Johdatus matematiikkaan

Luento 3

Mikko Salo

6.9.2018

JYVÄSKYLÄN YLIOPISTO
UNIVERSITY OF JYVÄSKYLÄ

Sisältö

1. Logiikasta
2. Suora ja epäsuora todistus
3. Jaollisuus ja alkuluvut

Todistus

Tähän asti esitetyt todistukset ovat olleet esimerkinomaisia. Aloitetaan nyt todistamisen hieman tarkempi (mutta ei vielä kovin täsmällinen!) käsittely.

Tällä kurssilla esitellään seuraavat todistustekniikat:

- suora todistus
- epäsuora todistus (*reductio ad absurdum*)
- induktiotodistus

Tänään käsitellään suoraa ja epäsuoraa todistusta.

Todistus

Modernin matematiikan ydin on *todistaminen* eli väitteiden huolellinen perusteleminen. Todistukset perustuvat *logiikkaan* ja *matemaattisiin käytäntöihin*. Nykyisin kautta maailman on yhteinen käsitys, mikä on tarkka matemaattinen todistus eikä matematiikan teoreemojen paikkaansapitävyydestä jää epäilyjä.

Antiikin Kreikan aikoina Pythagoraan koulukunta alkoi vaatia täsmällisiä todistuksia matematiikan väitteille. Sitä ennen matematiikan väitteet perusteltiin niiden uskottavuudella tai esimerkkien avulla. Myöhemmin Eukleides ($\sim$ 300 eKr.) kehitti geometriaan aksiomaattisen menetelmän ja käytti järjestelmällisesti täsmällistä todistusta ja formaalia logiikkaa.

1900-luvun alkupuolella moderni matematiikan todistaminen sai kaikkialla hyväksytyn muotonsa (David Hilbert, ...).

Todistus

Todistamisen täsmällinen käsittely nojautuu logiikan käsitteisiin:

- *Aksiooma* (perusoletus) on jotain, jonka oletetaan olevan totta ja jota ei kyseenalaisteta (kyseisessä teoriassa). Näiden määrä on syytä olla vähäinen eivätkä ne saa olla keskenään ristiriitaisia.
- Esimerkkiaksiooma (geometria): *Jos A ja B ovat tason pisteitä, on olemassa suora, joka kulkee A:n ja B:n läpi.*
- *Todistus* on väitteen yksityiskohtainen perustelu, jossa *aksioomista* ja tunnetuista (eli *todistetuista!*) lauseista johdetaan väite logiikan *päättelysääntöjä* käyttäen.

Moderni matematiikka perustuu *Zermelo-Fraenkelin joukko-oppiin ZFC* ($\sim$ 1922, 9 aksioomaa). Tällä kurssilla ei käsitellä aksioomia, vaan todistukset perustuvat tunnettuihin ominaisuuksiin.

Väitelauseet

Väitelause on lause, joka väittää jotain, ja josta voidaan sanoa, onko se tosi vai epätosi.

Esimerkki

- $4 > 13$ (väitelause, epätosi)
- Hauki on kala. (väitelause, tosi)
- $1 + 3 - \sqrt{2}$ (ei väitelause, ei väitä mitään)
- Tämä väite on valetta. (ei ole väitelause sillä ei voida määrittää totuusarvoa, ns. valehtelijan paradoksi)
- Jokainen parillinen luku ≥ 4 on kahden alkuluvun summa. (väitelause, ei tiedossa onko tosi vai epätosi, ns. Goldbachin konjektuuri)

Negaatio

Jokaisella väitelauseella A on vastakohta eli negaatio ($\neg A$).
Esimerkiksi:

Väite	Negaatio
$\sqrt{2} \geq 3$	$\sqrt{2} < 3$
$2 \leq \pi \leq 3$	$\pi < 2$ tai $\pi > 3$
Kaikki tiet vievät Roomaan.	Jokin tie ei vie Roomaan.
Jos f on derivoituva, niin f on jatkuva.	On olemassa derivoituva f, joka ei ole jatkuva.

Negaation muodostamista tarvitaan epäsuorassa todistuksessa.

Loogiset konnektiivit

Matemaattisessa todistamisessa voidaan käyttää logiikasta peräisin olevia symboleita (konnektiiveja):

$\Longrightarrow$	implikaationuoli, "'seuraa"
$\Longleftrightarrow$	ekvivalenssinuoli, "jos ja vain jos"
$\neg$	negaatio, "ei"
$\wedge$	konjunktio, "ja"
$\vee$	disjunktio, "tai"

Myöhemmin tapaamme myös universaalikvanttorin $\forall$ ("kaikille") ja eksistenssikvanttorin $\exists$ ("on olemassa").

Ylläolevat symbolit on hyvä tietää, kokeessa niitä ei vaadita.

Logiikan päättelysääntöjä

Erilaisia tapoja todistaa väite muotoa "Jos A, niin B":

- Suora todistus. Oletetaan A, ja osoitetaan B.
- Epäsuora (käänteinen/kontrapositio) todistus. Oletetaan B:n vastakohta, ja osoitetaan A:n vastakohta.
- Epäsuora todistus. Oletetaan A ja B:n vastakohta, ja johdetaan ristiriita.

Eräs tapa todistaa yleinen väite Q:

- Epäsuora todistus. Oletetaan Q:n vastakohta, ja johdetaan ristiriita.

Perustuvat logiikan sääntöihin, esim. $(\neg B \Rightarrow \neg A) \Leftrightarrow (A \Rightarrow B)$.
Tällä kurssilla riittää osata näihin liittyviä esimerkkejä.

Jos ja vain jos –lauseet

Matematiikassa esiintyy usein "jos ja vain jos"- eli "täsmälleen silloin kun"- lauseita:

Esimerkkilause

Kokonaisluku n on pariton jos ja vain jos n^2 on pariton.

Väite "A jos ja vain jos B" (merkitään $A \Leftrightarrow B$) tarkoittaa samaa kuin väite "A:sta seuraa B, ja B:stä seuraa A".

Jos ja vain jos –väitteessä on kaksi suuntaa ("$A \Rightarrow B$" ja "$A \Leftarrow B$"). Tällainen väite todistetaan yleensä kahdessa osassa (voidaan merkitä "$\Rightarrow$" ja "$\Leftarrow$").

Sisältö

Suora todistus

Suora todistus etenee vaiheittain suoraan oletuksista väitteeseen.

Väite. Jos luonnollinen luku n on pariton, niin n^2 on pariton.

Todistus. Olkoon n pariton. Tällöin $n = 2k + 1$ jollekin kokonaisluvulle k. Lasketaan n^2 käyttämällä binomin neliökaavaa:

$$\begin{aligned} n^2 &= (2k+1)^2 = (2k)^2 + 2 \cdot (2k) \cdot 1 + 1^2 \\ &= 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1. \end{aligned}$$

Siis $n^2 = 2m + 1$ missä $m = 2k^2 + 2k$ on kokonaisluku. Täten määritelmän mukaan n^2 on pariton. □

Suora todistus

Sama käyttäen implikaationuolta:

Väite. Jos luonnollinen luku n on pariton, niin n^2 on pariton.

Todistus.

$$
\begin{aligned}
n \text{ pariton} &\implies n = 2k + 1 \text{ jollekin } k \\
&\implies n^2 = (2k+1)^2 \\
&\implies n^2 = (2k)^2 + 2 \cdot 2k \cdot 1 + 1^2 \\
&\implies n^2 = 4k^2 + 4k + 1 \\
&\implies n^2 = 2(2k^2 + 2k) + 1 \\
&\implies n^2 \text{ pariton.}
\end{aligned}
$$

□

Suora todistus etenee vaiheittain suoraan oletuksista väitteeseen!

Epäsuora todistus

Tarkastellaan seuraavaa väitettä:

Jos n^2 on pariton, niin n on pariton.

Yritetään suoraa todistusta:

$$\begin{aligned} n^2 \text{ pariton} &\implies n^2 = 2k+1 \text{ jollekin } k \\ &\implies n = \sqrt{2k+1} \\ &\implies ??? \end{aligned}$$

Ei ratkennut. Kokeillaan *epäsuoraa todistusta*:
Oletetaan, että väite ei pidäkään paikkaansa, ja johdetaan tästä ristiriita oletuksen kanssa.

Epäsuora todistus

Lause. Jos n on positiivinen kokonaisluku ja n^2 on pariton, niin n on pariton.

Todistus. Oletetaan, että n^2 on pariton. Tehdään *vastaväite* (vastaoletus, antiteesi): n on parillinen. Tällöin pätee

$$n = 2k$$

jollekin kokonaisluvulle k. Lasketaan

$$n^2 = (2k)^2 = 4k^2 = 2(2k^2).$$

Siis n^2 on parillinen. Tämä on *ristiriita* oletuksen, että n^2 on pariton, kanssa. Täten vastaväitteen on pakko olla epätosi. Tämä todistaa lauseen. □

Epäsuora todistus

Epäsuora todistus on hyödyllinen menetelmä, mutta pitää tietää, mitä on tekemässä:

- Vastaväitteen muodostamisen kanssa on oltava tarkkana: täytyy osata muodostaa oikein väitteen negaatio.
- Etukäteen ei ole selvää, mistä ristiriita löydetään.
- Epäsuora todistus on ei-konstruktiivinen: se voi todistaa jonkin olion olemassaolon, mutta ei anna tapaa löytää tällaista oliota. (Tässä mielessä suora todistus voi olla informatiivisempi.)

Sisältö

Jaollisuus

Määritelmä

Kokonaisluku n on *jaollinen* positiivisella kokonaisluvulla m, jos

$$n = km$$

jollekin kokonaisluvulle k. Tällöin merkitään $m|n$, ja sanotaan, että luku m on luvun n *tekijä*.

Siis $m|n$ täsmälleen silloin kun $\frac{n}{m} =$ kokonaisluku.

Luvun n tekijät voi löytää käymällä läpi luvut 1, 2, ..., n (miksi ei tarvitse lukuja $> n$)?

Esimerkki

Luvun 12 tekijät ovat 1, 2, 3, 4, 6, ja 12.

Jaollisuus

Lause

Luku n on 9:llä jaollinen jos ja vain jos luvun n (10-järjestelmäesityksen) numeroiden summa on 9:llä jaollinen.

Esimerkki

Olkoon $n = 18162$. Numeroiden summa on

$$1 + 8 + 1 + 6 + 2 = 18 = 2 \cdot 9$$

Lauseen nojalla $9 \mid 18162$. (Itse asiassa $18162 = 9 \cdot 2018$.)

Huomautus

Vastaava tulos pätee 3:lla jaollisuudelle (harjoitustehtävä).

Jaollisuus

Lause. Luku n on 9:llä jaollinen jos ja vain jos luvun n (10-järjestelmäesityksen) numeroiden summa on 9:llä jaollinen.

Todistus. Olkoon $n = a_0 + a_1 \cdot 10 + \ldots + a_k \cdot 10^k$. Huomataan:

$$n - (a_0 + \ldots + a_k) = a_1 \cdot 9 + a_2 \cdot 99 + \ldots + a_k \cdot \underbrace{99\cdots9}_{k \text{ kertaa}}.$$

"$\Rightarrow$" Jos $n = 9m$, niin luvun n numeroiden summa on

$$\begin{aligned} a_0 + \ldots + a_k &= n - (n - (a_0 + \ldots + a_k)) \\ &= 9m - (a_1 \cdot 9 + \ldots + a_k \cdot 99\cdots9) \end{aligned}$$

Tämä on 9:llä jaollinen (ts. muotoa 9ℓ jollekin kok.luvulle ℓ).
"$\Leftarrow$" Jos $a_0 + \ldots + a_k = 9m$, niin

$$\begin{aligned} n &= a_0 + \ldots + a_k + (n - (a_0 + \ldots + a_k)) \\ &= 9m + (a_1 \cdot 9 + \ldots + a_k \cdot 99\cdots9). \end{aligned}$$

Tämäkin on 9:llä jaollinen. $\square$

Jaollisuus

Edellisellä luennolla esiintyi seuraava määritelmä:

Määritelmä

Luku n on parillinen, jos $n = 2k$ jollekin kokonaisluvulle k.
Luku n on pariton, jos $n = 2k + 1$ jollekin kokonaisluvulle k.

Huomataan, että n on parillinen täsmälleen silloin kun $2 \mid n$.

Harjoitellaan epäsuoraa todistusta todistamalla eilen käytetty tulos:

Lause

Jokainen positiivinen kokonaisluku n on joko parillinen tai pariton (mutta ei molempia).

Jaollisuus

Osoitetaan ensin lemma (apulause):

Lemma

(a) Jos n on parillinen, niin n ei ole pariton.
(b) Jos n on pariton, niin n ei ole parillinen.

Todistus.

(a) Olkoon n parillinen. Tehdään vastaoletus: n on myös pariton. Oletuksen nojalla $n = 2k$ jollekin kokonaisluvulle k. Lisäksi vastaoletuksen nojalla $n = 2m + 1$ jollekin kokonaisluvulle m. Tällöin

$$2k = 2m + 1 \implies 2(k - m) = 1 \implies k - m = \frac{1}{2}.$$

Tämä on ristiriita, sillä $k - m$ on kokonaisluku. Siis vastaoletus on väärä, ja n ei ole pariton. (b) todistetaan vastaavasti. □

Jaollisuus

Lause

Jokainen positiivinen kokonaisluku n on joko parillinen tai pariton (mutta ei molempia).

Todistus.

Lemman nojalla n ei voi olla sekä parillinen että pariton. Täytyy vielä osoittaa, että jokainen n on parillinen tai pariton.

Tehdään vastaoletus: on olemassa kokonaisluku, joka ei ole parillinen eikä pariton. Olkoon n_0 pienin tällainen kokonaisluku. Koska $1 = 2 \cdot 0 + 1$ on pariton, täytyy olla $n_0 \geq 2$.

Nyt $n_0 - 1$ ei voi olla parillinen (jos olisi $n_0 - 1 = 2k$, niin $n_0 = 2k + 1$ olisi pariton). Samoin $n_0 - 1$ ei voi olla pariton. Siis $n_0 - 1$ ei ole parillinen eikä pariton. Tämä on ristiriita, sillä n_0 oli pienin tällainen luku. Lause on todistettu. □

Alkuluvut

Määritelmä

Luku $n \geq 2$ on *alkuluku*, jos se on jaollinen ainoastaan luvuilla 1 ja n. Muussa tapauksessa $n \geq 2$ on *yhdistetty luku*.[1]

Ensimmäiset alkuluvut ovat 2, 3, 5, 7, 11, 13, 17, 19, ...
Suurin tunnettu alkuluku on $2^{77\,232\,917} - 1$ (löydetty 2017, luvussa on n. 23 milj. numeroa).

Eräs syy alkulukujen tärkeydelle on seuraava:

Aritmetiikan peruslause

Jokainen kokonaisluku $n \geq 2$ voidaan kirjoittaa muodossa $n = p_1 p_2 \cdots p_k$, missä $p_1, \ldots, p_k$ ovat alkulukuja.

---

[1] $n \geq 2$ on yhdistetty luku jos ja vain jos $n = k\ell$ joillekin $k \geq 2$, $\ell \geq 2$.

Rationaaliluvut

Määritelmä

Reaaliluku x on *rationaaliluku*, jos $x = \frac{m}{n}$ joillekin kokonaisluvuille m ja n, missä $n \geq 1$.

(Jos $x = \frac{m}{n}$ on rationaaliluku, aritmetiikan peruslauseen nojalla m (tai $-m$) ja n ovat alkulukujen tuloja. Supistamalla yhteiset tekijät lausekkeesta $\frac{m}{n}$ voidaan aina olettaa, että $x = \frac{k}{\ell}$ missä kokonaisluvuilla k ja ℓ ei ole yhteisiä tekijöitä.)

Määritelmä

Reaaliluku x on *irrationaaliluku*, jos se ei ole rationaaliluku.

Esimerkki

Luvut $\frac{7}{8}$, -2 ja $\frac{1}{100}$ ovat rationaalilukuja. Luvut $\sqrt{2}$ ja π ovat irrationaalilukuja.

$\sqrt{2}$ on irrationaalinen

Lause. $\sqrt{2}$ on irrationaalinen.

Todistus. Tehdään *vastaväite*: $\sqrt{2}$ on rationaaliluku. Tällöin

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

joillekin kokonaisluvuille m ja n, joilla ei ole yhteistä tekijää. Korotetaan toiseen potenssiin:

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

Siis $m^2 = 2n^2$. Tästä seuraa että m on parillinen[1], ts. $m = 2k$ jollekin k, ja $2n^2 = m^2 = (2k)^2 = 4k^2$. Tälloin $n^2 = 2k^2$ on parillinen, joten n on parillinen[1]. Siis m ja n ovat parillisia, mikä on *ristiriita*, sillä luvuilla m ja n ei ole yhteistä tekijää. □

[1] Perustele! (Epäsuora todistus tai aritmetiikan peruslause)

Alkuluvut

Suuria alkulukuja on harvassa ja ne ovat epäsäännöllisesti jakautuneet, mutta:

Lause

Alkulukuja on äärettömän monta.

Todistus.

(Eukleides $\sim$ 300 e.Kr.) Jos N on positiivinen kokonaisluku, niin mikään luvuista $2, 3, \ldots, N$ ei ole luvun $N! + 1$ tekijä. Täten luvulla $N! + 1$ on alkulukutekijä $p > N$. Siis alkulukuja on äärettömän monta. $\square$

Matematiikan tutkimuksesta

Konjektuuri (Alkulukuparit)

Löytyy äärettömän monta paria $(p, p+2)$, missä sekä p että $p+2$ ovat alkulukuja.

Alkulukupareja: $(3,5)$, $(5,7)$, $(11,13)$, $(17,19)$, $(29,31)$, $(41,43)$, $(59,61)$, ... Suuria alkulukupareja erittäin harvassa!

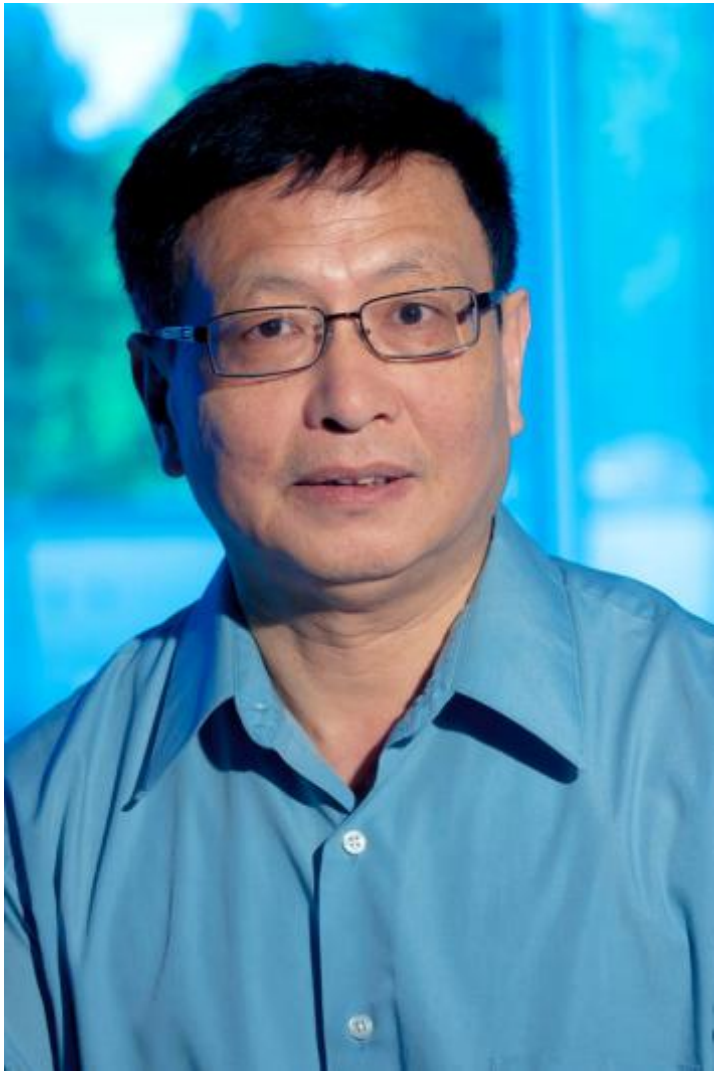
Yleisemmin: löytyykö äärettömän monta alkulukukaksikkoa $(p, p+N)$ jollekin kiinteälle N?

Goldston-Pintz-Yildirim (2007): *"Theorem 1 would appear to be within a hair's breadth of obtaining this result."*

Alkulukuparit

Lause (Yitang Zhang 2013)

Jollekin $N \leq 70\,000\,000$ löytyy äärettömän monta alkulukukaksikkoa muotoa $(p, p + N)$.



Alkulukuparit

Massiivinen Polymath –yhteistyötutkimus:

Lause (2014)

Jollekin $N \leq 246$ löytyy äärettömän monta alkulukukaksikkoa muotoa $(p, p + N)$.

Terence Tao (UC Los Angeles)

James Maynard (Oxford)

Esitehtävä maanantaille

Tutustu Juutisen Johdatus matematiikkaan –luentomonisteen lukuun 2.3.8 (Induktiotodistus).