Todistusmenetelmiä

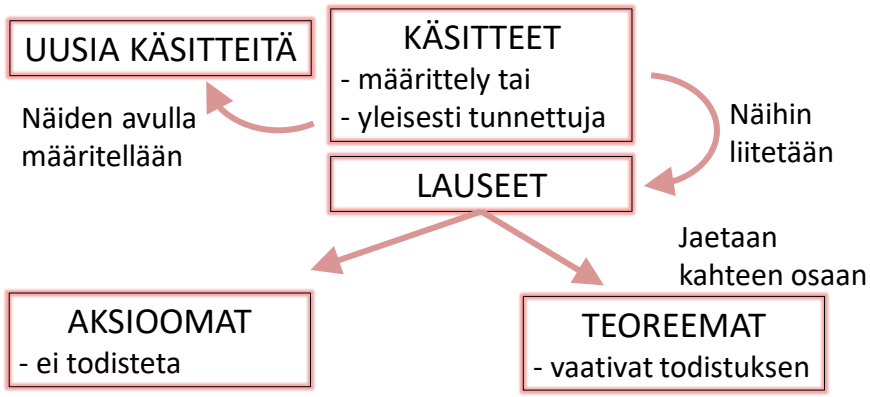
Miksi pitää todistaa?

Todistus on looginen päättelyketju, jossa oletuksista, määritelmistä, aksioomeista sekä aiemmin todistetuista tuloksista lähtien päätellään väite. Todistus antaa perustelut väitteille ja jäsentää matemaattista tietoa. *”Ei olla ns. tuuliajolla, vaan selkeällä kurssilla kohti päämäärää.”*

Mikä on aksiooma?

Matemaattisen teorian rakentamisessa käytetään *aksiomaattista menetelmää*. Lähtökohtina ovat tietyt *peruskäsitteet (-objektit)* esimerkiksi piste ja suora, joita ei määritellä ja tietyt niitä koskevat väitteet eli aksioomat, jotka hyväksytään tosiksi ilman todistusta. Siis aksiooma on jokin väite (väitelause), jota ei todisteta.

Perusobjektien avulla *määritellään* uusia käsitteitä ja niiden avulla edelleen uusia. Aksioomien ja määritelmien avulla *todistetaan lauseita eli teoreemoja*, joiden avulla todistetaan edelleen uusia lauseita.



TEOREEMA:	Tietyillä edellytyksillä on voimassa tietty matem.omin.
OLETUS:	Ilmoitetaan teoreemassa mainitut edellytykset ja otetaan käyttöön tarvittavat merkinnät.
VÄITE:	Ilmoitetaan teoreemassa mainittu ominaisuus käyttämällä sopivia merkintöjä. (Oletukset ja väite usein valmiina.)
TODISTUS:	Osoitetaan väite oikeaksi käyttämällä hyväksi oletusta, määritelmiä ja aiemmin tunnettuja lauseita.
HUOM!	ÄLÄ lähde liikkeelle väitteestä.

Teoreeman tulee siis aina sisältää tunnetuiksi otaksutut perusteet eli *oletukset* sekä päätelmä eli *väite*!

Teoreema voidaan aina(?) esittää ”Jos…, niin…” – muodossa, jolloin *jos*-sanaa seuraa oletus ja *niin*-sanaa väite. Esimerkiksi lause: *”Tasakylkisen kolmion kantakulmat ovat yhtä suuret.”* voidaan esittää muodossa: *”**Jos** kolmio on tasakylkinen, **niin** sen kantakulmat ovat yhtä suuret.”*

Todistuksen päättelyketjuun sisältyviä lauseita sitovat logiikan lait. Todistukseen ei saa sisältyä mitään uutta tietoa!

Matemaattiset todistukset jaetaan yleisesti neljään osaan:

1. **Suora todistus:** $p \wedge (p \Longrightarrow q) \Longrightarrow q$ Modus ponendo ponens,
2. **Käänteinen suora todistus:** Modus tollendo tollens
   $\neg q \wedge (p \Longrightarrow q) \Longrightarrow \neg p$
3. **Epäsuora todistus:** Reductio ad absurdum
   $p \wedge \big((p \wedge \neg q) \Longrightarrow (s \wedge \neg s)\big) \Longrightarrow q$ ja
4. **Induktiotodistus:** (luon. lukuja koskevat väitteet)

Palautetaan mieleen ero jonkin asian tai ilmiön toteutumisen *välttämättömän* ja *riittävän* ehdon välillä.
Lauseessa: ”Jos p, niin q” (joka on siis implikaatio $p \Longrightarrow q$) on p *riittävä* ehto q:lle (eli että q tapahtuu) ja toisaalta q on *välttämätön* ehto p:lle, sillä jos q ei tapahdu, ei myöskään p tapahdu.

Jos todistus on implikaatio $p \Longrightarrow q$, niin p on *oletus* ja q *väite*. Esimerkiksi

$$\underbrace{\text{Luku } n \text{ on parillinen.}}_{=p} \Longrightarrow \underbrace{\text{Luvun neliö } n^2 \text{ on parillinen.}}_{=q}$$

Jos todistus on ekvivalenssi $p \Longleftrightarrow q$, niin pitää osoittaa kaksi implikaatiota, nimittäin $p \Longrightarrow q$ ja $q \Longrightarrow p$.

Jos pitää todistaa, että kaksi joukkoa on samat, esim. $A = B$, niin on otettava mielivaltainen alkio $a \in A$ ja osoitettava, että $a \in B$. Tämän jälkeen on otettava mielivaltainen alkio $b \in B$ ja osoitettava, että $b \in A$.

1. Suora todistus $p \wedge (p \Longrightarrow q) \Longrightarrow q$

Esimerkki Osoita, että parittoman luonnollisen luvun neliö on aina pariton.
Oletus: $n \in \mathbb{N}, n$ on pariton.
Väite: n^2 on pariton.
Todistus: Koska $n \in \mathbb{N}$ on pariton, niin löytyy $k \in \mathbb{N}$ siten, että $n = 2k + 1$. Tällöin

$$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = \underbrace{2(2k^2 + 2k)}_{\text{parillinen}} + 1$$

Koska $k \in \mathbb{N}$, niin myös luku $(2k^2 + 2k) = m \in \mathbb{N}$ ja näin ollen

$$n^2 = 2m + 1,$$

eli n^2 on pariton.

MUISTA parittoman luvun määritelmä: $x \in \mathbb{N}$ on pariton, mikäli löytyy, eli on olemassa, sellainen $y \in \mathbb{N}$, että $x = 2y + 1$. Tai $x \in \mathbb{Z}$ on pariton , mikäli löytyy sellainen $y \in \mathbb{Z}$, että $x = 2y + 1$.

Vastaesimerkin käyttö

Mikäli lauseen totuusarvoa ei tunneta, lause voidaan yrittää todistaa oikeaksi tai vääräksi. Jos on annettu todistettavaksi lause, joka on muotoa $A \Longrightarrow B$, niin mikäli voidaan todistaa, että lause $A \Longrightarrow \neg B$ on tosi, niin edellinen lause $A \Longrightarrow B$ on tällöin epätosi.

Esimerkki Tutkitaan, pitääkö lause: ”Jos n on luonnollinen luku, niin $n^2 - n + 41$ on alkuluku.”
Oletus: $n \in \mathbb{N}$.
Väite: $n^2 - n + 41$ on alkuluku.
Todistus: Lause on muotoa $A \Longrightarrow B$. Pienillä alkuluvuilla kokeilu antaa viitteen, että väite olisi tosi. Kokeilu ei koskaan todista mitään! Nimittäin riittää löytää yksikin n, jolle väite ei päde ja asia on selvä. Havaitaan (kun on riittävästi kokeiltu tai muulla tavoin päätelty), että kun $n = 41$, niin

$\mathbb{P}$ on alkulukujen joukko.

$$n^2 - n + 41 = 41^2 - 41 + 41 = 41^2 = 1681 \notin \mathbb{P}.$$

Näin ollen tämä vastaesimerkki osoittaa lauseen $A \Longrightarrow \neg B$ todeksi ja alkuperäisen lauseen $A \Longrightarrow B$ epätodeksi, $n^2 - n + 41$ ei ole alkuluku.

Huomautus Väitteen kumoamiseksi riittää löytää yksikin vastaesimerkki. Mutta, vastaesimerkin puuttuminen ei osoita väitettä oikeaksi, eli annettua lausetta todeksi!

Matematiikassa on useita lauseita, joita ei voida osoittaa sen paremmin todeksi tai epätodeksi. Tiedetään myös, että on olemassa lauseita, joille ei ole olemassa todistusta eikä myöskään vastaesimerkkiä.

Lukuteoriassa on muutama tunnettu ns. *otaksuma* eli *konjektuuri*. Esimerkiksi Goldbach'in konjektuuri: *Jokainen kahta suurempi parillinen luku on 2 alkuluvun summa.*

$$p \wedge (\neg q \Longrightarrow \neg p) \Longrightarrow q$$

3. Epäsuora todistus $\quad p \wedge \big((p \wedge \neg q) \Longrightarrow (s \wedge \neg s)\big) \Longrightarrow q$

Epäsuorassa todistuksessa väite osoitetaan oikeaksi näyttämällä, että mikäli se ei pitäisikään paikkaa, syntyisi ristiriita $s \wedge \neg s$ minkä tahansa asian kanssa (eli oletuksen tai jonkin yleisesti tiedetyn toden kanssa). Todistuksen aluksi tehdään *vastaoletus* eli *antiteesi*. Ei vastaväite!
(Tosin tästä asiasta tuskin koskaan päästään yksimielisyyteen ☺)

Esimerkki Todista, että jos a on negatiivinen, niin myös $a - 1$ on negatiivinen.
Oletus: $a < 0$.
Väite: $a - 1 < 0$.
Todistus: Vastaoletus: $a - 1 \geq 0$. Tällöin vastaoletuksesta seuraa $a \geq 1$, ja yhdessä oletuksen $a < 0$ kanssa saadaan

$$0 > a \geq 1 \implies 0 \geq 1,$$

mikä on ristiriita. Näin ollen väite $a - 1 < 0$ pitää paikkansa.

Esimerkki Todista, että jos kokonaisluvun n neliö on parillinen, niin myös luku n itse on parillinen.
Oletus: $n \in \mathbb{Z}, n^2$ on parillinen.
Väite: n on parillinen.
Todistus: Vastaoletus: n on pariton, eli $n = 2k + 1$, jossa $k \in \mathbb{Z}$. Tällöin

$$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = \underbrace{2(2k^2 + 2k)}_{\text{parillinen}} + 1 = 2m + 1$$

Koska $k \in \mathbb{Z}$, niin myös luku $(2k^2 + 2k) = m \in \mathbb{Z}$ ja näin ollen n^2 on pariton. Tämä on ristiriita oletuksen n^2 on parillinen kanssa.

Esimerkki Todista, ettei joukossa $\mathbb{R}_+$ ole pienintä lukua.
Oletus: –
Väite: $\nexists\, r \in \mathbb{R}_+$ siten, että kaikilla $a \in \mathbb{R}_+, a \neq r, r < a$.
Todistus: Vastaoletus: $\exists\, r \in \mathbb{R}_+$ siten, että $\forall a \in \mathbb{R}_+, r < a$ ja $a \neq r$. Koska $r \in \mathbb{R}_+$, niin myös $\frac{r}{2} \in \mathbb{R}_+$, sillä selvästi $\frac{r}{2} > 0$. Mutta nyt

$$\frac{r}{2} =: a < r,$$

eli löydettiin vastaesimerkki. Ristiriita → alkuperäinen väite oikein.

Esimerkki Todista, että alkulukuja (luku $n \in \mathbb{N}, n > 2$ on alkuluku, jos se on jaollinen vain 1:llä ja itsellään) on äärettömän paljon. (Eukleides)
Oletus: –
Väite: Alkulukuja on äärettömän paljon.
Todistus: Vastaoletus: On olemassa suurin alkuluku, merkitään sitä p:llä. Tällöin alkulukujen joukko on

$$\{2, 3, 5, \dots, p\}.$$

Tarkastellaan lukua $2 \cdot 3 \cdot 5 \cdot \dots \cdot p + 1$. Selvästi se on suurempi kuin mikään alkuluku ja toisaalta se ei ole jaollinen millään alkuluvulla. Siis se on alkuluku. Tämä on ristiriita. Alkulukuja on äärettömän paljon.

4. Induktiotodistus

Induktioksi sanotaan ajatustoimintaa, joka johtaa yksittäisistä totuuksista yleiseen totuuteen. Äärellisen joukon kaikki alkiot (totuus) voidaan testata ja jos ääretön (numeroituvasti), niin tarvitaan induktiota. Induktiotodistus eli *matemaattinen induktio* nojautuu induktioaksioomaan.

Induktioaksiooma Olkoon A joukko luonnollisia lukuja eli $A \subset \mathbb{N}$. Jos kaksi seuraavaa ehtoa pätevät

1. $1 \in A$,
2. A sisältää jokaisen lukunsa $n \in A$ seuraajan $n + 1 \in A$,

niin silloin $A = \mathbb{N}$.

Induktio-oletusta on käytettävä jossakin vaiheessa todistusta!

Induktiotodistuksen rakenne on kolmivaiheinen:

perus-askel
1) Testataan, että väite pitää paikkansa, kun $n = 1$, eli $p(1)$ on tosi.

Niin sanottu *induktio-askel*
2) Tehdään ns. *induktio-oletus*, että väite on voimassa, kun $n = k$, eli $p(k)$ on tosi.
3) Osoitetaan, että väite pätee myös, kun $n = k + 1$.

Esimerkki Todista, että parittomien luonnollisten lukujen summa on n^2, eli $1 + 3 + 5 + \ldots + (2n-1) = n^2$.

Todistus: Aluksi havaitaan, että väite pätee ensimmäisillä parittomilla luonnollisilla luvuilla.

1
$1 + 3 = 4 = 2^2$
$1 + 3 + 5 = 9 = 3^2$
$1 + 3 + 5 + 7 = 16 = 4^2$

1) Alkuaskel eli perusaskel:
Kun $n = 1$, niin $(2 \cdot 1 - 1) = 1 = 1^2$

2) Induktio-oletus:
Tehdään induktio-oletus, että kun $n = k$, niin yhtälö

$$1 + 3 + 5 + \ldots + (2 \cdot k - 1) = k^2$$

pätee.

3) Induktio-väite: Yhtälö on voimassa myös, kun $n = k + 1$.
Nyt

$$\begin{aligned} 1 + 3 + \ldots + (2 \cdot (k+1) - 1) &= 1 + 3 + \ldots + (2k + 2 - 1) \\ &= 1 + 3 + \ldots + (2k+1) \\ &= \underbrace{1 + 3 + \ldots + (2k-1)}_{= k^2} + (2k+1) \end{aligned}$$

Summa kirjoitettu toisin →
Käytetty induktio-oletusta →

$$\begin{aligned} 1 + 3 + \ldots + (2 \cdot (k+1) - 1) &= 1 + 3 + \ldots + (2k + 2 - 1) \\ &= 1 + 3 + \ldots + (2k+1) \\ &= \underbrace{1 + 3 + \ldots + (2k-1)}_{= k^2} + (2k+1) \\ &= k^2 + 2k + 1 \\ &= (k+1)^2 \end{aligned}$$

Summa kirjoitettu toisin →
Käytetty induktio-oletusta →

Näin ollen yhtälö on voimassa myös, kun $n = k + 1$.

Esimerkki Osoita, että $n < 2^n$ kaikilla positiivisilla kokonaisluvuilla.

1) Kun $n = 1$, niin $1 < 2^1 = 2$, OK.
2) Oletetaan, että epäyhtälö $n < 2^n$ on tosi arvolla $n = k$, eli $k < 2^k$.
3) Osoitetaan, että epäyhtälö on tosi myös arvolla $n = k + 1$.
   Koska

$$k + 1 < k + k = 2 \cdot k \underbrace{\leq}_{\text{ind.ol.}} 2 \cdot 2^k = 2^{k+1},$$

aina kun $k > 1$, niin väite $k + 1 < 2^{k+1}$ osoitettu.