Äärettömistä joukoista

Markku Halmetoja

Mistä tietäisit, että sinulla on yhtä paljon sormia ja varpaita, jos et osaisi laskea niitä? Tiettyä voimisteluliikettä tehdessäsi huomaisit, että jokaista sormea vastaa yksi varvas ja päin vastoin. Äärettömiä joukkoja lasketaan samalla periaatteella. Alkioiden lukumääriä ei varsinaisesti voi laskea, niitähän on ääretön määrä, mutta ääretöntä joukkoa voi verrata esimerkiksi positiivisten kokonaislukujen joukkoon $\mathbb{Z}_+ = \{1, 2, 3, \ldots\}$.

Parillisia positiivisia kokonaislukuja on ääretön määrä. Asettamalla ne vastaavuuteen $\mathbb{Z}_+$:n lukujen kanssa nähdään ilmiö, jota jo Galilei[1] ihmetteli: näitä lukuja näyttää olevan yhtä paljon kuin positiivisia kokonaislukuja on

$$\begin{array}{ccccc} 1 & 2 & 3 & 4 & \ldots \\ \updownarrow & \updownarrow & \updownarrow & \updownarrow & \ldots \\ 2 & 4 & 6 & 8 & \ldots \end{array}$$

kaikkiaan, mutta toisaalta niiden määrän luulisi olevan vain puolet kaikkien positiivisten kokonaislukujen määrästä. Kummallisuus selittyy sillä, että molemmissa joukoissa on ääretön määrä lukuja. Molemmat joukot ovat tavallaan yhtä äärettömiä.

Cantor[2] tutki ensimmäisenä systemaattisesti äärettömiä joukkoja, ja hän määritteli *joukon mahtavuuden* käsitteen:

> *Joukot A ja B ovat yhtä mahtavia, jos niiden alkiot voidaan asettaa vastaamaan pareittain toisiaan.*

Parittainen vastaavuus määritellään tämän kirjoituksen liitteessä täsmällisemmin eräitä ehtoja toteuttavana funktiona $f : A \to B$.

On selvää, että kaksi äärellistä joukkoa ovat yhtä mahtavia, jos ja vain jos niissä on sama määrä alkioita. Äärellisiä joukkoja ja joukkoja, joilla on sama mahtavuus kuin $\mathbb{Z}_+$:lla, sanotaan *numeroituviksi joukoiksi.* Äärettömät numeroituvat joukot ovat *numeroituvasti äärettömiä.* Joukkojen mahtavuuksia voidaan myös vertailla. Kahdesta äärellisestä joukosta mahtavampi on se,

[1] Galileo Galilei (1564 – 1642), italialainen fyysikko ja matematiikko.
[2] Georg Cantor (1845 – 1918), saksalainen matemaatikko.

jossa on enemmän alkioita. Äärettömien joukkojen vertailuun riittää aluksi se, että jos A sisältyy B:hen, niin A:n mahtavuus on enintään yhtäsuuri kuin B:n mahtavuus, ja jos nämä joukot eivät ole yhtä mahtavia, niin B on mahtavampi kuin A. Yleisempi määritelmä on liitteessä.

Kokonaisluvuista

On selvää, että numeroituvan joukon jokainen osajoukko on numeroituva, mutta miten ääretön joukko A osoitetaan numeroituvaksi? Monissa tapauksissa on yksinkertaisinta osoittaa, että joukon alkioista voidaan muodostaa luettelo, josta koko joukko voidaan periaatteessa luetella yksi alkio kerrallaan. Tällöin joukon jokaiseen alkioon voidaan liittää järjestysluku joukosta $\mathbb{Z}_+$, mikä määrittelee parittaisen vastaavuuden. Esimerkiksi kokonaisluvut voidaan luetella jonona $0,\ 1,\ -1,\ 2,\ -2,\ 3,\ -3,\ 4,\ \ldots$, joten $\mathbb{Z}$ on numeroituva. Parittaisen vastaavuuden määrittävä funktio on liitteessä.

Alkuluvuista

Alkuluvut ovat ykköstä suurempia kokonaislukuja, joiden ainoat positiiviset tekijät ovat 1 ja luku itse. Esimerkiksi 2, 3 ja 5 ovat alkulukuja, mutta 10 on *yhdistetty luku*, sillä se on lukujen 2 ja 5 tulo. Lukiossa todistetaan *aritmetiikan peruslause*, jonka mukaan jokainen ykköstä suurempi kokonaisluku voidaan tekijöiden järjestystä vaille yksikäsitteisesti kirjoittaa alkulukujen tuloksi. Tällöin alkuluvut tulkitaan yksitekijäisiksi tuloiksi. Luvun 10 alkutekijät ovat 2 ja 5, eikä sitä siis voida kirjoittaa tuloksi, jonka tekijänä on esimerkiksi 3.

Merkitään $\mathbb{P}$:llä alkulukujen joukkoa. Kukaan ei toistaiseksi ole keksinyt mitään yksinkertaista funktiota $f : \mathbb{Z}_+ \to \mathbb{P}$, joka osoittaisi $\mathbb{P}$:n äärettömäksi. Silti $\mathbb{P}$ *on* ääretön. Eukleides[1] todisti tämän jo 2300 vuotta sitten. Hänen ajatuskulkuaan pidetään yleisesti yhtenä matematiikan historian kauneimmista:

> Olkoot $p_1, p_2, \ldots\ p_n$ äärellinen joukko alkulukuja. Tällöin luku
>
> $$m = 1 + p_1 p_2 \ldots\ p_n$$
>
> ei ole jaollinen yhdelläkään niistä, sillä jokaisesta jakolaskusta $m : p_\imath$ jää jakojäännökseksi ykkönen. Koska m kuitenkin voidaan esittää alkulukujen tulona, on olemassa muitakin alkulukuja kuin nuo mainitut. Siis mikään äärellinen alkulukujoukko ei sisällä kaikkia alkulukuja.

[1] Eukleides (325 – 265 eaa.), kreikkalainen matemaatikko.

Rationaaliluvuista

Rationaalilukujen peruslaskutoimitukset antavat tulokseksi aina rationaaliluvun, eli rationaalilukujen joukko $\mathbb{Q}$ on suljettu näiden toimitusten suhteen. Jos valitaan mielivaltaisesti kaksi rationaalilukua, niin niiden keskiarvo on myös rationaaliluku, ja se sijaitsee valittujen lukujen välissä. Täten kahden mielivaltaisesti valitun rationaaliluvun välissä on ääretön määrä rationaalilukuja. Siksi on varsin yllättävää, että rationaalilukujen joukko $\mathbb{Q}$ on kuitenkin ”vain” numeroituvasti ääretön. Tämän väitteen todistamiseksi osoitetaan aluksi, että positiivisista rationaaliluvuista voidaan muodostaa luettelo. Todistus perustuu kaavioon

$$
\begin{array}{ccccccccccccc}
1/1 & \rightarrow & 2/1 & & 3/1 & \rightarrow & 4/1 & & 5/1 & \rightarrow & 6/1 & & \ldots \\
 & \swarrow & & \nearrow & & \swarrow & & \nearrow & & \swarrow & & & \\
1/2 & & 2/2 & & 3/2 & & 4/2 & & 5/2 & & 6/2 & & \ldots \\
\downarrow & \nearrow & & \swarrow & & \nearrow & & \swarrow & & & & & \\
1/3 & & 2/3 & & 3/3 & & 4/3 & & 5/3 & & 6/3 & & \ldots \\
 & \swarrow & & \nearrow & & \swarrow & & & & & & & \\
1/4 & & 2/4 & & 3/4 & & 4/4 & & 5/4 & & 6/4 & & \ldots \\
\downarrow & \nearrow & & \swarrow & & & & & & & & & \\
1/5 & & 2/5 & & 3/5 & & 4/5 & & 5/5 & & 6/5 & & \ldots \\
 & \swarrow & & & & & & & & & & & \\
1/6 & & 2/6 & & 3/6 & & 4/6 & & 5/6 & & 6/6 & & \ldots \\
\vdots & & \vdots & & \vdots & & \vdots & & \vdots & & \vdots & & \ddots
\end{array}
$$

josta nuolia seuraamalla saadaan jono

$$1,\ 2,\ \tfrac{1}{2},\ \tfrac{1}{3},\ \tfrac{2}{2},\ 3,\ 4,\ \tfrac{3}{2},\ \ldots\ .$$

Jokainen positiivinen rationaaliluku esiintyy siinä äärettömän monta kertaa. Jättämällä alusta lähtien pois jokainen jo esiintynyt luku saadaan uusi jono

$$1,\ 2,\ \tfrac{1}{2},\ \tfrac{1}{3},\ 3,\ 4,\ \tfrac{3}{2},\ \tfrac{2}{3},\ \tfrac{1}{4},\ \tfrac{1}{5},\ 5,\ \ldots\ ,$$

jossa jokainen positiivinen rationaaliluku esiintyy vain kerran. Siis luettelo

$$0,\ 1,\ -1,\ 2,\ -2,\ \tfrac{1}{2},\ -\tfrac{1}{2},\ \tfrac{1}{3},\ -\tfrac{1}{3},\ 3,\ -3\ \ldots$$

sisältää jokaisen rationaaliluvun. Artikkelissa [3] ja teoksessa [4] esitetään muitakin menetelmiä positiivisten rationaalilukujen luetteloimiseksi.

Rationaaliluvut sijaitsevat lukusuoralla ”tiheästi”, mutta silti ne voidaan peittää janoilla, joiden yhteenlaskettu pituus on pienempi kuin minkä tahansa ennalta valitun janan pituus. Tämä hämmästyttävä tulos todistetaan liitteessä.

Reaaliluvuista

Reaalilukujen joukko

$$\mathbb{R} = \{\text{rationaaliluvut}\,, \text{irrationaaliluvut}\}.$$

Reaaliluvut voidaan esittää päättymättöminä desimaalilukuina. Tällöin sovitaan, että äärettömän moneen yhdeksikköön päättyvä luku esitetään kuten $2{,}3999\ldots = 2{,}4000\ldots$. Tässä ei tehdä mitään virhettä, sillä jos $x = 2{,}3999\ldots$, niin $100x = 239{,}999\ldots$ ja $10x = 23{,}999\ldots$, josta vähentämällä $90x = 216$. Siis $x = \frac{216}{90} = 2{,}4000\ldots$.

Jokaista reaalilukua vastaa lukusuoran piste, ja kääntäen jokaista lukusuoran pistettä vastaa reaaliluku. Luvut ja lukusuoran pisteet voidaan siis samastaa. Ehdon $a < x < b$ toteuttavien lukujen x joukko on *avoin väli* a:sta b:hen, ja se merkitään $]a,b[$. *Suljettu väli* $[a,b]$ sisältää ehdon $a \leq x \leq b$ toteuttavat luvut.

Olkoot $a, b \in \mathbb{R}$ ja $a < b$. Liitteessä todistetaan, että välin $]a\,,b[$ ja lukusuoran luvut voidaan asettaa pareittain vastaavuuteen. Reaalilukujen joukko $\mathbb{R}$ on siis yhtä mahtava jokaisen avoimen välin kanssa. Toisin sanoen, suoran ja janan pisteiden joukot ovat yhtä mahtavia.

Rationaalilukuja on siis numeroituva määrä, ja edellisen mukaan ne ”menevät varsin pieneen tilaan” lukusuoralla. Koska reaaliluvut kuitenkin täyttävät koko lukusuoran, voidaan ajatella, että reaalilukuja on enemmän kuin numeroituva määrä. Liitteessä todistetaankin, että näillä joukoilla todella on eri mahtavuus, jolloin, koska $\mathbb{Q}$ sisältyy $\mathbb{R}$:ään, $\mathbb{R}$:n mahtavuus on suurempi kuin $\mathbb{Q}$:n mahtavuus. Reaalilukuja sanotaan olevan *ylinumeroituva* määrä. Reaalilukujen joukko edustaa täten rationaalilukujen joukkoa suurempaa äärettömyyttä.

Suuremmista äärettömyyksistä

Cantor osoitti, että on olemassa numeroituvasti ääretön määrä toinen toistaan mahtavampia äärettömiä joukkoja. Tämän väitteen selvittämiseen tarvitaan hieman apukäsitteitä.

Olkoon A mikä tahansa joukko. Jos kaikki B:n alkiot ovat myös A:n alkioita, niin B on A:n osajoukko, mikä merkitään $B \subseteq A$. Joukko on aina itsensä osajoukko. Tyhjässä joukossa $\emptyset$ ei ole yhtään alkiota, ja se on jokaisen joukon osajoukko. Jos A:n alkiot ovat a ja b, siis $A = \{a, b\}$, niin A:n kaikki osajoukot ovat $\emptyset$, $\{a\}$, $\{b\}$ ja A. Joukon A osajoukkojen muodostama joukko on A:n *potenssijoukko* $\mathcal{P}\,(A)$. Siis

$$\mathcal{P}\,(A) = \Big\{\emptyset,\ \{a\},\ \{b\},\ A\Big\}.$$

Tyhjän joukon potenssijoukossa on vain tyhjä joukko. Yksialkioisen joukon potenssijoukossa on kaksi alkiota, nimittäin tyhjä joukko ja joukko itse. Kaksialkioisen joukon potenssijoukossa on $4 = 2^2$ alkiota. Jos mihin tahansa äärelliseen joukkoon lisätään yksi alkio, niin osajoukkojen määrä kaksinkertaistuu, sillä uuden joukon osajoukkoja ovat kaikki vanhan joukon osajoukot sekä nämä vanhat osajoukot, joihin on liitetty alkuperäiseen joukkoon liitetty alkio. Täten n-alkioisen joukon X_n potenssijoukossa on 2^n alkiota. Koska $n < 2^n$ kaikilla $n = 0, 1, 2, 3, \dots$, on potenssijoukon $\mathcal{P}(X_n)$ mahtavuus suurempi kuin X_n:n mahtavuus. Cantor päätteli, että äärettömille joukoille tilanne on samanlainen. Liitteessä on eräs versio hänen todistuksestaan.

Siis esimerkiksi $\mathcal{P}(\mathbb{R})$ on joukkoa $\mathbb{R}$ mahtavampi, $\mathcal{P}(\mathcal{P}(\mathbb{R}))$ on mahtavampi kuin $\mathcal{P}(\mathbb{R})$, $\mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbb{R})))$ on mahtavampi kuin $\mathcal{P}(\mathcal{P}(\mathbb{R}))$, jne.... Näin saadaan numeroituvasti ääretön määrä toinen toistaan mahtavampia joukkoja. Hilbert[1] piti Cantorin elämäntyötä yhtenä ihmisen älyllisen toiminnan kauneimmista saavutuksista. Cantor valitettavasti sai arvostusta osakseen liian myöhään, ja hän kuoli mielisairaalassa. Hänen työstään ja elämästään kerrotaan teoksissa [1], [2] ja nettiosoitteessa [5].

Kontinuumihypoteesista

Cantor esitti hypoteesin, jonka mukaan ei ole olemassa joukkoa, jonka mahtavuus olisi suurempi kuin kokonaislukujen joukon, mutta pienempi kuin reaalilukujen joukon. Gödel[2] ja Cohen[3] ovat osoittaneet, että tätä hypoteesia ei voi todistaa oikeaksi eikä vääräksi matematiikassa yleisesti hyväksytyn joukko-opin puitteissa. Tähän erittäin syvälliseen ongelmaan voi kunnolla perehtyä ainoastaan erikoistumalla yliopisto-opinnoissa matemaattiseen logiikkaan.

Sormista ja varpaista

Palataan alussa esitettyyn ongelmaan. Olkoon S sormien ja V varpaiden joukko sellaisella henkilöllä, jolla mainitut ruumiinosat ovat tallella. Näiden joukkojen välistä vastaavuutta esittäviä funktioita $f : S \to V$ ilmeisesti on olemassa, ja ne lienee mukavinta esittää taulukkoina, joissa kerrotaan, mikä varvas vastaa mitäkin sormea. Tänne asti jaksaneella lukijalla ei liene vaikeuksia ymmärtää, miksi niitä on 3628800 kappaletta!

[1] David Hilbert (1862 – 1943), saksalainen matemaatikko.

[2] Kurt Gödel (1906 – 1987), itävaltalais-yhdysvaltalainen loogikko ja matemaatikko.

[3] Paul Cohen (1934 – 2007), yhdysvaltalainen matemaatikko.

Liite

Funktioista

Olkoot A ja B ei-tyhjiä joukkoja ja $f : A \to B$ funktio. Funktion määritelmän mukaan f saa jokaisella A:n alkiolla x yksikäsitteisesti määrätyn arvon $y = f(x)$ joukossa B. Joukko A on funktion *määrittelyjoukko* ja B on sen *maalijoukko*. Jos $y = f(x)$, niin sanotaan myös, että y on x:n *kuva* ja x on y:n *alkukuva*, ja että x *kuvautuu* y:lle.

Funktion määritelmän mukaan kaikilla maalijoukon alkioilla $y \in B$ ei tarvitse olla alkukuvaa joukossa A, ja joillakin maalijoukon alkioilla saattaa olla useita alkukuvia. Jos kuitenkin jokaisella $y \in B$ on yksikäsitteisesti määrätty alkukuva $x \in A$, niin funktiota sanotaan *bijektioksi.* Jokaisella bijektiolla $f : A \to B$ on *käänteisfunktio* $g : B \to A$, joka on myös bijektio. Luonnollisesti f on tällöin g:n käänteisfunktio. Funktion f käänteisfunktio, jos se on olemassa, löytyy ehtoa

$$''\, y = f(x) \quad \textit{jos ja vain jos} \quad x = g(y)\,''$$

soveltamalla. Myös yhtälöt $g\left(f(x)\right) = x$ ja $f\left(g(y)\right) = y$ ovat tällöin voimassa kaikilla $x \in A$ ja $y \in B$.

Ainoastaan bijektiot $f : A \to B$ kelpaavat A:n ja B:n alkioiden lukumäärien vertailuun. Kirjoituksen alussa määriteltiin, milloin kaksi joukkoa ovat yhtä mahtavia. Määritelmä voidaan nyt täsmentää muotoon:

> *Joukot A ja B ovat yhtä mahtavia, jos on olemassa bijektio $f : A \to B$.*

Myös äärettömien joukkojen mahtavuuksien vertailua voidaan täsmentää:

> *Jos A ja B ovat äärettömiä joukkoja, ja jos A on yhtä mahtava B:n erään osajoukon kanssa, niin A on enintään yhtä mahtava kuin B. Jos lisäksi A:lla ja B:llä on eri mahtavuus, niin B on mahtavampi kuin A.*

Teoksessa [4] on syvällisempää tietoa funktioista, bijektioista ja joukkojen mahtavuuksien vertailusta.

Tutkitaan Galilein ihmettelemää esimerkkiä hieman täsmällisemmin. Olkoon $2\mathbb{Z}_+$ parillisten, siis kahdella jaollisten, positiivisten kokonaislukujen joukko. Funktio $f : \mathbb{Z}_+ \to 2\mathbb{Z}_+,\ y = f(x) = 2x$ on bijektio, koska

1° jos y on $2\mathbb{Z}_+$:n luku, niin se on kahdella jaollinen, ja on siis olemassa positiivinen k niin, että $y = 2k$. Luku $k \in \mathbb{Z}_+$ on y:n alkukuva, sillä $f(k) = 2k = y$. Siis, jokaisella $y \in 2\mathbb{Z}_+$ on alkukuva joukossa $\mathbb{Z}_+$.

2° millään $y \in 2\mathbb{Z}_+$ ei ole kahta eri alkukuvaa $\mathbb{Z}_+$:ssa, sillä jos $f(x_1) = y$ ja $f(x_2) = y$, niin $f(x_1) = f(x_2)$ eli $2x_1 = 2x_2$, mistä seuraa $x_1 = x_2$. Jokaisen y:n alkukuva on siis yksikäsitteisesti määrätty.

Tämän funktion käänteisfunktio on $g : 2\mathbb{Z}_+ \to \mathbb{Z}_+,\ x = g(y) = \frac{1}{2}y$.

Kokonaisluvuista

Kokonaislukujen joukko $\mathbb{Z}$ on numeroituva, sillä funktio

$$f : \mathbb{Z}_+ \to \mathbb{Z}, \quad f(x) = \begin{cases} \frac{1}{2}(x+1) & \text{kun } x = 1, 3, 5, \ldots \\ \\ \frac{1}{2}(2-x) & \text{kun } x = 2, 4, 6, \ldots \end{cases}$$

on bijektio. Väitteen todistamiseksi osoitetaan, että jokaisella kokonaisluvulla on yksikäsitteisesti määrätty alkukuva joukossa $\mathbb{Z}_+$, ts. osoitetaan, että yhtälöllä $f(x) = m$ on kaikilla $m \in \mathbb{Z}$ yksikäsitteisesti määrätty positiivinen kokonaislukuratkaisu. Jos $m \geq 1$, niin yhtälöllä

$$f(x) \;=\; \tfrac{1}{2}(x+1) \;=\; m$$

on yksikäsitteinen ratkaisu $x = 2m - 1 \in \mathbb{Z}_+$. Jos $m \leq 0$, niin yhtälöllä

$$f(x) \;=\; \tfrac{1}{2}(2-x) \;=\; m$$

on yksikäsitteinen ratkaisu $x = 2 - 2m \in \mathbb{Z}_+$. Siis f on bijektio.

Luonnollisesti bijektioita $f : \mathbb{Z}_+ \to \mathbb{Z}$ on äärettömän monta, eli kokonaisluvut voidaan äärettömän monella eri tavalla luetella jonossa. Myös luonnollisten lukujen joukko $\mathbb{N} = \{0, 1, 2, \ldots\}$ on yhtä mahtava kuin $\mathbb{Z}_+$, sillä

$$f : \mathbb{Z}_+ \to \mathbb{N}, \quad f(x) \;=\; x \;-\; 1$$

on bijektio.

Rationaaliluvuista

Todistetaan, että rationaaliluvut voidaan lukusuoralla peittää janoilla, joiden yhteenlaskettu pituus on pienempi kuin mikä tahansa ennalta valittu positiivinen luku ε. Todistus perustuu lukiossa opittavaan geometriseen sarjaan

$$1 \;+\; \tfrac{1}{2} \;+\; (\tfrac{1}{2})^2 \;+\; (\tfrac{1}{2})^3 \;+\; (\tfrac{1}{2})^4 \;+\; \ldots \;=\; 2.$$

Jättämällä siitä kaksi ensimmäistä termiä pois saadaan

$$(\tfrac{1}{2})^2 \;+\; (\tfrac{1}{2})^3 \;+\; (\tfrac{1}{2})^4 \;+\; \ldots \;=\; \tfrac{1}{2},$$

ja edelleen, jos ε on positiivinen luku, niin

$$(\tfrac{1}{2})^2\,\varepsilon + (\tfrac{1}{2})^3\,\varepsilon + (\tfrac{1}{2})^4\,\varepsilon + \ldots = \tfrac{1}{2}\,\varepsilon.$$

Koska rationaaliluvut voidaan luetella jonossa, voidaan $(\frac{1}{2})^2\varepsilon$-pituinen jana sijoittaa lukusuoralle niin, että jonon ensimmäinen rationaaliluku on janan keskipisteessä. Jonossa toisena olevan luvun päälle voidaan samalla tavalla asettaa jana, jonka pituus on $(\frac{1}{2})^3\varepsilon$. Kun näin jatketaan loputtomiin, tulevat kaikki rationaaliluvut peitetyiksi janoilla, joiden yhteenlaskettu pituus on

$$(\tfrac{1}{2})^2\,\varepsilon + (\tfrac{1}{2})^3\,\varepsilon + (\tfrac{1}{2})^4\,\varepsilon + \ldots = \tfrac{1}{2}\,\varepsilon < \varepsilon.$$

Yksi tämän tuloksen seuraus on, että lukusuoralla ei ole väliä $]a\,,b[$, jonka kaikki luvut olisivat rationaalisia, sillä rationaaliluvuthan voidaan peittää janoilla, joiden yhteenlaskettu pituus on pienempi kuin esimerkiksi $\frac{1}{2}(b-a)$. Lukusuoran jokaisella avoimella välillä on siis irrationaalulukuja. Jokaisella avoimella välillä on myös rationaalilukuja, sillä irrationaaliluvulle saadaan mielivaltaisen tarkka ala- ja ylälikiarvo korvaamalla sen jaksoton desimaalijono tietystä kohdasta alkaen nollilla ja yhdeksiköillä. Yliopistomatematiikassa todistetaan täsmällisemmin, että jokaisella avoimella välillä on äärettömän monta rationaali- ja irrationaalilukua.

Reaaliluvuista

Olkoot a ja b reaalilukuja, ja $a < b$. Funktio

$$f:]a\,,b[\to \mathbb{R}, \quad f(x) = (a-x)^{-1} - (x-b)^{-1}$$

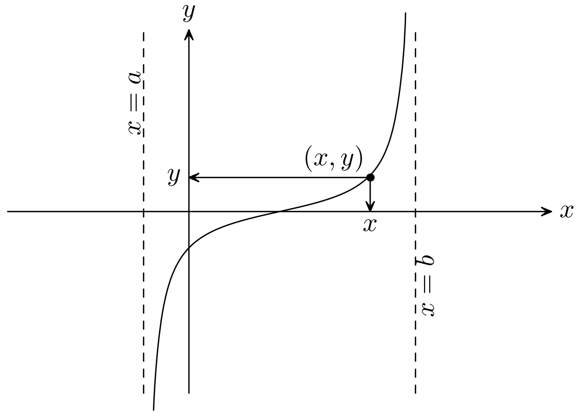
on derivoituva välillä $]a\,,b[$. Se on bijektio, sillä

1° sen derivaatta $f'(x) = (a-x)^{-2} + (x-b)^{-2}$ on positiivinen kaikilla $x \in]a\,,b[$, joten f on aidosti kasvava. Jokaisella $y \in \mathbb{R}$ on siis enintään yksi alkukuva välillä $]a\,,b[$.

2° funktio saa kaikki reaaliarvot, koska se on jatkuva, $f(x) \to -\infty$, kun $x \to a+$ ja $f(x) \to \infty$, kun $x \to b-$. Jokaisella $y \in \mathbb{R}$ on siis vähintään yksi alkukuva välillä $]a,b[$.

Kohtien 1° ja 2° perusteella jokaisella $y \in \mathbb{R}$ on täsmälleen yksi alkukuva välillä $]a\,,b[$. Reaalilukujen joukko $\mathbb{R}$ on siis yhtä mahtava jokaisen avoimen välin kanssa.

Funktion kuvaajalla on pystysuorat asymptootit $x = a$ ja $x = b$. Kun muuttuja x kulkee yli välin $]a\,,b[$ vasemmalta oikealle, kulkee kuvapiste y-akselilla $-\infty$:stä ∞:ään palaamatta kertaakaan alaspäin.



Seuraavassa on eräs versio *Cantorin diagonaalimenetelmästä*, jolla hän todisti $\mathbb{R}$:n ylinumeroituvaksi.

> Koska $\mathbb{R}$ ja $]0\,,1[$ ovat yhtä mahtavia, riittää todistaa väite mainitun välin luvuille. Tehdään vastaoletus, jonka mukaan nollan ja ykkösen välissä olevia reaalilukuja on numeroituva määrä. Tällöin niiden desimaaliesitykset voidaan esittää luettelona
>
> $$\begin{array}{rcl} r_1 & = & 0, a_{11}\, a_{12}\, a_{13}\, a_{14}\, \ldots \\ r_2 & = & 0, a_{21}\, a_{22}\, a_{23}\, a_{24}\, \ldots \\ r_3 & = & 0, a_{31}\, a_{32}\, a_{33}\, a_{34}\, \ldots \\ r_4 & = & 0, a_{41}\, a_{42}\, a_{43}\, a_{44}\, \ldots \\ r_5 & = & \ldots \end{array}$$
>
> Määritellään luku $t = 0, t_1\, t_2\, t_3\, t_4\, \ldots$ niin, että
>
> $$\text{jos } a_{\imath\imath} \neq 2, \text{ niin } t_\imath = 2 \text{ ja jos } a_{\imath\imath} = 2, \text{ niin } t_\imath = 3$$
>
> kaikilla $\imath \in \mathbb{Z}_+$. Tällöin t ei ole mikään luvuista $r_\imath$, mikä on ristiriidassa sen kanssa, että luettelossa on *kaikki* nollan ja ykkösen välissä olevat reaaliluvut. Ristiriita osoittaa, että reaalilukuja ei voi luetella. Joukko $\mathbb{R}$ ei siis ole numeroituva, ja koska se sisältää numeroituvan joukon $\mathbb{Q}$, on $\mathbb{R}$:n mahtavuus suurempi kuin $\mathbb{Q}$:n mahtavuus.

Suuremmista äärettömyyksistä

Edellä todettiin, että n-alkioisen joukon X_n mahtavuus on pienempi kuin potenssijoukon $\mathcal{P}(X_n)$ mahtavuus, eli bijektiota $f : X_n \to \mathcal{P}(X_n)$, joka merkitsisi kaikki X_n:n osajoukot X_n:n alkioilla, ei ole olemassa. Cantor oivalsi, että tämä asia on joukon alkioiden lukumäärästä riippumaton, eli jos X on mikä tahansa joukko, niin $\mathcal{P}(X)$ on sitä mahtavampi. Seuraavassa on havainnollinen versio Cantorin todistuksesta:

> Olkoon $X\,(\neq \emptyset)$ joukko. Tehdään vastaoletus, jonka mukaan on olemassa bijektio $f : X \to \mathcal{P}(X)$. Tällöin jokaista $\imath \in X$:n vastaa yksikäsitteisesti määrätty X:n osajoukko $A_\imath$, ja kääntäen, jos valitaan mikä tahansa X:n osajoukko, niin on olemassa yksikäsitteisesti määrätty *merkkialkio* $\jmath \in X$ niin, että valittu osajoukko on $A_\jmath$. Olkoon $\imath_0$ joukon X ja $\jmath_0$ tyhjän joukon merkkialkio. Osalle X:n osajoukoista on voimassa $\imath \in A_\imath$ ja osalle taas $\jmath \notin A_\jmath$. Jos $\imath \in A_\imath$, niin ajatellaan merkkialkio $\imath$ vihreäksi, ja päinvastaisessa tapauksessa punaiseksi. Kaikki X:n alkiot siis jakautuvat vihreiden joukkoon V ja punaisten joukkoon P. Nämä joukot eivät ole tyhjiä, sillä ainakin $\imath_0 \in V$ ja $\jmath_0 \in P$. Minkä värinen on joukon P merkkialkio? Jos tämä alkio on punainen, niin sen pitäisi olla joukossa V ja siis vihreä, mikä on mahdottomuus. Jos P:n merkkialkio on vihreä, niin silloin tämä merkkialkio on joukossa P ja on väriltään punainen, mikä niin'ikään on mahdottomuus. Ristiriita osoittaa vastaoletuksen epätodeksi, joten potenssijoukolla $\mathcal{P}(X)$ ja X:llä on eri mahtavuus. Koska X selvästi on yhtä mahtava X:n yksialkioisista osajoukoista muodostuvan $\mathcal{P}(X)$:n osajoukon kanssa, on $\mathcal{P}(X)$:n mahtavuus suurempi kuin X:n mahtavuus.

Kiitän dosentti Jorma Merikoskea tätä kirjoitusta oleellisesti parantaneista ja täsmentäneistä kommenteista.

Lähdeluettelo

[1] E.T. Bell, *Matematiikan miehiä*, WSOY, 1963.

[2] Miguel de Guzmán, *Matemaattisia seikkailuja*, Finn Lectura, 1990.

[3] Markku Halmetoja, *Calkinin-Wilfin jono*, Solmu 3/2005.

[4] Jorma Merikoski, Ari Virtanen, Pertti Koivisto, *Johdatus diskreettiin matematiikkaan*, WSOY, 2004.

[5] `http://www-groups.dcs.st-and.ac.uk/~history/`