4. PEATÜKK

TÕESTAMISE ERINEVAD MEETODID

"Siin on minu tulemus, kuid ma ei tea veel, kuidas temani jõuda!"
Carl Friedrich Gauss (1777 – 1855)

Kõikidele loodusteadustele on iseloomulik, et tulemuste saavutamiseks tehakse vaatlusi ja katseid. Matemaatikas ei tehta vaatlusi ega katseid, vaid tulemused saadakse rangete loogiliste arutluste abil, mida nimetatakse ***tõestusteks***.

Matemaatikas on teatud arv põhimõisteid ja põhitõdesid, mida ei tõestata. Põhitõdesid, mida ei tõestata ja mida eeldatakse tõesed olevat, nimetatakse ***aksioomideks***. Ülejäänud valemid ja tulemused sõnastatakse lausetena, mida nimetatakse teoreemideks. ***Teoreem*** on lause, mille õigsust tõestatakse range loogilise arutluse abil. Teoreemis esitatud väite õigsust tõestatakse aksioomidest ja varem tõestatud teoreemidest lähtudes.

Aksiomaatilise meetodi alusepanija on **Eukleides** (325 – 265 eKr), kes süstematiseeris oma teoses „Elemendid" sellisel viisil tolleaegse matemaatika. Eukleides esitas täpse ja loogiliselt tervikliku geomeetrilise süsteemi, mida nimetatakse "eukleidiliseks geomeetriaks". Selle süsteemi aluseks on definitsioonid ning aksioomid ja postulaadid (Eukleides eristas aksioome ja postulaate, kuid kaasaegses mõttes on need kõik aksioomid) ja nendest tuletas ta ülejäänud teoreemid. Aksioome pidas ta ilmseteks tõdedeks. Pikka aega (2000 aastat) tegelesid matemaatikud paralleelide postulaadi probleemiga, püüdes tõestada, et seda saab tuletada teistest aksioomidest. Paralleelide aksioom väidab, et *läbi punkti, mis ei asu antud sirgel, saab tõmmata ainult ühe sirge, mis on paralleelne selle sirgega*. Alles XIX–XX saj. näidati, et see aksioom on tõepoolest sõltumatu teistest aksioomidest ning korrektne saab olla ka geomeetria, kus aluseks on võetud selle aksioomi eitus. Eukleidese süsteem püsis 1820. aastani, mil silmapaistev vene matemaatik **Nikolai Lobatševki** (1792-1856) ja veidi hiljem ka ungari matemaatik **János Bolyai** (1802 – 1860) jõudsid paralleelide aksioomi muutes uue geomeetria avastamiseni. Teadmine, et võib üles ehitada geomeetria kui matemaatilise teooria, milles väljaspool sirget asuvat punkti läbib nendega samal tasandil rohkem kui üks sirge, mis ei lõika antud sirget või milles kolmnurkade sisenurkade summa on väiksem kui 180°, oli tollal isegi nimekatele matemaatikutele ootamatu. Tekkinud geomeetriat nimetatakse ***mitteeukleidiliseks geomeetriaks***. Selle loomine näitas, et aksioome võib mõista lihtsalt kui eeldusi. Eukleidese "Elementides" esinevate lünkade otsimine sai XIX sajandi lõpul matemaatikute üheks tähtsamaks ülesandeks. Selle ülesande lahendamise viis 1900. aastaks lõpule saksa matemaatik **David Hilbert** (1862 – 1943).

Gottlob Frege (1848 - 1925) lõi kaasaja loogika fundamentaalseima süsteemi, nn. esimest järku predikaatarvutuse, mis baseerub lausearvutusel, predikaatidel ja kvantoritel. Frege kindel seisukoht oli, et kogu matemaatika saab taandada elementaarsetele loogikareeglitele, st loogikareeglite abil saab tuletada ükskõik millise tõese matemaatikateoreemi. Frege süsteemi ja logitsistlikud vaated võtsid oma töös aluseks 20. sajandi alguse mõjukaimad loogikud **Bertrand Russell** (1872–1970) ja **Alfred North Whitehead** (1861–1947), kes formaliseerisid oma teoses *Principia Mathematica* (1910–1913) suure osa matemaatika alustest. Matemaatika tuletamist loogikast alustasid Russell ja Whitehead täisarvude teooriast ehk aritmeetikast, võttes aluseks **Giuseppe Peano** (1858–1932) aritmeetika baastõed, millest loodeti tuletada

aritmeetika ning seejärel ehitada sinna peale matemaatiline analüüs, algebra ja muud matemaatikaharud. Kolmekümnendatel aastatel tõestas **Kurt Gödel** (1906 – 1978) enamikule selleaja loogikutele ootamatult ühe praeguseks kuulsaima loogikateoreemi üldse: ***teoreemi mittetäielikkusest***. Nimetatud teoreem näitab, et aritmeetikat ei saa taandada loogikale, ehk konkreetsemalt, ei ole olemas lõplikku baasväidete (aksioomide) kogu, millest saaks tuletada kõiki aritmeetikateoreeme. Kui juba aritmeetikat ei saa lõpliku hulga baasväidete abil aksiomatiseerida, siis loomulikult ei saa seda teha ka enamike teiste matemaatikaharude jaoks. See ei tähenda samas, et loogikavahendid oleksid aritmeetika või muude keerulisemate valdkondade juures kasutud: reeglina piisab meile huvi pakkuvate väidete tõestamiseks siiski suhteliselt väikesest hulgast harilikest elementaaraksioomidest. Gödeli teoreem kahandas huvi loogika vastu, kuid elektronarvutite leiutamine sajandi keskel ja majanduse, teaduse ning ühiskonna süvenev arvutiseerimine andsid loogikateadusele uue võimsa tõuke. Alates 1980. aastate lõpust on arendatud matemaatika formaliseerimist arvutil (nt interaktiivsed teoreemitõestajad), nende jaoks on loodud palju standardteoreemide teeke. Loogika ja teoreetiline arvutiteadus on muutunud vastastikku üksteisest sõltuvaks ning mitmete konkreetsete valdkondade puhul raskesti eristatavateks.

Induktiivne ja deduktiivne järeldamine

Laias laastus saab mõtlemismehhanisme jagada kahte põhirühma: üldistuste tegemine ja järelduste tegemine. ***Induktiivne järeldamine*** ehk üldistuste tegemine toimub siis, kui üksikjuhtudel selgunud omadus üldistatakse üldomaduseks. Nähes enda ümber ainult valgeid luiki, kipume üldistavalt uskuma, et kõik luiged maailmas on valged. Kui märkame, et asjad, millega me kokku puutume, esinevad kas enamasti või alati koos (leek = kuumus = valu), üldistame selle kokkusattumuse sageli reegliks. Kuid enamik igapäevaselt õpitud reegleist ei pruugi erandlikes olukordades kehtida, neil reeglitel on tavaliselt erandid. Üldistuste tegemine ehk induktsioon on seega mõtlemisprotsess, mis ei anna mingeid kindlaid teadmisi. Induktiivselt saab järeldada ainult millegi tõenäolisust, mitte tõesust ehk üldistuste edukus on statistiline: mida sagedamini selliselt leitud reegel kehtib, seda parem, aga ei maksa loota, et ta alati kehtib. Tuleb meeles pidada, et matemaatikas ei kasutata tõestamist kogemuse abil!

Loogikareeglite kasutamist uute väidete järeldamiseks nimetatakse aga nende väidete tuletamiseks ehk ***deduktsiooniks*** ehk tõestamiseks. Suur osa loogikas kasutatavatest reeglitest ongi esitatud järelduse vormis: ühe või mitme väite tõesusest järeldub uus väide. Teiste sõnadega, peetakse võimatuks, et eelduste tõesuse korral oleks järeldus väär. Erinevalt induktsioonist garanteerib õigete reeglite rakendamine õigetele faktidele alati ka õige tulemuse.

Tõestamine

Teoreemid esinevad sageli *„Kui ..., siis ...“* kujul ehk matemaatiliselt kirjutatuna,

$$\forall x \in D, \text{ kui on tõene } P(x), \text{ siis on tõene ka } Q(x).$$

Tingimust $P(x)$ nimetatakse ***eelduseks*** ja tingimust $Q(x)$ ***väiteks***. Võimsaim tõestuse meetod on selline, mis üldistab ehk laiendab väite kehtivuspiirkonda. Antakse ette suvaline x mille korral eeldus $P(x)$ on tõene ja kasutades definitsioone, eelnevaid tulemusi ja reegleid järeldatakse, et $Q(x)$ on tõene.

Seega, teoreemi tõestamisel:

1) lähtutakse eeldusest;
2) viiakse läbi arutlus kasutades aksioome või varem tõestatud teoreemide väiteid;
3) loogilise arutluse käigus jõutakse lõpuks otsustuseni, et teoreemi väide tõesti kehtib.

Erinevad matemaatilised teooriad ei ole lihtsalt faktide kogumid, vaid loogilised süsteemid. Aksioomid, definitsioonid ja teoreemid ei ole mitte juhuslikus järjekorras loetletud, vaid on tavaliselt esitatud meisterlikus järjestuses. Iga teoreem peab olema paigutatud niisugusele kohale, et tema tõestus toetub varem esitatud aksioomidele, definitsioonidele ja teoreemidele. Eukleidese „Elemendid“ oli selliste rangelt loogiliste süsteemide esimene ning parim näide, mida teised teadused on püüdnud ja püüavad ikka veel jäljendada. Järgnevalt vaatamegi erinevaid tõestuse meetodeid.

Otsene tõestus

Enamus tõestusi, millega sa siiamaani kokku puutunud oled (kui sa neid üldse näinud või teinud oled) on olnud nn ***otsesed tõestused***, mille korral iga järgmine samm toetub eelnevalt näidatud sammule või olemasolevale faktile. Loogiliselt õiges järjekorras arutledes jõutakse lõpuks tulemuseni.

Tähistades eelduse tähega P ning väite tähega Q, on eesmärk otseselt näidata, et $P \Rightarrow Q$.

Kuigi otsese tõestuse juures kasutatavad matemaatilised meetodid erinevad üksteisest vastavalt tõestamist vajavale väitele, on siiski üleüldine lähenemine alati sama: alusta nende andmetega, mis eelduses on antud ja loogilise arutluse tulemusena jõua väiteni, mida oli vaja tõestada.

Tõestuse üldise esitusega tutvumiseks vaatleme järgmist näidet.

Teoreem 1. Iga $m \in \mathbb{Z}$ ja $n \in \mathbb{Z}$ korral, kui m ja n on paarisarvud, siis on seda ka $m + n$.

Tõestus. Olgu m ja n paarisarvud. Siis saame nad esitada kujul $m = 2k_1$ ja $n = 2k_2$, kus k_1 ja k_2 on mingid täisarvud. Nende summa $m + n$ saame esitada kujul $m + n = 2k_1 + 2k_2 = 2(k_1 + k_2) = 2k$. Kuna $k = k_1 + k_2 \in \mathbb{Z}$, siis on $2k$ paarisarv ehk $m + n$ on paarisarv. ■

Teoreem 2. Iga paaritu täisarvu ruut annab 8-ga jagades jäägi 1.

Tõestus. Olgu n suvaline paaritu täisarv. Kuna n on paaritu, siis leidub täisarv k nii, et $n = 2k + 1$. Järelikult $n^2 = (2k + 1)^2$ ehk $n^2 = 4k^2 + 4k + 1$ ehk $n^2 = 4k(k + 1) + 1$. Kuna kahest järjestikusest arvust üks on alati paaris, siis $k(k + 1)$ on kindlasti paarisarv. Järelikult $4k(k + 1)$ jagub 8-ga ja seega oleme näidanud, et n^2 annab 8-ga jagades jäägi 1.

■

Mõned tüüpilised vead teoreemide tõestamisel:

- Argumenteeritakse näidetega. See, et mõne näite korral teoreem kehtib, ei tähenda veel selle üldist kehtimist.
- Samade tähistuste kasutamine erinevate terminite jaoks. Näiteks, kui teoreemis 1 tähistada kahte suvalist paarisarvu m ja n mõlemat kujul $m = 2k$ ja $n = 2k$, tekib arutluses viga, sest tekib seos $m = n$, mis suvaliste täisarvude korral ei kehti.
- Hüppeline üleminek tulemusele.

- Tulemust ennast kasutatakse tõestuse sees.

Tõestus alamjuhtude põhjal

Tegemist on meetodiga, kus väide tõestatakse kõigil võimalikel juhtudel.

Näiteks, kui teoreem väidab midagi kõikide täisarvude n kohta, siis võib vaadelda eraldi kahte juhtu: 1) n on paarisarv ja 2) n on paaritu arv. Kui teoreem väidab midagi kõigi reaalarvude kohta, on mõnikord abiks vaadelda kolme juhtu 1) $x < 0$, 2) $x = 0$ ja 3) $x > 0$.

Teoreem 3. Tõestada, et iga positiivse täisarvu n korral on $n^3 + n$ paarisarv.

Tõestus: Jaotame positiivsete arvude hulga omakorda positiivseteks paaris- ja paarituteks arvudeks ehk saame kaks alamjuhtu, mille jaoks tõestuse läbi viime.

a) Olgu n positiivne paarisarv ehk $n = 2k$, kus $k \in \mathbb{N}$. Kirjutades $n^3 + n = (2k)^3 + 2k = 8k^3 + 2k = 2(4k^3 + k) = 2p$, näeme, et $n^3 + n$ on paarisarv, sest $p = 4k^3 + k$ on positiivne täisarv.
b) Olgu nüüd n positiivne paaritu arv ehk $n = 2k + 1$, kus $k \in \mathbb{N}$. Kirjutades $n^3 + n = (2k + 1)^3 + (2k + 1) = 8k^3 + 12k^2 + 6k + 1 + 2k + 1 = 2(4k^3 + 6k^2 + 4k + 1) = 2r$, näeme jällegi, et $n^3 + n$ on paarisarv, sest $r = 4k^3 + 6k^2 + 4k + 1$ on positiivne täisarv. ■

Teoreem 4. Tõestada, et reaalarvude x ja y korral kehtib $|x + y| \leq |x| + |y|$.

Tõestus. Antud tõestuses vaatame nelja alajuhtu.

a) Olgu $x \geq 0$ ja $y \geq 0$. Siis $x + y \geq 0$ ning absoluutväärtuse definitsiooni kohaselt $|x + y| = x + y = |x| + |y|$.
b) Olgu $x \geq 0$ ja $y < 0$. Siin on edasise vaatluse all omakorda kaks alamjuhtu.
    a. Kui $x + y \geq 0$, siis $|x + y| = x + y < x + 0 < |x| + |y|$.
    b. Kui $x + y < 0$, siis $|x + y| = -(x + y) = (-x) + (-y) \leq 0 + (-y) = |y| \leq |x| + |y|$.
c) Olgu $x < 0$ ja $y \geq 0$. Selle juhu tõestus viiakse läbi analoogiliselt juhule b). (püüa see ise kirja panna!)
d) Olgu $x < 0$ ja $y < 0$. Siis absoluutväärtuse definitsiooni põhjal $|x + y| = -(x + y) = (-x) + (-y) = |x| + |y|$. ■

Kaudsed tõestuse meetodid

Vastuväiteline tõestus

Sageli juhtub, et otsene tõestus ei võimalda eesmärkideni jõuda kas siis detailide vähesuse tõttu või on eesmärgiks hoopis tõestada „negatiivne“ tulemus, s.t. näidata, et teatud omadus ei kehti või mõnda elementi ei leidu, jne. Sellisel juhul kasutatakse matemaatikas teoreemide tõestamisel sageli **vastuväitelist tõestusviisi**, mille aluseks on loogikaseadus: iga väite korral on tõene kas väide ise või selle eitus, kolmandat võimalust ei ole. Eelnevatest peatükkidest peab sulle olema meelde jäänud, et teoreemi pöördvastandlause on samaväärne originaalse

teoreemiga, ehk selleks, et tõestada $P \Rightarrow Q$, võime samaväärselt tõestada hoopis, et $\neg Q \Rightarrow \neg P$ ehk teisisõnu $(P \Rightarrow Q) \Leftrightarrow (\neg Q \Rightarrow \neg P)$. (Kui on meelest läinud, püüa seda samaväärsust tõeväärtustabeli abil uuesti näidata!).

Vastuväiteline tõestus ehk **absurdsusele taandamine** (lad. *reductio ad absurdum*) on kaudse tõestamise meetod, mille korral oletatakse, et väide on väär (ehk tõene on hoopis selle väite eitus), ning tehakse sellest oletusest järeldusi. Tõestus on edukas, kui jõuame vastuoluni kas teoreemi esialgse eeldusega või mõne teadaoleva tõega. Seega järeldame, et meie vastuväiteline oletus ei saa olla tõene ehk tõene saab olla vaid väide ise.

Vastuväitelist tõestust kasutatakse tihti siis, kui on vaja tõestada, et teatava omadusega objekti ei leidu või et teataval objektil ei ole teatavat omadust. Seega, kui esialgne väide sisaldab eitust, siis eitades eitust saame alustada sobivama eeldusega. Järelikult, vastuväitelise tõestusviisi korral tuleb osata lauseid eitada.

Kui teoreemide tõestamisel üldiselt alustatakse eeldusest ja jõutakse loogilise arutelu käigus väite tõesuseni, siis vastuväitelise tõestuse puhul toimub kogu protsess vastupidi.

Vastuväitelise tõestuse korral:

1) alustatakse väitest ja oletatakse, et tõestatav väide on väär;
2) viiakse läbi arutlus kasutades vajadusel aksioome või varem tõestatud teoreeme;
3) arutluse tulemusel jõutakse järelduseni, et väite eitamine on võimatu, sest viib vastuollu kas teoreemi eelduse või tuntud tõdedega;
4) tehakse kokkuvõte, et kuna väite eitus ei kehti, siis kehtib väide ise.

Teoreem 5. Kui kaks sirget a ja b on paralleelsed kolmanda sirgega c, siis need sirged a ja b on paralleelsed teineteisega.

Eeldus. $a \parallel c$ ja $b \parallel c$.

Väide. $a \parallel b$.

Tõestus (vastuväiteliselt). Eitame väidet ja oletame, et a ja b ei ole paralleelsed. Sellest oletusest järeldub, et need sirged peavad lõikuma mingis punktis P, sest tasandil kahe sirge kohta kolmandat võimalust ei ole. Sellisel juhul aga läbib punkti P kaks sirget, mis eelduse kohaselt on mõlemad paralleelsed sirgega c. See on aga vastuolus paralleelide aksioomiga, mis väidab, et väljaspool sirget asuvat punkti läbib ainult üks antud sirgega paralleelne sirge. Seega sirged a ja b ei saa lõikuda. Et kolmandat võimalust ei ole, siis järelikult $a \parallel b$. ■

Teoreem 6. Naturaalarvude hulgas ei ole suurimat elementi.

Eeldus: Vaadeldav hulk on naturaalarvude hulk.

Väide. Selles hulgas ei ole suurimat elementi.

Tõestus. Tõestame vastuväiteliselt. Oletame, et teoreemi väide ei pea paika ja on olemas niisugune arv N, et kõik ülejäänud naturaalarvud on sellest väiksemad. Vastavalt aksioomile on iga naturaalarvu n korral ka $n + 1$ naturaalarv. Seejuures on $n + 1$ suurem kui n. Seega leidub ka arvu N jaoks naturaalarv $N + 1$, mis on sellest suurem. See on aga vastuolus oletusega, et N on suurim naturaalarv. Järelikult ei saa olla suurimat naturaalarvu. ■

Teoreem 7. Kõik positiivsed täisarvud on huvitavad. ☺

Tõestus: Tõestame vastuväiteliselt ehk oletame, et leidub mittehuvitavaid arvusid. See tähendab, et mittehuvitavate arvude hulk ei ole tühi. Zermelo aksioomi (uuri välja, mis aksioom see on!) põhjal teame, et siis see hulk on täielikult järjestatav ja saame leida vähima mittehuvitava positiivse täisarvu. Aga nüüd on juba päris huvitav, et mis arv see selline on!? Kõige Esimene Mittehuvitav Arv?... Huvitav-huvitav! Seega saime vastuolu. ■

Väga tihti näeb vastuväitelise tõestuse kasutamist irratsionaalarvudega seotud väidete korral. Tuleta meelde, et ***ratsionaalarvuks*** nimetatakse arvu, mida saab kirjutada kujul $r = \frac{m}{n}$, kus m ja n on täisarvud ja $n \neq 0$. Näiteks $\frac{1}{3}$, $-7\frac{2}{5}$, 5 ja 0 on ratsionaalarvud. Reaalarvu, mida ei saa kirjutada kahe täisarvu suhtena, nimetatakse ***irratsionaalarvuks***. Kui reaalarve tähistada tähega $\mathbb{R}$ ja ratsionaalarve tähega $\mathbb{Q}$, siis irratsionaalarve tähistatakse tähega $\mathbb{I}$, kusjuures $\mathbb{I} = \mathbb{R} \setminus \mathbb{Q}$. Mõningase tööga peaksid sa olema võimeline tõestama, et arvud $\sqrt{7}$, π ja e^2 on kõik irratsionaalsed.

Teoreem 8. Kui α on irratsionaalarv, siis ka 3α on irratsionaalarv.

Tõestus. Viimast väidet on võimalik sõnastada eitavalt ehk soovime näidata, et 3α ei ole ratsionaalarv. Seega, oletame vastuväiteliselt, et 3α on tegelikult ratsionaalarv. Siis võime kirjutada $3\alpha = \frac{m}{n}$, kus m ja n on täisarvud ja $n \neq 0$. Jagades võrrandi mõlemad pooled läbi arvuga 3, saame $\alpha = \frac{m}{3n}$, kus jällegi nii nimetaja kui ka lugeja on täisarvud. Oleme näidanud, et α on sellisel juhul ratsionaalarv, mis on aga vastuolus meie esialgse eeldusega, et α on irratsionaalarv. Seetõttu meie eeldus, et 3α on ratsionaalarv, ei pea paika ja järelikult peab 3α olema irratsionaalarv. ■

Samaväärsete tingimuste tõestamine (Ekvivalentsi tõestus)

Alustame kahe väite samaväärsusega, loogikas tähistatud kui $A \Leftrightarrow B$ ning loetud kui „*A siis ja ainult siis kui B*“ või „*tingimus A on tarvilik ja piisav tingimuse B jaoks*“ või „*tingimus A on samaväärne tingimusega B*“. Lausearvutuse peatükis näitasime ka, et $A \Leftrightarrow B$ on loogiliselt samaväärne valemiga $(A \Rightarrow B) \wedge (B \Rightarrow A)$. Viimane kirjutusviis annab meile aga selliste teoreemide tõestamise strateegia.

Selleks, et tõestada, et väited A ja B on samaväärsed (ekvivalentsed), tuleb näidata, et kumbki väide järeldub teisest. Seega, tõestamaks teoreemi „A siis ja ainult siis, kui B“, peame kõigepealt näitama, et $A \Rightarrow B$ ning seejärel näitama, et $B \Rightarrow A$, kasutades kummalgi juhul mistahes sobilikku tõestamise meetodit.

Teoreem 9. Olgu a ja b täisarvud. Korrutis ab on paarisarv siis ja ainult siis, kui vähemalt üks arvudest a või b on paarisarv.

Arutelu. Kuna teoreemi sõnastuses esineb väljend „… siis ja ainult siis …“, tuleb meil tõestada kaks implikatsiooni. Kõigepealt tuleb näidata, et 1) Kui ab on paarisarv, siis vähemalt üks arvudest a või b on paarisarv, ning seejärel teistpidi, et 2) Kui vähemalt üks arvudest a või b on paarisarv, siis ab on paarisarv. Ilma üldsust kitsendamata võime eeldada, et a on paarisarv. Me võiksime tõestuse anda ka alamjuhtude kaudu, kus kõigepealt on a paarisarv ja seejärel on b paarisarv, aga need tõestused saavad olema täpselt ühesugused ja seega võime lihtsalt valida

ühe arvudest ja eeldada, et see on paarisarv. Teiseks märkame, et kui sooviksime esimese implikatsiooni tõestamisel kasutada otsese tõestamise meetodit, siis alustaksime eeldusega, et $ab = 2k$, kus k on mingi täisarv. Edasi oleks meil aga väga raske öelda midagi arvude a ja b kohta eraldi. Seega on esimese implikatsiooni juures vaja teistsugust tõestusmeetodit. Püüame nüüd selle teoreemi ära tõestada.

Tõestus. 1) Tõestame implikatsiooni ⇒ vastuväiteliselt. Selleks oletame, et mõlemad arvud a ja b on paaritud. Siis võime kirjutada, et $a = 2m + 1$ ja $b = 2n + 1$, kus $m, n \in \mathbb{Z}$. Saame $ab = (2m + 1)(2n + 1) = 4mn + 2m + 2n + 1 = 2(2mn + m + n) + 1$. Kuna $2mn + m + n$ on täisarv, oleme näidanud, et ab on paaritu arv.

2) Vastupidise implikatsiooni ⇐ näitamiseks oletame, et kas a on paarisarv või b on paarisarv. Üldsust kitsendamata eeldame, et a on paarisarv ja seega kirjutatav kujul $a = 2k$, kus $k \in \mathbb{Z}$. Nüüd $ab = (2k)b = 2(kb)$ ja kuna $kb \in \mathbb{Z}$, oleme näidanud, et ab on paaris. ■

Konstruktiivne ehk olemasolu tõestus

Vaatleme nüüd selliseid tõestamise meetodeid, mida esitatakse kujul „ $\exists x$, mille korral $P(x)$“. Sellised teoreemid tagavad, et eksisteerib vähemalt üks x mille korral tingimus (omadus) $P(x)$ on õige. Sellist tõestust nimetatakse ***konstruktiivseks.***

Konstruktiivne tõestus sisaldab sellise x leidmist, mille korral $P(x)$ on tõene. See võib tähendada ka algoritmi koostamist sellise x leidmiseks. Aga võib ka juhtuda, et olemasolevate tulemuste baasil on võimalik loogilise arutlemise teel otsitava objekti eksisteerimine kindlaks teha ilma seda objekti otseselt leidmata. Näiteks peaks sulle tuntud olema teoreem, mis väidab, et igal paaritu astmelisel reaalarvuliste kordajatega polünoomil on vähemalt üks reaalne lahend, aga me ei tea, kuidas iga sellise polünoomi korral seda lahendit leida. David Hilbert kasutas oma loengutes olemasolu tõestuse idee illustreerimiseks järgmist näidet:

> *Siin klassis on vähemalt üks üliõpilane … olgu ta nimi 'X'… kelle kohta kehtib järgmine väide: Mitte ühelgi teisel üliõpilasel siis klassis ei ole rohkem juukseid peas kui üliõpilasel X. Kes see üliõpilane on? Seda ei saa me kunagi teada, aga tema olemasolus saame me absoluutselt kindlad olla.*

Näide 1. Tõestada, et leidub täisarv, mille ruut on 81.

Tõestus: Selleks arvuks sobib 9, sest $9 * 9 = 81$.

Näide 2. Tõestada, et leidub lausearvutuse valem, millest järeldub sama valemi eitus.

Tõestus. Vaatleme valemit $X \wedge \neg X$. Tõeväärtustabeli põhjal on valem $X \wedge \neg X \Rightarrow \neg(X \wedge \neg X)$

X	X	$\wedge$	$\neg$	X	$\Rightarrow$	$\neg$	$(X$	$\wedge$	$\neg$	$X)$
t		v	v		**t**	t		v	v	
v		v	t		**t**	t		v	t	

samaselt tõene. Seega valemist $X \wedge \neg X$ järeldub valem $\neg(X \wedge \neg X)$. See tähendab, et valem $X \wedge \neg X$ on vajaliku omadusega.

Näide 3. Leiduvad positiivsed reaalarvud x ja y, mille korral $\frac{1}{2}(x + y) \leq \sqrt{xy}$.

Lahendus. Valime $x = y = 5$. Sellisel juhul $\frac{1}{2}(x + y) = 5 = \sqrt{xy}$. Kahe avaldise võrdumine on parim, mida me teha saame, sest ei kehti $\frac{1}{2}(x + y) < \sqrt{xy}$.

Näide 4. Leiduvad reaalarvud a ja b nii, et $(a + b)^2 = a^2 + b^2$.

Lahendus. Olgu $a, b \in \mathbb{R}$ sellised, et $(a + b)^2 = a^2 + 2ab + b^2 = a^2 + b^2$. Sellisel juhul $2ab = 0$. Üks võimalik lahend oleks $a = 1$ ja $b = 0$, sest siis $(a + b)^2 = (1 + 0)^2 = 1^2 = 1^2 + 0^2 = a^2 + b^2$.

Matemaatikud, olles huvitatud seostest ja seaduspärasustest, kalduvad tihti otsima mingite kindlate omadustega objekte, kas siis lihtsast uudishimust või vajadusest. Näiteks võivad nad küsida, et kas leiduvad täisarvud a, b ja c nii, et $a + b + c = 3$ ja $a^3 + b^3 + c^3 = 3$, lisaks triviaalsele lahendusele $a = b = c = 1$? Või, kui tasandil on antud kaks suvalist ristkülikut, siis kas leidub selline sirge, mis jagab nende mõlema pindala täpselt pooleks? Tuleb välja, et mõlemale küsimusele saab jaatavalt vastata. Kas sa suudad lahenduse leida?

Pinnapealselt vaadatuna tundub, et olemasolu tõestusi on kergem teha kui muid tõestusi. Tuleb ju konstruktiivse tõestuse korral vaid üks teatud omadustega objekt leida ja vajadust pole tõestada, et mingi omadus kehtib hulga kõigi elementide jaoks. Sageli on aga selle ühe objekti leidmine väga raske. Sajandeid tagasi püstitas Euler hüpoteesi, et kolme täieliku neljanda astme arvu summa ei ole kunagi võrdne mõne muu arvu neljanda astmega. Aga aastal 1986 (arvutite ajastul!) Lükkas Noam Elkies Euleri väite ümber näidates, et

$$2682440^4 + 15365639^4 + 18796760^4 = 20615673^4.$$

Oletused ehk hüpoteesid

Üks põnevamaid asju, mida matemaatikaga teha saab, on otsida ja avastada uusi tulemusi. Seda pole aga kerge teha ja veelgi raskem on anda täpseid juhiseid, kuidas selline protsess toimuma peaks. Seoste ja mustrite leidmine on kunst, samamoodi nagu viljakate küsimuste küsimine. Üle lihtsustades võiks öelda, et edukad matemaatikud kombineerivad hoolsa uute ideede uurimise oma hästi väljakujunenud sisetundega saavutamaks uusi veetlevaid matemaatilisi tulemusi.

Vaatame järgmist täiuslike ruutude jada

0, 1, 4, 9, 16, 25, 36, 49, 64, 81, 100, 121, 144, 169, 196, 225, 256, 289, 324, 361, 400

ja hakkame otsima mõnda kena seost nende arvude vahel. Näiteks võid sa märgata (või eelnevalt teada), et kahe täiusliku ruudu summa on alati täiuslik ruut, näiteks nagu $64 + 225 = 289$. Nüüd võiksime aga küsida, et kas kahe täiusliku ruudu summa on võrdne mõne teiste täiuslike ruutude summaga? Aga mis juhtub, kui korrutada täiuslikku ruutu arvuga 2?

Tuleb välja, et selline arv pole ise kunagi täiuslikuks ruuduks, küll aga võib olla täiuslikule ruudule väga lähedal, nagu näiteks $2 * 25 = 50 = 49 + 1$ või $2 * 144 = 288 = 289 - 1$. Esitame oma leiud tabelina, et kergendada mustrite ja seoste leidmist.

$2m^2 = n^2 \pm 1$	m	n
$2 * 1 = 1 + 1$	1	1
$2 * 4 = 9 - 1$	2	3
$2 * 25 = 49 + 1$	5	7
$2 * 144 = 289 - 1$	12	17
$2 * 841 = 1681 + 1$	29	41

Tabelist märkame mitu toredat seost. Näiteks, igas reas liites m ja n väärtused, saame m väärtuse järgmises reas. Proovi nüüd ise teha veel vähemalt kolm oletust erinevate seoste ja mustrite kohta samas tabelis. Oma tähelepanekute põhjal oleta järgmise kahe rea väärtused ning kontrolli oma oletusi.

Pane tähele, et meie huvitav uurimus algas lihtsalt arvude ruutu tõstmisest, kuid siis küsisime hea küsimuse, et 'mis juhtub, kui me täiuslikke ruute kahega korrutame', ja noppisime hulga vilju oma hästi organiseeritud tabelist. Sellised sammud ja tegemised kirjeldavad üpris hästi teed uute tulemuste avastamiseni.

Intrigeerivad oletused meelitavad ligi palju matemaatikuid ning tavaliselt leiavad need oletused kiiresti ka tõestuse või kontranäite. Vahetevahel aga juhtub, et mõned oletused püsivad tõestuseta palju aastaid kuni uuem ja võimsam meetod või tõeliselt geniaalne idee need ara suudab lahendada. Üks kuulsamatest sellelaadsetest näidetest üldistab meie arvude ruutu tõstmise ideed ja väidab, et leiduvad täisarvud a, b ja c nii, et $a^2 + b^2 = c^2$. Esitame nüüd intrigeeriva küsimuse: Kas sarnane seos arvude a, b ja c vahel kehtib ka kõrgemate astendajate korral? See tähendab, et kas leiduvad täisarvud a, b ja c nii, et $a^3 + b^3 = c^3$ või $a^4 + b^4 = c^4$, jne? Aastal 1637 tegi Pierre de Fermat oletuse, et arvust 2 suuremate astendajate puhul selline seos ei kehti, kuid suutis selle tõestada vaid neljanda astme jaoks. Rohkem kui sajand hiljem näitas Euler, et see seos ei kehti ka kuupide korral. Seejärel võttis aega kuni aastani 1990, mil Wiles koos teiste matemaatikutega tõestas „Fermat' viimase teoreemi" näidates oletuse kehtivust kõigi täisarvuliste astendajate korral.

Veel üks kuulus hüpotees oli Francis Guthrie poolt 1852. a. välja pakutud nelja värvi probleem, mis küsis, et kas iga maakaart on värvitav nelja värviga nii, et naabermaad on eri värvi. Guthrie püüdis ise Inglismaad värvida. Mitmed tolle aja kuulsad matemaatikud tegelesid selle probleemiga ja jõudsid hüpoteesi sõnastamiseni, et seda on võimalik teha. Tõestus tuli aga alles aastal 1976 Kenneth Appeli ja Wolfgang Hakeni poolt kasutades arvutite abi. Nüüdseks on seega see hüpotees tõestatud ja temast on saanud teoreem.

Ümberlükkamised ehk kontranäited

Tihti aga osutuvad oletused vääraks. Kui see väär oletus sisaldab väidet kõigi antud hulka või klassi kuuluvate elementide kohta, siis tuleb leida vaid üks näide, mille korral tulemus ei kehti. Seega tuleb leida kontranäide.

Näide 5. Tõestada, et järgmine väide pole tõene:

$$\forall a,b \in R \text{ korral , kui } a < b \text{ siis ka } a^2 < b^2 .$$

Lahendus. Piisab leida vaid üks paar arve a ja b, mille korral väide ei kehti. Valime selleks $a = -2$ ja $b = -1$. Siis $a < b$, sest $-2 < -1$, kuid $a^2 > b^2$, sest $(-2)^2 > (-1)^2$. Sellega on väide ümber lükatud.

Näide 6. Tõestada, et järgmine väide pole tõene:

$$\forall n \in \mathbb{N}, \text{ kui } n \text{ on algarv, siis } 6n + 1 \text{ on algarv.}$$

Lahendus. Kontranäite leidmiseks eitame kõigepealt antud väidet: $\exists n \in \mathbb{N}$, kui n on algarv, siis $6n + 1$ ei ole algarv. Seega peame järjest läbi proovima kõik algarvud ja leidma sellise algarvu

n, mille korral $6n + 1$ ei ole algarv. Kannatlik töö viib sihile ja leiame, et $n = 19$ on selline algarv, mille korral $6n + 1 = 6 \cdot 19 + 1 = 115$ ei ole algarv.

Näide 7. Tõestada, et järgmine väide pole tõene:

$$\text{Kui } \alpha \text{ on reaalarv, siis } \tan^2 \alpha + 1 = \sec^2 \alpha.$$

Lahendus. Kuna $\tan \alpha$ ja $\sec \alpha$ pole kumbki määratud punktis $\alpha = \frac{\pi}{2}$, siis sellel punktis neil väärtused puuduvad ja seega ei saa ka antud avaldis punktis $\frac{\pi}{2}$ kehtida. Seega, $\alpha = \frac{\pi}{2}$ on kontranäide antud avaldisele.

Miks õpetada tõestamist?

Newtoni kohta räägitakse järgmist lugu. Noore üliõpilasena alustas ta geomeetria õppimist Eukleidese „Elementide“ lugemisest (nagu see tol ajal tavaline oli). Ta luges teoreeme, nägi, et need olid õiged ning jättis tõestused vahele. Ühtlasi ta imestas, miks peaks keegi sedavõrd ilmsete asjade tõestamisega nii palju vaeva nägema. Palju aastaid hiljem ta aga muutis oma seisukohta ja kiitis Eukleidest väga.

Miks peame õppima või õpetama tõestusi? Esimeseks vastuseks sellele küsimusele on muidugi tüüpiline väide, et tõestused on kesksel kohal matemaatikas ja seetõttu pole võimalik neid vältida ka matemaatikat õppides ja õpetades. Milleks matemaatikud üldse oma tulemusi tõestavad ja kolleegide tõestusi uurivad? Üheks põhjuseks on muidugi tulemuste üle kontrollimine − tõestus veenab meid väite paikapidavuses, st vastab küsimusele, „Kas on tõene?“. See ei ole matemaatikule aga ainuke ja kõige olulisem põhjus. Isegi professionaalsed matemaatikud on ilmselt valmis uskuma tarkades raamatutes või teadusajakirjades esitatud väiteid ilma tõestuseta. Miks nad siis ikkagi kolleegide tõestuskäike uurivad? Tähtsamaks põhjuseks on pigem selgitamine − tõestus viib meid sisulisele arusaamale väite olemusest, vastab küsimusele, „Miks on väide tõene?“. Ka matemaatikuid endid huvitab eelkõige just see aspekt ning küsimus „Miks?“, mitte pelgalt tõesuse konstateerimine ise. Lisaks aitab tõestus süstematiseerida, ta seob erinevaid teadmisi ühtseks terviklikuks deduktiivseks arutlusahelaks, andes sel moel edasi intuitiivselt tajutud tõde. Sageli just selle funktsiooni kaudu tajumegi matemaatika ilu ja näeme seal kehtivaid seoseid.

Näpunäiteid tõestuse kirjutamiseks

Hea tõestuse kirjutamine eeldab harjutamist ja juhiste järgimist. Tuleb endale selgeks teha kehtivad tavad, kasutada sümboleid ja märgistusi korrektselt, kohaneda uue sõnavaraga, harjutada erinevaid tõestusmeetodeid, olla enda suhtes rangem ja nõudlikum, jne. Kõik see on saavutatav, kui sa seda soovid.

Iga tõestuse selgrooks on täiuslik „vettpidav“ argument. Kuna matemaatilised meetodid selle eesmärgi saavutamiseks sõltuvad etteantud probleemist, siis arutleme range tõestuse üle igal juhul eraldi. Siiski saame juba praegu öelda midagi tõestuses kasutava detailide rohkuse üle. Üldine reegel ütleb, et peaksid kasutama piisaval hulgal detaile ja seletusi tõestuse iga sammu näitamisel, aga ei tohi detailidega ka üle pingutada, et lugejale koormavaks muutuda. Tõestuse kirjutamine on nagu luuletuse kirjutamine, kus hea poeet oskab öelda kõik mis vaja nii väheste sõnadega kui võimalik.

On mitmeid erinevaid võimalusi lühemate tõestuste saavutamiseks. Kindlasti aitab kaasa teadmine matemaatika sümbolitest ja keelest. Selle asemel, et öelda *„Olgu x hulga A_1 või A_2 või A_3 element, välja arvatud see, et me ei taha, et x=0“* võime kohe kirjutada *„Olgu* $x \in (A_1 \cup A_2 \cup A_3) - \{0\}$." On muidugi ka kartus minna teise äärmusesse ja liiga vähe kirjutada, kuid algajatel matemaatikutel nagu sina seda probleemi väga tihti ei juhtu. Kui võimalik, ehita oma tõestus üles olemasolevatele tulemustele, selle asemel, et iga olemasolevat tulemust jälle uuesti tõestada. Samuti, kui mitmes kohas tõestuse sees kasutatakse sarnast arutelu, siis pole vaja iga kord kõiki detaile välja tuua. Pigem ütle „Sarnaselt eelmisele juhule järeldub…“ või „Samamoodi võime väita, et …“. Ning lõpetuseks, selleks, et paberile kirja panna kena tõestus, tuleb see ka matemaatiliselt hästi läbi mõelda. Ilusad matemaatilised tulemused väärivad ilusalt esitatud tõestusi.

Veel mõningaid soovitusi hea stiili omandamiseks:

1) Liigenda oma tõestus sobiva pikkusega lõikudeks. Ei ole kohustuslik, et sa tõestuse alguses uuesti ütled, mida tõestada tuleb, aga kui sa seda teed, siis muudab see tõestuse kindlasti paremini loetavamaks. Sinu sõnastus peab selgelt väljendama, et väide tahab alles tõestamist, kirjutades näiteks, *„Meil on vaja näidata, et* $A \cap B \subseteq A \cup B$“, selle asemel, et lihtsalt öelda *„Hulkade A ja B jaoks kehtib* $A \cap B \subseteq A \cup B$“, nagu oleks see väide juba tõestatud. Järgmise lausena oleks alati hea anda väike suunajuhis, millise strateegia järgi sa seda väidet tõestama hakkad, näiteks „*Selleks näitame, et kui* $x \in A \cap B$, *siis* $x \in A \cup B$.“
2) Kasuta oma matemaatilise kirjakeele rikastamiseks võimalikke sünonüüme. Näiteks sõna *'tõestama'* asemel kasuta sõnu *'näitama', 'põhjendama', 'argumenteerima'*, jne. Samuti on hea, kui sul on tagavaraks alternatiivid sõnale *'seega'*. Võimalikud sünonüümid oleksid *'järelikult', 'niisiis', 'seetõttu', 'tähendab'*, jt.
3) Matemaatilistes tekstides kasutatakse sõna 'mina' asemel sõna 'meie'. Kuna matemaatilise teksti lugemine peaks olema aktiivne tegevus ja mitte passiivne, siis kasutades sõna 'meie' püüab autor kaasata ka lugejat tõestuse tegemise juurde.
4) Ära alusta lauseid sümboliga või matemaatilise valemiga. Eelista kirjutada „Võrrand $x^2 + 2x - 2 = 0$ on oluline, sest …“, selle asemel, et kirjutada „$x^2 + 2x - 2 = 0$ on oluline, sest …“. Sarnaselt, kirjuta *„Me teame, et n ei ole algarv, sest n on paarisarv ja* $n \geq 4$“ selle asemel, et kirjutada „*n ei ole algarv, sest n on paarisarv ja* $n \geq 4$“.
5) Tõestuses eriti olulised matemaatilised avaldised tuleks kirjutada eraldi reale suurema tähelepanu, aga ka selguse saamiseks. Näiteks esita järgmine avaldis omaette real
$$\bigcap_{r \in J} B_r = \{x \mid -1 < x \leq 0\}$$
selle asemel, et ta teksti sisse peita.
6) Tõestuse lõppu võib kirjutada fraase *„ …., nagu oligi soovitud näidata“, „ …, mis oligi meie eesmärgiks“* või lihtsalt *„Sellega on tõestus lõpetatud.“* Traditsiooniliselt lisavad matemaatikud ka tõestuse lõppu sümboli, et visuaalselt eraldada tõestus ülejäänud tekstist ja edasisest diskussioonist. Populaarseteks sümboliteks on 'QED' (ladina keelsest väljendist *quod erat demonstratum* ehk *'mida oligi tarvis tõestada'*), täidetud ■ või täitmata □ ruut.