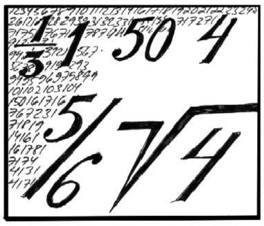

Joukkojen mahtavuudesta

Ari Koistinen
Helsingin ammattikorkeakoulu Stadia

Kaikki lienevät yhtä mieltä siitä, että joukko $\{1, 2, 3\}$ on suurempi tai *mahtavampi* kuin joukko $\{1, 2\}$. Samoin on ilmeistä, että ääretön joukko on aina mahtavampi kuin äärellinen joukko. Sen sijaan, kun kysytään, kummassa on enemmän alkioita, reaalilukujen vai luonnollisten lukujen joukossa, saattavat mielipiteet jakautua. Joku ehkä sanoo, että joukot ovat yhtä mahtavat, koska molemmissa on äärettömän monta lukua. Toisaalta voidaan väittää reaalilukujen joukon olevan selvästi suurempi, sillä pitäähän se sisällään koko luonnollisten lukujen joukon. On todettu, että kumpikaan näistä kriteereistä ei sovellu hyvin tämän ongelman tarkasteluun.

Jos joukko on äärellinen, sen mahtavuudeksi määritellään yksinkertaisesti sen alkioiden lukumäärä. Äärettömien joukkojen kohdalla asia ei ole näin yksinkertainen, mutta perustellusti voidaan sanoa, että on olemassa eri kokoisia äärettömyyksiä. Tähän liittyvä matemaattinen teoria on verrattain nuorta, vaikka ääretön käsitteenä on tunnettu jossain muodossa tuhansia vuosia. Runsaat sata vuotta sitten Georg Cantor (1845–1918) julkaisi käänteentekeviä ajatuksiaan äärettömistä joukoista. Monet sen ajan johtavat matemaatikot vastustivat voimakkaasti Cantorin teorioita, mutta nykyisin Cantorilla on kiistaton asema yhtenä historian merkittävimmistä matemaatikoista.

Ennen kuin esitämme tarkempia määritelmiä äärettömien joukkojen mahtavuuksille, kertaamme tärkeän bijektiivisyyden käsitteen:

Funktio $f : A \to B$ on *surjektio*, jos funktion arvojoukko on koko B, ts. jos jokaista joukon B alkiota y vastaa jokin joukon A alkio x siten, että $f(x) = y$. Funktio f on *injektio*, jos se ei saa samaa arvoa kahdessa eri pisteessä, ts. jos ehdosta $f(x) = f(y)$ seuraa $x = y$. Jos f on sekä surjektio että injektio, niin se on *bijektio*.

Käsitettä tarvitaan seuraavassa määritelmässä:

Joukot A ja B ovat *yhtä mahtavat*, jos on olemassa bijektio joukosta A joukkoon B.

Yhtä mahtavien joukkojen A ja B välille voidaan siis aina konstruoida yksi yhteen -vastaavuus. Määritelmä on sopusoinnussa arkijärjen mukaisen äärellisten joukkojen yhtämahtavuuden käsitteen kanssa: kahden yhtä monta alkiota sisältävän joukon

$$A = \{x_1, x_2, \ldots, x_n\} \text{ ja } B = \{y_1, y_2, \ldots, y_n\}$$

välille voidaan määritellä esimerkiksi bijektio

$$f : A \to B; f(x_i) = y_i$$

kaikilla kokonaisluvuilla $1 \le i \le n$. Jos jommassa kummassa joukossa on yksi alkio enemmän, ei bijektiota enää voida konstruoida, vaan joko maalijoukkoon jää ”ylimääräinen” alkio, jolloin f ei ole surjektio, tai sitten määrittelyjoukon kaksi alkiota joudutaan kuvaamaan samaksi alkioksi, jolloin f ei ole injektio.

Sanotaankin, että joukko B on *mahtavampi* kuin A, jos on olemassa (ainakin yksi) injektio $f : A \to B$, mutta ei yhtään surjektiota.

Voimme nyt todeta, että esimerkiksi parillisten lukujen joukon - merkitään sitä vaikkapa P:llä - ja kaikkien luonnollisten lukujen joukon $\mathbb{N}$ mahtavuuksilla ei ole asettamamme määritelmän mukaan eroa, sillä funktio

$$f : \mathbb{N} \to P; f(x) = 2x$$

kuvaa luonnolliset luvut bijektiivisesti parillisille luvuille. Parillisia lukuja – tai vaikkapa miljoonalla jaollisia lukuja – on siis saman verran kuin kaikkia luonnollisia lukuja!

Asetetaan seuraava määritelmä: jos joukko A on korkeintaan yhtä mahtava kuin luonnollisten lukujen joukko $\mathbb{N}$, niin A on *numeroituva*.

Käytännössä tämä tarkoittaa sitä, että numeroituvan joukon A alkiot voidaan indeksoida luonnollisilla luvuilla eli *luetella*, vaikka luettelo saattaakin olla päättymätön. On siis olemassa bijektio $\mathbb{N} \to A$ (jos A on äärellinen, on lähtöjoukkona jokin luonnollisten lukujen osajoukko). Esimerkiksi $\mathbb{N}$ voidaan luetella: $1, 2, 3, 4, \ldots$ ja parittomat luvut voidaan luetella: $1, 3, 5, 7, \ldots$.

On ehkä yllättävää, että on olemassa lukujoukkoja, joita ei voi tällä tavalla luetella ja joiden voi perustellusti sanoa olevan paljon suurempia kuin joukko $\mathbb{N}$. Tällaisia joukkoja kutsutaan *ylinumeroituviksi*. Cantorin kuuluisa diagonaaliargumentti osoittaa, että reaalilukujen joukko on ylinumeroituva. Päättely voidaan tehdä seuraavasti:

Riittää osoittaa ylinumeroituvaksi väli $[0, 1]$, sillä jos se on ylinumeroituva, niin täytyy olla myös koko $\mathbb{R}$:n. Todistettavan väitteen antiteesi eli vastaoletus on, että väli $[0, 1]$ on numeroituva. Jos tämän voidaan osoittaa johtavan ristiriitaan, niin täytyy antiteesi hylätä ja välin on oltava ylinumeroituva.

Mikäli antiteesi on totta, on olemassa välin $[0, 1]$ alkioiden luettelo. Olkoon se tässä 10-järjestelmän desimaalilukuina ilmaistuna seuraavanlainen (luvut $a_{ij} \in \mathbb{N}$ ovat desimaaleja):

$$\begin{array}{l} 0{,}a_{11}a_{12}a_{13}\ldots \\ 0{,}a_{21}a_{22}a_{23}\ldots \\ 0{,}a_{31}a_{32}a_{33}\ldots \\ \vdots \end{array}$$

On kuitenkin helppoa konstruoida luku, joka ei ole luettelossa, mutta joka kuuluu välille $[0, 1]$: valitaan luvun desimaalit niin, että poimitaan ylläolevan luettelon *diagonaalilla* olevat desimaalit a_{11}, a_{22}, a_{33} jne. ja *vaihdetaan ne*. Olkoon vaikkapa

$$b_i = 1, \text{ jos } a_{ii} \neq 1$$
$$\text{ja}$$
$$b_i = 0, \text{ jos } a_{ii} = 1$$

Nyt desimaaliluku $0, b_1 b_2 b_3 \ldots$ ei voi olla luettelossa!

Voidaan myös helposti todistaa, että rationaalilukujen joukko $\mathbb{Q}$ on "vain" numeroituva. Todistuksen löytäminen vaatii tosin hieman kekseliäisyyttä. Ideana on kirjoittaa rationaaliluvut tietyllä tavalla taulukoksi ja käydä taulukkoa läpi tietyssä järjestyksessä niin, että jokainen rationaaliluku tulee lueteltua.

Toinen tapa osoittaa $\mathbb{Q}$ yhtä mahtavaksi kuin $\mathbb{N}$ on todeta ensin, että positiivisten rationaalilukujen joukko on yhtä mahtava luonnollisten lukujen muotoa (m, n) olevien järjestettyjen parien joukon eli avaruuden $\mathbb{N}^2$ kanssa, sillä kaikki positiiviset rationaaliluvuthan ovat muotoa $\frac{m}{n}$, missä $n, m \in \mathbb{N}$. Joukko $\mathbb{N}^2$ taas on yhtä mahtava kuin $\mathbb{N}$, koska esimerkiksi funktio

$$f : \mathbb{N}^2 \to \mathbb{N}; f(n, m) = 2^n \cdot 3^m$$

on injektio. Muotoa $2^n \cdot 3^m$ oleva lauseke on jonkin luonnollisen luvun alkulukuhajotelma eikä samaa lukua voida jakaa alkulukutekijöihin kahdella eri tavalla. Koska on olemassa injektio $\mathbb{N}^2 \to \mathbb{N}$, on $\mathbb{N}^2$ korkeintaan yhtä mahtava kuin $\mathbb{N}$. Toisaalta $\mathbb{N}$ ei tietenkään voi olla mahtavampi kuin $\mathbb{N}^2$, sillä $\mathbb{N}$ voidaan samaistaa muotoa $(n, 0)$ olevien lukuparien eli avaruuden $\mathbb{N}^2$ osajoukon kanssa. Positiivisten rationaalilukujen joukko on siis numeroituva ja on helppoa päätellä, että jos mukaan otetaan negatiiviset rationaaliluvut ja nolla, on joukko edelleen numeroituva.

Nyt tutuksi ovat tulleet siis seuraavat eriasteiset joukkojen mahtavuudet: numeroituvat joukot, jotka voidaan jakaa äärellisiin ja numeroituvasti äärettömiin joukkoihin, sekä ylinumeroituvat joukot kuten $\mathbb{R}$.

Seuraavaksi herää kysymys, voidaanko ylinumeroituvia joukkoja jotenkin luokitella mahtavuuden perusteella. Onko olemassa joukkoa $\mathbb{R}$ mahtavampia joukkoja ja millaisia ne joukot ovat? Cantor osoitti vuosisadan vaihteessa myös, että tällainen joukko on $\mathbb{R}$:n osajoukkojen joukko eli $\mathbb{R}$:n potenssijoukko. Edelleen siirtymällä potenssijoukon potenssijoukkoon päästään aina vain mahtavampiin joukkoihin. Voidaan osoittaa, että $\mathbb{R}$ ja luonnollisten lukujen joukon $\mathbb{N}$ potenssijoukko ovat yhtä mahtavia.

Luonnollisten lukujen joukon mahtavuutta, jonka voidaan sanoa olevan pienin mahdollinen äärettömän joukon koko, merkitään symbolilla $\aleph_0$ (luetaan "aalef nolla"; $\aleph$ kuuluu heprealaisiin aakkosiin). Merkintätapa on peräisin Cantorilta. On helppoa osoittaa, että n alkiota sisältävällä (äärellisellä) joukolla on 2^n osajoukkoa, ja jos tämä yleistetään eriasteisiin äärettömyyksiin, niin päädytään siihen, että luonnollisten lukujen potenssijoukon ja samalla äsken todetun nojalla myös reaalilukujen joukon mahtavuus on $2^{\aleph_0}$, reaalilukujen joukon potenssijoukon mahtavuus on $2^{2^{\aleph_0}}$ jne.

Symbolilla $\aleph_1$ merkitään pienintä mahdollista ylinumeroituvan joukon mahtavuutta. Edelleen on ratkaisematta kysymys, onko $\aleph_1$ sama kuin reaalilukujen joukon mahtavuus vai onko olemassa joukkoja, joiden mahtavuus on suurempi kuin luonnollisten lukujen joukon mahtavuus mutta pienempi kuin reaalilukujen joukon mahtavuus. *K*ontinuumihypoteesina tunnettu väittämä sanoo, että tällaisia joukkoja ei ole, vaan että $2^{\aleph_0} = \aleph_1$. On osoitettu, että kontinuumihypoteesin totuusarvo on riippumaton yleisessä käytössä olevasta joukko-opin aksioomajärjestelmästä *ZFC* eli *Zermelo-Fraenkelin aksioomista*. Tältä kannalta katsoen kontinuumihypoteesi on väittämä, joka ei ole tosi eikä epätosi. Tällaisia väittämiä on löydetty paljon muitakin sen jälkeen, kun Kurt Gödel vuonna 1931 julkaisi kuuluisan epätäydellisyyslauseensa, jonka mukaan jokaisessa (1. kertaluvun) loogisessa teoriassa on mahdollista esittää lauseita, joita ei voi osoittaa todeksi tai epätodeksi.

On enemmän filosofinen kuin matemaattinen kysymys, voiko kontinuumihypoteesin kaltaisella väitteellä olla käytetystä aksioomajärjestelmästä ja valitusta mallista riippumaton totuusarvo. Nykyisistä loogikoista useimmat lienevät sillä kannalla, että väitteiden totuudesta tai epätotuudesta puhuminen on mieletöntä, ellei loogista viitekehystä ole määritelty. Platonistit ajattelevat kuitenkin toisin: muun muassa suomalainen matemaatikko ja filosofi Uuno Saarnio (1896–1977) esitti 1960-luvulla – sittemmin virheelliseksi todetun – todistuksensa kontinuumihypoteesille.

Voisi ajatella, että äärettömyyksien luokittelu on lähinnä kiinnostavaa teoretisointia, jolla tuskin on muuta kuin viihteellistä merkitystä. Näin ei kuitenkaan ole: varsinkin ylinumeroituvuuden ja numeroituvuuden välinen raja on monilla matematiikan aloilla hyvin tärkeä. On paljon perustavaa laatua olevia ominaisuuksia, jotka ovat vain numeroituvilla joukoilla, mutta eivät ylinumeroituvilla.

Näillä käsitteillä on käyttöä myös tietojenkäsittelytieteessä. Esimerkiksi laskettavuuden teorian keskeinen ratkeamattomuustulos nojaa siihen, että laskennallisia ongelmia tai täsmällisemmmin sanottuna ns. *päätösongelmia* on ylinumeroituva määrä. Minkä hyvänsä valitun ohjelmointikielen mahdollisia ohjelmia taas on vain numeroituva määrä, koska kaikki ohjelmat ovat äärellisen merkistön äärellismittaisia merkkijonoja, joita voidaan helposti osoittaa olevan saman verran kuin luonnollisia lukuja. Näin ollen on olemassa päätösongelmia, joita ei voida ratkaista kyseisellä ohjelmointikielellä. Ratkeavia päätösongelmia on siis numeroituva määrä, mutta kaikkia päätösongelmia ylinumeroituva määrä. Tällöin voidaan hieman epätäsmällisesti sanoa, että päätösongelmista vain häviävän pieni osa on ratkeavia. Ratkeamattomien ongelmien joukossa on myös monia käytännön kannalta mielenkiintoisia ongelmia, tunnetuimpana näistä pysähtymisongelma: pysähtyykö tietyn ohjelman suoritus jossain vaiheessa syötteellä x – vai jääkö ohjelma "ikuiseen luuppiin"?

Heräsikö kiinnostus aiheeseen? Äärettömyydestä on kirjoitettu paljon matematiikkaa popularisoivassa kirjallisuudessa. Esimerkkinä mainittakoon Rudy Ruckerin Mieli ja äärettömyys (Art House 1998).

Lopuksi haluan kiittää $\aleph$-merkintöihin liittyvän väärinkäsitykseni oikaisemisesta Aapo Halkoa, joka on aiemmin käsitellyt joukkojen mahtavuutta Solmussa 2/1998–1999 kirjoituksessaan "Joukko-oppia reaaliluvuilla". Kiitän myös kaikkia muita arvokkaita kommentteja ja parannusehdotuksia antaneita.