

Määritelmä

Joukot A ja B ovat **yhtä mahtavat** mikäli on olemassa bijektio $A \to B$.

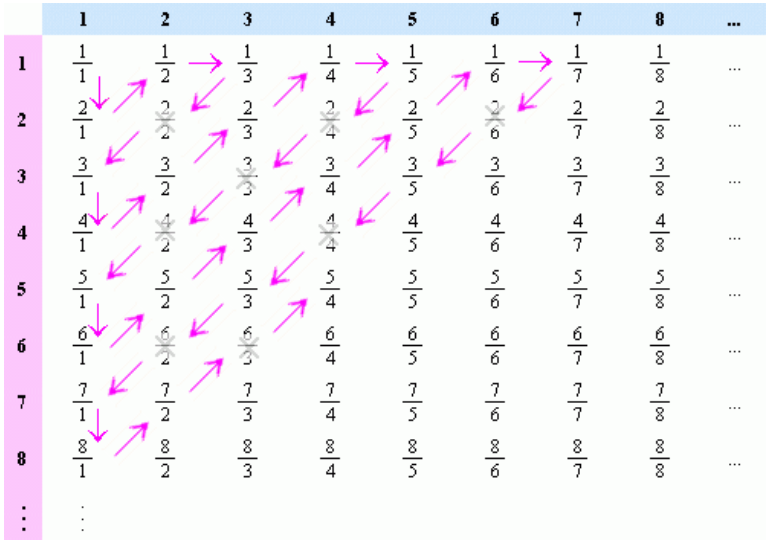
Luonnollisten lukujen joukko $\mathbb{N}$ on "pienin" ääretön joukko. Sen kanssa yhtä mahtavia joukkoja sanotaan **numeroituvasti äärettömiksi**. Esim. $\mathbb{N}$ ja $\{0, 2, 4, \ldots\}$ ovat yhtä mahtavat: $f(n) = 2n$ määrittelee bijektion niiden välille. Joukkojen välillä on siis vastaavuus

$$\begin{array}{ccccccc} 0 & 1 & 2 & 3 & 4 & \cdots \\ \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \cdots \\ 0 & 2 & 4 & 6 & 8 & \cdots \end{array}$$

Numeroituvuuden osoittamiseksi riittää oleellisesti löytää tapa luetella tarkasteltavan joukon jäsenet jossakin järjestyksessä. Vastaavasti nähdään helposti, että $\mathbb{Z}$ on numeroituva.

$\mathbb{Q}$ on numeroituva

Esitetään aluksi tapa luetella positiiviset rationaaliluvut. Taulukoidaan ne osoittajan ja nimittäjän suhteen kasvavaan järjestykseen ja lähdetään liikkeelle vasemmasta ylänurkasta, eli luvusta $\frac{1}{1}$ kuvan osoittamalla tavalla. Kuten kuvassa, hypätään vastaantulevan murtoluvun yli, mikäli sitä vastaava rationaaliluku on jo osunut kohdalle. Tällä tavoin saadaan käytyä läpi kaikki positiiviset rationaaliluvut. Huomaa, että lukuja ei lueteltu suuruusjärjestyksessä.



$\mathbb{Q}$ on numeroituva

Entäpä negatiiviset rationaaliluvut? Jos positiivisia rationaalilukuja, joiden joukko juuri osoitettiin numeroituvaksi, merkitään $q_1, q_2, q_3, \ldots$, niin voidaan määritellä vastaavuus

$$\begin{array}{ccccccc} 0 & 1 & 2 & 3 & 4 & \cdots \\ \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \cdots \\ 0 & q_1 & -q_1 & q_2 & -q_2 & \cdots \end{array}$$

On siis olemassa bijektio $\mathbb{N} \to \mathbb{Q}$, eli $\mathbb{Q}$ on numeroituva.

$\mathbb{Q}$ on numeroituva

Rationaalilukujen numeroituvuus voidaan nähdä myös toisella tavalla. Määritellään positiivisten kokonaislukujen pareilla (n, m) funktio $f(n, m) = 2^n 3^m$. Koska 2 ja 3 ovat alkulukuja (tutustutaan näihin ensi viikolla), niin f on injektio. Tämä tarkoittaa sitä, että positiivisten kokonaislukujen parien muodostama joukko on "korkeintaan" yhtä mahtava kuin $\mathbb{N}$. Takuulla noita pareja on kuitenkin äärettömän monta ja siten niiden joukko on yhtä mahtava kuin $\mathbb{N}$. Rationaaliluvut voidaan puolestaan ajatella kokonaislukuparien osajoukkona, kuten aiemminkin.

Aikaisemmin katsottiin kahden joukon yhdisteitä ja leikkauksia. Jos I on mikä tahansa *indeksijoukko* ja A_i on kullakin indeksillä $i \in I$ jokin joukko, niin voimme määritellä

$$\bigcup_{i \in I} A_i = \{x : x \in A_i \quad \text{jollakin } i \in I\}$$

ja

$$\bigcap_{i \in I} A_i = \{x : x \in A_i \quad \text{jokaisella } i \in I\}.$$

Jos I on numeroituva, ja jokainen A_i, $i \in I$, on numeroituva, niin yhdiste $\bigcup_{i \in I} A_i$ on numeroituva. Tämä nähdään oleellisesti samalla tavalla, kuin positiivisten rationaalilukujen joukon numeroituvuus.

$\mathbb{R}$ on ylinumeroituva

Osoitetaan, että $\mathbb{R}$ on **ylinumeroituva**, ts. että se ei ole numeroituva. Jokainen reaaliluku voidaan kirjoittaa yksikäsitteisesti päättymättömänä desimaalilukuna. Päättyvä luku, esim. $1,2$ kirjoitetaan tässä siis käyttämällä yhdeksikköjä, eli muodossa $1,1999\ldots$. Tehdään vastaoletus: $\mathbb{R}$ on numeroituva. Tässä tapauksessa, kaikki reaaliluvut voidaan esittää luettelossa

$$
\begin{array}{l}
n_{11}, c_{12}c_{13}c_{14}\ldots \\
n_{21}, c_{22}c_{23}c_{24}\ldots \\
n_{31}, c_{32}c_{33}c_{34}\ldots \\
\vdots
\end{array}
\qquad\qquad
\begin{array}{l}
m_1, c_{12}c_{13}c_{14}\ldots \\
n_{21}, d_2\ c_{23}c_{24}\ldots \\
n_{31}, c_{32}d_3\ c_{34}\ldots \\
\vdots
\end{array}
$$

missä n_{ij}:t ovat kokonaislukuja ja c_{ij}:t ovat numeroita $0,1,2,3,\ldots,9$. Konstruoidaan sitten reaaliluku, joka ei ole tuossa luettelossa: Olkoon ensin $m_1 \neq n_{11}$ kokonaisluku, sitten $d_2 \neq c_{22}$ numero,$d_3 \neq c_{33}$ jne. Näin saadaan reaaliluku $m_1, d_2d_3\ldots$, joka ei ole luettelossa (jokainen luettelon luvuista eroaa siitä vähintään yhden desimaalin kohdalla). Tämä on ristiriita, joten vastaoletuksen on oltava väärin.

Reaalilukujen ylinumeroituvia osajoukkoja

- Se, että reaaliluvut voivat olla rajoittamattoman suuria tai pieniä, ei ollut oleellista $\mathbb{R}$:n ylinumeroituvuuden kannalta. Vastaavanlainen konstruktio voitaisiin tehdä yksikkövälille $[0, 1[$, joka siis myös on ylinumeroituva.
- Koska $\mathbb{R} = \mathbb{Q} \cup (\mathbb{R} \setminus \mathbb{Q})$, ja $\mathbb{Q}$ on numeroituva, niin irrationaalilukujen joukon $\mathbb{R} \setminus \mathbb{Q}$ on oltava ylinumeroituva.
- Aiemmin esillä olleiden algebrallisten reaalilukujen joukko nähdään melko helposti numeroituvaksi. Siispä transendenttisten lukujen joukko on oltava ylinumeroituva. Huom. tämä on eräs tapa osoittaa, että niitä on yleensäkään olemassa.

Luonnollisten lukujen potenssijoukko

Luonnollisten lukujen äärellisten osajoukkojen muodostama joukko on numeroituva, kun taas $\mathbb{N}$:n äärettömien osajoukkojen joukko on ylinumeroituva. Luonnollisten lukujen potenssijoukko, joka koostuu siis $\mathbb{N}$:n äärellisistä ja äärettömistä osajoukoista, on siten ylinumeroituva. Itseasiassa se ja $\mathbb{R}$ ovat yhtä mahtavat.

$]0,1[$ ja $\mathbb{R}$ ovat yhtä mahtavat

Trigonometriaa opiskelleet tuntevat tangenttifunktion

$$\tan : \left]-\frac{\pi}{2}, \frac{\pi}{2}\right[\to \mathbb{R}, \quad \tan(x) = \frac{\sin(x)}{\cos(x)}.$$

tan on bijektio, joten $\left]-\frac{\pi}{2}, \frac{\pi}{2}\right[$ ja $\mathbb{R}$ ovat yhtä mahtavat. Toisaalta, olivatpa $a < b$ ja $c < d$ mitä tahansa reaalilukuja, funktio

$$f :]a, b[\to]c, d[, \quad f(x) = c + \frac{d-c}{b-a}(x-a)$$

on bijektio. Siis välit $]a, b[$ ja $]c, d[$ ovat yhtä mahtavat. Erityisesti välit $\left]-\frac{\pi}{2}, \frac{\pi}{2}\right[$ ja $]0,1[$ ovat yhtä mahtavat ja siten $]0,1[$ ja $\mathbb{R}$ ovat yhtä mahtavat.

Viiva on yhtä mahtava kuin neliö

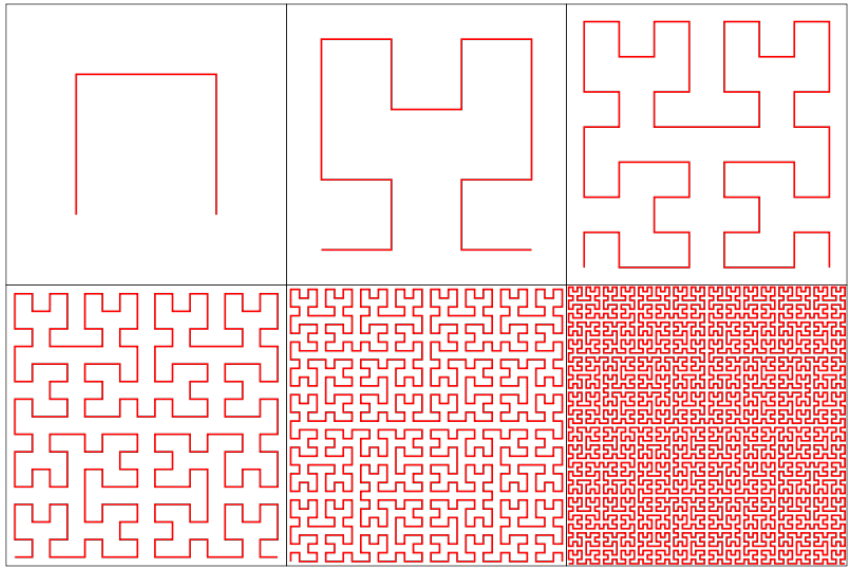
Georg Cantor onnistui ensimmäisenä konstruoimaan bijektion yksikkövälilltä $[0, 1]$ yksikköneliölle. Sitä seurasi Giuseppe Peanon löytämä ensimmäinen "avaruuden täyttävä käyrä". Myös David Hilbert konstruoi oman "avaruuden täyttävän käyränsä", jota katsomme nyt hieman tarkemmin.

Giuseppe Peano (1858-1932)

David Hilbert (1862-1943)

Hilbertin käyrä

Kuvassa näkyy Hilbertin käyrän konstruktion kuusi ensimmäistä vaihetta:



Käyrä joka lopulta täyttää yksikköneliön saadaan tämän konstruktion *rajafunktiona*. Näin saatu käyrä on analyysin mielessä *jatkuva*; se on seurausta konstruktiossa olevien funktioiden *tasaisesta suppenemisesta*. Se todellakin täyttää koko neliön: Tarkastellaanpa mitä hyvänsä neliön pistettä, löytyy konstruktiossa vaihe, joka kulkee mielivaltaisen läheltä tuota pistettä. Siten rajafunktion täytyy koskettaa tuota pistettä. Saatu avaruuden täyttävä käyrä kuitenkin leikkaa itseään, eli se ei ole injektio.

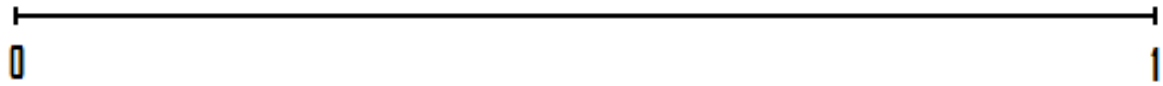
Hilbertin käyrä

Mahtavuuksien kannalta tämä tarkoittaa sitä, että yksikköväli on *ainakin yhtä mahtava* kuin neliö. Koska yksikköväli on neliön osajoukko, ovat ne yhtä mahtavat. Päättelyä voi vielä jatkaa toteamalla, että neliö ja taso ovat yhtä mahtavat (kuten reaalisuora ja yksikköväli). Siis yksikköväli on yhtä mahtava kuin taso.

Cantorin joukko

Konstruoidaan seuraavaksi Cantorin joukko. Lähdetään liikkeelle yksikkövälistä

$$C_0 = [0, 1]$$



Otetaan siitä pois keskimmäinen kolmannes, jolloin jäljelle jää

$$C_1 = \left[0, \frac{1}{3}\right] \cup \left[\frac{2}{3}, 1\right]$$

Otetaan taas molemmista väleistä pois keskimmäinen kolmannes:

$$C_2 = \left[0, \frac{1}{9}\right] \cup \left[\frac{2}{9}, \frac{1}{3}\right] \cup \left[\frac{2}{3}, \frac{7}{9}\right] \cup \left[\frac{8}{9}, 1\right]$$

Cantorin joukko

Jatketaan samaan malliin, eli määritellään C_i kaikilla positiivisilla kokonaisluvuilla i ottamalla edellisen joukon muodostavista väleistä pois keskimmäinen kolmannes. Määritellään Cantorin joukko näiden leikkauksena:

$$C = \bigcap_{i \in \mathbb{N}} C_i.$$

Mitkä reaaliluvut kuuluvat tähän joukkoon vai onko se kenties tyhjä joukko? Tarkastelemalla välin $[0, 1]$ lukuja 3-kantaisessa järjestelmässä huomataan, että C_1 koostuu luvuista joiden desimaaliesitys kannassa kolme alkaa $0,0\ldots_3$ tai $0,2\ldots_3$. Esim. $1/3 = 0,1_3 = 0,0\overline{2}_3$ ja $1 = 0,\overline{2}_3$ kuuluvat C_1:een , mutta $1/2 = 0,\overline{1}_3$ ei. Vastaavasti C_2 koostuu luvuista joiden desimaaliesitys kannassa kolme alkaa $0,a_1a_2\ldots_3$, missä $a_1, a_2 \in \{0, 2\}$. Esim. $2/9 = 0,02_3$ ja $7/9 = 0,21_3 = 0,20\overline{2}_3$ kuuluvat C_2:een, mutta $5/9 = 0,12_3$ ei.

Cantorin joukko

Yleisesti, C_i koostuu reaaliluvuista joiden (eräs) desimaaliesitys kannassa kolme on muotoa $0, a_1 a_2 a_3 \ldots_3$, missä $a_1, a_2, \ldots, a_i \in \{0, 2\}$. Loppujen lopuksi, koko Cantorin joukko C koostuu reaaliluvuista, joiden (jossakin) kolmikantaisessa esityksessä esiintyy vain nollia ja kakkosia. Tällaisten lukujen joukko on ylinumeroituva, ts. C on ylinumeroituva. Kuitenkin kukin C_i koostuu $(2/3)^i$ kokoisista väleistä, joten C sisältyy mielivaltaisen pieneen välien yhdisteeseen. Toisin sanoen, sen mitta, eli pituus on nolla. Eikä siinä vielä kaikki. Dimensio eli ulottuvuus voidaan määritellä järkevästi tällaisellekin "fraktaalijoukolle". Cantorin joukon ulottuvuudeksi voidaan laskea

$$\frac{\log 2}{\log 3}.$$

Eksponentti- ja logaritmifunktio

Eksponentti- ja logaritmifunktiot

Eksponentti- ja logaritmifunktiot liittyvät läheisesti toisiinsa. Eksponenttifunktio tulee vastaan ilmiöissä, joissa tarkasteltava suure kasvaa tai vähenee suhteessa senhetkiseen arvoonsa. Niinpä esimerkiksi eksponentiaalinen kasvaminen on hyvin nopeata. Logaritmifunktio on tietyssä mielessä eksponenttifunktion *käänteisfunktio*. Sekin kasvaa (kun kantaluku > 1), mutta erittäin hitaasti.

Potenssin määritelmä

Määritellään *kantaluvun* $a > 0$ potenssi:

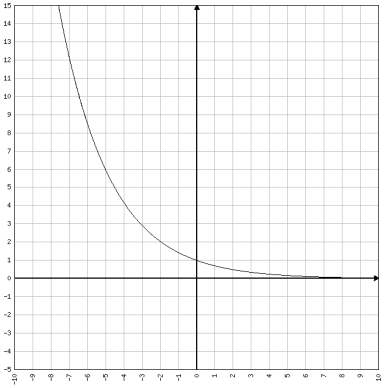
- Jos $m \in \mathbb{Z}$ on positiivinen, niin $a^m = a \cdot a \cdot \ldots \cdot a$ (m kertaa) ja $a^{-m} = 1/a^m$.
- Jos $q = \frac{m}{n}$ $(n > 0)$, niin $a^q = \sqrt[n]{a^m}$.
- Voidaan määritellä a^r kaikille reaaliluvuille r siten, että seuraavat laskusäännöt ovat voimassa kaikilla $a, b > 0$ ja $r, s \in \mathbb{R}$:

$$a^r a^s = a^{r+s}, \quad \frac{a^r}{a^s} = a^{r-s}, \quad (a^r)^s = a^{rs}, \quad (ab)^r = a^r b^r.$$

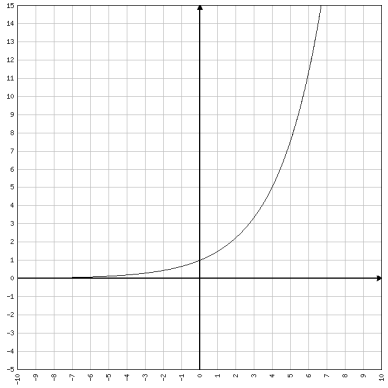
Eksponenttifunktio

Määritellään kantaluvulle $a > 0$ **eksponenttifunktio**

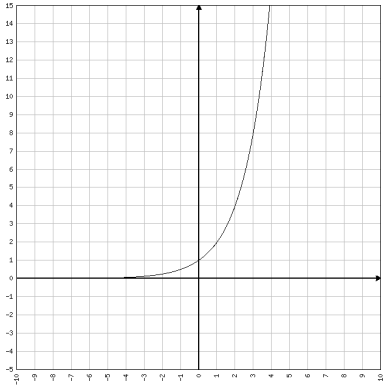
$$f : \mathbb{R} \to \mathbb{R}, \quad f(x) = a^x.$$



$a = 0.7$



$a = 1.5$



$a = 2$

Käytännön esimerkki

Valon voimakkuus vähenee 30% sen kulkiessa annetun muovilevyn läpi. Paljonko voimakkuus vähenee, jos valo kulkee kolmen samanlaisen peräkkäin asetetun levyn läpi?

Ratkaisu. Ensimmäisen levyn läpäistyään valon voimakkuudesta on jäljellä 70%. Läpäistessää toisen levyn, voimakkuus heikkenee vielä 30%, joten voimakkuudesta on jäljellä $0.7 \cdot 0.7 = 0.49$, eli 49%. Kolmannen levyn läpäistessään valon voimakkuus heikkenee taas 30%, joten lopulta voimakkuudesta on jäljellä $0.49 \cdot 0.7 = 0.343$, eli 34.3%. Jos asia ilmaistaan eksponenttifunktion avulla ja merkitään $f(n)$:llä valon voimakkuuden osuutta alkuperäisestä voimakkuudesta valon läpäistyä n identtistä (tehtävänantoa vastaavaa) peräkkäin asetettua levyä, saadaan kaava $f(n) = 0.7^n$. Yo. tapauksessa $f(3) = 0.7^3 = 0.343$.

Käytännön esimerkki

Valon voimakkuus vähenee 30% sen kulkiessa 1 cm paksuisen muovilevyn läpi. Paljonko voimakkuus vähenisi, jos levyn paksuus olisi
a) 3 mm
b) 5.4 cm?

Ratkaisu. Eksponenttifunktio $f(x) = 0.7^x$ kuvaa valon voimakkuuden osuutta alkuperäisestä sen läpäistyä x cm paksuinen muovilevy.
a) $f(0.3) = 0.7^{0.3} \approx 0.90$. eli vähenisi noin 10%.
b) $f(5.4) = 0.7^{5.4} \approx 0.15$. eli vähenisi noin 85%.

Logaritmin määritelmä

Olkoon *kantaluku* $a > 0$, $a \neq 1$. Positiivisen luvun $y \in \mathbb{R}$ a-kantainen logaritmi $\log_a y$ on luku $x \in \mathbb{R}$, jolle $a^x = y$, siis

$$\log_a y = x \iff a^x = y.$$

Toisin sanoen $a^{\log_a y} = y$, eli $\log_a y$ on vastaus kysymykseen "Mihin potenssiin a täytyy korottaa jotta saadaan y?"

Logaritmille on voimassa seuraavat laskusäännöt: Kun $y, z > 0$ ja $a > 0$, $a \neq 1$,

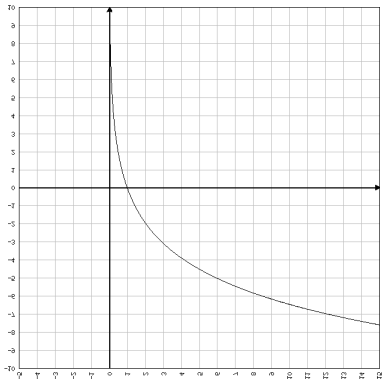
$$\log_a(yz) = \log_a y + \log_a z, \quad \log_a \frac{y}{z} = \log_a y - \log_a z, \quad \log_a(y^z) = z \log_a y.$$

Huom. koska $a^0 = 1$ ja $a^1 = a$, niin $\log_a 1 = 0$ ja $\log_a a = 1$.

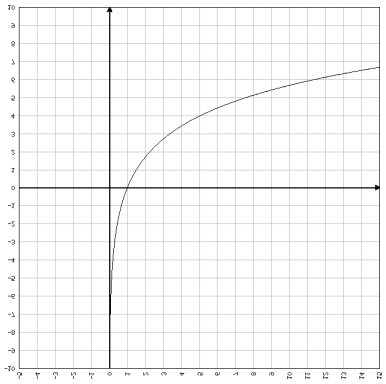
Logaritmifunktio

Määritellään kantaluvulle $a > 0$, $a \neq 1$, **logaritmifunktio**

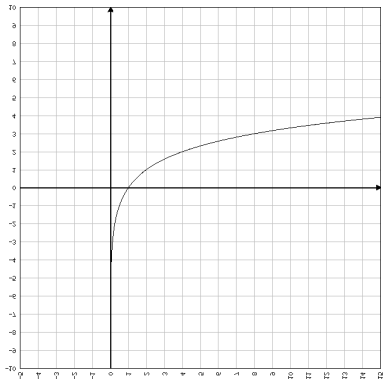
$$g : (0, \infty) \to \mathbb{R}, \quad g(y) = \log_a y$$



$a = 0.7$



$a = 1.5$



$a = 2$

Neperin luku

Kantalukuna käytetään usein ns. Neperin lukua

$$e := \lim_{n\to\infty} \left(1 + \frac{1}{n}\right)^n \approx 2.72.$$

e on π:n ohella esimerkki paitsi irrationaalisesta, myös transendenttisesta reaaliluvusta. Kantaluvun e logaritmia sanotaan luonnolliseksi logaritmiksi ja merkitään $\log_e y = \ln y$.

John Napier (1550-1617)

Esimerkkejä yhtälöistä

Ratkaistaan yhtälö

a) $5^{x^2+2x-1} \cdot 25 = 1 \iff 5^{x^2+2x-1} \cdot 5^2 = 1$
$\iff 5^{x^2+2x+1} = 1 \iff x^2 + 2x + 1 = 0$
$\iff x = -1$

b) $\log_a y^2 + \log_a 2y = \log_a 2$
$\iff 2\log_a y + \log_a 2 + \log_a y = \log_a 2$
$\iff 3\log_a y = 0$
$\iff \log_a y = 0 \iff y = 1$

c) $2^{2x+1} \cdot 5^{-x} = 3 \iff 2 \cdot 4^x \cdot (\frac{1}{5})^x = 3$
$\iff (\frac{4}{5})^x = \frac{3}{2}$
$\iff x = \ln \frac{3}{2} / \ln \frac{4}{5}$
$\iff x = \frac{\ln 3 - \ln 2}{\ln 4 - \ln 5}$

Esimerkki yhtälöstä

Ratkaise yhtälö $3^{2x+1} = \frac{1}{9}$.

$$3^{2x+1} = \frac{1}{9} \iff 2x+1 = \log_3 \frac{1}{9} \iff 2x+1 = -2 \iff x = -\frac{3}{2}.$$

Kantaluvun vaihto

Usein on hyödyllistä tarkastella ongelmaa eri kantaisissa logaritmeissa, jolloin on tarpeen voida vaihtaa esimerkiksi a-kantaisesta logaritmista b-kantaiseen. Kantaluvun vaihto voidaan suorittaa seuraavan kaavan mukaan:

$$\log_a y = \frac{\log_b y}{\log_b a}.$$

Todistetaan tämä:
Aina pätee (logaritmin määritelmän nojalla)

$$y = a^{\log_a y}.$$

Ottamalla b-kantaiset logaritmin puolittain saadaan

$$\log_b y = \log_b a^{\log_a y} = (\log_a y)(\log_b a) \iff \log_a y = \frac{\log_b y}{\log_b a}.$$

Käytännön esimerkki

Kuten aikaisemmassa esimerkissä, oletetaan, että valon voimakkuus vähenee 30% sen kulkiessa 1 cm paksuisen muovilevyn läpi. Kuinka paksu levyn tulisi olla, jotta se päästäisi valosta lävitseen
a) 60%, b) 20%?

Ratkaisu. Kuten aiemmin, eksponenttifunktio $f(x) = 0.7^x$ kuvaa valon voimakkuuden osuutta alkuperäisestä sen läpäistyä x cm paksuinen muovilevy.
a)-kohdassa saamme siis yhtälön

$$f(x) = 0.6 \iff 0,7^x = 0.6 \iff x = \log_{0.7} 0.6 = \frac{\ln 0.6}{\ln 0.7} \approx 1.4$$

Levyn on siis oltava noin $1,4$ cm paksu.
Laske b)-kohta! Nyt

$$f(x) = 0.2 \iff 0.7^x = 0.2 \iff x = \log_{0.7} 0.2 = \frac{\ln 0.2}{\ln 0.7} \approx 4.5$$

Levyn on siis oltava noin 4.5 cm paksu.

Maanjäristykset ja Richterin asteikko

Maanjäristysten voimakkuutta voidaan mitata Richterin asteikkona tunnetulla logaritmisella asteikolla. Asteikko perustuu kymmenkantaiseen logaritmiin, minkä seurauksena yhden yksikön lisäys Richterin asteikolla tarkoittaa kymmenkertaista voimistumista (voimakkuudesta puhuminen on tietysti hieman epämääräsitä ja riippuu mitataanko energiaa vai jotain muuta).

Radioaktiivisen aineen puoliintumisaika

Aikaa, joka kuluu, kun radioaktiivisen aineen (esim. radon, uraani) atomiytimistä puolet on hajonnut toisiksi atomiytimiksi, sanotaan *puoliintumisajaksi*. Puoliintumisaika on aineelle ominainen vakio ja puoliintumisajat vaihtelevatkin aineesta riippuen sekunnin murto-osista miljardeihin vuosiin.

Esimerkiksi ydinenergian tuotannossa käytettävä uraanin isotooppi ^{235}U puoliintuu noin 700 miljoonassa vuodessa.

Merkitään radioaktiivisen aineen puoliintumisaikaa kirjaimella T ja aineen alkuperäistä määrää kirjaimella N_0. Tällöin ajan t kuluttua radioaktiivisen aineen määrä on

$$N(t) = N_0 \cdot \left(\frac{1}{2}\right)^{\frac{t}{T}}.$$

Yhtälöstä voidaan myös ratkaista puoliintumisaika T, jos tiedetään hajaantuvan aineen alkuperäinen määrä N_0 sekä aineen määrä N_t hetkellä t.

$$T = t \ln(2) / \ln(N_0/N_t).$$

Derivaatta

Differentiaali- ja integraalilaskenta

Differentiaali- ja integraalilaskennalla tarkoitetaan *derivaattaan* ja *integraaliin* liittyvää matematiikkaa. Derivaatta ja integraali ovat joillekin reaalifunktioille (funktioille $f : \mathbb{R} \to \mathbb{R}$) määriteltyjä operaatioita.

Derivaatta

Derivaatta kuvaa funktion muutosnopeutta. Mitä suurempi funktion derivaatta jossakin pisteessä on, sitä jyrkemmin funktio siinä pisteessä kasvaa. Funktion f derivaattaa merkitään yleensä joko f' tai Df. Olkoon $f : \mathbb{R} \to \mathbb{R}$ ja $x \in \mathbb{R}$. Mikäli

- $f'(x) > 0$, funktio f on kasvava pisteessä x.
- $f'(x) < 0$, funktio f on vähenevä pisteessä x.

Suoran kulmakerroin

Suoran kulmakerroin kuvaa sitä, kuinka jyrkästi suora nousee, eli kuinka paljon suoralla olevan pisteen y-koordinaatti muuttuu, kun x-koordinaatti kasvaa yhdellä yksiköllä.
Jos l on suora, ja pisteet (x_1, y_1) ja (x_2, y_2) ovat suoralla l, suoran kulmakerroin saadaan lausekkeesta

$$\frac{y\text{-koordinaattien muutos}}{x\text{-koordinaattien muutos}} = \frac{y_2 - y_1}{x_2 - x_1}.$$

Mikäli suora l on funktion f kuvaaja, lauseke saa muodon

$$\frac{f(x_2) - f(x_1)}{x_2 - x_1}.$$

Suoran kulmakerroin

Moni funktio näyttää läheltä katsottuna suoralta. ”Jyrkkyys” voidaan tämän huomion avulla määritellä myös monille muille funktioille kuin suorille.

Derivaatta

Derivaatan täsmällinen määritelmä on:

Definition

Olkoon $f : \mathbb{R} \to \mathbb{R}$ funktio, ja $x \in \mathbb{R}$. Funktion f *derivaatta pisteessä* x on

$$f'(x) = \lim_{y \to x} \frac{f(y) - f(x)}{y - x}.$$

Derivaatta ja funktion tangentti

Funktion f derivaatta pisteessä x on funktion f kuvaajalle kohtaan x piirretyn tangentin kulmakerroin.

Esimerkki derivaatan määritelmästä

Funktion $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x^2 - x + 1$, derivaatta pisteessä 0 on

$$\begin{aligned}
\lim_{y \to 0} \frac{f(y) - f(0)}{y - 0} &= \lim_{y \to 0} \frac{y^2 - y + 1 - (0^2 - 0 + 1)}{y} \\
&= \lim_{y \to 0} \frac{y^2 - y}{y} \\
&= \lim_{y \to 0} y - 1 \\
&= 0 - 1 = -1
\end{aligned}$$

Voidaan siis merkitä $f'(0) = -1$. Pisteen 0 lähellä funktio f siis vähenee.

Alkeisfunktioiden derivaatat

Derivaatan määritelmä on monessa tilanteessa hieman kömpelö tapa laskea derivaatta. Derivointi onnistuu usein (muttei aina) seuraavien yhtälöiden avulla:

- $D(c) = 0$ (c vakio)
- $D(cf(x)) = cf'(x)$
- $D(x^p) = p \cdot x^{p-1}$, kun $p \neq 0$.
- Summa: $D(f(x) + g(x)) = f'(x) + g'(x)$
- Tulo: $D(f(x) \cdot g(x)) = f(x)g'(x) + f'(x)g(x)$
- Osamäärä: $D\left(\frac{f(x)}{g(x)}\right) = \frac{f'(x)g(x) - f(x)g'(x)}{(g(x))^2}$
- Yhdistetty funktio: $D(f(g(x))) = f'(g(x))g'(x)$ (f on *ulkofunktio* ja g on *sisäfunktio*)

Lisää derivaattoja

Eksponentti-, logaritmi- ja trigonometrisiin funktioihin liittyy seuraavia yhtälöitä:

- $D(a^x) = \ln(a) \cdot a^x$, kun $a > 0$.
- $D(\log_a(x)) = \frac{1}{x \ln(a)}$
- $D(\sin(x)) = \cos(x)$
- $D(\cos(x)) = -\sin(x)$

Esimerkkejä

Derivoidaan funktio $f(x) = 2x^3 + 3x^2 - 7x + 2$. Summasta derivaatat voidaan ottaa erikseen, joten

$$f'(x) = D(2x^3) + D(3x^2) + D(-7x) + D(2).$$

Toisaalta vakion 2 derivaatta on 0 ja muista termeistä kertoimet voidaan ottaa derivaatan eteen, joten

$$f'(x) = 2D(x^3) + 3D(x^2) - 7D(x).$$

Koska $D(x^3) = 3x^2$, $D(x^2) = 2x$ ja $D(x) = 1$,

$$f'(x) = 2 \cdot (3x^2) + 3 \cdot (2x) - 7 \cdot 1 = 6x^2 + 6x - 7.$$

Esimerkkejä

Derivoidaan funktio $2^{\sin(x)}$. Tämä on yhdistetty funktio, jonka ulkofunktio on 2^x ja sisäfunktio $\sin(x)$. Funktion 2^x derivaatta on $\ln(2)2^x$ ja funktion $\sin(x)$ derivaatta on $\cos(x)$. Siis

$$D(2^{\sin(x)}) = \ln(2)2^{\sin(x)}\cos(x).$$

Esimerkkejä

Johdetaan sääntö $D\left(\frac{f(x)}{g(x)}\right) = \frac{f'(x)g(x)-f(x)g'(x)}{(g(x))^2}$ käyttämällä muita sääntöjä. Ilmaistaan aluksi $f(x)/g(x)$ tulona $f(x) \cdot (1/g(x))$ ja sen jälkeen $1/g(x)$ yhdistettynä funktiona funktioista $x \mapsto 1/x$ ja g.

$$
\begin{aligned}
D\left(\frac{f(x)}{g(x)}\right) &= D\left(f(x) \cdot \frac{1}{g(x)}\right) \\
&= f(x) \cdot D\left(\frac{1}{g(x)}\right) + f'(x) \cdot \frac{1}{g(x)} \\
&= f(x) \cdot D\left((g(x))^{-1}\right) + \frac{f'(x)}{g(x)} \\
&= f(x) \cdot (-1)g(x)^{-2} \cdot g'(x) + \frac{f'(x)}{g(x)}
\end{aligned}
$$

jatkuu...

Esimerkkejä

$$
\begin{aligned}
&= f(x) \cdot (-1) \frac{1}{(g(x))^2} \cdot g'(x) + \frac{f'(x)}{g(x)} \\
&= \frac{-f(x)g'(x)}{(g(x))^2} + \frac{f'(x)g(x)}{(g(x))^2} \\
&= \frac{f'(x)g(x) - f(x)g'(x)}{(g(x))^2}
\end{aligned}
$$

Derivaatan sovelluksia

Derivaatan avulla on kätevä ratkaista maksimointi/minimointiongelmia. Mikäli funktio on derivoituva, sen suurin ja pienin mahdollinen arvo löytyvät sen derivaatan nollakohdista. Jos derivaatta nimittäin on jossakin pisteessä positiivinen tai negatiivinen, funktio on siinä kohtaa kasvava tai vähenevä, eli funktiolla ei voi olla maksimia eikä minimiä kyseisessä pisteessä.
Eli hyvä motto on: *Jos derivoituvalla funktiolla* $f : \mathbb{R} \to \mathbb{R}$ *on maksimi tai minimi, se löytyy sellaisesta pisteestä* x*, jossa* $f'(x) = 0$.

Derivaatan sovelluksia

Mistä pisteestä löytyy paraabelin $y = 4 + 4x - x^2$ huippu?
Ratkaisu. Derivaatan nollakohdasta. Derivoimalla funktiota $f : \mathbb{R} \to \mathbb{R}$, $f(x) = 4 + 4x - x^2$, saadaan $f'(x) = 4 - 2x$. Ratkaistaan yhtälö $f'(x) = 0$:

$$\begin{aligned} & f'(x) &=& \ 0 \\ \iff & 4 - 2x &=& \ 0 \\ \iff & -2x &=& -4 \\ \iff & x &=& \ 2 \end{aligned}$$

Siispä huipun x-koordinaatti on 2. Huipun y-koordinaatti on $f(2) = 4 + 4 \cdot 2 - 2^2 = 8$. Huippu on siis pisteessä $(2, 4)$.

Derivaatan sovelluksia

Talon seinän viereen rakennetaan porsaille neliskulmainen aitaus. Aitaa on käytettävissä 30m, ja tästä määrästä pitäisi aitaukselle tehdä kolme sivua (yksi sivu on talon seinä). Kuinka pitkäksi talon seinää vasten kohtisuorassa olevat sivut tulisi rakentaa, jotta aitauksen pinta-ala olisi suurin mahdollinen?

Derivaatan sovelluksia

Ratkaisu. Merkitään muuttujalla x kohtisuorassa olevan aidan pituutta. Tällöin talon seinän kanssa yhdensuuntaisen sivun pituudeksi jää $30 - 2x$ metriä, joten aitauksen pinta-alaa kuvaa funktio
$A(x) = (30 - 2x)x = 30x - 2x^2$. Funktion suurin arvo löytyy derivaatan nollakohdasta, joten derivoidaan funktio:

$$A'(x) = D(30x - 2x^2) = 30 - 4x.$$

Derivaatta on nolla kun $30 - 4x = 0 \iff 4x = 30 \iff x = 7{,}5$.
Kohtisuoran sivun pituudeksi tulisi siis valita 7,5 metriä.

Alkuluvut ja jaollisuus

Lukuteoria

Lukuteoria on eräs vanhimmista matematiikan aloista. On sanottu, että siinä missä matematiikka on tieteiden kuningatar, on lukuteoria matematiikan kuningatar. Perehdymme seuraavassa luonnollisten lukujen jaollisuuteen ja alkulukuihin.

Eukleides Aleksandrialainen
(n. 300 eaa)

Jaollisuus

Määritelmä

Luku $m \in \mathbb{Z}$ jakaa luvun $n \in \mathbb{Z}$, merkitään $m|n$, mikäli on olemassa sellainen $k \in \mathbb{Z}$, että $n = m \cdot k$.

Sanomme tällöin myös, että n on jaollinen m:llä.
Tämä tarkoittaa sitä, että jako n/m menee tasan, eikä jakojäännöstä jää.

- esim. $6 = 2 \cdot 3$, joten $2|6$ ja $3|6$
- Määritelmästä seuraa, että jokainen luonnollinen luku on jaollinen itsellään ja ykkösellä!

Määritelmä

Ykköstä suurempaa luonnollista lukua p, joka ei ole jaollinen muilla luonnollisilla luvuilla kuin itsellään ja ykkösellä, sanotaan **alkuluvuksi**.

Ts. luonnollinen luku $p \geq 2$ on alkuluku jos $\{n \in \mathbb{N} \colon n|p\} = \{1, p\}$.
Alkulukuja: $2, 3, 5, 7, 11, 13, 17, 19, 23, \ldots$

Jakoyhtälö

Kun luonnollinen luku n jaetaan nollasta poikkeavalla luonnollisella luvulla m, saadaan osamäärä k, joka kertoo kuinka monta kokonaista kertaa luku m mahtuu lukuun n, sekä jakojäännös r, joka kertoo, kuinka paljon jää yli. Jakojäännös on aina vähintään 0 mutta alle m. Näin saadaan *jakoyhtälö*:

Lause (Jakoyhtälö)

Olkoot n ja m luonnollisia lukuja, ja $m > 0$. Tällöin on olemassa luonnolliset luvut k ja r, joilla pätee:

$$n = m \cdot k + r,$$

ja $0 \leq r < m$.

Esimerkkejä jakoyhtälöstä

Muodostetaan jakoyhtälö, kun luku 18 jaetaan luvulla 7. 7 menee lukuun 18 kaksi kokonaista kertaa, ja jakojäännös on 4. Siispä jakoyhtälö on

$$18 = 7 \cdot 2 + 4.$$

Kun taas luku 251 jaetaan luvulla 20, saadaan osamääräksi 12 ja jakojäännökseksi 11. Tällöin jakoyhtälö on

$$251 = 20 \cdot 12 + 11.$$

Parillisuus

Kahdella jaollista luonnollista lukua sanotaan **parilliseksi**. Parilliset luvut ovat siis muotoa $2k$ jollakin $k \in \mathbb{N}$.
Muotoa $2k + 1$ olevat luvut ovat **parittomia**. Soveltamalla jakoyhtälöä tapauksessa $m = 2$ tiedetään, että jokainen luonnollinen luku on joko parillinen tai pariton.
Jos taas sovelletaan jakoyhtälöä esimerkiksi valinnalla $m = 3$, voidaan jokainen luonnollinen luku n kirjoittaa jossain seuraavista muodoista:

- $n = 3k$ jollakin $k \in \mathbb{N}$ (kun n on jaollinen kolmella)
- $n = 3k + 1$ jollakin $k \in \mathbb{N}$ (kun laskettaessa $n/3$ jakojäännös on 1)
- $n = 3k + 2$ jollakin $k \in \mathbb{N}$ (kun laskettaessa $n/3$ jakojäännös on 2)

Esimerkkitehtävä

Olkoon n luonnollinen luku. Osoitetaan, että tällöin $n^2 - n$ on parillinen.
Jakoyhtälön nojalla joko $n = 2k$ jollakin $k \in \mathbb{N}$ tai $n = 2k + 1$ jollakin $k \in \mathbb{N}$.
Tarkastellaan nämä tapaukset erikseen:
Jos $n = 2k$ jollakin $k \in \mathbb{N}$, niin
$n^2 - n = (2k)^2 - 2k = 4k^2 - 2k = 2(2k^2 - k)$. Tämä on jaollinen luvulla 2.
Jos taas $n = 2k + 1$ jollakin $k \in \mathbb{N}$, niin
$n^2 - n = (2k+1)^2 - (2k+1) = 4k^2 + 4k + 1 - 2k - 1 = 4k^2 + 2k = 2(2k^2 + k)$.
Tämä on jaollinen luvulla 2.
Siispä kummassakin tapauksessa $n^2 - n$ on parillinen.

Esimerkkitehtävä

Olkoon n luonnollinen luku. Osoitetaan, että $n(n^2+2)$ on jaollinen luvulla 3.
Tarkastellaan eri tapaukset:
Jos $n = 3k$ jollakin $k \in \mathbb{N}$, niin

$$n(n^2+2) = 3k((3k)^2+2),$$

mikä on kolmella jaollinen.
Jos taas $n = 3k+1$ jollakin $k \in \mathbb{N}$, niin

$$n(n^2+2) = (3k+1)((3k+1)^2+2) = (3k+1)(9k^2+6k+2+1),$$

mikä myös on kolmella jaollinen.
Lopuksi, jos $n = 3k+2$ jollakin $k \in \mathbb{N}$, niin

$$n(n^2+2) = (3k+2)((3k+2)^2+2) = (3k+2)(9k^2+12k+4+2),$$

mikä jälleen on kolmella jaollinen.
Siis kaikissa tapuksissa luku $n(n^2+2)$ on kolmella jaollinen.

Jaollisuussääntöjä

Lukujen jaollisuus annetulla luvulla voidaan usein päätellä nopeasti sen numeroista mm. seuraavien sääntöjen avulla:

- Luku on jaollinen kolmella, jos sen numeroiden summa on jaollinen kolmella.
  Esim. $3|51741$, sillä $5+1+7+4+1=18$ on jaollinen kolmella.
- Luku on jaollinen seitsemällä, jos vähentämällä sen "ensimmäisten" numeroiden muodostamasta luvusta kaksi kertaa viimeinen numero saadaan seitsemällä jaollinen luku.
  Esim. $7|791$, sillä $79-2\cdot 1=77$ on jaollinen seitsemällä.
  $7|1512$, sillä $151-2\cdot 2=147=21\cdot 7$
- Luku on jaollinen yhdellätoista, jos sen numerot kerrottuna vuorotelleen $+1$:llä ja -1:llä oikealta lähtien muodostavat yhteenlaskettuna yhdellätoista jaollisen luvun.
  Esim. $11|14729$, sillä $9-2+7-4+1=11$ on jaollinen yhdellätoista.

Eratostheneen seula

Eratostheneen seula on algoritmi, jolla löydetään kaikki alkuluvut annettuun lukuun $n \in \mathbb{N}$ asti. Kokeillaan algoritmia arvolla $n = 100$:

1. listaa järjestyksessä luonnolliset luvut $2, 3, \ldots, n$
2. merkitse punaisella listan ensimmäinen merkitsemätön luku p
3. pyyhi listasta kaikki p:n monikerrat
4. toista vaiheet 2 ja 3 kunnes $p^2 > n$
5. loput listan luvut ovat alkulukuja!

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Aritmetiikan peruslause

Alkuluvut ovat luonnollisten lukujen "rakennuspalikoita", kuten Aritmetiikan peruslause kertoo:

Lause

Jokainen luonnollinen luku (poislukien 0 *ja* 1*) voidaan esittää yksikäsitteisesti alkulukujen äärellisenä tulona.*

Yksikäsitteisyys on voimassa tekijöiden järjestystä lukuunottamatta.
Huomaa, että kukin tekijä voi esiintyä tulossa useamman kerran.
Esim.
$308 = 2 \cdot 154 = 2^2 \cdot 77 = 2^2 \cdot 7 \cdot 11$
$975 = 3 \cdot 325 = 3 \cdot 5 \cdot 65 = 3 \cdot 5^2 \cdot 13$
Luonnollisen luvun esitystä alkulukujen tulona sanotaan luvun **alkutekijähajotelmaksi**.

Alkulukujen äärettömyys

Lause

Alkulukuja on äärettömän monta.

Todistus.

Tehdään vastaoletus: Alkulukuja on vain äärellisen monta, merkitään niitä $p_1, p_2, \ldots, p_n$. Tarkastellaan sitten lukua

$$N = p_1 \cdot p_2 \cdots p_n + 1.$$

Aritmeriikan peruslauseesta seuraa, että N on jaollinen jollakin alkuluvuista $p_1, p_2, \ldots, p_n$. Siis jokin luvuista p_i, $i = 1, \ldots, n$ jakaa N:n ja tulon $p_1 \cdot p_2 \ldots p_n$, joten se jakaa myös erotuksen

$$N - p_1 \cdot p_2 \cdots p_k = 1.$$

Tämä on ristiriita, sillä ykkönen ei ole jaollinen millään (alku)luvulla, joten alkuperäinen väite on todistettu. □

$\sqrt{2}$ on irrationaalinen

Todistetaan nyt aikaisemmin esittämämme väite $\sqrt{2}$:n irrationaalisuudesta.
Tehdään vastaoletus: $\sqrt{2}$ on rationaalinen, eli muotoa $\frac{m}{n}$, joillakin luonnollisilla luvuilla m ja n. Siten

$$n\sqrt{2} = m,$$

josta korottamalla puolittain toiseen saadaan

$$2n^2 = m^2.$$

Yhtälön oikean puolen luvussa tekijä 2 esiintyy parillisen määrän kertoja (jos m on parillinen, sisältää m^2 parillisen määrän tekijää 2). Vasemman puolen luvussa tekijä 2 esiintyy sen sijaan parittoman määrän kertoja. Tämä on ristiriidassa Aritmetiikan peruslauseen kanssa, joten vastaoletuksen on oltava väärin ja väitteen siten totta.

$\log_2 3$ on irrationaalinen

Osoita, että $\log_2 3$ on irrationaalinen.
Tehdään vastaoletus: $\log_2 3$ on rationaalinen, eli muotoa $\frac{m}{n}$ joillakin luonnollisilla luvuilla m ja n. Logaritmin määritelmän mukaan tällöin

$$3 = 2^{\frac{m}{n}}.$$

Korottamalla puolittain potenssiin n saadaan

$$3^n = 2^m.$$

Tämä on ristiriidassa Aritmetiikan peruslauseen kanssa, joten vastaoletuksen on oltava väärin ja väitteen totta.

$\mathbb{Q}$ on numeroituva

Eräs tapa osoittaa positiivisten rationaalilukujen joukko (ja siten koko $\mathbb{Q}$) numeroituvaksi on tarkastella positiivisten kokonaislukujen pareilla määriteltyä funktiota

$$f(n, m) = 2^n 3^m, \quad n, m \in \mathbb{Z}_+.$$

Koska 2 ja 3 ovat alkulukuja, niin Aritmetiikan peruslauseen nojalla

$$2^{n_1} 3^{m_1} = 2^{n_2} 3^{m_2} \quad \Longleftrightarrow \quad n_1 = n_2 \quad \text{ja} \quad m_1 = m_2.$$

Jos siis $f(n_1, m_1) = f(n_2, m_2)$, niin $(n_1, m_1) = (n_2, m_2)$, eli f on injektio. Tämä tarkoittaa sitä, että positiivisten kokonaislukujen parien muodostama joukko on "korkeintaan" yhtä mahtava kuin $\mathbb{N}$. Takuulla noita pareja on kuitenkin äärettömän monta ja siten niiden joukko on yhtä mahtava kuin $\mathbb{N}$. Positiiviset rationaaliluvut voidaan puolestaan ajatella positiivisten kokonaislukujen parien joukon osajoukkona.

Alkulukujen lukumääristä

Tiedämme, että alkulukuja on kaikkiaan äärettömän monta. Entä kuinka monta alkulukua on kullakin rajoitetulla reaalilukuvälillä ja kuinka niiden lukumäärä riippuu tämän välin pituudesta?
Merkitään korkeintaan n:n suuruisten alkulukujen lukumäärää $\pi(n)$:llä.
Saadaan siis funktio

$$\pi : \mathbb{Z}_+ \to \mathbb{N}, \quad \pi(n) = \#\{p \in \mathbb{Z}_+ : p \text{ alkuluku }, p \leq n\}.$$

Lasketaan muutamia pieniä arvoja:
$\pi(1) = 0$, $\pi(2) = 1$, $\pi(3) = 2$, $\pi(4) = 2$, $\pi(5) = 3$, ...

Alkulukulause

Arvojen $\pi(n)$ suuruusluokkaa voidaan arvioida logaritmifunktion avulla:

$$\pi(n) \sim \frac{n}{\ln n}$$

Tämä tulos tunnetaan Alkulukulauseena ja sillä tarkoitetaan sitä, että

$$\frac{\pi(n)}{n/\ln n} \to 1, \quad \text{kun } n \to \infty,$$

eli osamäärä lähestyy ykköstä, kun n kasvaa rajatta.

Alkulukulausen taulukointia

n	$\pi(n)$	osuus %	$n/\ln n \approx$
10	4	$40,0$	4
10^2	25	$25,0$	22
10^3	168	$16,8$	145
10^4	1229	$12,3$	1086
10^5	9592	$9,6$	8686
10^6	78498	$7,8$	72382
10^7	664579	$6,6$	620421
10^8	5761455	$5,8$	5428681
10^9	50847534	$5,1$	48254942
10^{10}	455052511	$4,6$	434294482

Mersennen alkuluvut

Tarkastellaan muotoa $2^n - 1$ olevia lukuja arvoilla $n \geq 2$:
$2^2 - 1 = 3$, $2^3 - 1 = 7$, $2^4 - 1 = 15$, $2^5 - 1 = 31$, $2^6 - 1 = 63$, ...
Huomataan, että tapauksissa $n = 2, 3, 5$ luku $2^n - 1$ on alkuluku, kun taas tapauksissa $n = 4, 6$ näin ei ole.
Onko $2^n - 1$ alkuluku aina, kun n on alkuluku?
Ei: $2^{11} - 1 = 2047 = 23 \cdot 89$.
Käänteinen väite on kuitenkin voimassa:
Jos $2^n - 1$ on alkuluku, niin myös n on alkuluku.

Määritelmä

Muotoa $2^p - 1$ olevia alkulukuja sanotaan *Mersennen alkuluvuiksi*.

Käytämme eksponentissa kirjainta p, koska tiedämme sen olevan alkuluku edellisen nojalla.

The Great Internet Mersenne Prime Search (GIMPS)

Tällä hetkellä tunnetaan 47 Mersennen alkulukua. Suurin tunnettu alkuluku on Mersennen alkuluku

$$2^{43112609} - 1.$$

Tammikuusta 1996 lähtien on Mersennen alkulukuja etsitty yhteisvoimin internetissä The Great Internet Mersenne Prime Search -projektissa. Käy tutustumassa ja osallistu etsintään!

Avoimia ongelmia

Alkulukuihin liittyy vielä tällä hetkellä avoimia ongelmia. Esimerkiksi

- Onko Mersennen alkulukuja äärettömän monta?
- *Alkulukuparit:* Onko olemassa äärettömän monta alkulukua p, jolle myös $p+2$ on alkuluku?
  Esim. 3 ja 5, 5 ja 7, 11 ja 13, 17 ja 19, 29 ja 31, ...?
- *Goldbachin konjektuuri:* Jokainen kakkosta suurempi parillinen luku voidaan lausua kahden alkuluvun summana.
  Esim. $4 = 2+2$, $6 = 3+3$, $8 = 3+5$, $10 = 3+7$, $12 = 5+7$, $14 = 7+7$, ...?

Kryptografia

Kryptografiassa tutkitaan menetelmiä salata välitettävää tietoa. Menetelmät voi jakaa kahteen tyyppiin:

- **Salaisen avaimen menetelmissä** kutkin keskenään tietoa välittävät henkilöt joutuvat sopimaan salaisesti avaimesta keskenään. Siitä syystä menetelmä soveltuu vain pienen ryhmän käyttöön. Jo muinaiset roomalaiset käyttivät näitä menetelmiä.
- **Julkisen avaimen menetelmissä** kukin tiedonvälittäjä julkistaa oman avaimensa. Salaisia avaimenvaihtoja ei siis tarvita ja siten nämä menetelmät soveltuva suurille joukoille. Mutta kuinka tällainen menetelmä voi onnistua salaamaan tiedonkulun?

Kaksoislukko

Esitetään seuraavaksi klassinen esimerkki salausmenettelystä, jossa salaista avaimenvaihtoa ei tarvita.
Oletetaan, että henkilö A haluaa lähettää salaisen viestin henkilölle B. He toimivat näin:

1. A laittaa viestinsä laatikkoon, jonka lukitsee omalla lukollaan L_A (vain A:lla on avain lukkoon L_A) ja lähettää laatikon B:lle
2. B vastaanottaa laatikon, lukitsee sen lisäksi omalla lukollaan L_B (vain B:llä on avain lukkoon L_B) ja lähettää "kaksoislukitun" laatikon takaisin A:lle
3. A vastaanottaa kaksoislukitun laatikon, poistaa siitä oman lukkonsa L_A ja lähettää laatikon B:lle
4. vastaanotettuaan laatikon voi B avata oman lukkonsa L_B ja lukea viestin

Menetelmän turvallisuus perustuu siis siihen, että kullakin tiedonvälittäjällä on avain vain omaan lukkoonsa. Myöskään salaista avaimenvaihtoa ei tarvita.

Suurin yhteinen tekijä ja Eulerin funktio

Olkoot a ja b positiivisia kokonaislukuja. Suurinta positiivista kokonaislukua, joka jakaa sekä a:n että b:n sanotaan niiden *suurimmaksi yhteiseksi tekijäksi*, merk. $\text{syt}(a, b)$.
Esim. $\text{syt}(3, 6) = 3$, $\text{syt}(20, 8) = 4$, $\text{syt}(5, 4) = 1$
Eulerin funktio on kuvaus $\varphi : \mathbb{Z}_+ \to \mathbb{Z}_+$, jolle

$$\varphi(n) = \text{niiden lukujen } k \in \mathbb{Z}_+ \text{ lukumäärä, joilla } k \leq n \text{ ja } \text{syt}(k, n) = 1$$

ts.

$$\varphi(n) = \#\{k \in \mathbb{Z}_+ : k \leq n, \text{syt}(k, n) = 1\}.$$

Pieniä arvoja: $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(5) = 4$, $\varphi(6) = 2$, $\varphi(7) = 6, \ldots$
Huom.

- $\varphi(p) = p - 1$, joss p on alkuluku.
- Jos $\text{syt}(m, n) = 1$, niin $\varphi(mn) = \varphi(m)\varphi(n)$. Erityisesti, jos p ja q ovat eri alkulukuja, niin $\varphi(pq) = \varphi(p)\varphi(q) = (p - 1)(q - 1)$.

RSA

Ron Rivest, Adi Shamir ja Len Adleman esittivät vuonna 1978 seuraavanlaisen salausalgoritmin:
Oletetaan, että henkilö A haluaa lähettää salaisen viestin henkilölle B.

1. B valitsee satunnaisesti kaksi suurta alkulukua $p \neq q$ ja laskee luvut $N = pq$ ja $\varphi(N) = (p-1)(q-1)$
2. B valitsee vielä positiivisen kokonaisluvun e, jolle $1 < e < \varphi(N)$ ja $\text{syt}(e, \varphi(N)) = 1$ ja etsii positiivisen kokonaisluvun d, jolle $ed \equiv 1 \pmod{\varphi(N)}$, ts. kun luku ed jaetaan luvulla $\varphi(N)$, jää jakojäännökseksi 1
3. B julkistaa luvut N ja e
4. A koodaa viestinsä luvuksi (tai luvuiksi) M, jolle $M \leq N$
5. A laskee luvun M^e, jakaa sen luvulla N, ja lähetää jakojäännöksen B:lle
6. B korottaa saamansa luvun (salaiseen) potenssiin d ja laskee jakojäännöksen luvulla N jaettaessa.
7. B on siis laskenut luvun $(M^e)^d$ jakojäännöksen luvulla N jaettaessa. Koska $ed \equiv 1 \pmod{\varphi(N)}$, niin Fermat'n pienen lauseen nojalla $M^{ed} \equiv M \pmod{N}$, eli B:n laskema jakojäännös on täsmälleen alkuperäinen viesti!

RSA

Mihin menetelmän turvallisuus perustuu? Viestin purkamiseen riittää siis tietää luku d. Laskeakseen luvun d, tarvitsee tietää e (julkinen) ja $\varphi(N)$. Mutta vaikka N on julkinen, on luvun $\varphi(N)$ laskeminen suunnilleen yhtä työlästä kuin luvun $N = pq$ tekijöihinjako, joka puolestaan on erittäin työlästä, koska p ja q ovat suuria (salaisia) alkulukuja.

Induktio ja lukujonot

Induktio, jonot ja summat

Matemaattinen induktio on erittäin hyödyllinen todistusmenetelmä, jota sovelletaan laajasti. Sitä verrataan usein dominoefektiin eli ketjureaktioon, jossa ensimmäisen dominopalikka kaataa kaatuessaan toisen, toinen kolmannen, jne. jolloin kukin jonon palikoista kaatuu lopulta. Tulemme käyttämään induktiota tällä kurssilla myöhemminkin vielä useita kertoja.

Induktioperiaate

Matematiikassa on usein tarve todistaa että jokaisella luonnollisella luvulla on jokin ominaisuus, tai että jokin väite pätee millä tahansa luonnollisella luvulla, esim. "jokainen luku on joko pariton tai parillinen", "kaikilla $n \in \mathbb{N}$, joukossa jossa on n reaalilukua, on suurin reaaliluku". Jos halutaan osoittaa todeksi tällainen väite, on usein käytettävä induktiota sen sijaan, että tutkittaisiin jokainen tapaus erikseen, mikä ei ole mahdotonta äärellisellä todistuksella.

Induktioperiaate: Tarkastellaan väittämää $P(n)$, joka koskee jotakin lukua n. Oletetaan, että

1. väittämä pätee, kun $n = 1$
2. voidaan osoittaa todeksi, että jos väittämä pätee jollain $n = k$, niin se pätee myös kun $n = k + 1$.

Tällöin induktioperiaatteen nojalla väittämä pätee millä tahansa n.

Induktio - Esimerkki 1

Osoitetaan, että

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$$

kaikilla luonnollisilla luvuilla $n \geq 1$.
Tarkastetaan ensin, että kaava pätee kun $n = 1$:
Vasen puoli on tällöin 1, kun taas oikea puoli

$$\frac{1 \cdot (1+1)}{2} = \frac{2}{2} = 1,$$

eli kaava pätee.

Induktio - Esimerkki 1

Tehdään sitten **induktio-oletus**: Kaava pätee jollakin $n \geq 1$, ts.

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}.$$

Induktio-oletukseen nojautuen tulisi nyt todistaa **induktioväite**: Kaava pätee arvolla $n + 1$, ts.

$$1 + 2 + \cdots + n + (n+1) = \frac{(n+1)(n+2)}{2}.$$

Lähdetään liikkeelle kaavan vasemmasta puolesta:

$$\begin{aligned} 1 + 2 + \cdots + n + (n+1) &\overset{i.o.}{=} \frac{n(n+1)}{2} + (n+1) \\ &= \frac{n(n+1) + 2(n+1)}{2} = \frac{(n+1)(n+2)}{2}, \end{aligned}$$

kuten halusimmekin. Induktioperiaatteen nojalla kaava pätee siten kaikilla $n \geq 1$.

Lyhennysmerkintä summalle ja tulolle

Olkoot $a_1, a_2, \ldots, a_n$ reaalilukuja. Niiden summasta ja tulosta käytetään seuraavia lyhennysmerkintöjä:

$$a_1 + a_2 + \cdots + a_n = \sum_{k=1}^{n} a_k$$

ja

$$a_1 \cdot a_2 \cdots a_n = \prod_{k=1}^{n} a_k .$$

Juuri äskettäin todistamamme summakaava voidaan kirjoittaa tällä lyhennysmerkinnällä kun asetetaan $a_1 = 1, a_2 = 2, \ldots, a_n = n$, ts. $a_k = k$, missä $k = 1, 2, \ldots, n$:

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}.$$

Induktio - Esimerkki 2

Osoitetaan induktiolla, että kaikilla $n \geq 1$ pätee

$$\sum_{k=1}^{n} 2^{k-1} = 2^n - 1.$$

Tapaus $n = 1$: Vasen puoli $= 2^{1-1} = 2^0 = 1$.
Oikea puoli $= 2^1 - 1 = 2 - 1 = 1$.
Tehdään induktio-oletus: Yo. summakaava pätee jollakin $n \geq 1$ ja todistetaan, että tällöin pätee (induktioväite)

$$\sum_{k=1}^{n+1} 2^{k-1} = 2^{n+1} - 1.$$

Nyt

$$\sum_{k=1}^{n+1} 2^{k-1} = 2^n + \sum_{k=1}^{n} 2^{k-1} \overset{i.o.}{=} 2^n + 2^n - 1 = 2 \cdot 2^n - 1 = 2^{n+1} - 1,$$

joten induktioväite pätee. Induktioperiaatteen nojalla väite pätee kaikilla $n \geq 1$.

Induktio - Esimerkki 3

Osoitetaan induktiolla, että kaikilla $n \geq 1$ pätee

$$\sum_{k=1}^{n}(2k-1) = n^2.$$

Tapaus $n = 1$: Vasen puoli $= 2 \cdot 1 - 1 = 1$. Oikea puoli $= 1^2 = 1$.
Induktio-oletus: Kaava pätee jollakin $n \geq 1$, eli

$$\sum_{k=1}^{n}(2k-1) = n^2.$$

Todista, että tällöin

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

Yhteys aiempaan esimerkkiin

Funktioiden yhteydessä kävimme läpi esimerkin, jossa tuli etsiä bijektio joukolta $A = \{1, 3, 5, 7, \ldots\}$ joukolle $B = \{1, 4, 9, 16, \ldots\}$. Kuvaus

$$f : A \to B, \quad f(m) = \left(\frac{m+1}{2}\right)^2$$

osoitettiin harjoituksissa bijektioksi. Joukko A koostuu parittomista luonnollisista luvuista $a_1 = 1, a_2 = 3, a_3 = 5, a_4 = 7, \ldots$, joiden summille osoitimme juuri kaavan

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

Jokaisen luonnollisen luvun n neliö (eli joukon B n:s alkio) saadaan siis laskemalla yhteen n ensimmäistä paritonta lukua. Siis f voidaan määritellä summana

$$f(a_n) = \sum_{k=1}^{n} a_k = n^2.$$

Induktio - Esimerkki 4

Osoitetaan induktiolla, että $n(n^2+2)$ on jaollinen luvulla 3 aina, kun $n \geq 1$.
Väite pätee selvästikin, kun $n = 1$.
Tehdään induktio-oletus: $n(n^2+2)$ on jaollinen kolmella jollakin $n \geq 1$.
Osoitetaan induktioväite: Tällöin myös $(n+1)((n+1)^2+2)$ on jaollinen kolmella. Nyt

$$\begin{aligned}(n+1)((n+1)^2+2) &= (n+1)(n^2+2n+3)\\ &= n^3+3n^2+5n+3\\ &= n(n^2+2)+3n^2+3n+3.\end{aligned}$$

Toinen termi on selvästi kolmella jaollinen ja niin on induktio-oletuksen nojalla myös ensimmäinen termi $n(n^2+2)$. Siis induktioväite on todistettu ja induktioperiaatteen nojalla väite on tosi.

Lukujonojen merkinnöistä

Merkitsemme lukujen $a_1, a_2, \ldots, a_n$ muodostamaa jonoa $(a_1, a_2, \ldots, a_n) = (a_k)_{k=1}^n$, missä a_k on jonon k:s termi (tai jäsen). Jono voi olla myös päättymätön, jolloin merkitään $(a_1, a_2, \ldots) = (a_k)_{k=1}^\infty$. Esim.

- $a_k = k$, $(a_k)_{k=1}^n = (1, 2, 3, \ldots, n)$
- $a_k = k^2$, $(a_k)_{k=1}^\infty = (1, 4, 9, \ldots)$

Huomautus

On hyvä pitää mielessä, että periaatteessa jonon ensimmäisten termien luetteleminen ei riitä yksikäsitteisesti määräämään jonossa myöhemmin tulevia termejä.
Mikä on seuraava luku jonossa $(1, 2, 3, 4, 5, \ldots)$? Luonnollisesti miellämme, että kyseessä on jono $(k)_{k=1}^{\infty}$, jolloin seuraava luku on 6, mutta eihän näin täydy välttämättä olla!
Miksei kyseessä voisi olla vaikka jono $(a_k)_{k=1}^{\infty}$, missä

$$a_k = k + (k-1)(k-2)(k-3)(k-4)(k-5)?$$

Tällöin
$a_1 = 1 + (0)(-1)(-2)(-3)(-4) = 1$
$a_2 = 2 + (1)(0)(-1)(-2)(-3) = 2$
$a_3 = 3 + (2)(1)(0)(-1)(-2) = 3$
$a_4 = 4 + (3)(2)(1)(0)(-1) = 4$
$a_5 = 5 + (4)(3)(2)(1)(0) = 5$
$a_6 = 6 + (5)(4)(3)(2)(1) = 126$

Aritmeettinen jono

Aritmeettisessa jonossa kahden peräkkäisen termin erotus on vakio, ts. $(a_k)_{k=1}^{\infty}$ on aritmeettinen, jos on olemassa sellainen $d \in \mathbb{R}$, että

$$a_{k+1} - a_k = d$$

kaikilla $k \geq 1$. Aritmeettisen jonon, jonka peräkkäisten termien erotus on d, k:s termi on siis $a_k = a_1 + (k-1)d$: (perustellaan induktiolla)
Tapaus $k = 1$ selvä. Jos $a_k = a_1 + (k-1)d$ jollakin $k \geq 1$, niin $a_{k+1} = a_k + d = a_1 + (k-1)d + d = a_1 + kd$.
Esim.

- $a_k = k$, $(a_k)_{k=1}^{\infty} = (1, 2, 3, \ldots)$ on aritmeettinen $(d = 1)$
- $a_k = 2k - 1$, $(a_k)_{k=1}^{\infty} = (1, 3, 5, \ldots)$ on aritmeettinen $(d = 2)$
- $a_k = k^2$, $(a_k)_{k=1}^{\infty} = (1, 4, 9, \ldots)$ ei ole aritmeettinen
- $a_k = 2^{k-1}$, $(a_k)_{k=1}^{\infty} = (1, 2, 4, 8, \ldots)$ ei ole aritmeettinen

Aritmeettisen jonon summa

Aritmeettisen jonon $(a_k)_{k=1}^n$, jonka peräkkäisten termien erotus on d, summa saadaan kaavasta

$$\sum_{k=1}^{n} a_k = na_1 + \frac{n(n-1)}{2}d.$$

Todistus:

$$\sum_{k=1}^{n} a_k = \sum_{k=1}^{n}(a_1 + (k-1)d) = \sum_{k=1}^{n} a_1 + \sum_{k=1}^{n}(k-1)d$$

$$= na_1 + d\sum_{k=1}^{n}(k-1) = na_1 + d\sum_{k=1}^{n-1} k = na_1 + \frac{(n-1)n}{2}d$$

Tätä kaavaa on hyvä käyttää, kun tietää peräkkäisten termien erotuksen. Summan voi kuitenkin laskea ilmankin d:tä, mikäli tietää jonon pituuden lisäksi ensimmäisen ja viimeisen termin:

$$\sum_{k=1}^{n} a_k = na_1 + \frac{n(n-1)}{2}d = n\frac{a_1 + a_1 + (n-1)d}{2} = n\frac{a_1 + a_n}{2}.$$

Aritmeettisen jonon summa - Esimerkki 1

- Jonon $(2k-1)_{k=1}^{10} = (1, 3, 5, 7, \ldots, 19)$ summa on

$$n\frac{a_1 + a_n}{2} = 10 \cdot \frac{1 + 19}{2} = 100.$$

- Jonon $(5, 8, 11, \ldots)$ kahdenkymmenen ensimmäisen termin summa on

$$na_1 + \frac{n(n-1)}{2}d = 20 \cdot 5 + \frac{20 \cdot 19}{2} \cdot 3 = 670.$$

Aritmeettisen jonon summa - Esimerkki 2

Tien pituus on 50 km. Tien varteen asetetaan sähkötolppia 50 m välein. Ensimmäinen tolppa on pystytetty tien alkuun ja loput 1000 tolppaa on kasattu sen viereen, mistä kuorma-auto vie niitä paikoilleen, 20 tolppaa yhdessä kuormassa. Kuinka pitkän matkan kuorma-auto joutuu kulkemaan ennen kuin kaikki tolpat ovat paikoillaan?

Ratkaisu

Pystyttäessään 20 tolppaa 50 metrin välein kuorma-auto kulkee kilometrin matkan. Ensimmäisellä edestakaisella matkalla auto kulkee siis kaksi kilometriä. Seuraavalla matkalla auton on ensin ajettava kilometri päästäkseen tolpattoman osuuden alkuun, pystytettävä sitten mukana olevat 20 tolppaa ja palattava lopuksi takaisin. Voidaan ajatella, että auto kulkee edestakaisin tuon kilometrin matkan ja tekee sitten ensimmäistä matkaa vastaavan matkan. Matkaa kertyy toisella kertaa siis $2 + 2 = 4$ kilometriä. Kolmas matka on vastaavalla tavalla $4 + 2 = 6$ kilometriä. Viimeisen, eli 50. matkan pituus on kaksi kertaa koko tien pituus eli 100 km. Kuljetusmatkojen pituudet muodostavat aritmeettisen jonon $(2k)_{k=1}^{50}$. Jonon termien summaksi saadaan

$$50 \cdot \frac{2 + 100}{2} = 2550.$$

Kuorma-auto joutuu siis kulkemaan 2550 km ennen kuin urakka on valmis.

Greenin-Taon lause

Matemaatikot Ben Green ja Terence Tao todistivat vuonna 2004 vanhan konjektuurin alkulukujen aritmeettisista jonoista:

Lause

Alkuluvut sisältävät mielivaltaisen pitkiä aritmeettisia jonoja.

Olipa siis n mikä hyvänsä luonnollinen luku, niin löytyy n:n alkuluvun jono, jonka peräkkäiset termit ovat vakioetäisyydellä d toisistaan. Esim.
$n = 3$: $(3, 5, 7)$, $(d = 2)$
$n = 4$: $(5, 17, 29, 41)$, $(d = 12)$
$n = 5$: $(5, 11, 17, 23, 29)$, $(d = 6)$
Onnistutko löytämään lisää samanpituisia tai pidempiä?

Geometrinen jono

Geometrisessa jonossa kahden peräkkäisen termin suhde on vakio, ts. $(a_k)_{k=1}^{\infty}$ on geometrinen, jos on olemassa sellainen $r \in \mathbb{R}$, $r \neq 0$, että $\frac{a_{k+1}}{a_k} = r$ kaikilla $k \geq 1$. Geometrisen jonon, jonka peräkkäisten termien suhde on r, k:s termi $a_k = a_1 r^{k-1}$. Niinpä geometrinen jono on aina muotoa $(a, ar, ar^2, \ldots)$, missä $a \neq 0$ ja $r \neq 0$
Esim.

- $a_k = (\frac{1}{2})^{k-1}$, $(a_k)_{k=1}^{\infty} = (1, \frac{1}{2}, \frac{1}{4}, \ldots)$ on geometrinen.
- $a_k = 2 \cdot 3^{k-1}$, $(a_k)_{k=1}^{4} = (2, 6, 18, 54)$ on geometrinen.

Pankkitili

Pankkitilillä oli vuonna 2001 a euroa. Joka vuodenvaihteessa tilille lisätään korko, joka on 3% tilin saldosta. Vuonna 2002 tilillä on

$$a + \frac{3}{100}a = \frac{103}{100}a \quad \text{euroa,}$$

vuonna 2003 siellä on

$$\frac{103}{100}a + \frac{3}{100}\left(\frac{103}{100}a\right) = \frac{103}{100}a\left(1 + \frac{3}{100}\right) = \left(\frac{103}{100}\right)^2 a \quad \text{euroa.}$$

Merkitään s_k:lla tilin saldoa vuonna $2000 + k$. Saamme geometrisen jonon $(s_1, s_2, s_3, \ldots)$, jonka ensimmäinen termi on a ja peräkkäisten termien suhde on $\frac{103}{100}$, ts.

$$s_k = \left(\frac{103}{100}\right)^{k-1} a$$

kaikilla $k \geq 1$ eli $(s_k)_{k=1}^{\infty}$ on geometrinen.

Geometrisen jonon summa

Geometrisen jonon $(a_k)_{k=1}^n = (a, ar, ar^2, \ldots, ar^{n-1})$, $r \neq 1$, summa saadaan kaavasta

$$\sum_{k=1}^{n} a_k = a\frac{1-r^n}{1-r}.$$

Tämä nähdään kertomalla summaa $1-r$:llä ja huomioimalla kumoutuminen:

$$(1-r)\sum_{k=1}^{n} a_k = (a+ar+\cdots+ar^{n-1})-(ar+ar^2+\cdots+ar^n) = a-ar^n = a(1-r^n)$$

$$\iff \sum_{k=1}^{n} a_k = a\frac{1-r^n}{1-r}$$

Geometrisen jonon summa - Esimerkki

- $a = 1, r = \frac{1}{2}, (a_k)_{k=1}^{5} = \left(\left(\frac{1}{2} \right)^{k-1} \right)_{k=1}^{5} = (1, \frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \frac{1}{16})$

$$\sum_{k=1}^{5} a_k = 1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \frac{1}{16} = \frac{1 - (\frac{1}{2})^5}{1 - \frac{1}{2}} = \frac{1 - \frac{1}{32}}{\frac{1}{2}} = \frac{31}{16}$$

Akilleus ja kilpikonna

Antiikin aikaisen paradoksin mukaan Akilleus ei voi kilpajuoksussa saavuttaa kilpikonnaa, jos kilpikonnalle annetaan etumatkaa. Oletetaan vaikkapa että etumatka on 100 metriä. Akilleus juoksee 20 metriä sekunnissa ja kilpikonna "juoksee" kaksi senttimetriä sekunnissa. Akilleus juoksee etumatkan kiinni viidessä sekunnissa, mutta tänä aikana kilpikonna on edennyt kymmenen senttimetriä. Akilleus juoksee 10 cm matkan $\frac{5}{1000}$ sekunnissa, mutta silloin kilpikonna on edennyt $\frac{1}{10}$ millimetriä. Eli alkaa näyttää siltä, että aina kun Akilleus pääsee sinne, missä kilpikonna oli, niin kilpikonna onkin jo ehtinyt kauemmaksi. Eikö Akilleus siis koskaan saavuta kilpikonnaa?

Akilleus ja kilpikonna

Tasaisen nopeuden kaavasta "matka = aika $\times$ nopeus", saamme yhtälön sille ajanhetkelle t, jolloin Akilleus saavuttaa kilpikonnan:

$$100 + \frac{2}{100} \cdot t = 20 \cdot t.$$

Yhtälön ratkaisu on $t = \frac{5000}{999} \approx 5,005$ eli "todellisuudessa" Akilleus saavuttaa kilpikonnan noin $5 + \frac{1}{200}$ sekunnin päästä. Paradoksin kuvailussa tuo aika pilkotaan yhä pieneneviin osiin, jolloin rupeaa näyttämään, ettei Akilleus milloinkaan saa kilpikonnaa kiinni. Tarkastellaan asiaa seuraavasti: Merkitään a_1:llä aikaa, joka Akilleukselta menee etumatkan kiinniottamiseen, a_2:lla aikaa, joka Akilleukselta menee kilpikonnan ajassa a_1 kulkeman matkan suorittamiseen, a_3:lla aikaa, joka Akilleukselta kuluu kilpikonnan ajassa a_2 kulkeman matkan suorittamiseen, jne.

Akilleus ja kilpikonna

Koska kilpikonna kulkee ajassa a matkan $a \cdot \frac{2}{100}$ metriä ja Akilleus juoksee tuon matkan $(a \cdot \frac{2}{100})/20 = \frac{a}{1000}$ sekunnissa, niin on voimassa

$$a_1 = 5 \quad \text{sekuntia ja} \quad a_{n+1} = \frac{a_n}{1000} \quad \text{jokaisella } n = 1, 2, \ldots$$

Täten paradoksissa tarkastellut aikavälit muodostavat geometrisen jonon, jonka ensimmäinen termi on 5 ja jossa peräkkäisten termien suhde on $\frac{1}{1000}$. Geometrisen summan kaavan nojalla on voimassa

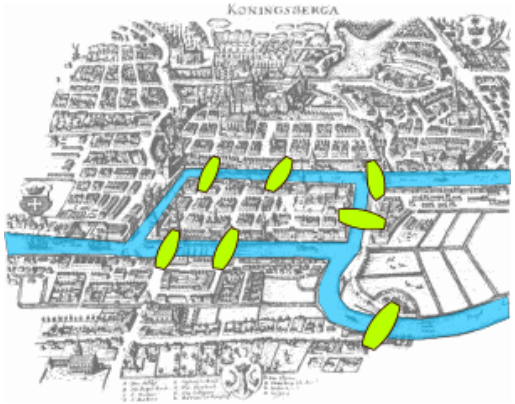
$$a_1 + a_2 + \cdots + a_n = 5 \cdot \frac{1 - (\frac{1}{1000})^n}{1 - \frac{1}{1000}} = 5 \cdot \left(1 - \frac{1}{1000^n}\right) \cdot \frac{1000}{999} = \frac{5000}{999} - \frac{5}{999 \cdot 10^{n-1}}$$

Tästä näemme, että aika on paradoksissa pilkottu osiin, joiden yhteenlaskettu kesto ei milloinkaan ylitä $\frac{5000}{999}$ sekuntia, eli sitä aikaa, joka Akilleukselta kului kilpikonnan kiinnisaamiseen. Oikea johtopäätös ei siis ole, ettei Akilleus saavuta "koskaan" kilpikonnaa, vaan ettei Akilleus saavuta kilpikonnaa "koskaan ennen kuin $\frac{5000}{999}$ sekunnin päästä".

Verkot

Königsbergin sillat

1700-luvun Königsbergin (nykyisen Kaliningradin) läpi virtasi joki, jonka ylitti seitsemän siltaa. Sanotaan, että kaupungin asukkaat yrittivät löytää reittiä, joka lähtisi heidän kotoaan, ylittäisi kaikki seitsemän siltaa täsmälleen kerran ja palaisi kotiin. Reittiä ei tahtonut löytyä. Ongelmaan tarttui matemaatikko Leonhard Euler, joka osoitti reitin olevan mahdoton.



Königsberg 1700-luvulla

Leonhard Euler (1707-1783)

Königsbergin sillat

Hän aloitti palauttamalla ongelman verkoiksi eli graafiksi, jossa pisteet kuvaavat maamassoja ja viivat niitä yhdistäviä siltoja.

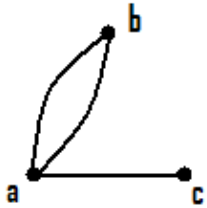
Sitten hän päätteli:
Jos haluttu reitti olisi olemassa, niin aina kun tätä reittiä kulkien saavuttaisiin jotakin viivaa pitkin pisteeseen, täytyisi pisteestä poistua toista viivaa pitkin. Siis jokaiseen pisteeseen täytyisi mennä parillinen määrä viivoja. Koska näin ei ole, ei haluttua reittiä ole olemassa. Vaikka tingittäisiin vaatimuksesta, että reitti päättyy kotiovelle (eli sinne mistä lähdettiinkin) täytyisi kahta kotimantereesta eroavia maamassoja yhdistää parillinen määrä siltoja. Tämäkään ei pidä paikkaansa, joten edes tällaista reittiä ei ole olemassa. Tästä sai alkunsa verkkoteoria.

Kauppamatkustajan ongelma

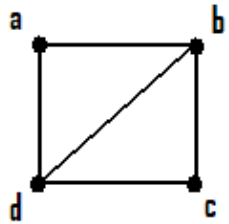
Kauppamatkustaja kiertää kaupungista toiseen kaupustelemassa. Oletetaan, että jokaisesta kaupungista pääsee toiseen ja että kauppamatkustaja tietää kaupunkien väliset etäisyydet. Kuinka hän löytää mahdollisimman lyhyen kerran kussakin kaupungissa käyvän ja lopulta kotiin palaavan reitin? Palataan tähän ongelmaan määriteltyämme verkkoihin liittyvät käsitteet hieman tarkemmin.

Määritelmiä

Verkko koostuu äärellisestä määrästä pisteitä, ja niitä yhdistäviä viivoja. Huomaa, että määritelmässämme kahta pistettä voi yhdistää useampi viiva (kuten Königsbergin siltaongelmassa)! Verkkoa sanotaan **yksinkertaiseksi** mikäli kahta pistettä yhdistää korkeintaan yksi viiva. Kuhunkin pisteeseen menevien viivojen lukumäärää sanotaan tuon pisteen **asteeksi**. Esim.



Tämä verkko ei ole yksinkertainen. Pisteiden *a*, *b* ja *c* asteet: 3, 2, 1. Viivojen lukumäärä 3.

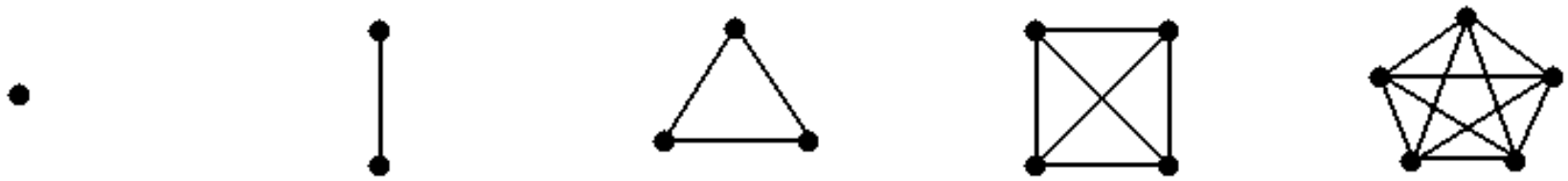


Tämä verkko on yksinkertainen. Pisteiden *a*, *b*, *c* ja *d* asteet: 2, 3, 2, 3. Viivojen lukumäärä 5.

Huomaa: Kaikkien pisteiden asteiden summa on yhtäsuuri kuin kaksi kertaa viivojen lukumäärä.
Tämä seuraa siitä, että jokainen viiva lisää asteiden summaa kahdella.
Tästä seuraa myös, että asteiden summa on parillinen.

Täydelliset verkot

Täydellinen verkko K_p on yksinkertainen verkko, jossa on p pistettä ja jossa jokaista pisteparia yhdistää viiva.

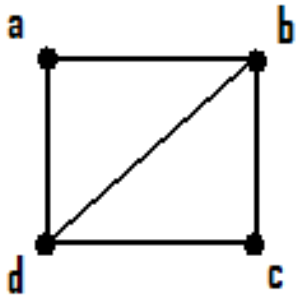


K_1 K_2 K_3 K_4 K_5

Koska verkossa K_p jokaisen pisteen aste on $p-1$, toteuttaa viivojen lukumäärä q edellisen huomion nojalla yhtälön $2q = p(p-1)$, eli $q = \frac{1}{2}p(p-1)$.

Kulku verkossa

Kulku tarkoittaa sellaista äärellistä jonoa verkon viivoja, jossa kukin viiva jatkaa siitä mihin edellinen loppui. Yksinkertaisessa verkossa kulkua voidaan kuvata jonolla verkon pisteitä, jossa peräkkäisiä pisteitä yhdistää viiva. Korkeintaan kerran kutakin viivaa kulkevaa kulkua, joka päättyy samaan pisteeseen mistä lähtikin, sanotaan **kierrokseksi**. Kierros verkossa voidaan aina ajatella alkavan mistä tahansa kierroksen pisteestä. Siten ei ole tarvetta tehdä eroa eri pisteistä alkavien, mutta samoja viivoja kulkevien kierrosten välille. Tarkastellaan esimerkiksi yksinkertaista verkkoa



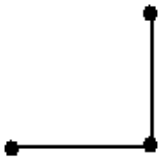
(a, b, c) on eräs kulku
(a, c, b) ei ole kulku, sillä pisteitä a ja c ei yhdistä viiva
(a, b, d, a) on eräs kierros
(a, b, d, a), (b, d, a, b) ja (d, a, b, d) ovat oleellisesti sama kierros
(a, b, c, d, a) on täsmälleen kerran jokaisen pisteen kautta kulkeva kierros

Königsbergin siltaongelma

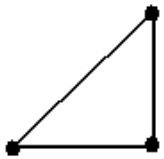
Königsbergin siltaongelma oli siis löytää verkosta täsmälleen kerran jokaista viivaa kulkeva kierros. Eulerin päättely osoitti tämän olevan mahdollista mielivaltaisessa verkossa vain jos jokaisen pisteen aste on parillinen. Koska ylläolevassa Königsbergin siltoja kuvaavassa verkossa näin ei ole, ei Königsbergin siltaongelmalla ole ratkaisua.

Puut

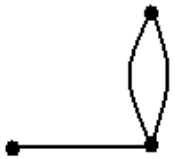
Verkkoa, jossa jokaista pisteparia yhdistää jokin kulku, sanotaan **yhtenäiseksi**. Sanomme **puuksi** yhtenäistä verkkoa, jossa ei ole kierroksia. (Puut saatetaan joskus määritellä hieman eri tavoin.) Esim.



puu



ei puu

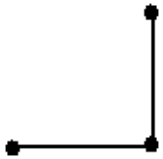


ei puu

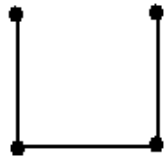
Erityisesti puu on aina yksinkertainen, muuten siinä olisi kierros.

Puut

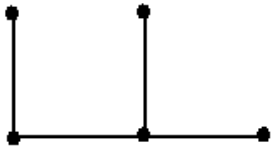
Tarkastellaan muutamia pieniä puita:



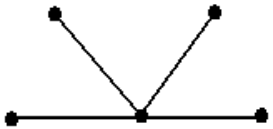
3 pistettä, 2 viivaa



4 pistettä, 3 viivaa



5 pistettä, 4 viivaa



5 pistettä, 4 viivaa

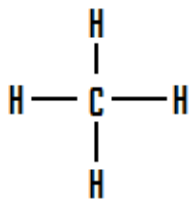
Se, että viivoja on yksi vähemmän kuin pisteitä, riittää itseasiassa "karakterisoimaan" puut:

Lause

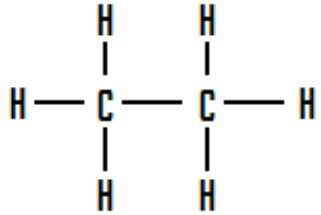
Olkoon T yksinkertainen verkko, jossa on p pistettä. Tällöin T on puu, jos ja vain jos se on yhtenäinen ja siinä on $p-1$ viivaa.

Alkaanit

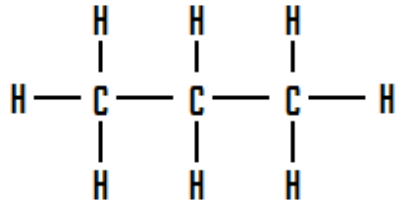
Hiilivetyä (tarkemmin alkaania) C_nH_{2n+2}, missä $n \geq 1$ on luonnollinen luku, esittää yhtenäinen verkko jonka pisteet ovat kyseisen molekyylin atomeja ja viivat sidoksia. Esim.



metaani CH_4



etaani C_2H_6



propaani C_3H_8

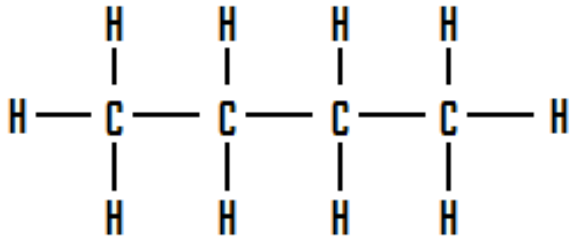
Molekyylin C_nH_{2n+2} verkossa on siis $p = 3n + 2$ pistettä. Jokainen n:stä hiiliatomista on astetta 4, kun taas kaikki $2n + 2$ vetyatomia ovat astetta 1. Kun merkitään viivojen lukumäärää q:lla, saadaan

$$q = \frac{1}{2}(4n + 2n + 2) = 3n + 1 = p - 1,$$

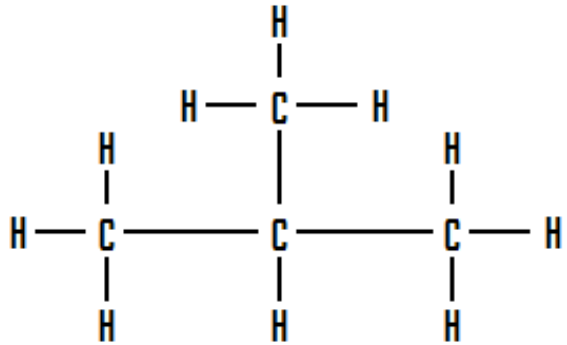
eli kyseinen verkko on puu.

Isomorfisuus

Verkkoteoriassa on oleellista verkkojen isomorfisuuden eli "samanrakenteisuuden" käsite. Kahden verkon sanotaan olevan isomorfiset, mikäli niiden pisteillä on sellainen bijektiivinen vastaavuus, että toisiaan vastaavia pistepareja yhdistää molemmissa verkoissa yhtä monta viivaa. Tähän käsitteeseen perehdytään tarkemmin muilla kursseilla. Huomataan kuitenkin, että hiilivetyä C_4H_{10} vastaa kaksi erirakenteista verkkoa



butaani C_4H_{10}



isobutaani C_4H_{10}

Painotetut verkot ja kauppamatkustajan ongelma

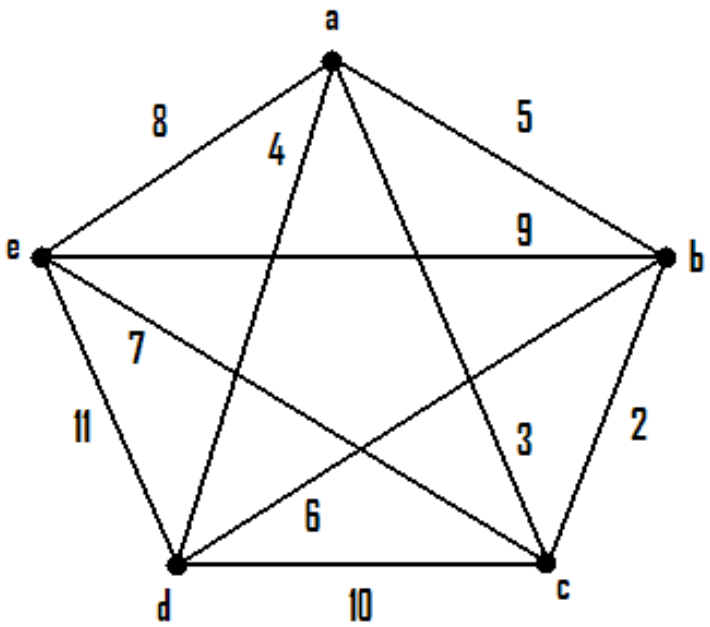
Painotetuksi verkoksi sanomme verkkoa, jonka jokaiseen viivaan on yhdistetty jokin luku eli "paino", joka voi kuvata esimerkiksi viivan pituutta eli pisteiden etäisyyttä tms. Kauppamatkustajan ongelma voidaan siis p:n kaupungin tapauksessa muotoilla seuraavalla tavalla: Olkoon täydellinen verkko K_p painotettu positiivisilla reaaliluvuilla. Etsi halvin kierros, joka kulkee täsmälleen kerran verkon jokaisen pisteen kautta. Painojen voi ajatella olevan etäisyyksiä, mikäli ne toteuttavat ns. kolmioepäyhtälön:
Kulku suoraan on aina korkeintaan yhtä kallis kuin kiertoteitse. Painojen ei kuitenkaan välttämättä tarvitse kuvata (ajallisia) etäisyyksiä, voihan kauppamatkustaja käyttää erilaisia kulkuyhteyksiä. Esim. lentäen kiertoteitse voi olla perillä nopeammin (tai halvemmin) kuin suoralla junayhteydellä. Ongelman kannalta oleellisesti erilaisia kierroksia on

$$\frac{1}{2}(p-1)\cdot(p-2)\cdots 3\cdot 2\cdot 1 \quad \text{kappaletta.}$$

Palataan kierrosten lukumäärän laskemiseen ensi viikolla.

Esimerkki

Etsitään halvin kierros verkossa K_5. Tarkasteltavia kierroksia on $\frac{1}{2} \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 12$ kappaletta.



(a, b, c, d, e, a) :
$5 + 2 + 10 + 11 + 8 = 36$
(a, b, c, e, d, a) :
$5 + 2 + 7 + 11 + 4 = 29$
(a, b, d, c, e, a) : 36
(a, b, d, e, c, a) : 32
(a, b, e, c, d, a) : 35
(a, b, e, d, c, a) : 38
(a, c, b, d, e, a) : 30
(a, c, b, e, d, a) : 29
(a, c, e, b, d, a) : 29
(a, c, d, b, e, a) : 36
(a, d, c, b, e, a) : 31
(a, d, b, c, e, a) : 27

Kierros (a, d, b, c, e, a) on siis halvin. Huomaa, että tarkastellut painot eivät kuvaa etäisyyksiä: $(c, d) : 10$, mutta $(c, b, d) : 2 + 6 = 8$.

Todennäköisyys ja kombinatoriikka

Todennäköisyys

Todennäköisyys on "epävarman matematiikkaa". Matemaattinen todennäköisyys mallintaa *satunnaisia ilmiöitä*, kuten esimerkiksi nopan- tai lantinheitto. Todennäköisyyttä voi lähestyä mm. tilastollisesti tutkimalla toistokokeessa tietyn lopputuloksen tai havaintoarvojen esiintymiskertojen lukumäärää.

Alunperin todennäköisyyslaskenta kehittyi uhkapelien (esim. pokeri) teoriana.

Määritelmiä

Satunnaisilmiön **perusjoukko** Ω koostuu kaikista mahdollisista **alkeistapauksista** $\omega_1, \omega_2, \ldots, \omega_n$. Tällöin perusjoukon Ω koko eli sen alkioiden lukumäärä $\#\Omega = n$. Oletetaan toistaiseksi, että $n < \infty$.

Esim. Lantinheitossa ω_1 =”saadaan kruuna”, ω_2 =”saadaan klaava” ja siis $\Omega = \{\omega_1, \omega_2\}$, jolloin $\#\Omega = 2$.
Nopanheitossa taas ω_1 =”saadaan 1”, ω_2 =”saadaan 2”, …, ω_6 =”saadaan 6” ja koska $\Omega = \{\omega_1, \omega_2, \ldots, \omega_6\}$ on $\#\Omega = 6$.

Alkeistapausten yhdistelminä saadaan **tapahtumat**, jotka ovat siis perusjoukon Ω osajoukkoja.

Esim. Nopanheitossa voidaan asettaa tapahtumaksi
A =”saadaan parillinen” =”saadaan 2, 4 tai 6” $= \{\omega_2, \omega_4, \omega_6\}$.

Symmetrinen todennäköisyys

Tarkastellaan seuraavaksi vain **symmetristä todennäköisyyttä**, toisin sanoen oletetaan, että perusjoukko Ω on äärellinen ja kaikilla alkeistapahtumilla on sama todennäköisyys.

Symmetriseen satunnaisilmiöön liittyvän tapahtuman A todennäköisyys $P(A)$ on luku

$$P(A) = \frac{\#A}{\#\Omega}$$

ja tulkinta: A tapahtuu $100 \cdot P(A)\%$ varmuudella.
Huomaa, että $P(\emptyset) = 0$ ja $P(\Omega) = 1$ eli "jotain tapahtuu varmasti".
Selvästi $P(A) \in [0, 1]$.

Esim. Nopanheitossa $\#A = 3$, kun $A =$"saadaan parillinen" ja tapahtuman todennäköisyys $P(A) = \frac{\#A}{\#\Omega} = \frac{3}{6} = 0,5$. Siis parillinen saadaan 50% varmuudella.

Esim. Heitetään kahta noppaa. Millä tn:llä ainakin toinen on kakkonen?

Vastatapahtuma

Tapahtuman A **vastatapahtuma** on $A^{\complement}$ =”A ei tapahdu” ja sen todennäköisyys

$$P(A^{\complement}) = 1 - P(A).$$

Esim. Nopanheitossa A =”saadaan parillinen”, jolloin $A^{\complement}$ =”ei saada parillista” ja siten

$$P(A^{\complement}) = 1 - P(A) = 1 - 0,5 = 0,5.$$

Samaan tulokseen oltaisiin päädytty laskemalla suoraan tapahtuman $A^{\complement}$ =”ei saada parillista”=”saadaan 1, 3 tai 5” todennäköisyys.

Ongelma - Biologit ja matemaatikot

Oletetaan, että meillä on b kpl biologeja ja m kpl matemaatikkoja. Näiden joukosta valitaan satunnaisesti 5 henkilön joukko. Millä todennäköisyydellä tässä viiden joukossa on tasan 3 biologia ja 2 matemaatikkoa?

Tehtävän ratkaisemiseksi pitäisi tietää, kuinka monta erilaista 5 henkilön joukkoa voidaan valita $b + m$ henkilön joukosta (eli perusjoukon alkioiden lukumäärä) ja kuinka monta erilaista, täsmälleen halutunlaista viisikkoa on näistä kaikista (tapahtuman alkioiden lukumäärä).

Työkaluja tähän ongelmaan saamme *kombinatoriikasta*. (Yo. ongelman ratkaisu harjoitustehtävänä.)

Kombinatoriikka

Kombinatoriikassa tarkastellaan mm. äärellisiä joukkoja, niiden relaatioita ja osajoukkoja sekä näiden välisiä kuvauksia. Kombinatoriikan klassisimmassa osassa keskeinen ongelma on joukon alkioiden lukumäärän laskeminen ja se liittyykin läheisesti todennäköisyyslaskentaan. Monialainen tiedemies Blaise Pascal oli eräs kombinatoriikan kehitykseen vaikuttaneista. Hänen mukaansa on nimetty ns. binomikertoimet sisältävä Pascalin kolmio, johon tutustumme hetken kuluttua.

Blaise Pascal (1623-1662)

Tuloperiaate

Tarkastellaan toimintaa, joka voidaan suorittaa n:ssä **toisistaan riippumattomassa** (peräkkäisessä) vaiheessa.
Oletetaan, että
vaihe 1 voidaan suorittaa α_1 eri tavalla
vaihe 2 voidaan suorittaa α_2 eri tavalla
$\vdots$
vaihe n voidaan suorittaa α_n eri tavalla.
Yleisesti: k:s vaihe ($1 \leq k \leq n$) voidaan suorittaa α_k eri tavalla riippumatta siitä miten muut vaiheet suoritetaan. Tällöin koko toiminta voidaan suorittaa

$$\alpha_1 \alpha_2 \cdots \alpha_n \text{ eri tavalla.}$$

Esim. Ravintola tarjoilee kolmea erilaista alkupalaa, kuutta erilaista pääruokaa ja viittä erilaista jälkiruokaa. Kolmen ruokalajin ateria voidaan valita $3 \cdot 6 \cdot 5 = 90$ eri tavalla.

Summaperiaate

Tarkastellaan toimintaa, joka voidaan suorittaa n:llä **toisensa poissulkevalla** vaihtoehtoisella menetelmällä. Oletetaan, että
menetelmä 1 voidaan toteuttaa α_1 eri tavalla
menetelmä 2 voidaan toteuttaa α_2 eri tavalla
$\vdots$
menetelmä n voidaan toteuttaa α_n eri tavalla.
Yleisesti: k:s menetelmä voidaan toteuttaa α_k eri tavalla.
Eri keinoja suorittaa toiminta on tällöin

$$\alpha_1 + \alpha_2 + \cdots + \alpha_n \text{ kpl.}$$

Esim. Montako kahden ruokalajin (pääruoan sisältävää) ateriaa voidaan tällöin valita edellisen esimerkin ravintolassa?
Voidaan valita joko alkupala ja pääruoka, tai pääruoka ja jälkiruoka. Alkupala ja pääruoka voidaan tuloperiaatteen mukaan valita $3 \cdot 6 = 18$ eri tavalla, kun taas pääruoka ja jälkiruoka voidaan valita $6 \cdot 5 = 30$ eri tavalla. Summaperiaatteen mukaan erilaisia kahden ruokalajin (pääruoan sisältäviä) aterioita on $18 + 30 = 48$ kappaletta.

Esimerkki - Syntymäpäivä

Millä todennäköisyydellä n:n henkilön joukossa ainakin kahdella on sama syntymäpäivä?
Ratkaisu: Nyt alkeistapauksina ovat kaikki jonot, joissa on n kappaletta päivämääriä eli kaikki mahdolliset n henkilön syntymäpäivät. Näistä n:stä päivämäärästä jokainen voi olla mikä tahansa 365:stä päivämäärästä. Siis perusjoukko Ω sisältää nämä kaikki $365^n (= \#\Omega)$ jonoa.
Tapahtuman $A =$"ainakin kahdella on sama syntymäpäivä" vastatapahtuma on $A^{\complement} =$"kaikilla eri syntymäpäivä". Tuloperiaatteen nojalla $\#A^{\complement} = 365 \cdot 364 \cdots (365 - n + 1)$. Siis

$$P(A) = 1 - P(A^{\complement}) = 1 - \frac{365 \cdot 364 \cdots (365 - n + 1)}{365^n}.$$

Kun $n \geq 23$, niin $P(A) > 0,5$
Kun $n \geq 41$, niin $P(A) > 0,9$
Kun $n \geq 57$, niin $P(A) > 0,99$.

Kertoma

Neljä henkilöä A, B, C ja D muodostavat komitean. Heistä yhden on oltava puheenjohtaja, yhden sihteeri, yhden rahastonhoitaja ja yhden PR-henkilö. Kuinka monella eri tavalla tehtävät voidaan jakaa?
Ratkaisu:
Puheenjohtajaksi voidaan valita kuka tahansa neljästä. Jäljelle jäävistä kolmesta valitaan sitten sihteeri, ja loput kaksi jakavat rahastonhoitajan ja PR-henkilön tehtävät. Vaihtoehtoja on siis $4 \cdot 3 \cdot 2 \cdot 1 = 24$ kappaletta. Lukua sanotaan neljän kertomaksi ja sille käytetään merkintää 4!.

Määritellään luonnollisen luvun n **kertoma**

$$n! = 1 \cdot 2 \cdot 3 \cdots n = \prod_{k=1}^{n} k$$

ja sovitaan, että $0! = 1$.
Yleisesti, n objektia voidaan järjestää jonoon $n!$ eri tavalla.

Kertoman $n!$ arvoja

Kertoman $n!$ arvot on helppo laskea pienillä luvuilla n:
$1! = 1$, $2! = 2$, $3! = 6$, $4! = 24$, $5! = 120$, $6! = 720$, $7! = 5040$,
$8! = 40320$, $9! = 362880$, $10! = 3628800$, ...
Huomataan, että kertoma kasvaa kuitenkin hyvin nopeasti. Sen suuruusluokkaa voidaan arvioida Stirlingin kaavalla:

$$n! \sim \sqrt{2\pi n}\left(\frac{n}{e}\right)^n.$$

Tässä merkinnällä $\sim$ tarkoitetaan sitä, että

$$\frac{\sqrt{2\pi n}\left(\frac{n}{e}\right)^n}{n!} \to 1, \quad \text{kun} \quad n \to \infty,$$

eli toisin sanoen yo. osamäärä lähestyy lukua 1, kun n kasvaa rajatta.
Huomaa: Olipa $a > 0$ mikä hyvänsä kantaluku , niin $n! > a^n$ kaikilla tarpeeksi suurilla n.

Täydellisten graafien kierroksista

Tarkastellaan täydellistä graafia K_p. Monellako eri tavalla voimme tehdä kierroksen K_p:ssä? Eri pisteistä alkavat, mutta samoja viivoja kulkevat kierrokset on mielekästä samaistaa. Siten voimme valita kierroksen alkupisteen vapaasti. Alkupisteestä kierros voi jatkua $p-1$ pisteeseen, josta edelleen $p-2$ pisteeseen. Jatkamalla tällä tavoin ollaan tilanteessa, jossa kaikki graafin pisteet on käyty läpi ja viimeisestä pisteestä palataan alkupisteeseen. Tuloperiaatteen mukaan eri vaihtoehtoja on siten $(p-1)!$. Kutakin kierrosta kohti graafissa on samat viivat käänteisessä järjestyksessä kulkeva kierros. Kauppamatkustajan ongelmassa on yhdentekevää kuljetaanko kierros etu- vai takaperin. Siten tuota ongelmaa (p:n kaupungin tapauksessa) tarkasteltaessa on huomioitava $\frac{1}{2}(p-1)!$ kierrosta.

Kertoma kasvaa kuitenkin niin nopeasti, että lyhimmän (tai halvimman) reitin löytäminen on tietokoneellekin mahdotonta, kun kaupunkeja on tarpeeksi monta.

Jonojen muodostus isommasta valikoimasta objekteja

Aiemmin esillä olleeseen neljän hengen komiteaan pyrkii 20 ihmistä. Montako erilaista komiteaa voidaan muodostaa?
Ratkaisu:
Puheenjohtaja voidaan ensin valita kahdestakymmenestä pyrkijästä, sitten sihteeri yhdeksästätoista, jonka jälkeen rahastonhoitaja kahdeksastatoista ja lopulta PR-henkilö seitsemästätoista. Vaihtoehtoja on siis $20 \cdot 19 \cdot 18 \cdot 17 = 116280$ kappaletta.

Yleisesti, n:stä objektista voidaan muodostaa k:n mittaisia jonoja

$$n(n-1)\cdots(n-k+1) = \frac{n!}{(n-k)!} \text{ kappaletta.}$$

Osajoukkojen muodostus isommasta valikoimasta objekteja

Tarkastellaan taas tilannetta, jossa neljän hengen komiteaan pyrkii 20 ihmistä, mutta kiinnittämättä huomiota eri tehtäviin. Montako eri kokoonpanoa voidaan pyrkijöistä valita?

Ratkaisu:

Eri komiteoita on edellisen esimerkin mukaan $\frac{20!}{16!}$ kappaletta. Osassa niistä on kuitenkin samat ihmiset, koska kussakin kokoonpanossa tehtävät voidaan jakaa 4! eri tavalla, kuten aikaisemmin todettiin. Erilaisia kokoonpanoja (huomioimatta tehtävänjakoa) on siten

$$\frac{20!}{4!16!} = 4845 \text{ kappaletta.}$$

Yleisesti, n:stä objektista voidaan muodostaa erilaisia k:n objektin (järjestämättömiä) joukkoja

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

kappaletta. Merkintä $\binom{n}{k}$ luetaan 'n yli k:n'.

Esimerkki - Lottorivit

Montako erilaista lottoriviä on?
Ratkaisu:
Lottorivi on 7 lottonumeron osajoukko 39 lottonumeron joukosta.
Erilaisia lottorivejä on siis

$$\binom{39}{7} = \frac{39!}{7! \cdot (39-7)!} = \frac{39 \cdot 38 \cdot 37 \cdot 36 \cdot 35 \cdot 34 \cdot 33 \cdot 32!}{7! \cdot 32!} = 15380937$$

kappaletta.

Millä todennäköisyydellä lottoaja voittaa täysosuman valitsemillaan seitsemällä numerolla? *Vastaus:* $\frac{1}{15380937} \approx 0,000000065$ eli $0,000007\%$ varmuudella.

Esimerkki - Jalkapallo

Jalkapalloturnaukseen osallistuu 8 joukkuetta. Montako peliä on pelattava, jos kaikkien joukkueiden halutaan kohtaavan toisensa täsmälleen kerran?

Ratkaisu:

Otteluita vaaditaan yhtä monta kuin on tapoja valita 2 joukkuetta 8:n joukosta, eli

$$\binom{8}{2} = \frac{8!}{2! \cdot (8-2)!} = \frac{8 \cdot 7 \cdot 6!}{2! \cdot 6!} = \frac{8 \cdot 7}{2} = 7 \cdot 4 = 28.$$

Potenssijoukon alkioiden lukumäärä

Muistetaan, että potenssijoukolla $\mathcal{P}(X)$ tarkoitettiin kaikkien joukon X osajoukkojen muodostamaa joukkoa. Esimerkiksi kun $X = \{1, 2, 3\}$, niin

$$\mathcal{P}(\{1,2,3\}) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}.$$

Esimerkissämme $\#X = 3$ ja $\#\mathcal{P}(X) = 8 = 2^3$. Myös yleisesti pätee $\#\mathcal{P}(X) = 2^n$, kun $\#X = n < \infty$.

Tämä voidaan nähdä esimerkiksi tuloperiaatteen avulla: Muodostetaan mielivaltainen joukon X osajoukko. Tämä voidaan suorittaa niin, että jokaisen alkion kohdalla päätetään, otetaanko se osajoukkoon vai ei. Näin jokaisen alkion kohdalla on tasan 2 vaihtoehtoa (otetaan - ei oteta). Koska valinnat eri alkioiden välillä ovat toisistaan riippumattomia, niin erilaisia joukon X osajoukkoja on $\underbrace{2 \cdot 2 \cdots 2}_{n \text{ kpl}} = 2^n$ kpl.

Potenssijoukon alkioiden lukumäärä - jatkuu

Toisaalta, tilannetta voidaan tarkastella jakamalla joukon X osajoukot luokkiin niiden alkioiden lukumäärän mukaan. Nyt esimerkiksi joukon X 3-alkioisia osajoukkoja on $\binom{n}{3}$ kpl. Summaamalla yhteen kaikkien k-alkioisten ($0 \leq k \leq n$) osajoukkojen lukumäärät saadaan kaikkien (erityisesti kaiken kokoisten) joukon X osajoukkojen lukumäärä yhteensä.

Siis $\#\mathcal{P}(X) = \sum_{k=0}^{n} \binom{n}{k}$. Tällä *kombinatorisella päättelyllä* on saatu identiteetti

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n.$$

(Täsmällinen todistus induktiolla harjoitustehtävänä.)

Symmetrisyys

Olkoot $n \geq 1$ ja $0 \leq k \leq n$. Tällöin

$$\binom{n}{k} = \binom{n}{n-k}.$$

Tämä on selvää, sillä kutakin k objektin valintaa n objektista vastaa $n-k$ objektin (jäljelle jääneet) valinta. Siis esim.

$$\binom{7}{2} = \binom{7}{5} \quad \text{ja} \quad \binom{13}{4} = \binom{13}{9}.$$

Pascalin identiteetti

Olkoot $n \geq 1$ ja $0 < k < n$. Tällöin

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}.$$

Lähdetään liikkeelle yhtälön vasemmasta puolesta ja lasketaan määritelmää käyttäen

$$\binom{n-1}{k-1} + \binom{n-1}{k} = \frac{(n-1)!}{(k-1)!((n-1)-(k-1))!} + \frac{(n-1)!}{k!(n-1-k)!}.$$

Laventamalla ensimmäistä termiä k:lla ja toista $n-k$:lla saadaan

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

Yhdistämällä termit, ottamalla $(n-1)!$ yhteiseksi tekijäksi ja sieventämällä saadaan lopulta

$$= \frac{(n-1)!(k+n-k)}{k!(n-k)!} = \frac{n!}{k!(n-k)!} = \binom{n}{k}.$$

Binomikertoimet

Lukuja $\binom{n}{k}$ kutsutaan **binomikertoimiksi**, koska $\binom{n}{k}$ on termin $x^{n-k}y^k$ kertoimena aukikerrotussa binomin $x+y$ potenssissa $(x+y)^n$.
Esim.

$$(x+y)^2 = x^2 + 2xy + y^2 = \binom{2}{0}x^2 + \binom{2}{1}xy + \binom{2}{2}y^2$$

$$(x+y)^3 = x^3+3x^2y+3xy^2+y^3 = \binom{3}{0}x^3 + \binom{3}{1}x^2y + \binom{3}{2}xy^2 + \binom{3}{3}y^3$$

$$(x+y)^4 = x^4 + 4x^3y + 6x^2y^2 + 4xy^3 + y^4$$

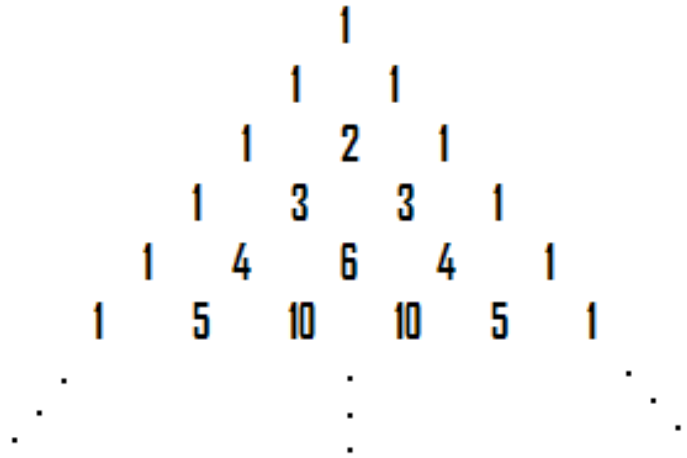
$$= \binom{4}{0}x^4 + \binom{4}{1}x^3y + \binom{4}{2}x^2y^2 + \binom{4}{3}xy^3 + \binom{4}{4}y^4$$

Yleisesti:

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

Pascalin kolmio

Binomikertoimet muodostavat ns. Pascalin kolmion. Kerroin $\binom{n}{k}$ on kolmion $n+1$:nnen rivin $k+1$:s luku. Pascalin identiteetin mukaan kolmiossa oleva luku on saatu sen yläpuolella olevien vierekkäisten lukujen summana.



Ongelma - Tikkataulu

Heitetään umpimähkäisesti tikkaa (kuitenkin niin, että tikka osuu tauluun). Millä todennäköisyydellä tikka osuu kymppiin?

Otetaan perusjoukoksi tikkataulun määrittämä pistejoukko. Mutta aiemmilta luennoiltahan tiedetään, että kymppiympyrässä on (numeroituvasti) äärettömän verran pisteitä - samoin kuin tikkataulussa!

Lisäksi todennäköisyydet tapahtumien $A_k =$"saadaan k", $1 \leq k \leq 10$, välillä eivät tuntuisi olevan samat. Miksi?

Todennäköisyysfunktio

Määritellään todennäköisyys funktiona $p : \mathcal{P}(\Omega) \longrightarrow [0, 1]$, missä funktio p liittää jokaiseen tapahtumaan $A \in \mathcal{P}(\Omega)$ sen todennäköisyyden $p(A)$. Todennäköisyysfunktiolle pätee

- $p(A) \geq 0$ kaikilla $A \in \mathcal{P}(\Omega)$
- $p(\Omega) = 1$ ja $p(\emptyset) = 0$
- Jos $A, B \in \mathcal{P}(\Omega)$ ja $A \cap B = \emptyset$, niin $p(A \cup B) = p(A) + p(B)$.

Äärettömän perusjoukon tapauksessa alkeistapausten todennäköisyydet *eivät välttämättä* määrää muiden tapahtumien todennäköisyyksiä (tikkatauluesimerkki!). Geometrisessä todennäköisyysmallissa todennäköisyysmitta voidaan rakentaa minkä tahansa äärellisen *mitta-avaruuden* pohjalta. Lyhyesti: jos perusjoukkomme Ω on jollakin tapaa *äärellismitallinen* (lukumäärältään, pituudeltaan, pinta-alaltaan,...), niin

$$p(A) = \frac{\mu(A)}{\mu(\Omega)}, \text{missä } \mu \text{ on mitta.}$$

Ratkaisu - Tikkataulu

Kuten huomattiin, klassinen (symmetrinen) todennäköisyysmalli ei tässä riitä, vaan mallia täytyy laajentaa geometriseen todennäköisyysmalliin. Luonteva (geometrinen) mitta tapahtuman $A =$"tikka osuu kymppiin" todennäköisyydelle on joukon A pinta-ala jaettuna koko taulun pinta-alalla. Olkoot tikkataulun säde R ja kymppiympyrän r $(0 < r < R)$. Nyt koko tikkataulun ala on πR^2 ja kymppiympyrän ala πr^2. Siten todennäköisyys sille, että tikka osuu kymppiin on

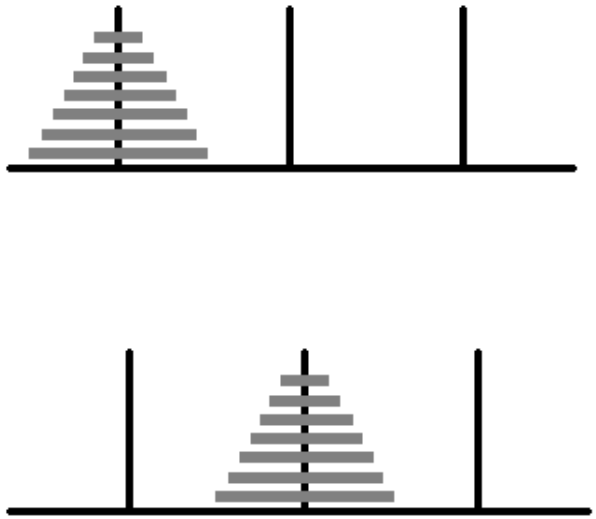
$$p(A) := P(A) = \frac{\pi r^2}{\pi R^2} = \left(\frac{r}{R}\right)^2.$$

Tässä alkeistapaukset vastaavat yhden pisteen joukkoja, jotka ovat nollamitallisia, joten tapahtuman todennäköisyyttä ei voi laskea siihen sisältyvien alkeistapausten todennäköisyyksien summana.

Rekursio

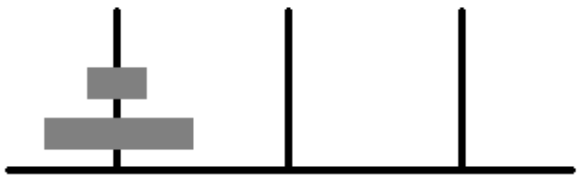
Hanoin tornit

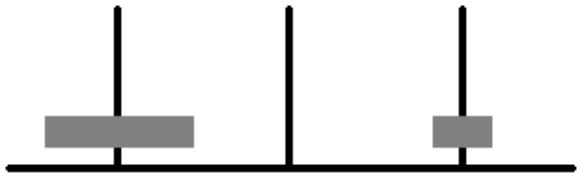
Olkoot n kiekkoa asetettu kolmeen tankoon kuvan osoittamalla tavalla (kuvassa $n = 7$). Siirtämällä yhtä kiekkoa kerrallaan tangosta toiseen, kiekot on asetettava toiseen tankoon samaan järjestykseen. Isompaa kiekkoa ei missään vaiheessa saa asettaa pienemmän päälle. Mikä on pienin määrä tarvittavia siirtoja?

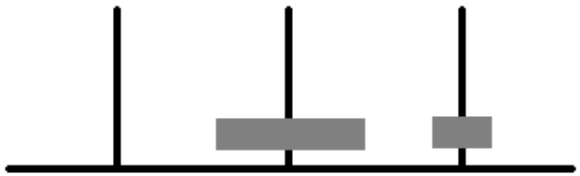


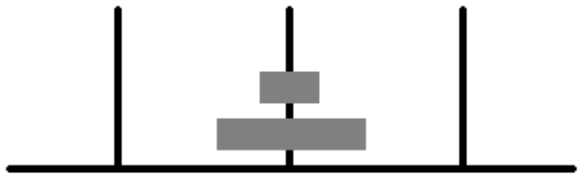
Hanoin tornit

Merkitään a_n:llä pienintä tarvittavaa määrää siirtoja n:lle kiekolle.
Tietysti $a_1 = 1$. Helposti nähdään myös, että $a_2 = 3$:



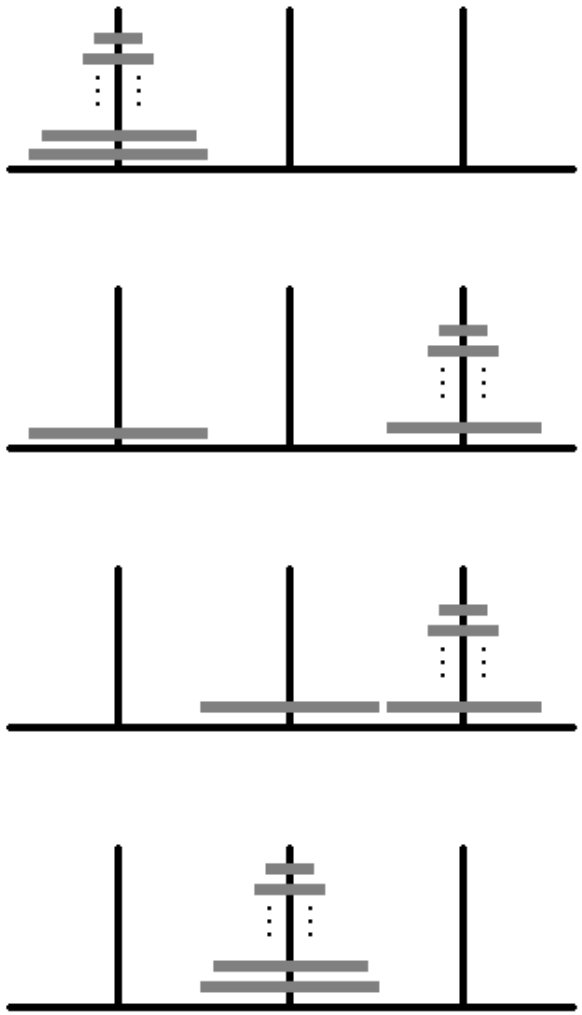






Hanoin tornit

Entäpä a_n? Jotta pohjimmaista kiekkoa voitaisiin siirtää, täytyy yhden tangoista olla tyhjä ja muut $n-1$ kiekkoa siirrettynä kolmanteen tankoon. Tähän vaiheeseen päästäksemme tarvitsemme a_{n-1} siirtoa. Siirretään sitten isoin kiekko tyhjään tankoon. Tehdään lopuksi tarvittavat a_{n-1} siirtoa, jotta pienemmät kiekot saadaan isoimman päälle. Siis $a_n = 2a_{n-1} + 1$.



Hanoin tornit

Rekursiorelaatiosta $a_n = 2a_{n-1} + 1$ saamme tiedon $a_1 = 1$ avulla laskettua luvut a_n:

$a_1 = 1$,
$a_2 = 2 \cdot a_1 + 1 = 2 \cdot 1 + 1 = 3$,
$a_3 = 2 \cdot a_2 + 1 = 2 \cdot 3 + 1 = 7$,
$a_4 = 2 \cdot a_3 + 1 = 2 \cdot 7 + 1 = 15, \ldots$
Näyttää siltä, että $a_n = 2^n - 1$. Todistetaan tämä:

$$
\begin{aligned}
a_n &= 1 + 2a_{n-1} = 1 + 2(1 + 2a_{n-2}) \\
&= 1 + 2 + 2^2 a_{n-2} \\
&= 1 + 2 + 2^2(1 + 2a_{n-3}) \\
&= 1 + 2 + 2^2 + 2^3 a_{n-3} \\
&= \ldots \\
&= 1 + 2 + 2^2 + \cdots + 2^{n-2} + 2^{n-1} a_1 \\
&= 1 + 2 + 2^2 + \cdots + 2^{n-2} + 2^{n-1} \\
&= 2^n - 1.
\end{aligned}
$$

Legenda

Legendan mukaan maailmanloppu tulee, kun erään vietnamilaisen temppelin papit ovat saaneet siirrettyä yllä olevan pulman tavoin järjestetyt 64 kultaista kiekkoa tangosta toiseen. Ei kuitenkaan syytä huoleen, sillä vaikka papit siirtäisivät yhden kiekon sekunnissa, kuluisi heiltä tähän

$$2^{64} - 1 = 18446744073709551615 \quad \text{sekuntia}$$

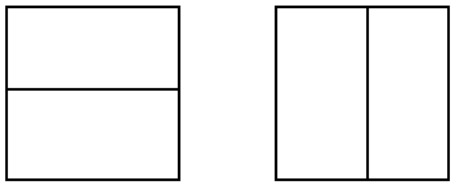
eli noin $5,82 \cdot 10^{11}$ vuotta.

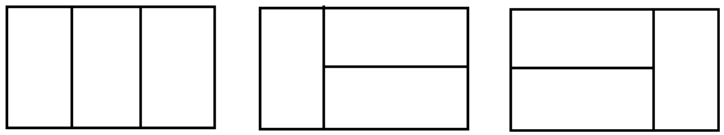
Polun laatoitus

Polku on 2 metriä leveä ja n metriä pitkä. Se on tarkoitus laatoittaa $1m \times 2m$ laatoilla. Monellako eri tavalla tämä voidaan tehdä?

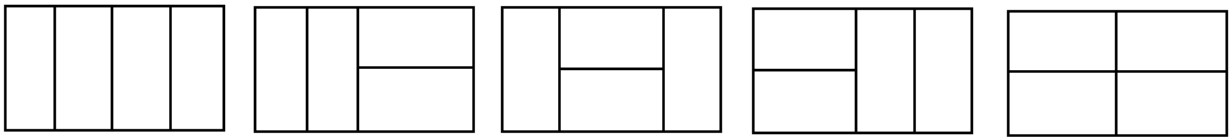
Ratkaisu:

Merkitään n metrin pituisen polun erilaisten laatoitusten lukumäärää p_n:llä. Selvästi $p_1 = 1$, sillä yksi laatta riittää. Huomataan lisäksi, että $p_2 = 2$ ja $p_3 = 3$.





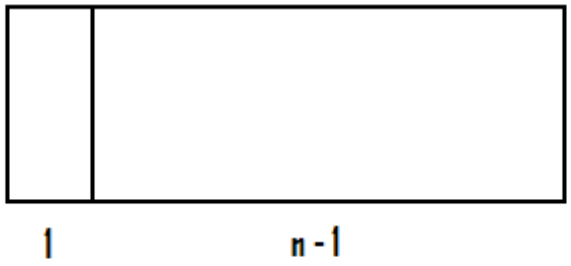
Onko $p_n = n$? Ei, $p_4 = 5$:

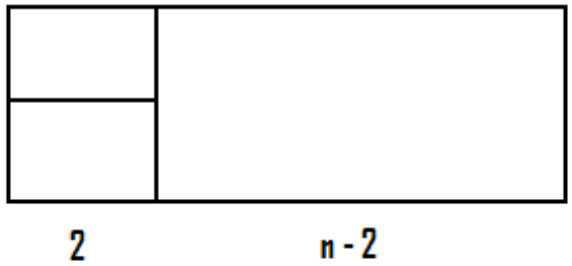


Mikä p_n sitten on?

Polun laatoitus

$2 \times n$ kokoisen polun laatoitus täytyy aloittaa jommalla kummalla seuraavista tavoista:



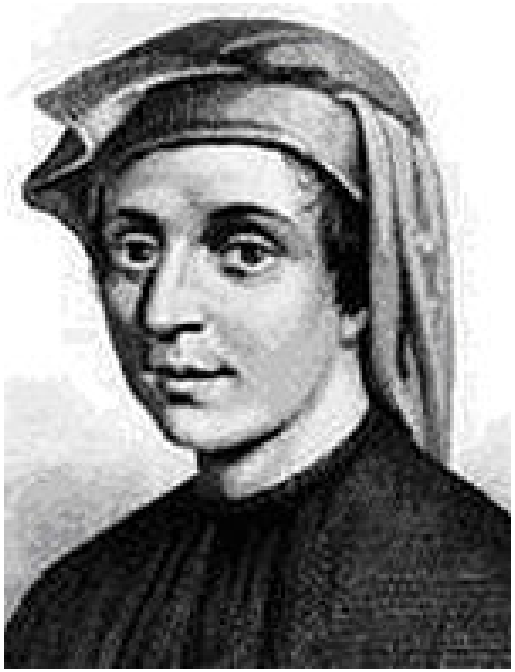


Ensimmäisessä tapauksessa (vasen) se voidaan jatkaa loppuun p_{n-1} tavalla, kun taas toisessa tapauksessa (oikea) se voidaan jatkaa loppuun p_{n-2} tavalla. Siis summaperiaatteen mukaan $p_n = p_{n-1} + p_{n-2}$. Saatu rekursiorelaatio ottaa siis huomioon paitsi edellisen, myös sitä edellisen vaiheen. Voidaan laskea:
$p_5 = p_4 + p_3 = 5 + 3 = 8$,
$p_6 = p_5 + p_4 = 8 + 5 = 13$,
$p_7 = p_6 + p_5 = 13 + 8 = 21$, ja niin edelleen.

Fibonaccin jono

Saatua jonoa
$(1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, \ldots)$
sanotaan **Fibonaccin jonoksi** (alussa on yksi ykkönen lisää poikkeuksena edelliseen).
Tähän jonoon voi törmätä useissa paikoissa luonnossa!
Esim. kukkien terälehtien lukumäärissä:

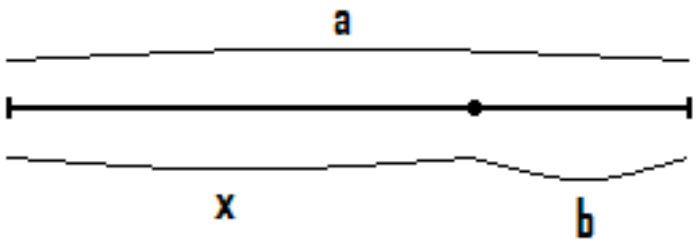
3	liljat ja iirikset
5	akileijat, leinikit ja ritarinkannus
8	kukonkannus
13	keltainen päivänkakkara
21	asteri
34, 55	kaunokaiset



Leonardo Pisalainen alias Fibonacci

Kultainen suhde

Etsi annetulta janalta piste, joka jakaa janan kahteen osaan siten, että koko janan ja suuremman osan pituuksien suhde $\frac{a}{x}$ on sama kuin suuremman ja pienemmän osan pituuksien suhde $\frac{x}{b}$.



Kultainen suhde φ on suuremman ja pienemmän osan pituuksien suhde tässä *kultaisessa leikkauksessa*. Määritetään φ:n arvo:
Olkoon $b = 1$, jolloin $\varphi = x$ ja koko janan pituus $a = x + 1$. Nyt

$$\frac{a}{x} = \frac{x}{b} \iff \frac{x+1}{x} = \frac{x}{1} \iff x + 1 = x^2 \iff x^2 - x - 1 = 0,$$

joten

$$\varphi = x = \frac{1 + \sqrt{1+4}}{2} = \frac{1+\sqrt{5}}{2} \approx 1,618.$$

Kultainen suhde ja Fibonaccin jono

Tarkastelimme aikaisemmin Fibonaccin jonoa
$(1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, \ldots)$ rekursiivisesti eli "askel kerrallaan".
Voidaanko jonon luvut esittää *suljetussa muodossa*? Voidaan:

$$F_n = \frac{\varphi^n - (1-\varphi)^n}{\sqrt{5}}, \quad \text{missä} \quad \varphi = \frac{1+\sqrt{5}}{2}.$$

Todistetaan tämä induktiolla:
Tapaus $n = 1$:

$$\frac{\varphi - (1-\varphi)}{\sqrt{5}} = \frac{2\varphi - 1}{\sqrt{5}} = \frac{\sqrt{5}}{\sqrt{5}} = 1 = F_1$$

Tapaus $n = 2$: (käytetään tietoa $\varphi^2 = \varphi + 1$ ja $(1-\varphi)^2 = 2 - \varphi$)

$$\frac{\varphi^2 - (1-\varphi)^2}{\sqrt{5}} = \frac{\varphi + 1 - (2-\varphi)}{\sqrt{5}} = \frac{2\varphi - 1}{\sqrt{5}} = 1 = F_2$$

Kultainen suhde ja Fibonaccin jono

Induktio-oletus:

$$F_k = \frac{\varphi^k - (1-\varphi)^k}{\sqrt{5}} \quad \text{kaikilla } k \leq n, \quad n \geq 3$$

Induktioväite:

$$F_{n+1} = \frac{\varphi^{n+1} - (1-\varphi)^{n+1}}{\sqrt{5}}$$

Todistetaan induktioväite:

$$F_{n+1} = F_n + F_{n-1} \overset{i.o.}{=} \frac{\varphi^n - (1-\varphi)^n}{\sqrt{5}} + \frac{\varphi^{n-1} - (1-\varphi)^{n-1}}{\sqrt{5}}$$

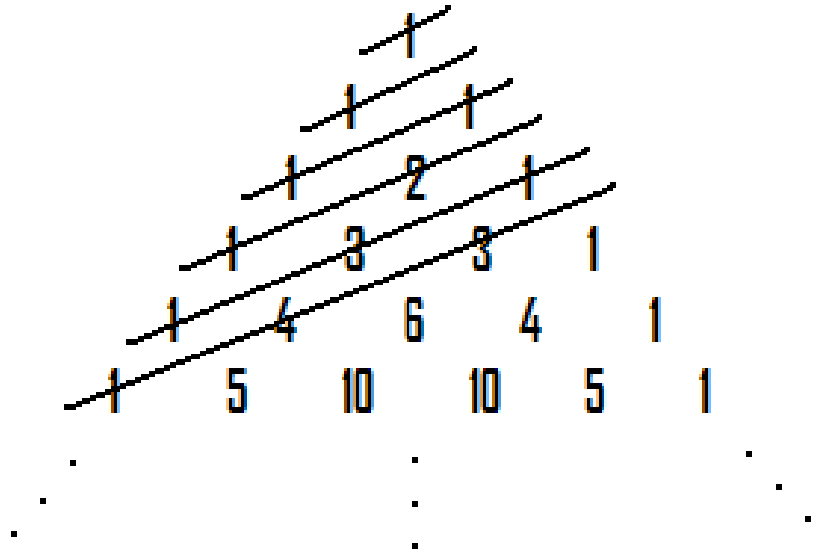
$$= \frac{1}{\sqrt{5}}\left(\varphi^{n-1}\cdot\varphi^2 - (1-\varphi)^{n-1}(2-\varphi)\right) \quad \text{(Muista: } \varphi+1 = \varphi^2 \text{ ja } 2-\varphi = (\varphi-1)^2\text{)}$$

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

Induktioväite on siis tosi. Induktioperiaatteen nojalla väite pätee kaikilla $n \geq 1$.

Fibonaccin lukujono ja Pascalin kolmio

Lasketaan yhteen Pascalin kolmion *diagonaaleilla* olevat luvut:



$$1$$
$$1$$
$$1+1=2$$
$$1+2=3$$
$$1+3+1=5$$
$$1+4+3=8$$

Oikealle näyttäisi muodostuvan Fibonaccin lukujono! Kuinka tästä muotoillaan väite? Muista, että $\binom{n}{k}$ on Pascalin kolmion $n+1$:nnen rivin $k+1$:s luku. Näyttää siltä, että n:s Fibonaccin luku F_n saadaan laskemalla yhteen n:nnen rivin ensimmäinen luku $\binom{n-1}{0}$, sitä edeltävän rivin toinen luku $\binom{n-2}{1}$, edelleen sitä edeltävän rivin kolmas luku $\binom{n-3}{2}$, jne. kunnes luvut loppuvat.

Fibonaccin lukujono ja Pascalin kolmio

Väitämme siis, että

$$F_n = \sum_{k \geq 0} \binom{n-k-1}{k} \quad \text{kaikilla} \quad n \geq 1.$$

Todistetaan tämä induktiolla.
Tapauksessa $n = 1$ on

$$\sum_{k \geq 0} \binom{n-k-1}{k} = \binom{0}{0} = 1 = F_1,$$

eli väite pätee kun $n = 1$.
Tehdään induktio-oletus: Jollakin $n \geq 1$ on voimassa

$$F_m = \sum_{k \geq 0} \binom{m-k-1}{k}, \quad \text{kun} \quad m \leq n.$$

Todistetaan, että tällöin on voimassa induktioväite:

$$F_{n+1} = \sum_{k \geq 0} \binom{n-k}{k}.$$

Fibonaccin lukujono ja Pascalin kolmio

Käyttämällä Fibonaccin lukujonon määritelmää ja induktio-oletusta saadaan

$$F_{n+1} = F_n + F_{n-1} = \sum_{k\geq 0} \binom{n-k-1}{k} + \sum_{k\geq 0} \binom{n-k-2}{k},$$

josta muuttamalla ensimmäisen termin summausindeksiä saadaan

$$= 1 + \sum_{k\geq 0} \binom{n-k-2}{k+1} + \sum_{k\geq 0} \binom{n-k-2}{k}.$$

Pascalin indentiteetin nojalla

$$= 1 + \sum_{k\geq 0} \binom{n-k-1}{k+1} = 1 + \sum_{k\geq 1} \binom{n-k}{k} = \sum_{k\geq 0} \binom{n-k}{k},$$

eli induktioväite on tosi. Induktioperiaatteen nojalla väite on tosi kaikilla $n \geq 1$.

Rekursiiviset määritelmät

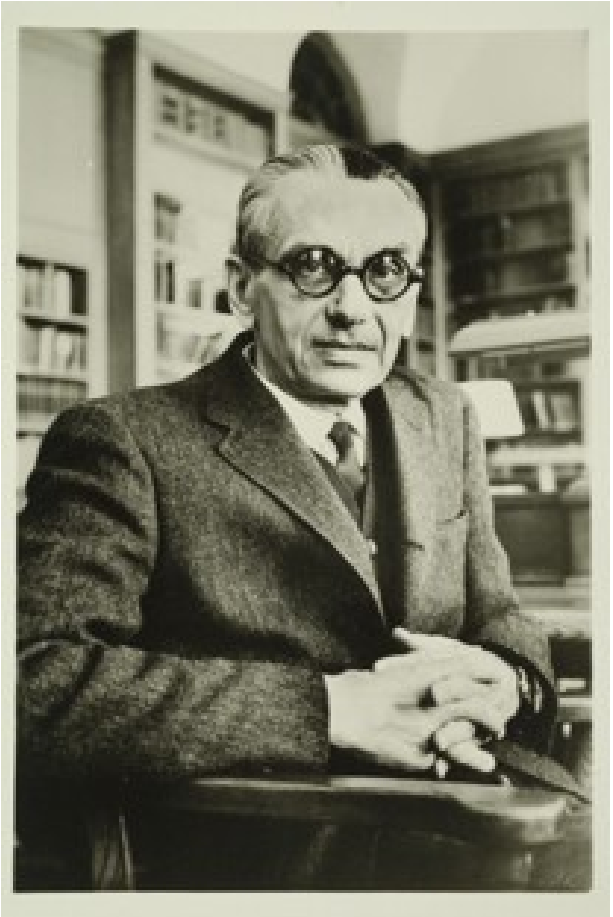
Useat tähän mennessä esillä olleistä käsitteistä voidaan määritellä rekursiivisesti:

- Aritmeettinen jono: a_1 annettu, $a_{k+1} = a_k + d$, $k \geq 1$
- Geometrinen jono: a_1 annettu, $a_{k+1} = ra_k$, $k \geq 1$
- Kertoma: $1! = 1$, $(n+1)! = n! \cdot (n+1)$, $n \geq 1$
- Binomikertoimet: $\binom{n}{0} = \binom{n}{n} = 1$, $n \geq 0$, $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$, $0 < k < n$

Logiikka

Logiikka

Tutustumme seuraavaksi propositio- eli lauselogiikkaan, jossa tarkastellaan formaalien lauseiden ominaisuuksia, ennenkaikkea niiden totuusarvoja. Formalisoimalla luonnollisen kielen lauseet propositiologiikan kielelle on helppo tarkastella monimutkaisiakin lauseita. Eräs merkittävimmistä loogikoista oli itävaltalais-amerikkalainen Kurt Gödel, joka tunnetaan parhaiten syvällisistä ja käänteentekevistä epätäydellisyyslauseistaan. Näihin tuloksiin voi tutustua matemaattisen logiikan syventävillä kursseilla.



Kurt Gödel (1906-1978)

Propositiosymbolit ja konnektiivit

Propositio eli lause koostuu jakamattomista väittämistä (propositiosymboleista) kuten $A =$ "sataa" ja $B =$ "tuulee" sekä niitä yhdistävistä **konnektiiveista** :

negaatio	$\neg A$	"ei A" ("ei sada")
konjunktio	$A \wedge B$	"A ja B" ("sataa ja tuulee")
disjunktio	$A \vee B$	"A tai B" ("sataa tai tuulee")
implikaatio	$A \rightarrow B$	"jos A, niin B" ("jos sataa, niin tuulee")
ekvivalenssi	$A \leftrightarrow B$	"A jos ja vain jos B" ("sataa jos ja vain jos tuulee")

Sulkeet ja sidontajärjestys

Konnektiivien välinen sidontajärjestys:

1. $\neg$ on vahvin
2. $\wedge$ ja $\vee$ ovat heikompia kuin $\neg$, mutta vahvempia kuin $\rightarrow$ ja $\leftrightarrow$
3. $\rightarrow$ ja $\leftrightarrow$ ovat heikoimmat

Konnektiiveista vahvin sitoo argumenttinsa ensin. (Vertaa laskutoimituksiin: $2 + 3 \cdot 5 = 2 + (3 \cdot 5)$.)
Esimerkiksi

- $\neg A \wedge B$ tarkoittaa samaa kuin $(\neg A) \wedge B$, ei $\neg(A \wedge B)$
- $A \wedge B \rightarrow B \vee C$ tarkoittaa samaa kuin $(A \wedge B) \rightarrow (B \vee C)$, ei $A \wedge (B \rightarrow B) \vee C$
- sulkeita ei voi poistaa lauseesta $(A \rightarrow B) \vee (B \leftrightarrow C)$ ilman, että merkitys muuttuu

Konjunktioiden ja disjunktioiden ketjutus

Ketjutettaessa konjunktioita tai disjunktioita voidaan sulkeet jättää pois:

- $(A \wedge B) \wedge C$ tarkoittaa samaa kuin $A \wedge (B \wedge C)$, joten voimme kirjoittaa kyseisen proposition ilman sulkeita $A \wedge B \wedge C$
- $(A \vee B) \vee C$ tarkoittaa samaa kuin $A \vee (B \vee C)$, joista kirjoitamme $A \vee B \vee C$

Sulkeita ei kuitenkaan voi jättää pois molempia $\wedge$ ja $\vee$ sisältävistä propositioista. $(A \wedge B) \vee C$ ei tarkoita samaa kuin $A \wedge (B \vee C)$.

Luonnollisen kielen lauseiden formalisointi

Luonnollisen kielen lauseen formalisointi etenee kahdessa vaiheessa:

- tunnistetaan "jakamattomat väittämät"
- tunnistetaan konnektiivit

Esim.

"On pilvistä ja ajan autoa."

$A \quad \wedge \quad B$

"Jos on pilvistä, ajan autoa."

$A \quad \rightarrow \quad B$

"En aja autoa, jos ei ole pilvistä."

$\neg A \quad \rightarrow \quad \neg B$

Totuusarvot

Propositiolla on **totuusarvo** 1 (tosi) tai 0 (epätosi).
Konnektiivien totuusarvotaulukko:

A	B	$\neg A$	$A \wedge B$	$A \vee B$	$A \rightarrow B$	$A \leftrightarrow B$
1	1	0	1	1	1	1
1	0	0	0	1	0	0
0	1	1	0	1	1	0
0	0	1	0	0	1	1

Esimerkki totuusarvoista

Millä propositioiden A ja B totuusarvoilla lause $\neg(A \vee \neg B)$ on tosi?

A	B	$\neg B$	$A \vee \neg B$	$\neg(A \vee \neg B)$
1	1	0	1	0
1	0	1	1	0
0	1	0	0	1
0	0	1	1	0

$\neg(A \vee \neg B)$ on siis tosi

täsmälleen silloin, kun A on epätosi ja B on tosi.

Toinen esimerkki totuusarvoista

Millä propositioiden A, B ja C totuusarvoilla lause $A \to B \wedge C$ on epätosi?

A	B	C	$B \wedge C$	$A \to B \wedge C$
1	1	1	1	1
1	1	0	0	0
1	0	1	0	0
1	0	0	0	0
0	1	1	1	1
0	1	0	0	1
0	0	1	0	1
0	0	0	0	1

$A \to B \wedge C$ on siis epätosi täsmälleen silloin, kun A ja B ovat tosia ja C epätosi , tai kun A ja C ovat tosia ja B on epätosi , tai kun A on tosi ja B ja C ovat epätosia.

Tehtävä totuusarvoista

Millä propositioiden A ja B totuusarvoilla lause $(A \leftrightarrow \neg B) \rightarrow A \wedge B$ on tosi?
Ratkaisu:
Kyseisen proposition totuustaulu on

A	B	$\neg B$	$A \leftrightarrow \neg B$	$A \wedge B$	$(A \leftrightarrow \neg B) \rightarrow A \wedge B$
1	1	0	0	1	1
1	0	1	1	0	0
0	1	0	1	0	0
0	0	1	0	0	1

Propositio $(A \leftrightarrow \neg B) \rightarrow A \wedge B$ on siis tosi täsmälleen silloin kun A:lla ja B:llä on sama totuusarvo.

Aarne, Boris ja Camilla

Tiedetään, että yksi kolmesta epäillystä (Aarne, Boris ja Camilla) on syyllinen rikokseen. Tiedetään lisäksi, että syyttömät puhuvat totta ja syylliset valehtelevat. Kuulusteluissa sanottua:

- Aarne: "Minä olen syyllinen tai Camilla on syyllinen."
- Boris: "Syyllinen en ole minä eikä Aarne."
- Camilla: "Aarne on syyllinen tai Boris on syyllinen."

Kuka on syyllinen?
Ratkaisu:
$A =$ "Aarne on syytön."
$B =$ "Boris on syytön."
$C =$ "Camilla on syytön."

Aarnen tunnustus: $\neg A \vee \neg C$

Boriksen tunnustus: $A \wedge B$

Camillan tunnustus: $\neg A \vee \neg B$

Aarne, Boris ja Camilla

Laaditaan totuustaulu. Kaikkia vaakarivejä ei tarvita, sillä täsmälleen yksi on syyllinen:

A	B	C	$\neg A$	$\neg B$	$\neg C$	$\neg A \vee \neg C$	$A \wedge B$	$\neg A \vee \neg B$
1	1	0	0	0	1	1	1	0
1	0	1	0	1	0	0	0	1
0	1	1	1	0	0	1	0	1

Syyllinen valehtelee ja syyttömät puhuvat totta. Etsitään siis vaakarivi, jolla A:lla on sama totuusarvo kuin Aarnen tunnustuksella , B:llä sama totuusarvo kuin Boriksen tunnustuksella ja C:llä sama totuusarvo kuin Camillan tunnustuksella. Ensimmäinen vaakarivi on sellainen, joten Camilla on syyllinen.

Arvoitus

There is an island upon which a tribe resides. The tribe consists of 1000 people, with various eye colours. Yet, their religion forbids them to know their own eye color, or even to discuss the topic; thus, each resident can (and does) see the eye colors of all other residents, but has no way of discovering his or her own (there are no reflective surfaces). If a tribesperson does discover his or her own eye color, then their religion compels them to commit ritual suicide at noon the following day in the village square for all to witness. All the tribespeople are highly logical and devout, and they all know that each other is also highly logical and devout (and they all know that they all know that each other is highly logical and devout, and so forth).
[For the purposes of this logic puzzle, "highly logical" means that any conclusion that can logically deduced from the information and observations available to an islander, will automatically be known to that islander.]
Of the 1000 islanders, it turns out that 100 of them have blue eyes and 900 of them have brown eyes, although the islanders are not initially aware of these statistics (each of them can of course only see 999 of the 1000 tribespeople).
One day, a blue-eyed foreigner visits to the island and wins the complete trust of the tribe.
One evening, he addresses the entire tribe to thank them for their hospitality.
However, not knowing the customs, the foreigner makes the mistake of mentioning eye color in his address, remarking "how unusual it is to see another blue-eyed person like myself in this region of the world".

What effect, if anything, does this faux pas have on the tribe?

Arvoituksen ratkaisu

Todistetaan hieman yleisempi väite:
Jos saarella asuvista n on sinisilmäisiä, niin n päivän kuluttua matkailijan ilmoituksesta he kaikki surmaavat itsensä.

- Jos $n = 1$, niin ainoa sinisilmäinen asukas ei näe yhtään sinisilmäistä ja ymmärtää siten matkailijan viittaavan itseensä.
- Jos $n = 2$, niin kumpikin sinisilmäinen asukas näkee yhden sinisilmäisen ja päättelee:
  "Jos silmäni ovat ruskeat, on saarella vain yksi sinisilmäinen. Tämä sinisilmäinen surmaa itsensä seuraavana päivänä pääteltyään silmiensä värin."
  Kumpikaan sinisilmäisistä ei kuitenkaan surmaa itseään seuraavana päivänä, joten kumpikin voi päätellä silmiensä olevan siniset.
- Jos $n = 3$, niin kukin sinisilmäinen asukas näkee kaksi sinisilmäistä ja päättelee:
  "Jos silmäni ovat ruskeat, on saarella kaksi sinisilmäistä. Nämä sinisilmäiset surmaavat itsensä kahden päivän kuluttua pääteltyään silmiensä värin."
  Kukaan sinisilmäisistä ei kuitenkaan surmaa itseään kahden päivän kuluttua, joten kaikki sinisilmäiset voivat päätellä silmiensä värin.

Arvoituksen ratkaisu

Väite voidaan todistaa yleisessä tapauksessa induktiolla:
Tapaus $n = 1$ katsottiin jo.
Oletetaan, että väite pätee kun sinisilmäisiä on $n - 1$ ja tarkastellaan tilannetta, jossa sinisilmäisiä on n.
Nyt jokainen sinisilmäinen näkee $n - 1$ sinisilmäistä ja päättelee:
"Jos silmäni ovat ruskeat, on saarella $n - 1$ sinisilmäistä. Nämä sinisilmäiset surmaavat itsensä $n - 1$ päivän kuluttua pääteltyään silmiensä värin."
Kukaan sinisilmäisistä ei kuitenkaan surmaa itseään $n - 1$ päivän kuluttua, joten kaikki sinisilmäiset voivat päätellä silmiensä värin.
Induktioväite on siis tosi ja induktioperiaatteen mukaan väite pätee kaikilla n, erityisesti tapauksessa $n = 100$.

Tautologia

Propositio on **tautologia**, jos sen totuusarvo on 1 kaikilla siinä esiintyvien propositiosymbolien totuusarvoilla. Tautologioita ovat esimerkiksi

- $A \vee \neg A$ (poissuljetun kolmannen laki)
- $\neg(A \wedge \neg A)$ (poissuljetun ristiriidan laki)
- $A \wedge (A \to B) \to B$ (modus ponens)
- $A \wedge (\neg B \to \neg A) \to B$ (kontrapositio)

Totea näistä valitsemasi propositio tautologiaksi.

Looginen ekvivalenssi

Propositiot A ja B ovat **loogisesti ekvivalentit**, merkitään $A \equiv B$, jos $A \leftrightarrow B$ on tautologia , ts. jos A ja B eivät eroa toisistaan totuusarvojen suhteen. Loogisia ekvivalensseja ovat esimerkiksi

- $\neg(\neg A) \equiv A$
- $A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C)$
- $A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C)$
- $\neg(A \vee B) \equiv \neg A \wedge \neg B$
- $\neg(A \wedge B) \equiv \neg A \vee \neg B$
- $A \rightarrow B \equiv \neg B \rightarrow \neg A$
- $A \rightarrow B \equiv \neg(A \wedge \neg B)$
- $A \leftrightarrow B \equiv (A \rightarrow B) \wedge (B \rightarrow A)$

Totea näistä valitsemasi looginen ekvivalenssi.

Konnektiivien keskinäinen määriteltävyys

Negaatio yhdessä minkä tahansa konnektiivin $\wedge$, $\vee$ tai $\rightarrow$ kanssa riittää määrittelemään muut. Sovelletaan edellä esitettyjä loogisia ekvivalensseja.

Negaatio ja konjunktio

$$A \vee B \equiv \neg(\neg(A \vee B)) \equiv \neg(\neg A \wedge \neg B)$$

$$A \rightarrow B \equiv \neg(A \wedge \neg B)$$

$$A \leftrightarrow B \equiv (A \rightarrow B) \wedge (B \rightarrow A) \equiv \neg(A \wedge \neg B) \wedge \neg(B \wedge \neg A)$$

Negaatio ja disjunktio

$$A \wedge B \equiv \neg(\neg(A \wedge B)) \equiv \neg(\neg A \vee \neg B)$$

$$A \rightarrow B \equiv \neg A \vee B$$

$$\begin{aligned} A \leftrightarrow B &\equiv (A \rightarrow B) \wedge (B \rightarrow A) \\ &\equiv (\neg A \vee B) \wedge (\neg B \vee A) \\ &\equiv \neg(\neg(\neg A \vee B) \vee \neg(\neg B \vee A)) \end{aligned}$$

Negaatio ja implikaatio

$$A \wedge B \equiv \neg(A \to \neg B)$$

$$A \vee B \equiv \neg A \to B$$

$$A \leftrightarrow B \equiv (A \to B) \wedge (B \to A) \equiv \neg((A \to B) \to \neg(B \to A))$$