

Anna-Maija Partanen

Antti Rasila

Mika Setälä

Vapaa matikka 11

MAA11 - Lukuteoria ja logiikka

Avoimet oppimateriaalit ry



Sisältö on lisensoitu avoimella CC BY 3.0 -lisenssillä.

LUKUTEORIA JA LOGIIKKA

”How often have I said to you that when you have eliminated the impossible, whatever remains, *however improbable*, must be the truth?” – Sherlock Holmes¹

SISÄLTÖ

1. Logiikka ja päättely (esimerkit ja tehtävät lisämateriaalia)	3
Tehtäviä	7
2. Loogiset lauseet	10
2.1. Atomilauseet, konnektiivit ja totuusarvot	10
Tutkimustehtävä	10
Tehtäviä	15
2.2. Implikaatio ja ekvivalenssi	22
Tutkimustehtävä	22
Tehtäviä	27
2.3. Monimutkaisempia loogisia rakenteita	31
Tutkimustehtävä	31
Tehtäviä	35
3. Logiikka ja matematiikka	39
3.1. Joukko-oppia (mahdollisesti lisämateriaalia)	39
Tutkimustehtävä	39
Tehtäviä	45
3.2. Avoin lause ja konnektiivien joukko-opillinen tulkinta.	50
Tutkimustehtävä	50
Tehtäviä	55
3.3. Kvanttorit	59
Tutkimustehtävä	59
Tehtäviä	63

Date: 20. joulukuuta 2012.

¹The Sign of the Four (1890), Chap. 6, p. 111

4. Matemaattisen väitteen todistaminen	66
Tutkimustehtävä	66
Tehtäviä	70
5. Johdanto lukuteoriaan	72
5.1. Jaollisuus ja jakojäännös	72
Tutkimustehtävä	72
Tehtäviä	75
5.2. Kongruenssi	79
Tutkimustehtävä	79
Tehtäviä	84
5.3. Kongruenssin sovelluksia	88
Tehtäviä	91
5.4. Luonnolliset luvut ja induktioperiaate (lisämateriaalia)	93
Tutkimustehtävä	93
Tehtäviä.	98
6. Lukuteorian tuloksia	102
6.1. Suurin yhteinen tekijä ja Eukleideen algoritmi	102
Tutkimustehtävä	102
Tehtäviä	105
6.2. Diofantoksen yhtälöt	107
Tutkimustehtävä	107
Tehtäviä	114
6.3. Alkuluvut ja aritmetiikan peruslause	116
Tutkimustehtävä	116
Tehtäviä	126
7. Harjoitustehtävien ratkaisuja	130
8. Looginen algebra ja Boolean algebra (Lisämateriaalia)	131
8.1. Looginen algebra	131
Tehtäviä.	133
8.2. Boolean algebra	134
Tehtäviä.	136

1. LOGIIKKA JA PÄÄTTELY (ESIMERKIT JA TEHTÄVÄT LISÄMATERIAALIA)

Logiikka on tieteenala, joka tutkii päättelyä ja ajattelua. Erityisesti logiikassa tutkitaan *deduktiivista* päättelyä. Deduktiivista päättelyä tutki ensimmäisenä kreikkalainen filosofi Aristoteles (384 eaa. – 322 eaa.), jonka mukaan deduktio etenee yleisestä erityiseen. Esimerkki Aristoteleella esiintyvistä päätelmistä on seuraava:

- | | |
|-------|---------------------------|
| (1) | Ihmiset ovat kuolevaisia. |
| (2) | Sokrates on ihminen. |
| <hr/> | |
| (3) | Sokrates on kuolevainen. |

Esimerkissä rivit (1) ja (2) ovat päätelmän *oletuksia* ja rivillä (3) on päätelmän *johtopäätös*. Johtopäätös erotetaan yleensä viivalla. Deduktiivinen päättely on *loogisesti pätevää* eli tosista oletuksista tehtyjen päättelyiden johtopäätökset ovat tosia kaikissa (todellisissa ja kuviteluissa) tilanteissa.

Toista usein esiintyvää päättelymenetelmää kutsutaan filosofiassa *induktiopäätteleyksi*. Aristoteleen mukaan induktio etenee erityisestä yleiseen. Induktiopäätteleyä käytetään usein arkiajattelussa, vaikka se ei ole loogisesti pätevää. Esimerkki induktiopäätelmästä on seuraava:

- | | |
|-----|---|
| (1) | Kaikki tunnetut joutsenet ovat valkoisia. |
| (2) | Kaikki joutsenet ovat valkoisia. |

Tämä päättely ei säilytä väitteiden totuutta, koska on olemassa myös mustia joutsenia². Niitä ei kuitenkaan tunnettu Euroopassa ennen Australian löytämistä, joten siihen asti päättelyn oletusta (1) on voinut pitää totena. Silti johtopäätös (2) ei ole tosi.

Aristoteleen tekemä jako deduktiivisiin ja induktiivisiin päättelyihin ei ole enää nykypäivänä täysin toimiva. Toisaalta tämä johtuu induktiopäätteleyyn liittyvistä ongelmista, toisaalta siitä, että esimerkiksi tilastollisia päättelymenetelmiä ei ole helppo luokitella tällä tavoin. Filosofissa tutkitaan deduktion ja induktion lisäksi myös niin kutsuttuja *abduktiivisia* päättelyjä. Lisämateriaalina olevassa kappaleessa 5.4 esitellään *matemaattinen* eli *täydellinen induktio*, jota ei pidä sekoittaa filosofissa esiintyvään induktiopäätteleyyn.

Deduktiivista päättelyä on mahdollista soveltaa monenlaisissa tilanteissa. Merkittävä deduktiivisen päättelyn sovellus on matemaattinen

²Mustajoutsen (*Cygnus atratus*) on australialainen vesilintu.

todistaminen, jota tutkivaa logiikan osa-aluetta sanotaan joskus *matemaattiseksi logiikaksi* erotuksena yleisemmin päättelyjä ja ajattelua tutkivasta *filosofisesta logiikasta*. Nykyään tärkeä logiikan sovelluskohde on tietotekniikka, joten logiikkaa tutkitaan myös teoreettisen tietojenkäsittelytieteen osana. Tässä kurssissa keskitytään ensisijaisesti matemaattiseen logiikkaan.

Esimerkki 1. Ovatko seuraavat päättelyt loogisesti päteviä? Perustele.

- (1) Kaikki örjyt ovat nouvareita.
- a) (2) Mikään surjimus ei ole nouvari.
- (3) Mikään surjimus ei ole örjy.
- (1) Kuusi on puu.
- b) (2) Näre on puu.
- (3) Näre on kuusi.
- (1) Kaikki kohtaamani joulupukit ovat olleet tavallisia ihmisiä,
- c) jotka ovat vain pukeutuneet joulupukiksi.
- (2) Oikeaa joulupukkia ei ole olemassa.

Ratkaisu:

a) On. Jos jokin surjimus olisi örjy, niin silloin se oletuksen (1) nojalla olisi myös nouvari. Mutta oletuksen (2) mukaan mikään surjimus ei ole nouvari. Siis ei ole mahdollista, että jokin surjimus olisi örjy.

b) Ei. Vaikka kuusi ja näre ovat molemmat puita, niin ei siitä tarvitse seurata, että näre on kuusi. Itse asiassa näre tarkoittaa nuorta kuusta, mutta tämä on kielellinen sopimus. Logiikka ei suoraan ota kantaa sanojen merkityksiin. Vaikka väite on sinällään tosi, niin se ei seuraa oletuksista ja siksi päättely ei ole loogisesti pätevä.

c) Ei. Kyseessä on induktiivinen päättely, joka ei ole loogisesti pätevä.

Vastaus:

a) on, b) ei, c) ei.

Esimerkki 2. Ovatko seuraavat päättelyt loogisesti päteviä? Perustele.

- a) Kaikki ajavat joskus ylinopeutta, joten pienestä lipsahduksesta ei tarvitse antaa rangaistusta.
- b) Pariisin tiedeakatemia professorit julistivat, että meteoriitteja ei ole olemassa, koska taivaalla ei ole kiviä. Siis meteoriitteja ei ole olemassa³.

³Pariisin tiedeakatemia julisti vuonna 1772 kuuluisan kemistin Lavoisier'n johdolla, että löydetty meteoriitit ovat maanpäällisiä kiviä, joihin salama on iskenyt, ja kivien putoaminen taivaasta on fyysikaalisesti mahdotonta. Vielä vuonna 1790 tiedemies Berthollet julisti Barbotaniin pudonneen meteoriitin olevan valitettava osoitus kansanuskomusten ja satujen kyvystä ottaa valtaansa kokonainen kaupunki. Nämä

- c) Lingvistiikan professori Miettisen mukaan Suomen voimassaolevat ravintoainesuositukset eivät perustu uusimpiin tutkimustuloksiin. Ongelmia on erityisesti rasvojen käyttöä koskevissa suosituksissa. Siis Suomen nykyiset ravintoainesuositukset ovat vanhentuneet.
- d) Tunnettu pikkurikollinen Lipa Luihu nähtiin lauantai-iltana rautatieasemalla. Samana iltana varastettiin Urho Kestävän maastopyörä aseman pyörätelineestä. Siis Luihu oli varastanut Kestävän pyörän.
- e) Kolme prosenttia ihmisistä on nähnyt lentävän lautasen. Siis lentäviä lautasia on olemassa.

Ratkaisut:

a) Kysymyksessä oleva päättely on virheellinen, koska se vetoaa sääntöjen rikkojien määrään eikä kyseisen rikkomuksen olosuhteisiin. Se, että useimmat ihmiset toimivat tai ajattelevat jollakin tavalla, ei logiikan mielessä todista mitään, koska enemmistö voi olla väärässä.

Tätä päättelyvirhettä kutsutaan filosofiassa nimellä *argumentum ad populum* eli vetoaminen lukumäärään. Yleisimmin se esiintyy yleiseen mielipiteeseen tai toimintatapaan vetoavissa johtopäätöksissä. Joskus vedotaan myös pienemmän mutta ylivertaisten joukon näkemykseen, esimerkiksi: ”Kaikki ne, jotka oikeasti osaavat ajaa autoa, ajavat joskus ylinopeutta.” Myös tämä päättely on virheellinen.

b) Vaikkakin Pariisin tiedeakatemia edusti 1700-luvun parasta asiantuntemusta, myös asiantuntijat voivat olla väärässä. Lisäksi luonnon-tieteelliset tulokset eivät ole koskaan logiikan mielessä todistettuja ja mahdollisuus virheeseen on suuri erityisesti uusien ja mullistavien löydösten kohdalla.

Tieteellisessä menetelmässä kuitenkin pyritään siihen, että esitetyt väitteet ovat *falsifioituvia*. Ne voidaan kokeella tai havainnolla osoittaa vääräksi, kuten tässä tapauksessa tapahtuikin. Siksi tieteellinen tieto on itsensä korjaavaa ja lukuisissa koetilanteissa testattuja teorioita voidaan pitää käytännössä hyvin luotettavina, joten vetoaminen asiantuntijan näkemykseen on hyväksyttävää argumentaatiota. Tällöin tulisi kuitenkin ensisijaisesti vedota asiantuntijoiden esittämiin perusteluihin eikä heidän asemaansa tai lukumääräänsä. Pelkästään useimpien asiantuntijoiden mielipiteeseen vetoava argumentti on tiukasti tulkittuna virhepäätelmä (katso a-kohta).

kriittiset kommentit johtivat siihen, että monet museot poistivat kokoelmistaan meteoriitteja väärennöksinä. Vasta vuonna 1803 Jean-Baptiste Biot’n uraauurtava tutkimus L’Aiglen meteoriitista johti meteoriittien alkuperän selviämiseen ja niiden yleiseen hyväksyntään tiedepiireissä. Lähde: Lindsay, E. M., Maskelyne and Meteors, Irish Astronomical Journal, vol. 8(3), p. 69, 1967.

c) Professori Miettinen ei ole ravitsemustieteen asiantuntija, joten hänen mielipidettään ei voida pitää asiantuntijan näkemyksenä. Kysymyksessä on virheellinen argumentti, josta käytetään filosofiassa myös nimitystä *argumentum ad verecundiam* eli vetoaminen väärään auktoriteettiin. Lisäksi vetoaminen edes oikean asiantuntijan näkemykseen ei koskaan ole logiikan mielessä pätevä päättely.

d) Päättely ei ole logiikan mielessä pätevä eikä myöskään hyväksyttävää argumentaatiota, koska päättely perustuu ensisijaisesti Lipa Luihun henkilökohtaisiin ominaisuuksiin eikä itse rikokseen liittyviin havaintoihin. Tällaisesta päätelmästä käytetään filosofiassa nimitystä *argumentum ad hominem* eli argumentoiminen henkilöä vastaan.

Juridiikassa esimerkiksi tietoa henkilön aikaisemmasta rikoshistorias-
ta pidetään kuitenkin hyväksyttävänä aihetodisteena eli todisteena,
jonka perusteella syyllisyyttä voidaan pitää todennäköisenä, vaikka se
ei suoraan osoitakaan syyllisyyttä.

e) Tämä päättely on logiikan mielessä pätevä, vaikka harvat asiantuntijat pitävät johtopäätöstä oikeana. Vika ei kuitenkaan ole päättelyssä vaan oletuksessa, jonka mukaan kolme prosenttia ihmisistä on nähnyt lentävän lautasen. Tällaisia havaintoja ei voida pitää kovin luotettavina, koska ihmiset saattavat tehdä virheellisiä havaintoja tai tarkoituk-
sellisesti vääristellä totuutta.

Vastaukset:

a) ei, b) ei, c) ei, d), ei, e) on (varauksin).

Tehtäviä.

- (1) Onko päättely loogisesti pätevä? Perustele.
 - a) Kaikki ihmiset ovat kuolevaisia. Lasse-kissa on kuolevainen. Siis Lasse-kissa on ihminen.
 - b) Kaikki koirat osaavat haukkua. Halli on koira. Siis Halli osaa haukkua.
- (2) Ovatko seuraavat päättelyt loogisesti päteviä? Perustele.
 - (1) Kaikki tetraedrit ovat pyramideja.
 - a) (2) Jotkut kartiot ovat tetraedreja.
 (3) Jotkut kartiot ovat pyramideja.
 - (1) Kaikki sylinterit ovat lieriöitä.
 - b) (2) Mikään lieriö ei ole kartio.
 (3) Jotkut sylinterit ovat kartioita.
 - (1) Luku 345 päättyy numeroon 5.
 - c) (2) Nollaan päättyvä luku on viidellä jaollinen.
 (3) Luku 345 on viidellä jaollinen.
- (3) Onko seuraava päättely loogisesti pätevä? Perustele.
 - a) Jos ulkona on pakkanen, menen hiihtämään. Ulkona ei ole pakkanen. Siis en mene hiihtämään.
 - b) Jos ulkona on pakkanen, menen hiihtämään. En mene hiihtämään. Siis ulkona ei ole pakkanen.
 - c) Jos tiedän nukkuvani, niin nukun. Jos tiedän nukkuvani, niin en nuku. Siis en tiedä nukkuvani.
- (4) Tutkitaan polynomia

$$P(x) = x^5 - 10x^4 + 35x^3 - 50x^2 + 25x.$$

- a) Laske $P(0)$, $P(1)$, $P(2)$, $P(3)$ ja $P(4)$.
- b) Mitä voit sanoa luvuista $P(n)$, kun n on luonnollinen luku?
- c) Testaa päätelmäsi kokeilemalla myös muilla luonnollisilla luvuilla esimerkiksi laskinta käyttäen.
- (5) Arkiajattelussa käytetään usein ajattelumalleja, jotka eivät ole loogisesti perusteltavissa. Mikä virhe on seuraavissa päätelmissä?
 - a) Ilta Sanomien kyselyssä 66% vastaajista uskoo maan ulkopuoliseen elämään. Maan ulkopuolista elämää on olemassa.
 - b) The Sunday Times -lehden haastattelussa kuuluisa tiedemies Stephen Hawking totesi pitävänsä lähes varmana, että avaruudessa on maan ulkopuolista älykästä elämää. Maan ulkopuolista elämää on olemassa.
 - c) Tiedemiehistä 90% väittää, että nykyinen ilmastonmuutos on ihmisen aiheuttamaa eikä johdu maapallon lämpötilan luontaisesta jaksollisuudesta. Siis nykyinen ilmastonmuutos on ihmisen aiheuttamaa.

- d) Televisiouutisissa kerrottiin, että toisen maailmansodan aikainen holokausti oli vain liittoutuneiden propagandaa. Siis holokaustia ei tapahtunut toisen maailmansodan aikana.
- (6) Ovatko seuraavat päättelyt loogisesti päteviä? Perustele.
- (1) Kaikilla x toteutuu y .
 - a) (2) Joillakin z toteutuu x .

(3) Joillakin z toteutuu y .
 - (1) Kaikilla A toteutuu B .
 - b) (2) C toteuttaa B :n.

(3) C toteuttaa A :n.
 - (1) Kaikilla A toteutuu B .
 - c) (2) Millään C ei toteudu B .

(3) Millään C ei toteudu A .

Kotitehtävät.

- (1) Ovatko seuraavat päättelyt päteviä? Perustele.
- (1) Kaikki kissat osaavat kehrätä.
 - a) (2) Tämä eläin osaa kehrätä.

(3) Tämä eläin on kissa.
 - (1) Kukaan laiska opiskelija ei selviä kokeesta.
 - b) (2) On opiskelijoita, jotka selviävät kokeesta.

(3) On opiskelijoita, jotka eivät ole laiskoja.
- (2) Ovatko seuraavat päättelyt päteviä? Perustele.
- (1) Neljäkkään lävistäjät ovat kohtisuorassa toisiaan vastaan.
 - a) (2) Neljäkäs on suunnikas.

(3) Suunnikkaan lävistäjät ovat kohtisuorassa toisiaan vastaan.
 - (1) Kaikki suorakulmiot ovat suunnikkaita.
 - b) (2) Jotkut nelikulmiot ovat suorakulmioita.

(3) Jotkut nelikulmiot ovat suunnikkaita.
 - (1) Kolmio ABC on tasakylkinen.
 - c) (2) Tasasivuiset kolmiot ovat tasakylkisiä.

(3) Kolmio ABC on tasasivuinen.
- (3) Ovatko seuraavat päättelyt päteviä? Perustele.
- (1) Kaikki lammasfarmin lampaat ovat joko mustia tai valkoisia.
 - a) (2) Kaikki lampaat ovat mustia tai valkoisia.

(1) Tavallisessa korttipakassa kortti on aina joko pata, risti, hertta tai ruutu.
 - (2) Pata- ja risti-kortit ovat mustia.
 - b) (3) Hertta- ja ruutu-kortit ovat punaisia.

(4) Kaikki tavallisten korttipakkojen kortit ovat joko mustia tai punaisia.
- (4) Jäämaa on kokonaan Merimaan itäpuolella. Kummallakin on eteläraja Aurinkomaan kanssa. Merimaalla ja Aurinkomaalla on länsiraja Lumimaan kanssa. Kukkamaa on kokonaan Jäämaan

ja Aurinkomaan itäpuolella. a) Onko Merimaalla ja Kukkamaalla yhteistä rajaa? b) Voiko Lumimaalla ja Kukkamaalla olla yhteistä rajaa?

(5) Ovatko seuraavat päättelyt päteviä? Perustele.

- | | | |
|----|-----|------------------------------|
| | (1) | Millään x ei toteudu y . |
| a) | (2) | Kaikilla z toteutuu x . |
| | (3) | Millään z ei toteudu y . |
| | (1) | Kaikilla A toteutuu B . |
| b) | (2) | Joillakin C toteutuu B . |
| | (3) | Joillakin A toteutuu C . |

2. LOOGISET LAUSEET

Logiikkaa ja erilaisia päättelyitä käytetään jatkuvasti arkipäivän tilanteissa. Logiikan tutkimuksessa tarvitaan kuitenkin täsmällisiä määritelmiä ja systemaattisia päättelysääntöjä, joihin tutustutaan tässä luvussa.

2.1. Atomilauseet, konnektiivit ja totuusarvot.

Tutkimustehtävä. Neljä opiskelijaa hakee kesätöihin huvipuistoon. Tutustu heidän hakutietoihinsa. Vastaa kysymyksiin hakijoiden soveltuvuudesta eri tehtäviin.

Hanna (17 v.) on opiskellut kaksi vuotta ammattilukiossa. Opintoihinsa liittyen hän on suorittanut hygieniapassin. Hanna harrastaa tennistä ja kalliokiipeilyä.

Heikki (18 v.) on opiskellut kaksi vuotta lukiossa. Hänellä on ajokortti ja hygieniapassi. Heikki pelkää korkeita paikkoja.

Jussi (18 v.) on opiskellut yhden vuoden lukiossa ja on juuri palannut Uudesta-Seelannista, missä hän oli vaihto-opiskelijana yhdeksän kuukautta.

Saara (19 v.) on suorittanut ylioppilastutkinnon. Hän kirjoitti mm. pitkän englannin ja lyhyen ranskan. Saara on ollut vuoden vaihto-opiskelijana Englannissa, ja hänellä on ajokortti.

- (1) Jarrumieheksi vuoristoradalle voidaan valita henkilö, joka ei pelkää korkeita paikkoja. Sopiiko a) Hanna b) Heikki tehtävään?
- (2) Oppaalta vaaditaan lukion pitkän englannin oppimäärä tai yli puolen vuoden oleskelu englanninkielisessä maassa. Sopiiko a) Jussi b) Saara c) Hanna tehtävään?
- (3) Jäätelökärryn kuljettajalta vaaditaan täysi-ikäisyyttä ja hygieniapassia. Sopiiko a) Saara b) Hanna c) Heikki tehtävään?

Yksinkertaisimpia loogisia lauseita kutsutaan *atomilauseiksi*. Atomilauseita käytetään ilmaisemaan asioiden tilaa. Esimeriksi seuraavat lauseet ovat atomilauseita:

- A : On yö.
- B : Aurinko paistaa.
- C : Pariisi on Italiassa.
- D : Oulu on Suomessa.

Atomilauseita ajatellaan eräänlaisina totuusmuuttujina, jotka voivat saada kaksi arvoa: tosi tai epätosi. Yllä olevista lauseista C on epätosi,

D on tosi ja kaksi ensimmäistä voivat olla tosia tai epätosia ajankohdasta riippuen. Tässä kurssissa atomilauseita merkitään isoilla kirjaimilla A, B, C , jne. Todelle ja epätodelle käytetään tietotekniikasta tuttuja merkintöjä 1 ja 0.

Loogisia lauseita voidaan myös muodostaa yhdistelemällä atomilauseita *konnektiivien* avulla. Konnektiiveja ovat esimerkiksi *ei, ja, tai* sekä *jos ... niin*. Näillä sanoilla on myös arkikielessä merkityksiä, jotka joskus eivät täysin vastaa niiden merkitystä logiikassa. Lausetta, jossa on vähintään yksi konnektiivi, kutsutaan *yhdistetyksi lauseeksi*. Yhdistetyn lauseen totuusarvoa tutkitaan *totuustaulujen* avulla.

Negaatio. Yksinkertaisin esimerkki konnektiivista on looginen *ei*, jota kutsutaan *negaatioksi*. Lauseen A negaatiota merkitään $\neg A$. Negaation totuusarvo on vastakkainen sille lauseelle, johon negaatio liittyy. Jos A on tosi, niin $\neg A$ on epätosi. Jos A on epätosi, niin $\neg A$ on tosi.

Esimerkiksi lauseen A : ”uimahalli on auki” negaatio on $\neg A$: ”uimahalli on suljettu”.

Negaation totuustaulu on seuraava:

A	A :n negaatio
tosi	epätosi
epätosi	tosi

Aikaisemmin mainittuja merkintöjä käyttäen totuustaulu voidaan kirjoittaa lyhyemmin:

A	$\neg A$
1	0
0	1

Konjunktio. Loogista ja-konnektiivia sanotaan *konjunktiksi*. Kahden lauseen A ja B konjunktio $A \wedge B$ on tosi vain silloin, kun molemmat kyseisistä lauseista ovat tosia. Muussa tapauksessa se on epätosi.

Esimerkiksi lauseiden A : ”olen vaaleatukkainen” ja B : ”olen ruskeasilmäinen” konjunktio on $A \wedge B$: ”olen vaaleatukkainen ja ruskeasilmäinen”.

Konjunktion totuustaulu:

A	B	$A \wedge B$
1	1	1
1	0	0
0	1	0
0	0	0

Disjunktio. Loogista tai-konnektiivia sanotaan *disjunktiksi*. Lauseiden A ja B disjunktio $A \vee B$ on tosi silloin, kun ainakin toinen lauseista A ja B on tosi.

Esimerkiksi lauseiden A : ”henkilöllä on B-ajokortti” ja B : ”henkilöllä on moottoripyöräkortti” disjunktio on $A \vee B$: ”henkilöllä on B-ajokortti tai hänellä on moottoripyöräkortti”.

Disjunktion totuustaulu:

A	B	$A \vee B$
1	1	1
1	0	1
0	1	1
0	0	0

Kannattaa huomata, että arkikielessä sanalla tai on usein eri merkitys kuin logiikassa, koska tai-lauseen ei aina ajatella olevan tosi tapauksessa, jossa sekä A että B ovat tosia.

Esimerkiksi hampurilaisateriaan voi valita ranskalaiset perunat tai minisalaatin mutta ei molempia. Toisaalta henkilö on vapaa oppivelvollisuudesta, jos hänellä on peruskoulun päästötodistus tai jos koulun aloittamisesta on kulunut kymmenen vuotta. Kumpi tahansa ehto yksinään riittää. Suurimmalla osalla oppivelvollisuudesta vapaista ihmisistä on kummatkin ominaisuudet.

Esimerkki 1. Olkoot lauseet A : ”on kesä”, B : ”käyn töissä” ja C : ”pelaan jalkapalloliigassa”. Suomenna lauseet

- a) $\neg A$,
- b) $B \vee C$,
- c) $\neg A \wedge B$,
- d) $B \vee (A \wedge C)$.

Ratkaisu:

- a) Ei ole kesä.
- b) Käyn töissä tai pelaan jalkapalloliigassa.
- c) Ei ole kesä ja käyn töissä.
- d) Käyn töissä, tai sitten on kesä ja pelaan jalkapalloliigassa.

Formalisointi. *Formalisoinnilla* tarkoitetaan luonnollisen kielen, esimerkiksi suomen kielen, lauseiden kääntämistä logiikan kielelle. Tällöin on esimerkiksi valittava, mitkä ovat atomilauseita. Samalla ilmaisulla voi olla useita mielekkäitä formalisointeja. Formalisoinnin tarkoituksena on löytää vastaavuuksia logiikan ja arkielämän tilanteiden välille. Näin voidaan esimerkiksi tutkia erilaisia väitelauseita ja päätelmiä. Formalisointi on tärkeä väline eräiden filosofian ja tietojenkäsittelyn ongelmien tutkimuksessa.

Arkikielen lauseiden kääntäminen logiikan kielelle ei ole aina helppoa ja tulkinnanvaraisuuttakin voi esiintyä. Erityisen ongelmallisia ovat paljon konnektiiveja sisältävät lauseet, koska luonnollisessa kielessä konnektiivien suorituseräjästä ei määritellä eikä tavallisesti käytetä sulkeita.

Esimerkki 2. Formalisoi lauseet

- a) Liisalla ei ole alibia.
- b) Liisalla on alibi tai hänellä ei ole motiivia.
- c) Liisalla on motiivi, mutta hänellä on myös alibi.
- d) Alibin puuttuessa Liisalla ei ole motiivia.

Ratkaisu: Käytetään atomilauseita A : ”Liisalla on alibi” ja M : ”Liisalla on motiivi”. Formalisoidut lauseet ovat:

- a) $\neg A$.
- b) $A \vee \neg M$.
- c) $M \wedge A$.
- d) Lause voidaan ymmärtää niin, että Liisalla ei ole alibia eikä hänellä myöskään ole motiivia. Silloin sen formalisointi on $\neg A \wedge \neg M$. Toisaalta lause voidaan tulkita niin, että alibin puuttumisesta seuraa se, että Liisalla ei ole motiivia. Tätä lausetta ei ole suoraviivaista formalisoida negaation, konjunktion ja disjunktion avulla. Siihen tarvitaan niiden lisäksi seuraavassa kappaaleessa esiteltävä implikaatio.

Vastaus: a) $\neg A$, b) $A \vee \neg M$, c) $M \wedge A$, d) esimerkiksi $\neg A \wedge \neg M$.

Esimerkki 3. Lomamatkallaan Liina ja Pasi halusivat osallistua rullaluistelutapahtumaan. He näkivät tarjouksen: ”Vuokraa 5 eurolla rullaluistimet tai suojat ja kypärä.” Miten tarjous pitäisi ymmärtää?

Ratkaisu: Tarjous ei ole yksiselitteinen. Käytetään atomilauseita R : ”vuokraan kuuluu rullaluistimet”, S : ”vuokraan kuuluu suojat” ja K : ”vuokraan kuuluu kypärä”. Tarjous olisi formalisoituna $R \vee S \wedge K$. Lauseen merkitys riippuu kuitenkin siitä, kumpaa konnektiivia sovelletaan ensin. Lause $R \vee (S \wedge K)$ tarkoittaa, että viidellä eurolla voi vuokrata joko pelkästään rullaluistimet tai sitten sekä suojat että kypärän.

Lause $(R \vee S) \wedge K$ tarkoittaa, että viidellä eurolla voi vuokrata joko rullaluistimet tai suojat ja niiden lisäksi kypärän.

Vastaus: Tarjouksen voi ymmärtää kahdella tavalla: viidellä eurolla voi vuokrata joko pelkästään rullaluistimet tai sitten sekä suojat että kypärän; viidellä eurolla voi vuokrata joko rullaluistimet tai suojat ja niiden lisäksi kypärän.

Formalisoinnin jälkeen lauseen totuusarvoa voidaan tutkia esimerkiksi totuustaulujen avulla.

Esimerkki 4. Laadi totuustaulu lauseelle a) $\neg(A \wedge \neg B)$, b) $(A \wedge B) \vee \neg C$.

Ratkaisu:

- a) Lauseessa $\neg(A \wedge \neg B)$ on kaksi atomilauseetta. Totuustauluun merkitään kaikki lauseiden A ja B eri totuusarvojen yhdistelmät. Sen jälkeen kirjoitetaan sarakkeet lauseiden $\neg B$, $A \wedge \neg B$ sekä $\neg(A \wedge \neg B)$ totuusarvoille.

A	B	$\neg B$	$A \wedge \neg B$	$\neg(A \wedge \neg B)$
1	1	0	0	1
1	0	1	1	0
0	1	0	0	1
0	0	1	0	1

- b) Lauseessa $(A \wedge B) \vee \neg C$ on kolme atomilauseetta. Kaikkia lauseiden A , B ja C totuusarvojen yhdistelmiä varten tarvitaan kahdeksan riviä.

A	B	C	$\neg C$	$A \wedge B$	$(A \wedge B) \vee \neg C$
1	1	1	0	1	1
1	1	0	1	1	1
1	0	1	0	0	0
1	0	0	1	0	1
0	1	1	0	0	0
0	1	0	1	0	1
0	0	1	0	0	0
0	0	0	1	0	1

Tehtäviä.

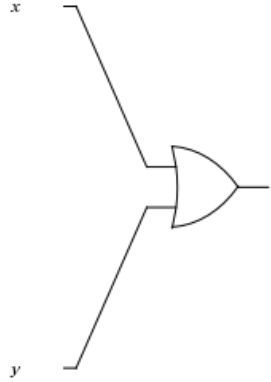
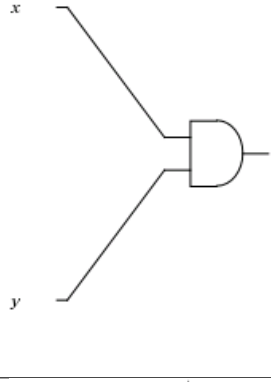
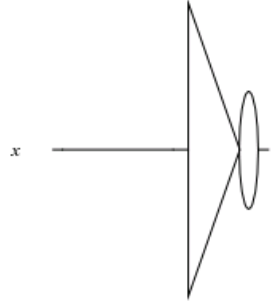
- (1) Onko lause atomilause? a) Tampere on Pirkanmaalla. b) Kajaa-ni on Suomen pääkaupunki. c) Hattu pois päästä! d) On olemas-sa suurin alkuluku. e) Onko avaruudessa elämää? f) $5 + 12 = 18$.
- (2) Kirjoita lauseen negaatio.
 - a) Tänään on maanantai.
 - b) $2 + 3 = 5$.
 - c) Luku on negatiivinen.
 - d) Ainakin yhdellä ryhmämme opiskelijalla on ruskeat silmät.
 - e) Kymmenessä sivussa tekstiä on vähintään seitsemän vir-hettä.
 - f) Kesä Välimerellä on kuuma ja aurinkoinen.
- (3) Olkoot lause A : ”veikkasin lottorivin” ja lause B : ”voitin mil-joona euroa”. Kirjoita suomen kielellä lauseet a) $\neg A$, b) $A \vee B$, c) $A \wedge B$, d) $A \wedge \neg B$, e) $\neg A \vee (A \wedge B)$, f) $\neg A \wedge \neg B$.
- (4) Olkoot lause A : ”on kaunis kesäpäivä”, lause B : ”lokit kirkuvat” ja lause C : ”kävelen rannalla”. Kirjoita suomen kielellä lauseet a) $\neg A \vee B$, b) $A \wedge B \wedge C$, c) $\neg(A \wedge C)$, d) $(A \wedge C) \vee (B \wedge \neg C)$.
- (5) Olkoot A : ”on pilvistä” ja B : ”sataa lunta”. Formalisoi seuraa-vat lauseet eli kirjoita ne lauseiden A ja B sekä konnektiivien \neg , \wedge ja \vee avulla.
 - a) On pilvistä ja sataa lunta.
 - b) On pilvistä, mutta ei sada lunta.
 - c) Ei ole pilvistä eikä sada lunta.
 - d) On pilvistä tai sataa lunta.
 - e) On pilvistä ja sataa lunta tai ei ole pilvistä eikä sada lunta.
- (6) Formalisoi lauseet:
 - a) Mustikat polun varrella ovat kypsiä tai alueella ei ole nähty karhuja.
 - b) Ei ole totta, että mustikat polun varrella ovat kypsiä tai alueella on nähty karhuja.
 - c) Mustikat polun varrella ovat kypsiä, mutta alueella ei ole nähty karhuja, tai sitten mustikat eivät ole kypsiä ja alu-eella on nähty karhuja.
 - d) Karhuja ei ole nähty alueella ja polulla vaeltaminen on tur-vallista, mutta mustikat ovat kypsiä.
- (7)
 - a) Laadi totuustaulu lauseelle $\neg A \vee \neg B$. Millä atomilauseiden A ja B totuusarvoilla lause on tosi?
 - b) Laadi totuustaulu lauseelle $\neg(A \wedge B)$. Millä atomilausei-den A ja B totuusarvoilla lause on tosi? Vertaa a-kohdan tulokseen.
 - c) Etsi atomilauseet A ja B ja ilmaise a- ja b-kohtien lauseet suomen kielellä.
- (8) Laadi totuustaulu lauseelle $(A \wedge B) \vee \neg(B \vee C)$.

- (9) Olkoot atomilauseet A : " $x < -1$ ", B : " $x > 1$ " ja C : " $x = 1$ ". Formalisoi lauseet a) $x \neq 1$, b) $x \geq 1$, c) $x \geq -1$, d) $x < 1$, e) $-1 \leq x \leq 1$, f) $x < -1$ tai $x \geq 1$.
- (10) Saarella asuu haltijoita ja menninkäisiä. Turisti tapasi kaksi saarelaista, Hipsun ja Vipsun. Hipsu sanoi: "Hillat ovat kypsiä ja kalaonni on suotuista, tai sitten hillat eivät ole kypsiä tai kalaonni ei ole suotuista." Vipsu väitti: "Hillat ovat kypsiä ja kalaonni on suotuista, mutta hillat eivät ole kypsiä tai kalaonni ei ole suotuista." Tutki totuustaulun avulla Hipsun ja Vipsun väitteiden totuusarvoja. Mitä voidaan päätellä totuustaulun avulla, kun tiedetään, että saaren asukkaista haltijat valehtelevat aina ja menninkäiset puhuvat aina totta? Saiko vierailija käyttökelpoista tietoa marjasadosta tai kalaonnesta?
- (11) Loogisilla piireillä suoritetaan digitaalisissa laitteissa erilaisia loogisia operaatioita. Loogisen piirin toimintaa voidaan kuvata esimerkiksi seuraavalla kaaviolla.

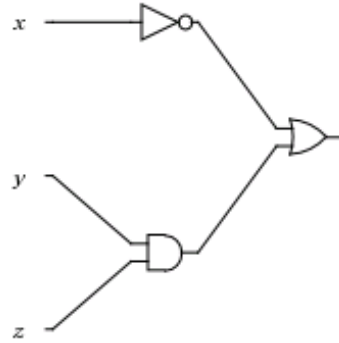


Loogisella piirillä on yksi tai useampi sisäänmeno ja yksi ulostulo. Sisäänmenojen ja ulostulon signaalin arvo voi olla 1 tai 0. Edellisessä tapauksessa johtimessa on jännite, jälkimmäisessä tapauksessa ei ole.

Loogiset piirit kootaan loogisista porteista. Seuraavassa taulukossa on lueteltu loogiset portit, niiden toiminta ja toimintaa vastaava looginen konnektiivi.

Looginen portti	Toiminta	Piirrosmerkki	Toimintaa vastaava looginen konnektiivi
Tai	Tai-portti antaa jännitteen, kun ainakin toisessa sisäänmenossa on jännite.		$A \vee B$
Ja	Ja-portti antaa jännitteen vain silloin, kun molemmissa sisäänmenoissa on jännite.		$A \wedge B$
Ei	Ei-portti antaa jännitteen silloin, kun sisäänmenossa ei ole jännitettä, ja kääntäen.		$\neg A$

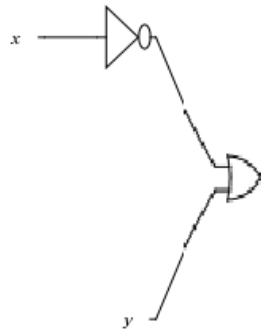
Esimerkiksi looginen piiri



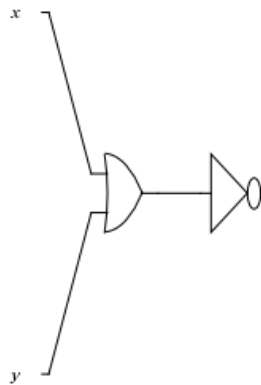
koostuu kolmesta loogisesta portista ja se vastaa lausetta $\neg A \vee (B \wedge C)$.

Muodosta seuraavia piirejä vastaavat lauseet.

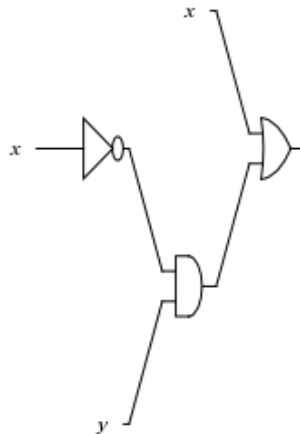
a)



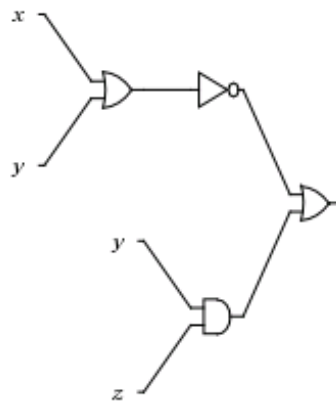
b)



c)



d)



- (12) Piirrä lausetta a) $\neg A \wedge B$ b) $A \vee \neg(B \wedge C)$ c) $(A \wedge B) \vee (\neg A \wedge C)$ vastaava looginen piiri.

Kotitehtäviä.

- (1) Kirjoita lauseen negaatio.
 - a) $100 > 101$.
 - b) Lompakossani on rahaa korkeintaan 10 euroa.
 - c) Kaikki ryhmämme opiskelijat ovat Facebookissa.
 - d) Koulussamme on täsmälleen kaksi vasenkätistä opettajaa.
 - e) En opiskele latinaa enkä kreikkaa.
 - f) Maarit pitää lumilautailusta tai käsitöistä muttei molemmista.
- (2) Olkoot lauseet A : ”puutarhan portti on auki”, B : ”ruusut kukkivat” ja C : ”menen puutarhaan”. Kirjoita suomen kielellä lauseet
 - a) $\neg A$, b) $B \wedge C$, c) $A \vee B$, d) $\neg B \wedge \neg C$, e) $\neg(A \wedge B)$ f) $A \vee \neg B$, g) $(A \wedge C) \vee (\neg B \wedge C)$.
- (3) Formalisoi lause.
 - a) Kaino ei ole vanha ja Kaino on mies.
 - b) Kaino on vanha tai Kaino ei ole mies.
 - c) Kaino ei ole vanha mies.

- d) Kaino ei ole vanha eikä hän ole mies.
- (4) Formalisoi lause.
- Amadeus kuuntelee klassista tai Klaus kuuntelee jazzia.
 - Amadeus ei kuuntele klassista, mutta Klaus kuuntelee jazzia.
 - Amadeus kuuntelee klassista, mutta Klaus ei kuuntele jazzia, tai sitten Hassinen kuuntelee progea.
 - Ei ole niin, että Amadeus kuuntelisi klassista, Klaus jazzia ja Hassinen progea.
- (5) a) Laadi totuustaulu lauseille $A \wedge \neg A$ ja $A \vee \neg A$.
b) Etsi atomilause A ja ilmaise kohdan a) lauseet suomen kielellä.
- (6) Laadi totuustaulu lauseille a) $\neg(A \vee B)$, b) $\neg A \wedge B$, c) $(\neg A \vee B) \wedge (A \vee \neg B)$. Millä atomilauseiden A ja B totuusarvojen yhdistelmillä lauseet ovat tosia?
- (7) a) Laadi totuustaulu lauseelle $A \vee (B \wedge C)$.
b) Laadi totuustaulu lauseelle $(A \vee B) \wedge C$.
c) Vertaa kohtien a) ja b) lauseiden totuusarvoja. Mitä voit päätellä?
- (8) Olkoot lauseet A : " $x \in [-3, 1]$ " ja B : " $x \in [-1, 5]$ ". Formalisoi lause. a) $x \in [-3, 5]$, b) $x \in [-1, 1]$, c) $x \in [-3, -1[$ d) $x \in] - \infty, -3[$ tai $x \in]1, \infty[$, e) $x \in] - \infty, -3[$ tai $x \in]5, \infty[$.
- (9) Kolme koiranpentua, Alli, Buh ja Caesar ovat epäiltyinä isännän tohvelin repimisestä. Luotettava henkilö, joka puhuu aina totta, antaa seuraavan todistuksen: "Ei ole totta, että Alli on syyllinen tai Buh ei ole syyllinen. Mutta kuitenkin Alli on syyllinen tai Caesar on syyllinen." Käytä atomilauseita A : "Alli on syyllinen", B : "Buh on syyllinen" ja C : "Caesar on syyllinen" ja formalisoi luotettavan henkilön lausunto. Muodosta sille totuustaulu ja päättelä, mikä tai mitkä koiranpennuista ovat syyllisiä.
- (10) Tutkitaan lausetta "Suomen kuningas ei ole viiksekäs". Lause voidaan tulkita ainakin kahdella eri tavalla:
a) Suomella on kuningas, joka ei ole viiksekäs.
b) Ei ole niin, että olisi olemassa Suomen viiksekästä kuningat.
- Oletetaan, että Suomessa ei ole kuningat. Onko lause tosi vai epätosi?
- (11) Kissoilla lyhyen karvan aiheuttaa dominoiva geeni ja pitkän karvan resessiivinen geeni. Merkitään lyhyen karvan geeniä S ja pitkän karvan geeniä s . Kaikilla nisäkkäillä tiettyyn ominaisuuteen vaikuttaa geenipari, joista toinen geeni on saatu isältä ja toinen emolta. Jos kissan geneistä ainakin toinen on S , niin se on lyhytkarvainen. Kissa on pitkäkarvainen vain siinä tapauksessa, että se on saanut geenin s molemmilta vanhemmiltaan.

Pentujen emokissa on pitkäkarvainen (ss) ja isäkissa lyhytkarvainen (SS tai Ss). Millaisia pentuja kissat voivat saada, kun isäkissan geenipari on a) SS b) Ss?

2.2. Implikaatio ja ekvivalenssi. Tässä kappaleessa esitellään kaksi usein käytettyä konnektiivia: *implikaatio* eli *looginen seuraus* sekä *ekvivalenssi* eli *looginen yhtäpitävyys*.

Tutkimustehtävä.



Tarkastellaan oheisen kuvan mukaisia kortteja. Korttien toisella puolella on jokin kirjain ja toisella puolella jokin luku.

1) Ongelmana on selvittää, toteuttavatko kortit seuraavan säännön: Jos kortin toisella puolella on vokaali, niin sen toisella puolella on parillinen luku. Mitkä kortit täytyy vähintään kääntää?

2) Ongelmana on selvittää, toteuttavatko kortit seuraavan säännön: Kortin toisella puolella on parillinen luku, jos ja vain jos sen toisella puolella on vokaali. Mitkä kortit täytyy vähintään kääntää?

Psykologi Jean Piaget (1896 – 1980) käytti ensimmäistä kysymystä tutkiessaan nuorten ja aikuisten abstraktia ajattelua (webpace.ship.edu/cgboer/piaget.html).

Implikaatio

Loogista jos A niin B -rakennetta sanotaan implikaatioksi. Implikaatiota merkitään $A \rightarrow B$. Implikaatiota kutsutaan toisinaan loogiseksi seuraukseksi, mutta tämä ilmaisu on hieman tulkinnanvarainen. Sanalla seuraus on nimittäin puhekielessä kaksi sanan loogisesta merkityksestä poikkeavaa mutta tavallisempaa merkitystä. Seuraus voi tarkoittaa esimerkiksi ajallista seurausta, eli asia tapahtuu toisen jälkeen. Sanalla voidaan myös tarkoittaa kausaalista seurausta, eli asia on toisen aiheuttava syy. Logiikassa ei yleensä kiinnitetä huomiota tällaisiin näkökohtiin. Joskus asiat voivat olla toistensa loogisia seurauksia, vaikka niillä ei olisi kausaalisesti mitään tekemistä toistensa kanssa. Esimerkiksi lause ”jos Caesar elää, niin Helsinki sijaitsee Afrikassa” on logiikan mielessä tosi.

Looginen implikaatio $A \rightarrow B$ määritellään niin, että se on epätosi ainoastaan tapauksessa, jossa A on tosi mutta B ei ole. Kaikissa muissa tapauksissa se on tosi. Siksi logiikassa usein sanotaan, että epätodesta oletuksesta voi päätellä mitä tahansa.

Esimerkiksi lauseista A : ”Anne on suomalainen” ja B : ”Anne on eurooppalainen” saadaan implikaation avulla lauseet $A \rightarrow B$: ”jos Anne on suomalainen, niin hän on eurooppalainen” sekä myös $B \rightarrow A$: ”jos Anne on eurooppalainen, niin hän on suomalainen”.

Implikaation totuustaulu:

A	B	$A \rightarrow B$
1	1	1
1	0	0
0	1	1
0	0	1

Kappaleessa 2.3 osoitetaan, että implikaatiota voidaan ajatella lyhennysmerkintänä lauseelle $\neg A \vee B$, koska implikaatiolla on sama totuustaulu kuin kyseisellä lauseella.

Ekvivalenssi. Jos sekä $A \rightarrow B$ että $B \rightarrow A$ ovat tosia lauseita, sanotaan, että lauseet A ja B ovat ekvivalentit, $A \leftrightarrow B$. Ekvivalenssia voi ajatella lyhennysmerkintänä lauseelle $(A \rightarrow B) \wedge (B \rightarrow A)$. Intuitiivisesti se tarkoittaa lauseiden A ja B yhtäpitävyyttä (vrt. yhtäsuuruus), eli molemmat lauseet saavat samat totuusarvot.

Esimerkiksi lauseiden A : ”Pekka menee hammaslääkəriin” ja B : ”Pekan hammasta särkee” ekvivalenssi on $A \leftrightarrow B$: ”Pekka menee hammaslääkəriin, jos ja vain jos hänen hammastaan särkee”.

Ekvivalenssin totuustaulu:

A	B	$A \leftrightarrow B$
1	1	1
1	0	0
0	1	0
0	0	1

Ekvivalenssi $A \leftrightarrow B$ voidaan lukea ” A , jos ja vain jos B ”. Tämä ilmaisu esiintyy usein matemaattisessa tekstissä. Voidaan käyttää myös esimerkiksi ilmaisuja ” A silloin ja vain silloin, kun B ” ja ” A ja B ovat yhtäpitävät”.

Esimerkki 1. Formalisoi lause. Missä tilanteissa lause on tosi? a) On kesä, ja jos on kesä, järvivesi on lämmintä. b) Uin silloin ja vain silloin, kun on kesä ja järvivesi on lämmintä.

Ratkaisu: Käytetään atomilauseita A : ”on kesä”, B : ”järvivesi on lämmintä” ja C : ”uin”.

a) Lause on $A \wedge (A \rightarrow B)$. Muodostetaan lauseen totuustaulu.

A	B	$A \rightarrow B$	$A \wedge (A \rightarrow B)$
1	1	1	1
1	0	0	0
0	1	1	0
0	0	1	0

Lause on tosi täsmälleen silloin, kun A ja B ovat molemmat tosia eli kun on kesä ja järvivesi on lämmintä.

b) Lause on $C \leftrightarrow (A \wedge B)$. Muodostetaan lauseen totuustaulu.

A	B	C	$A \wedge B$	$C \leftrightarrow (A \wedge B)$
1	1	1	1	1
1	1	0	1	0
1	0	1	0	0
1	0	0	0	1
0	1	1	0	0
0	1	0	0	1
0	0	1	0	0
0	0	0	0	1

Lause on tosi, kun atomilauseet A , B ja C ovat kaikki tosia, kun A on tosi sekä B ja C ovat epätosia, kun B on tosi sekä A ja C ovat epätosia tai kun kaikki atomilauseet ovat epätosia. Tämä vastaa seuraavia tilanteita: on kesä, järvivesi on lämmintä ja uin; on kesä, järvivesi ei ole lämmintä enkä ui; ei ole kesä, järvivesi on lämmintä, mutta en ui; ei ole kesä, järvivesi ei ole lämmintä enkä ui.

Vastaus: a) Lause on tosi, kun on kesä ja järvivesi on lämmintä.

b) Lause on tosi seuraavissa tilanteissa: on kesä, järvivesi on lämmintä ja uin; on kesä, järvivesi ei ole lämmintä enkä ui; ei ole kesä, järvivesi on lämmintä, mutta en ui; ei ole kesä, järvivesi ei ole lämmintä enkä ui.

Esimerkki 2. Matti, Seppo ja Teppo ovat epäiltyinä rikoksesta. Heitä kuulustelevala konstaapeli Reinikainen tietää, että syytön puhuu aina totta ja syyllinen valehtelee aina.

Matti sanoi: ”Jos Seppo on syytön, niin minäkin olen.”

Seppo väitti: ”Minä olen syytön, jos ja vain jos Teppo on syytön.”

Teppo sanoi: ”Seppo yksin on syyllinen.”

Ratkaise totuustaulun avulla, kuka tai ketkä ovat syyllisiä.

Ratkaisu: Tarkastellaan lauseita M : ”Matti on syytön”, S : ”Seppo on syytön” ja T : ”Teppo on syytön”.

Matin, Sepon ja Tepon väitteet formalisoituina ovat $S \rightarrow M$, $S \leftrightarrow T$ ja $M \wedge \neg S \wedge T$. Tutkitaan, kuinka väitteet riippuvat lauseiden M , S ja T totuusarvoista. Muodostetaan totuustaulu:

M	S	T	$S \rightarrow M$	$S \leftrightarrow T$	$\neg S$	$M \wedge \neg S$	$M \wedge \neg S \wedge T$
1	1	1	1	1	0	0	0
1	1	0	1	0	0	0	0
1	0	1	1	0	1	1	1
1	0	0	1	1	1	1	0
0	1	1	0	1	0	0	0
0	1	0	0	0	0	0	0
0	0	1	1	0	1	0	0
0	0	0	1	1	1	0	0

Koska syytön puhuu totta ja syyllinen valehtelee, on löydettävä totuustaulusta rivi, jolla väitteillä $S \rightarrow M$, $S \leftrightarrow T$ ja $M \wedge \neg S \wedge T$ on samat totuusarvot kuin lauseilla M , S ja T . Tällainen rivi on totuustaulun kolmas rivi. Siten Seppo on yksin syyllinen.

Vastaus: Seppo on yksin syyllinen.

Konnektiivien suoritusjärjestys. Loogisten lauseiden lukeminen helpottuu ja tarve sulkeiden käyttämiseen vähenee, jos sovitaan konnektiivien suoritusjärjestyksestä. Nykyään yleisimmin käytetään seuraavaa suoritusjärjestystä, jota noudatetaan myös tässä kirjassa: \neg , \wedge , \vee , \rightarrow , \leftrightarrow , ja vasemmalta oikealle.

Suoritusjärjestystä voidaan muuttaa käyttämällä sulkeita. Sulkeita kannattaa myös käyttää aina silloin, kun se helpottaa loogisen lauseen lukemista.

Esimerkki 3. Mikä on lauseiden a) $B \leftrightarrow \neg A \vee B \wedge A \rightarrow B$, ja b) $(B \leftrightarrow \neg A) \vee B \wedge (A \rightarrow B)$ totuusarvo, kun A on tosi ja B epätosi?

Ratkaisu:

a) Muodostetaan totuustaulu:

A	B	$\neg A$	$B \wedge A$	$\neg A \vee B \wedge A$	$\neg A \vee B \wedge A \rightarrow B$	$B \leftrightarrow \neg A \vee B \wedge A \rightarrow B$
1	0	0	0	0	1	0

Ensin suoritetaan negatio. Sen jälkeen tulevat konjunktio ja disjunktio. Implikaatio suoritetaan ennen ekvivalenssia. Kun A on tosi ja B epätosi, lause on epätosi.

b) Muodostetaan totuustaulu:

A	B	$\neg A$	$B \leftrightarrow \neg A$	$A \rightarrow B$	$B \wedge (A \rightarrow B)$	$(B \leftrightarrow \neg A) \vee B \wedge (A \rightarrow B)$
1	0	0	1	0	0	1

Ensin suoritetaan negaatio. Sen jälkeen tulevat sulkeissa olevat ekvivalenssi ja implikaatio. Konjunktio suoritetaan ennen disjunktia. Kun A on tosi ja B epätosi, lause on tosi.

Vastaus: a) epätosi, b) tosi

Harvinaisempia konnektiiveja (Lisämateriaalia). Logiikassa ja tietotekniikassa esiintyy myös muita, harvinaisempia loogisia konnektiiveja. Esimerkki tällaisesta on *poissulkeva tai* (engl. exclusive or), josta usein käytetään tietotekniikasta tulevaa lyhennettä *xor*. Poissulkevan tain totuustaulu on seuraava:

A	B	$A \text{ xor } B$
1	1	0
1	0	1
0	1	1
0	0	0

Kuten kappaleessa 2.1 todettiin, arkikielessä sana tai saattaa tarkoittaa asiayhteydestä riippuen joskus poissulkevaa tai-operaatiota ja toisinaan loogista disjunktia.

Lisää loogisia konnektiiveja esitellään harjoitustehtävissä.

Tehtäviä.

- (1) Olkoot A : ”Matti on insinööri” ja B : ”Matilla on hyvä työpaikka”. Suomeksi lause.
 - a) $A \wedge B$,
 - b) $\neg A \vee B$,
 - c) $A \rightarrow B$,
 - d) $\neg B \rightarrow A$,
 - e) $\neg(B \rightarrow A)$.
 - f) $B \leftrightarrow A$.
- (2) Olkoot A : ”Liisa on lomalla” ja B : ”Liisa on iloinen”. Formalisoi lauseet:
 - a) Jos Liisa on lomalla, hän on iloinen.
 - b) Liisa on lomalla, mutta hän ei ole iloinen.
 - c) Liisa on iloinen silloin ja vain silloin, kun hän on lomalla.
 - d) Jos Liisa ei ole iloinen, hän ei ole lomalla.
- (3) Onko lause tosi?
 - a) Jos Tallinna on Norjan pääkaupunki, niin Tukholma on Ruotsin pääkaupunki.
 - b) Jos Tallinna on Norjan pääkaupunki, niin Budapest on Ruotsin pääkaupunki.
 - c) Jos Leonardo da Vinci on kuollut, niin Aleksis Kivi on saksalainen ralliautoilija.
 - d) Jos Leonardo da Vinci on kuollut, niin Leo Tolstoi on venäläinen kirjailija.
- (4) Laadi lauseen totuustaulu.
 - a) $\neg A \rightarrow B$
 - b) $A \leftrightarrow \neg B$
 - c) $\neg(A \wedge B) \rightarrow A$
- (5) Laadi lauseen totuustaulu.
 - a) $\neg A \vee B \rightarrow C \wedge A$
 - b) $(A \rightarrow B) \leftrightarrow (C \rightarrow B)$
- (6) Formalisoi lause. Missä tilanteissa lause on tosi?
 - a) Jos mustikat polun varrella eivät ole kypsiä, niin polulla vaeltaminen on turvallista.
 - b) Jos mustikat polun varrella ovat kypsiä, niin silloin polulla vaeltaminen on turvallista, jos ja vain jos karhuja ei ole nähty alueella.
 - c) Polulla vaeltaminen on turvallista silloin ja vain silloin, kun mustikat eivät ole kypsiä tai alueella ei ole nähty karhuja.
- (7) Formalisoi lause ja laadi lauseen totuustaulu. Mitä huomaat? Kertooko lause mitään siitä, onko logiikan opiskelu oikeasti hauskaa juuri tällä hetkellä?
 - a) Jos sataa ja ei sada, niin logiikan opiskelu on hauskaa.
 - b) Jos sataa ja ei sada, niin logiikan opiskelu ei ole hauskaa.

- (8) Perheen lapsia Annaa ja Markusta epäillään kaappiin piilotetun suklaalevyn katoamisesta. Luotettava todistaja kertoo tiedot: Anna on syyllinen tai Markus on syyllinen. Anna on syytön tai Markus on syytön. Jos Anna on syyllinen, niin Markus on syyllinen.
- Kumpi lapsista on käynyt suklaavarkaissa?
- (9) Edwards, Petterson ja Smith ovat syytettyinä omenavarkaudesta. Neiti Marble kuulustelee heitä. Edwards sanoo: ”Jos Petterson on syytön, niin minä olen syyllinen.” Petterson toteaa: ”Minä olen syyllinen, jos ja vain jos Edwards on syyllinen.” Smith väittää: ”Olemme kaikki syyttömiä.” Neiti Marble tietää, että syylliset valehtelevat aina ja syyttömät puhuvat aina totta. Ratkaise totuustaulun avulla, kuka tai ketkä syytetyistä ovat käyneet omenavarkaissa.
- (10) Eräässä maassa kaikki kuuluvat joko hattujen tai myssyjen puoleeseen. Hatut valehtelevat aina ja myssyt puhuvat aina totta. Kolme kansalaista keskusteli keskenään. Heidän joukossaan saattoi olla vieraan puolueen vakoilija. Arthur sanoi, että Claus on myssy. Berit totesi, että Arthur on myssy ja myös hän itse on myssy. Claus väitti, että jos Arthur on hattu, niin myös hän itse on hattu. Tutki totuustaulun avulla, kuka oli mahdollinen vakoilija.
- (11) Olkoot lauseet A : ”herään ajoissa”, B : ”menen kouluun” ja C : ”opiskelen logiikkaa”. Esitä sanoin lause $A \rightarrow B \vee C$. Onko lauseen tulkinta $A \rightarrow (B \vee C)$ vai $(A \rightarrow B) \vee C$? Miten tulkinat eroavat toisistaan?
- (12) Vertaa lauseiden totuusarvoja atomilauseiden A , B ja C eri totuusarvoilla. Onko sulkeiden muuttamisella vaikutusta lauseen totuusarvoon?
- $(A \rightarrow B) \rightarrow C$ ja $A \rightarrow (B \rightarrow C)$.
 - $(A \wedge B) \wedge C$ ja $A \wedge (B \wedge C)$.
- (13) (Lisämateriaalia) Tietokoneet käsittelevät tietoa käyttäen bittejä. Bitillä on kaksi mahdollista arvoa, 0 ja 1. Bittijono on jono, jossa on yksi tai useampia bittejä. Esimerkiksi 1001 0010 on bittijono, jonka pituus on 8 bittiä. Samanpituksille bittijonoille määritellään bittikohtaiset tai, ja sekä poissulkeva tai (or, and sekä xor). Esimerkiksi bittijonojen 1100 ja 1010 bittikohtainen tai on jono 1110, bittikohtainen ja on jono 1000 sekä bittikohtainen poissulkeva tai on jono 0110. Muodosta a) bittikohtainen tai b) bittikohtainen ja c) bittikohtainen poissulkeva tai jonoille 1111 0000 ja 1010 1010.
- (14) (Lisämateriaalia) Muodosta bittijono a) $(0\ 1111 \wedge 1\ 0101) \vee 0\ 1000$
 b) $(0\ 1010 \text{ xor } 1\ 1011) \text{ xor } 0\ 1001$.

Kotitehtäviä.

- (1) Olkoot A : ”Timo opiskelee matematiikkaa”, B : ”Timo osallistuu logiikan kurssille” ja C : ”Timo opiskelee filosofiaa”. Suomenna lause.
 - a) $\neg A \rightarrow \neg B$.
 - b) $A \leftrightarrow B$.
 - c) $A \vee C \rightarrow B$.
 - d) $C \leftrightarrow (B \rightarrow \neg A)$.
- (2) Onko lause tosi?
 - a) Jos $(-2)^3 = -8$, niin $(-2)^3 = -8$.
 - b) Jos $(-2)^3 = -8$, niin $(-2)^3 = 8$.
 - c) Jos luku 8 on pariton, niin luku 8 on pariton.
 - d) Jos luku 8 on pariton, niin luku 8 on parillinen.
- (3) Formalisoi lause.
 - a) Jos opettaja on pirteä, niin televisiosta ei ole tullut illalla jalkapalloa.
 - b) Suomi voittaa jalkapallon maailmanmestaruuden silloin ja vain silloin, kun lehmät lentävät ja vaaleanpunaiset norsut kävelevät kadulla.
 - c) En seuraa jalkapalloa eikä Suomen maajoukkue menesty.
 - d) Jos ottelu ei pääty tasapeliin, niin joko kotijoukkue tai vierasjoukkue voittaa pelin.
- (4) Laadi lauseen totuustaulu.
 - a) $A \wedge B \rightarrow \neg B$
 - b) $(A \leftrightarrow B) \wedge B \rightarrow C \vee A$
 - c) $(\neg A \rightarrow B) \leftrightarrow (C \rightarrow B \wedge A)$
- (5) Olkoot A : ”Timo opiskelee matematiikkaa”, B : ”Timo osallistuu logiikan kurssille” ja C : ”Timo opiskelee filosofiaa”. Formalisoi lause. Missä tilanteissa lause on tosi?
 - a) Timo opiskelee matematiikkaa ja filosofiaa.
 - b) Jos Timo opiskelee matematiikkaa, hän osallistuu logiikan kurssille.
 - c) Timo osallistuu logiikan kurssille silloin ja vain silloin, kun hän opiskelee filosofiaa tai matematiikkaa.
 - d) Jos Timo osallistuu logiikan kurssille, opiskelee hän joko matematiikka tai filosofiaa, muttei molempia.
- (6) Poliisit Mauno ja Martti saavat kiinni rikoksesta epäilemänsä Jaskan. Tiedetään, että Jaska ei koskaan valehtelee. Mauno toteaa Martille: ”Jos Jaska on syyllinen, on hänellä ollut rikostoveri.” Jaska vastaa: ”Tuo ei ole totta!” Tähän Martti tokaisee: ”Sehän tunnusti helpolla!” Tutki Maunon lausetta ja osoita Martin johtopäätös oikeaksi.
- (7) Mattia, Seppoa ja Teppoa epäillään polkupyörävarkaudesta. Konstaapeli Reinikainen tietää, että syytön puhuu aina totta ja syyllinen valehtelee aina. Reinikainen kuulustelee kolmea epäiltyä. Matti sanoo: ”Teppo on syyllinen.” Seppo väittää: ”Matti on

syyllinen tai Teppo valehtelee.” Teppo toteaa: ”Seppo on syyllinen.” Ratkaise totuustaulun avulla, kuka on syyllinen.

- (8) Helinä, Heljä ja Helena asuvat samassa talossa. Epäilläään, että loton päävoitto on osunut taloon. Luotettavalta taholta on tullut tietoja:

Jos Heljä on voittaja, niin Helinäkin on. Heljä on voittaja, jos ja vain jos Helena on voittaja. Ainakin yksi naisista on voittaja, mutta kaikki eivät ole.

Kuka tai ketkä ovat voittaneet lotossa?

- (9) Mitä eroa on seuraavissa ehdoissa?
- (a) Henkilö saa työpaikan matkamuistomyymälässä, jos hänellä on kokemusta kassakoneen käytöstä.
 - (b) Matkamuistomyymälässä työskentelevältä edellytetään kokemusta kassakoneen käytöstä.
 - (c) Henkilö saa työpaikan matkamuistomyymälässä silloin ja vain silloin, kun hänellä on kokemusta kassakoneen käytöstä.
- (10) Vertaa lauseiden totuusarvoja atomilauseiden A , B ja C eri totuusarvoilla. Onko sulkeiden muuttamisella vaikutusta lauseen totuusarvoon?
- a) $(A \vee B) \vee C$ ja $A \vee (B \vee C)$.
 - b) $(A \leftrightarrow B) \leftrightarrow C$ ja $A \leftrightarrow (B \leftrightarrow C)$.
 - c) $\neg A \leftrightarrow (B \wedge C)$ ja $\neg(A \leftrightarrow B) \wedge C$.
- (11) Olkoon v sellainen funktio, että $v(A) = 1$, jos lause A on tosi, ja $v(A) = 0$, jos lause A on epätosi. Osoita, että yhtälö pätee kaikilla lauseiden A ja B totuusarvojen yhdistelmillä.
- a) $v(A \wedge B) = v(A)v(B)$,
 - b) $v(A \vee B) = v(A) + v(B) - v(A)v(B)$,
 - c) $v(A \rightarrow B) = 1 - v(A)(1 - v(B))$.
- (12) Peircen nuoli on konnektiivi, joka luonnollisessa kielessä tarkoittaa samaa kuin ”ei A eikä B ”. Shefferin viiva on konnektiivi, joka luonnollisessa kielessä tarkoittaa samaa kuin ”ei molemmat A ja B ”. Laadi näiden konnektiivien totuustaulut.

2.3. Monimutkaisempia loogisia rakenteita. Seuraavaksi tarkastellaan eräitä usein esiintyviä loogisia rakenteita. Tällaisia rakenteita ovat *tautologiat*, *loogisesti ekvivalentit* ja *ristiriitaiset lauseet*. On tärkeää oppia tunnistamaan nämä rakenteet, koska niitä käytetään usein logiikan yhteydessä.

Tutkimustehtävä. Turisti tapasi kaksi saarelaista, Hipsun ja Vipsun. Hän kyseli heiltä, kuinka hyvin kala syö, ja sai seuraavat vastaukset.

- a) On pilvistä, tai sitten jos kala ei syö, niin ei ole pilvistä.
- b) On pilvistä tai kala syö, mutta ei ole pilvistä eikä kala syö.

Formalisoi lauseet käyttäen atomilauseita P : ”on pilvistä” ja K : ”kala syö”. Tutki totuustaulun avulla, milloin väitteet ovat tosia. Mitä huomaat?

Tautologia. Tautologialla tarkoitetaan lausetta, joka on tosi riippumatta asioiden tilasta. Tällainen lause on esimerkiksi: ”Huominen on aina tulevaisuutta.” Sanaa tautologia käytetään filosofiassa myös argumenteista, joita ei voi kumota tekemättä ristiriitaisia oletuksia.

Esimerkki 1. Osoita, että lause $(A \wedge B) \vee (\neg A \vee \neg B)$ on tautologia.

Ratkaisu: Muodostetaan lauseen $(A \wedge B) \vee (\neg A \vee \neg B)$ totuustaulu:

A	B	$A \wedge B$	$\neg A$	$\neg B$	$\neg A \vee \neg B$	$(A \wedge B) \vee (\neg A \vee \neg B)$
1	1	1	0	0	0	1
1	0	0	0	1	1	1
0	1	0	1	0	1	1
0	0	0	1	1	1	1

Koska lause on aina tosi, se on tautologia.

Looginen ekvivalenssi. Loogisesti ekvivalentit lauseet saavat samat totuusarvot kaikissa tilanteissa. Kaksi lausetta L_1 ja L_2 ovat siis loogisesti ekvivalentteja, jos niillä on samat totuustaulut. Toisin sanoen lause $L_1 \leftrightarrow L_2$ on tautologia.

Esimerkki 2. Osoita, että lauseet $A \rightarrow B$ ja $\neg A \vee B$ ovat loogisesti ekvivalentit.

Ratkaisu: Verrataan lauseiden $A \rightarrow B$ ja $\neg A \vee B$ totuustauluja:

A	B	$A \rightarrow B$	$\neg A$	$\neg A \vee B$
1	1	1	0	1
1	0	0	0	0
0	1	1	1	1
0	0	1	1	1

Koska lauseiden $A \rightarrow B$ ja $\neg A \vee B$ totuusarvot ovat aina samat, lauseet ovat loogisesti ekvivalentit.

Kolmannen poissulkevan laki sanoo, että kaikki lauseet ovat joko tosia tai epätosia. Formaalilla kielellä kolmannen poissulkevan laki tarkoittaa, että lause $A \vee \neg A$ on tautologia. Tämä voidaan nähdä seuraavasta totuustaulusta:

A	$\neg A$	$A \vee \neg A$
1	0	1
0	1	1

Moniarvoiset logiikat (lisämateriaalia). Lauseen $A \vee \neg A$ tautologisuus liittyy klassisen logiikan kaksiarvoisuuteen. Voidaan ajatella myös sellaisia päättelymalleja, joissa lause $A \vee \neg A$ ei ole tautologia. Esimerkki tällaisesta on *kolmiarvoinen logiikka*, jossa mahdollisia totuusarvoja ovat tosi, epätosi ja epävarma. Toinen esimerkki on niin kutsuttu *sumean logiikka*, jossa on äärettömän monta totuusarvoa. Erilaiset päättelyjärjestelmät eivät kuitenkaan kumoa toisiaan, vaan logiikkaa sovellettaessa käytetään kuhunkin tilanteeseen sopivaa päättelyjärjestelmää. Esimerkiksi kolmiarvoinen logiikka soveltuu tilanteisiin, joissa käytössä oleva informaatio ajatellaan epätäydelliseksi.

Ristiriitainen lause. Lausetta, joka ei toteudu missään tilanteessa, kutsutaan loogisesti ristiriitaiseksi. Lauseen ristiriitaisuutta voidaan jälleen tutkia totuustaulun avulla. Loogisesti ristiriitaisen lauseen negaatio on tautologia.

Yksinkertaisin esimerkki ristiriitaisesta lauseesta on lause $A \wedge \neg A$. Sen totuustaulu on seuraava:

A	$\neg A$	$A \wedge \neg A$
1	0	0
0	1	0

Päättelysääntöjä. Logiikassa esiintyy monia hyödyllisiksi havaittuja päättelysääntöjä, joille on annettu nimi. Nämä päättelysäännöt ovat esimerkkejä tautologioista, ja niiden tautologisuus voidaan osoittaa esimerkiksi totuustaulua käyttämällä.

Tärkeitä päättelysääntöjä ovat esimerkiksi *De Morganin lait*

$$\neg(A \wedge B) \leftrightarrow \neg A \vee \neg B$$

ja

$$\neg(A \vee B) \leftrightarrow \neg A \wedge \neg B,$$

jotka liittävät toisiinsa loogiset ja- sekä tai-konnektiivit.

Kaksoisnegaation laki sanoo, että lauseen A kaksinkertainen negaatio $\neg\neg A$ on loogisesti ekvivalentti lauseen A kanssa:

$$\neg\neg A \leftrightarrow A.$$

Kontraposition laki puolestaan sanoo, että lauseet $A \rightarrow B$ ja $\neg B \rightarrow \neg A$ ovat loogisesti ekvivalentit. Tämän voi osoittaa paitsi totuustauluja käyttämällä myös soveltamalla De Morganin lakeja. Matematiikassa tärkeä todistusmenetelmä, niin sanottu käänteinen todistus, perustuu kontraposition lakiin. Käänteistä todistusta käsitellään luvussa 4.

Seuraavaan taulukkoon on koottu edellisten lisäksi muutamia muita tunnetuimpia päättelysääntöjä:

Päättelysääntöjä	
<i>De Morganin 1. laki</i>	$\neg(A \wedge B) \leftrightarrow \neg A \vee \neg B$
<i>De Morganin 2. laki</i>	$\neg(A \vee B) \leftrightarrow \neg A \wedge \neg B$
<i>Kaksoisnegaation laki</i>	$\neg\neg A \leftrightarrow A$
<i>Kontraposition laki</i>	$(A \rightarrow B) \leftrightarrow (\neg B \rightarrow \neg A)$
<i>Modus ponens</i>	$(A \wedge (A \rightarrow B)) \rightarrow B$
<i>Modus tollens</i>	$((A \rightarrow B) \wedge \neg B) \rightarrow \neg A$
<i>Reductio ad absurdum</i>	$(\neg A \rightarrow (B \wedge \neg B)) \rightarrow A$

Esimerkki 3. Esitä sanallinen muotoilu a) De Morganin 1. laille

$$\neg(A \wedge B) \leftrightarrow \neg A \vee \neg B,$$

b) modus tollens -päättelysäännölle

$$((A \rightarrow B) \wedge \neg B) \rightarrow \neg A.$$

Ratkaisu:

a) Jos A ja B ei ole tosi, niin A ei ole tosi tai B ei ole tosi. Jos A ei ole tosi tai B ei ole tosi, niin A ja B ei ole tosi.

b) Jos B on A :n looginen seuraus ja B ei ole tosi, niin A ei ole tosi.

Esimerkki 4. Osoita kontraposition laki oikeaksi totuustaulun avulla.

Ratkaisu: Muodostetaan totuustaulu lauseille $A \rightarrow B$ ja $\neg B \rightarrow \neg A$.

A	B	$A \rightarrow B$	$\neg A$	$\neg B$	$\neg B \rightarrow \neg A$
1	1	1	0	0	1
1	0	0	0	1	0
0	1	1	1	0	1
0	0	1	1	1	1

Koska lauseiden $A \rightarrow B$ ja $\neg B \rightarrow \neg A$ totuusarvot ovat samat kaikilla atomilauseiden A ja B totuusarvoilla, lauseet ovat loogisesti ekvivalentit.

Esimerkki 5. Osoita ilman totuustauluja, että lauseet a) $\neg(A \wedge \neg B)$ ja $\neg A \vee B$, b) $\neg C \rightarrow A \vee B$ ja $\neg A \wedge \neg B \rightarrow C$ ovat loogisesti ekvivalentit.

Ratkaisu: Logiikan päättelysääntöjen avulla voidaan muodostaa uusia, alkuperäisen lauseen kanssa loogisesti ekvivalentteja lauseita.

a)

$$\begin{aligned} \neg(A \wedge \neg B) & \quad \text{De Morganin laki} \\ \neg A \vee \neg(\neg B) & \quad \text{kaksoisnegaation laki} \\ \neg A \vee B & \end{aligned}$$

Lauseet $\neg(A \wedge \neg B)$ ja $\neg A \vee B$ ovat loogisesti ekvivalentit.

b)

$$\begin{aligned} \neg C \rightarrow A \vee B & \quad \text{kontraposition laki} \\ \neg(A \vee B) \rightarrow \neg(\neg C) & \quad \text{kaksoisnegaation laki} \\ \neg(A \vee B) \rightarrow C & \quad \text{De Morganin laki} \\ \neg A \wedge \neg B \rightarrow C & \end{aligned}$$

Lauseet $\neg C \rightarrow A \vee B$ ja $\neg A \wedge \neg B \rightarrow C$ ovat loogisesti ekvivalentit.

Tehtäviä.

- (1) Tutki, onko lause tautologia.
 - a) $A \vee \neg A$,
 - b) $A \wedge \neg A$,
 - c) $A \rightarrow B \vee A$,
 - d) $A \rightarrow B \wedge A$,
- (2) Osoita lause tautologiaksi.
 - a) $A \rightarrow B \wedge \neg B \leftrightarrow \neg A$.
 - b) $(A \rightarrow B) \wedge (B \rightarrow C) \rightarrow (A \rightarrow C)$.
- (3) Olkoot A : ”kello soi” ja B : ”tunti loppuu”. Kirjoita luonnollisella kielellä lauseet $A \rightarrow B$ ja $\neg(A \wedge \neg B)$. Tarkoittavatko ne samaa?
- (4) Osoita lauseet loogisesti ekvivalenteiksi totuustaulujen avulla.
 - a) $A \wedge B$ ja $\neg(\neg A \vee \neg B)$.
 - b) $A \leftrightarrow B$ ja $(A \rightarrow B) \wedge (B \rightarrow A)$.
 - c) $A \leftrightarrow B$ ja $(A \wedge B) \vee (\neg A \wedge \neg B)$.

- (5) Osoita vaihdantalait

a)

$$A \wedge B \leftrightarrow B \wedge A,$$

b)

$$A \vee B \leftrightarrow B \vee A$$

oikeaksi totuustaulujen avulla.

- (6) Muodosta atomilauseista A ja B lause, joka on loogisesti ekvivalentti lauseen X kanssa.

A	B	X
1	1	0
1	0	1
0	1	1
0	0	1

- (7) Tutki, onko lause loogisesti ristiriitainen.
 - a) $\neg(A \vee B) \wedge \neg(A \wedge B)$,
 - b) $(\neg A \wedge B) \wedge (A \leftrightarrow B)$,
 - c) $(\neg(A \rightarrow B) \wedge C) \wedge B$.
- (8) Tulkitse sanallisesti a) De Morganin 2. laki

$$\neg(A \vee B) \leftrightarrow \neg A \wedge \neg B$$

b) modus ponens -päätelysääntö

$$(A \wedge (A \rightarrow B)) \rightarrow B$$

c) reductio ad absurdum -päätelysääntö.

$$(\neg A \rightarrow (B \wedge \neg B)) \rightarrow A$$

- (9) Osoita

- a) kaksoisnegaation laki,
- b) De Morganin 1. laki,

- c) modus ponens -päätelysääntö oikeaksi totuustaulujen avulla.
- (10) Osoita kontraposition laki oikeaksi ilman totuustauluja. Vihe: Voit korvata implikaation $A \rightarrow B$ loogisesti ekvivalentilla lauseella $\neg A \vee B$.
- (11) Esitä lauseelle ”jos Jaakko saa logiikan kurssista arvosanan 10, hän tarjoaa ystävilleen kahvit” kolme loogisesti ekvivalenttia lausetta.
- (12) Osoita lauseet loogisesti ekvivalenteiksi päätelysääntöjen avulla ilman totuustauluja.
- a) $A \wedge B$ ja $\neg(\neg A \vee \neg B)$,
 b) $C \rightarrow (\neg A \wedge B)$ ja $(A \vee \neg B) \rightarrow \neg C$.
 c) $A \wedge (A \rightarrow \neg B) \rightarrow \neg B$ ja $B \rightarrow \neg A \vee \neg(B \rightarrow \neg A)$.
- (13) (Lisämateriaalia) Kolmiarvologiikassa on kolme totuusarvoa 1 tosi, 0 epätosi ja u epävarma. Kleenen totuustaulut perustuvat ajatukseen, että epävarma voi myöhemmin osoittautua todeksi tai epätodeksi. Alla on esitetty negaation ja konjunktion totuustaulut. Täydennä oheinen disjunktion totuustaulu. Laadi implikaation ja ekvivalenssin totuustaulut.

A	$\neg A$
1	0
0	1
u	u

A	B	$A \wedge B$
1	1	1
1	0	0
0	1	0
0	0	0
1	u	u
u	1	u
0	u	0
u	0	0
u	u	u

A	B	$A \vee B$
1	1	
1	0	
0	1	
0	0	
1	u	
u	1	
0	u	
u	0	
u	u	

Kotitehtäviä.

- (1) Osoita lause tautologiaksi.
- a) $A \rightarrow A$.
 b) $A \wedge B \rightarrow A$.
 c) $(A \leftrightarrow B) \rightarrow (B \rightarrow A)$.
- (2) Tutki, onko lause tautologia.
- a) $(A \wedge B \rightarrow \neg C) \leftrightarrow (A \rightarrow (B \rightarrow C))$.
 b) $(\neg A \leftrightarrow (B \wedge C)) \leftrightarrow \neg(A \leftrightarrow B \wedge C)$.
- (3) Olkoot A : ”tunti jatkuu” ja B : ”kello soi”. Kirjoita luonnollisella kielellä lauseet $A \rightarrow \neg B$ ja $B \rightarrow \neg A$. Osoita totuustaulujen avulla, että lauseet ovat loogisesti ekvivalentit.
- (4) Osoita, että lauseet ovat loogisesti ekvivalentit.
- a) ”Tero soittaa kitaraa, mutta Suvi ei laskettele” ja ”ei ole niin, että jos Tero soittaa kitaraa, niin Suvi laskettelee”.

- b) ”Jos Tero soittaa kitaraa tai Suvi laskettelee, niin Anni kirjoittaa runoja” ja ”jos Tero soittaa kitaraa, niin Anni kirjoittaa runoja, ja jos Suvi laskettelee, niin Anni kirjoittaa runoja”.
- (5) Sievennä lause eli muodosta mahdollisimman yksinkertainen lause, joka on loogisesti ekvivalentti alkuperäisen lauseen kanssa.
- a) $(A \wedge B) \vee A$.
 b) $(A \vee B) \wedge A$.
 c) $(A \vee B) \wedge (A \vee \neg B)$
- (6) Osoita osittelulait
- a)

$$A \wedge (B \vee C) \leftrightarrow (A \wedge B) \vee (A \wedge C),$$

b)

$$A \vee (B \wedge C) \leftrightarrow (A \vee B) \wedge (A \vee C)$$

oikeaksi totuustaulujen avulla.

- (7) Muodosta atomilauseista A ja B lause, joka on loogisesti ekvivalentti lauseen Y kanssa.

A	B	Y
1	1	1
1	0	1
0	1	1
0	0	1

- (8) Tarkastele seuraavaa ennustetta: maapallon öljyvarat ehtyvät, jos ja vain jos länsimaiset demokratiat romahtavat, mutta ei pidä paikkaansa, että jos maapallon öljyvarat ehtyvät, niin länsimaiset demokratiat romahtavat. Miten ennusteeseen pitäisi suhtautua?
- (9) Mainitse esimerkki tilanteesta, jossa olet käyttänyt
- a) modus ponens -päättelysääntöä
 b) modus tollens -päättelysääntöä.
- (10) Osoita
- a) De Morganin 2. laki,
 b) modus tollens -päättelysääntö,
 c) reductio ad absurdum -päättelysääntö
 oikeaksi totuustaulujen avulla.
- (11) Osoita lauseet loogisesti ekvivalenteiksi päättelysääntöjen avulla ilman totuustauluja.
- a) $\neg\neg\neg\neg A$ ja $\neg A$,
 b) $A \rightarrow (B \rightarrow C)$ ja $\neg(\neg C \rightarrow \neg B) \rightarrow \neg A$.
 c) $\neg(A \wedge B \wedge \neg C)$ ja $\neg A \vee \neg B \vee C$.
- (12) Shefferin viivaan ja Peircen nuoleen on tutustuttu edellisen kapaleen kotitehtävässä XX. Esitä negatio, konjunktio ja disjunktio a) Shefferin viivan avulla b) Peircen nuolen avulla.

- (13) (Lisämateriaalia) Sumean logiikka on kaksiarvoisen logiikan laajennus, jossa lauseella on diskreetin totuusarvon (tosi tai epätosi) sijasta reaalinen totuusarvo, joka kuuluu välille $[0, 1]$. Konnektiivit voidaan määritellä esimerkiksi seuraavasti:

$$\begin{aligned}\neg A &= 1 - A, \\ A \wedge B &= \min(A, B), \\ A \vee B &= \max(A, B), \\ A \rightarrow B &= \min(1, 1 - A + B),\end{aligned}$$

missä \min tarkoittaa luvuista pienempää ja \max suurempaa.

- a) Olkoot lauseen A totuusarvo $0,3$ ja lauseen B totuusarvo $0,5$. Laske lauseiden $\neg A$, $A \wedge B$, $A \vee B$ ja $A \rightarrow B$ totuusarvot.
- b) Osoita, että jos lauseet A ja B saavat vain arvoja 0 ja 1 , niin edellä mainitut määritelmät johtavat klassisen kaksiarvoisen logiikan totuustauluihin.
- c) Osoita, että sumean logiikassa $\neg(A \wedge B) \leftrightarrow \neg A \vee \neg B$.
- d) Etsi Internetistä sumean logiikan käyttökohteita.

- (14) (Lisämateriaalia?) Tutustu Wolfram Alphan logiikkatoimintoihin

<http://www.wolframalpha.com/examples/BooleanAlgebra.html>
ja yritä laskea sen avulla joitakin kirjan tehtäviä.

3. LOGIIKKA JA MATEMATIIKKA

Matematiikka on logiikan keskeinen sovellusalue. Matematiikan rakenteita tutkivaa logiikan aluetta kutsutaan matemaattiseksi logiikaksi. Matemaattisessa logiikassa tutkitaan lauseita, joissa loogisten symbolien lisäksi voi esiintyä matemaattisia merkintöjä, kuten yhtäsuuruus, lukuja, muuttujia tai laskutoimituksia. Matemaattisen logiikan tutkimuskohteita ovat matemaattiset teoriat ja todistukset.

3.1. Joukko-oppia (mahdollisesti lisämateriaalia). Seuraavaksi tutkitaan logiikan soveltamista matemaattisiin rakenteisiin, joita kutsutaan *joukoiksi*.

Tutkimustehtävä. Luokalla on 34 opiskelijaa. Heistä 21 laulaa kuorossa ja 16 soittaa jotain soitinta. Neljä opiskelijaa ei laula kuorossa eikä soita mitään soitinta.

- a) Kuinka moni luokan opiskelijoista ei laula kuorossa?
- b) Kuinka moni opiskelija laulaa kuorossa tai soittaa jotain soitinta?
- c) Kuinka moni opiskelija laulaa kuorossa ja soittaa jotain soitinta?
- d) Kuinka moni kuorossa laulavista opiskelijoista ei soita mitään soitinta?

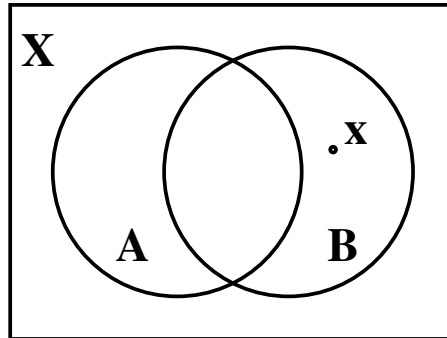
Joukko on kokoelma *alkioita*. Jos x on joukon A alkio, merkitään $x \in A$. Äärellinen joukko voidaan määritellä luettelemalla sen alkiot aaltosulkeiden sisällä:

$$A = \{x_1, x_2, \dots, x_n\}.$$

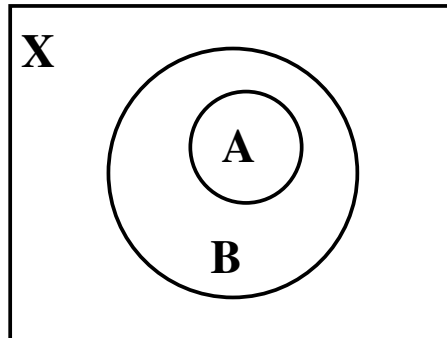
Joukot A ja B ovat samat, jos niillä on samat alkiot. Alkioiden järjestyksellä ei ole merkitystä. Sama alkio voi esiintyä joukossa vain kerran.

Tarkastelun kohteena olevien asioiden joukkoa kutsutaan joukko-opissa *perusjoukoksi*. Perusjoukkoa merkitään X . Kaikkien alkioiden ajatellaan kuuluvan perusjoukkoon X , eli lause $x \in X$ on aina tosi. Perusjoukko on usein lukujoukko, esimerkiksi luonnollisten lukujen joukko \mathbb{N} tai reaali lukujen joukko \mathbb{R} .

Alkion x kuulumista joukkoon havainnollistetaan usein niin kutsutun *Venn-diagrammin* avulla. Venn-diagrammissa perusjoukkoa X merkitään yleensä suorakulmiolla, jonka sisään piirretään ympyröitä kuvaamaan tutkittavia joukkoja A , B , jne. Jos x ei kuulu joukkoon A , niin merkitään $x \notin A$. Kuvassa alkio x kuuluu joukkoon B mutta ei joukkoon A .



Jos kaikki joukon A alkiot ovat myös joukon B alkioita, niin joukkoa A kutsutaan joukon B *osajoukoksi*. Osajoukkoa merkitään $A \subset B$.



Jos $A \subset B$ ja $B \subset A$, niin A ja B ovat sama joukko. Tällöin merkitään $A = B$. Samuus tarkoittaa sitä, että kyseisillä joukoilla on samat alkiot.

Esimerkki 1. Akaan kaupunki muodostuu Toijalan, Viialan ja Kylmäkosken kylistä. Akaa taas on osa Pirkanmaan maakuntaa. Olkoot $A = \{\text{akaalaiset}\}$, $T = \{\text{toijalalaiset}\}$, $V = \{\text{viialalaiset}\}$, $K = \{\text{kylmäkoskelaiset}\}$ ja $P = \{\text{pirkanmaalaiset}\}$. Onko lause tosi?

- a) $V \subset A$
- b) $A \subset T$
- c) $A \subset P$
- d) $K \subset P$

(Sopiva kuva/kartta?)

Ratkaisu. a) Kaikki viialalaiset ovat akaalaisia, joten lause on tosi.

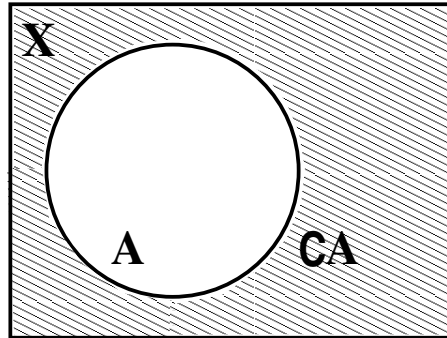
b) Lauseen mukaan kaikki akaalaiset ovat toijalalaisia. Lause on epätosi.

c) Kaikki akaalaiset ovat pirkanmaalaisia, joten lause on tosi.

d) Lauseen mukaan kaikki kylmäkoskelaiset ovat pirkanmaalaisia. Koska kylmäkoskelaiset ovat akaalaisia ja akaalaiset pirkanmaalaisia, niin lause on tosi.

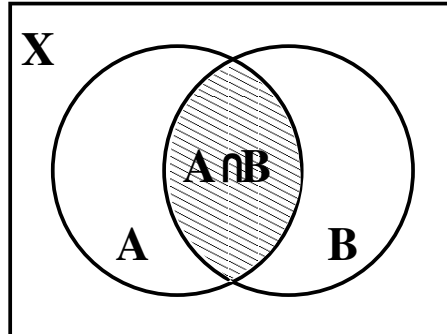
Vastaus: a) On. b) Ei ole. c) On. d) On.

Ne perusjoukon X alkiot, jotka eivät kuulu joukkoon A , muodostavat joukon A *komplementin*. Joukon A komplementtia merkitään $\complement A$.

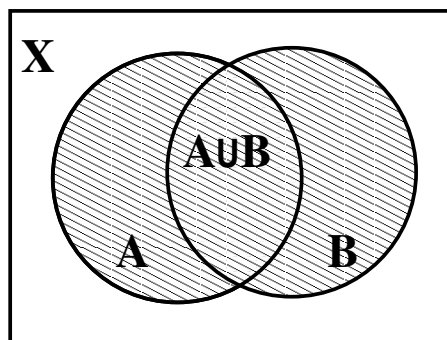


Perusjoukon X komplementti on *tyhjä joukko*, jota merkitään \emptyset . Tyhjässä joukossa ei ole alkioita. Erityisesti tyhjä joukko on minkä tahansa joukon osajoukko.

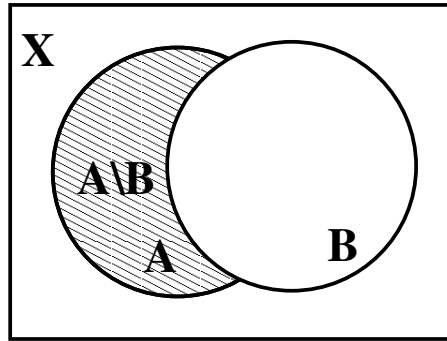
Joukkojen A ja B *leikkaus* $A \cap B$ on niiden perusjoukon alkioiden joukko, jotka kuuluvat sekä joukkoon A että joukkoon B . Leikkausta voidaan havainnollistaa Venn-diagrammilla:



Joukkojen A ja B *yhdiste* $A \cup B$ muodostuu niistä perusjoukon alkioista, jotka kuuluvat jompaankumpaan joukoista A ja B . Joukkojen yhdistettä voidaan jälleen havainnollistaa Venn-diagrammin avulla:



Joukkojen A ja B *erotuksella* tarkoitetaan joukkoa, joka jää jäljelle, kun joukosta A poistetaan kaikki joukon B alkiot. Tätä joukkoa merkitään $A \setminus B$.



Esimerkki 2. Olkoot $A = \{0, 1, 2, 3, 4, 5, 6\}$ ja $B = \{2, 4, 6, 8, 10\}$. Määritä joukot a) $A \cup B$ b) $A \cap B$ c) $A \setminus B$ d) $B \setminus A$.

Ratkaisu: a) Joukkojen A ja B yhdisteeseen $A \cup B$ kuuluvat ne alkiot, jotka kuuluvat jompaankumpaan joukoista A ja B . Siten $A \cup B = \{0, 1, 2, 3, 4, 5, 6, 8, 10\}$.

b) Joukkojen A ja B leikkaukseen $A \cap B$ kuuluvat ne alkiot, jotka kuuluvat sekä joukkoon A että joukkoon B . Siten $A \cap B = \{2, 4, 6\}$.

c) Joukkojen A ja B erotukseen $A \setminus B$ kuuluvat ne alkiot, jotka kuuluvat joukkoon A , mutta eivät joukkoon B . Siten $A \setminus B = \{0, 1, 3, 5\}$.

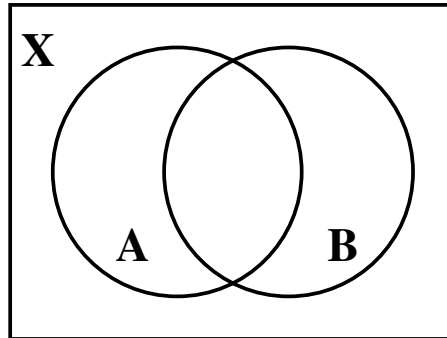
d) Vastaavasti erotukseen $B \setminus A$ kuuluvat ne alkiot, jotka kuuluvat joukkoon B , mutta eivät joukkoon A . Siten $B \setminus A = \{8, 10\}$.

Vastaus: a) $A \cup B = \{0, 1, 2, 3, 4, 5, 6, 8, 10\}$, b) $A \cap B = \{2, 4, 6\}$, c) $A \setminus B = \{0, 1, 3, 5\}$, d) $B \setminus A = \{8, 10\}$.

Esimerkki 3. Koulussa on 700 opiskelijaa. Erään kyselyn tuloksena saatiin selville, että 550 heistä seuraa uutisia säännöllisesti sanomalehdistä ja 400 Internetistä. Opiskelijoista 350 seuraa uutisia säännöllisesti kummastakin lähteestä. Havainnollista tilannetta Venn-diagrammilla ja vastaa seuraaviin kysymyksiin.

- a) Kuinka moni opiskelija seuraa uutisia vain Internetistä?
- b) Kuinka moni opiskelija ei seuraa uutisia ollenkaan?

Ratkaisu:



Perusjoukko X sisältää kaikki koulun opiskelijat. Joukkoon A kuuluvat opiskelijat, jotka seuraavat uutisia sanomalehdistä, ja joukkoon B opiskelijat, jotka seuraavat uutisia Internetistä.

a) Opiskelijoista 400 seuraa uutisia Internetistä ja 350 heistä seuraa uutisia myös sanomalehdistä. Näin ollen $400 - 350 = 50$ opiskelijaa seuraa uutisia vain Internetistä. Tämä on joukon $B \setminus A$ alkioden lukumäärää.

b) Ainakin toisesta lähteestä uutisia seuraa $550 + 400 - 350 = 600$ opiskelijaa. Tällöin $700 - 600 = 100$ opiskelijaa ei seuraa uutisia ollenkaan. Tämä on joukon $\mathbb{C}(A \cup B)$ alkioden lukumäärä.

Vastaus: a) 50 opiskelijaa b) 100 opiskelijaa

Esimerkki 4. Olkoot perusjoukko \mathbb{R} sekä joukot A ja B reaalilukuvälit $A =] - 5, 1]$ ja $B =] - 2, 4]$. Ilmaise välimerkintää käyttäen joukot a) $A \cup B$, b) $A \setminus B$, c) $\mathbb{C}A$, d) $\mathbb{C}(A \cap B)$. (**lukusuora jonnekin?**)

Ratkaisu:

- Joukkojen A ja B yhdisteeseen $A \cup B$ kuuluvat ne luvut, jotka kuuluvat jompaankumpaan joukoista A ja B . Siten $A \cup B =] - 5, 4]$.
- Joukkojen A ja B erotukseen $A \setminus B$ kuuluvat ne luvut, jotka kuuluvat joukkoon A , mutta eivät joukkoon B . Siten $A \setminus B =] - 5, -2]$.
- Joukon A komplementtiin $\mathbb{C}A$ kuuluvat ne reaaliluvut, jotka eivät kuulu joukkoon A . Komplementti muodostuu väleistä $] - \infty, -5]$ ja $]1, \infty[$. Siten $\mathbb{C}A =] - \infty, -5] \cup]1, \infty[$.
- Joukkojen A ja B leikkaukseen kuuluvat ne luvut, joka kuuluvat sekä joukkoon A että joukkoon B . Siten $A \cap B =] - 2, 1]$. Leikkauksen komplementtiin kuuluvat kaikki muut reaaliluvut, joten $\mathbb{C}(A \cap B) =] - \infty, -2] \cup]1, \infty[$.

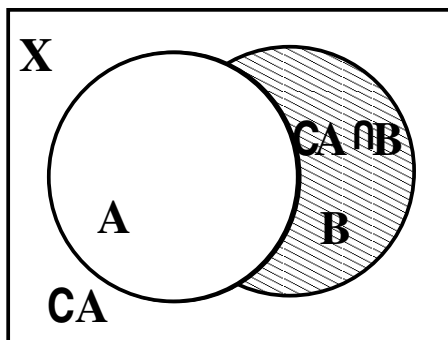
Vastaus:

- $A \cup B =] - 5, 4]$,

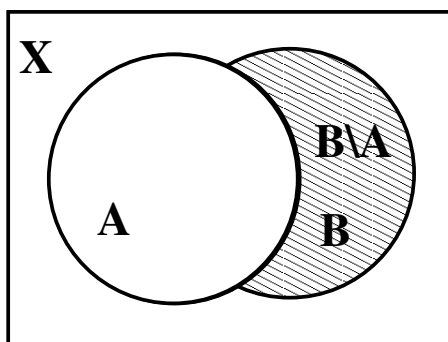
- b) $A \setminus B =]-5, -2]$,
 c) $\complement A =]-\infty, -5] \cup]1, \infty[$,
 d) $\complement(A \cap B) =]-\infty, -2] \cup]1, \infty[$.

Esimerkki 5. Osoita Venn-diagrammia käyttäen, että $\complement A \cap B = B \setminus A$.

Ratkaisu:



Joukon A komplementtijoukko $\complement A$ on niiden perusjoukon alkioiden joukko, jotka eivät kuulu joukkoon A , ja $\complement A \cap B$ on tämän joukon leikkaus joukon B kanssa.



Joukko $B \setminus A$ sisältää ne joukon B alkiot, jotka eivät kuulu joukkoon A . Venn-diagrammit havainnollistavat, että on kyse samasta joukosta. Siis $\complement A \cap B = B \setminus A$.

Tehtäviä.

(1) Onko lause tosi?

- a) $K \subset A$
- b) $A \subset V$
- c) $V \subset P$
- d) $V \subset T$

Merkinnät ovat samat kuin esimerkissä 1.

(2) Olkoot $A = \{7, 8, 9\}$ ja $B = \{5, 6, 7\}$. Määritä joukot

- a) $A \cup B$,
- b) $A \cap B$,
- c) $A \setminus B$,
- d) $B \setminus A$.

(3) Olkoot perusjoukko X aakkoset, A vokaalit ja $B = \{x, y, z\}$.

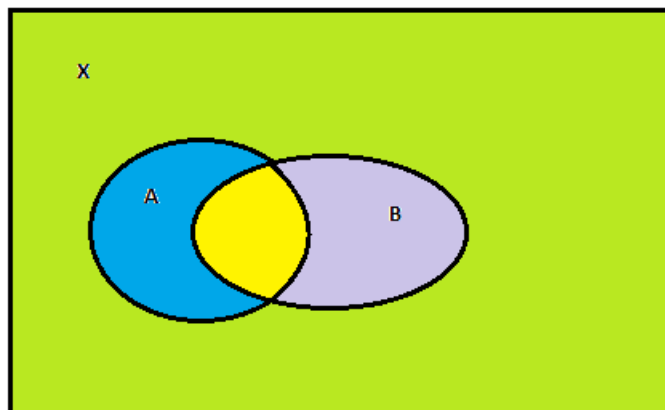
Määritä joukot

- a) $B \setminus A$,
- b) $A \cap B$,
- c) $\complement A$,
- d) $A \setminus X$.

(4) Olkoot A koulussa opiskelevien täysi-ikäisten opiskelijoiden joukko ja B niiden opiskelijoiden joukko, jotka asuvat vanhempiansa luona. Millaiset opiskelijat kuuluvat joukkoon a) $A \cap B$, b) $\complement A$, c) $A \cup \complement B$, d) $A \setminus B$, e) $B \setminus A$, f) $\complement(A \cup B)$?

(5) Ilmaise joukkomerkintöjä käyttäen kuvan

- a) keltainen alue,
- b) sininen alue,
- c) violetti alue,
- d) vihreä alue.



(6) Olkoot $A \cap B$, $A \setminus B$ ja $B \setminus A$ epätyhjiä joukkoja. Esitä Venn-diagrammissa varjostettuna alue, joka kuvaa joukkoa a) $\complement(A \cup B)$, b) $\complement(A \cap B)$, c) $\complement B \cap A$.

- (7) Luokalla on 30 opiskelijaa. Heistä 14 harrastaa jääkiekkoa, 12 jalkapalloa ja 3 molempia.

- Kuinka moni opiskelija harrastaa pelkkää jääkiekkoa?
- Kuinka moni opiskelija harrastaa pelkkää jalkapalloa?
- Kuinka moni opiskelija ei harrasta kumpaakaan?

Vihje: Tilanteesta kannattaa piirtää Venn-diagrammi.

- (8) Olkoot perusjoukko \mathbb{R} sekä joukot A ja B reaalilukuvälit $A = [1, 5]$ ja $B = [3, 6]$. Ilmaise välimerkintää käyttäen joukot

- $A \cap B$,
- $A \cup B$,
- $A \setminus B$,
- $\complement A$.

- (9) Yhdistä samaa tarkoittavat lauseet.

A	$(x \in A) \wedge (x \in B)$	1	$x \in \complement A$
B	$x \notin A$	2	$x \in A \setminus B$
C	$(x \in A) \vee (x \in B)$	3	$x \in (A \cap B)$
D	$(x \in A) \wedge (x \notin B)$	4	$x \in (A \cup B)$

- (10) Osoita Venn-diagrammin avulla, että

a)

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C),$$

b)

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C).$$

- (11) Sievennä Venn-diagrammin avulla.

- $(B \cap A) \cup (B \cap \complement A)$
- $\complement(A \cup B) \cup (A \setminus B) \cup (B \setminus A)$

- (12) Olkoot perusjoukko kokonaislukujen joukko \mathbb{Z} , W parillisten kokonaislukujen joukko ja Y luvulla 3 jaollisten kokonaislukujen joukko. Näitä joukkoja voidaan merkitä $W = \{2n \mid n \in \mathbb{Z}\}$ ja $Y = \{3n \mid n \in \mathbb{Z}\}$. Määritä joukot a) $W \cap Y$, b) $W \setminus Y$, c) $W \cup Y$.

- (13) Onko lause tosi?

- $\sqrt{2} \in \mathbb{R}$
- $-3 \in \mathbb{N}$
- $\pi \in \mathbb{R} \setminus \mathbb{Q}$
- $\frac{4}{2} \in \mathbb{Q} \setminus \mathbb{Z}$
- $\emptyset \subset \mathbb{Z}$

- (14) Määritä joukon a) $\{1, 2\}$ b) $\{1, 2, 3\}$ kaikki osajoukot.

- (15) (Lisämateriaalia) Joukon A *potenssijoukoksi* $\mathcal{P}(A)$ kutsutaan kaikkien joukon A osajoukkojen muodostamaa joukkoa:

$$\mathcal{P}(A) = \{B \mid B \subset A\}.$$

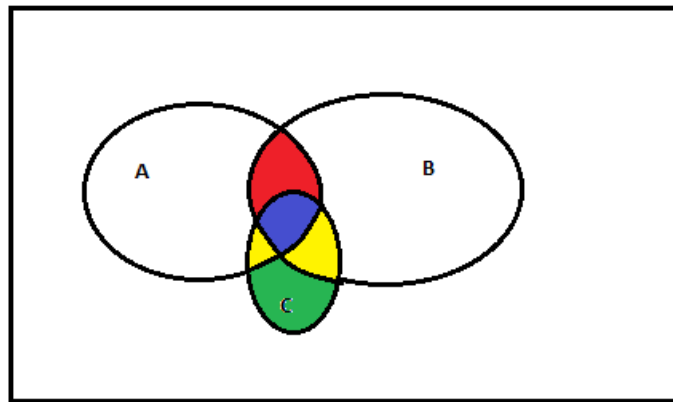
- Määritä joukon $\{1, 2, 3\}$ potenssijoukko.
- Määritä tyhjän joukon \emptyset potenssijoukko.
- Joukko $\{\emptyset\}$ on joukko, jonka ainut alkio on tyhjä joukko. Määritä joukon $\{\emptyset\}$ potenssijoukko.

- (16) (Lisämateriaalia) Luonnolliset luvut voidaan tulkita joukko-opillisesti käyttämällä edellisessä tehtävässä esitettyä potenssijoukon käsitettä. Ajatuksena on, että lukua 0 vastaa tyhjä joukko \emptyset ja kutakin luonnollista lukua $n+1$ vastaava joukko on luonnollista lukua n vastaavan joukon potenssijoukko. Siis esimerkiksi lukua 1 vastaa tyhjän joukon \emptyset potenssijoukko $\mathcal{P}(\emptyset)$, lukua 2 potenssijoukko $\mathcal{P}(\mathcal{P}(\emptyset))$ ja niin edelleen.
- Määritä lukuja 3 ja 4 vastaavat joukot.
 - Mitä luonnollista lukua vastaa joukko $\{\emptyset, \{\emptyset\}\}$?
 - Vastaako joukko $\{\{\emptyset\}\}$ jotakin luonnollista lukua? Miksi?

Kotitehtäviä

- Olkooot $A = \{a, b, c, d\}$ ja $B = \{a, c, e\}$. Määritä joukot
 - $A \cup B$,
 - $A \cap B$,
 - $A \setminus B$,
 - $B \setminus A$.
- Onko lukujoukkoja koskeva lause tosi?
 - $\mathbb{Z} \subset \mathbb{N}$
 - $\mathbb{Z} \subset \mathbb{Q}$
 - $\mathbb{R} \subset \mathbb{Z}$
 - $\mathbb{Q} \subset \mathbb{N}$
 - $\mathbb{Q} \subset \mathbb{Q}$
- Olkooot perusjoukko X aakkoset, $A = \{j, o, k, u\}$, $B = \{k, o, j, u\}$ ja $C = \{k, a, j, o\}$. Määritä joukot
 - $A \setminus B$,
 - $(A \cap B) \cup C$,
 - $A \setminus \mathcal{C}(B \cup C)$.
- Olkooot X perusjoukko ja A jokin perusjoukon osajoukko. Sievennä.
 - $A \cup \emptyset$
 - $A \cap \emptyset$
 - $A \cap X$
 - $A \cup X$
- Olkooot $A \subset B$ ja $B \setminus A$ epätyhjä. Esitä Venn-diagrammissa varjostettuna alue, joka kuvaa joukkoa a) $B \setminus A$, b) $\mathcal{C}A \cap B$, c) $A \cup \mathcal{C}B$.
- Olkoon perusjoukko X kaikkien kalenterivuoden päivien joukko. Olkooot A arkipäivien (maanantai–perjantai) joukko, L liputuspäivien joukko ja T toukokuulle ajoittuvien päivien joukko. Millaiset päivät kuuluvat joukkoon
 - $\mathcal{C}A$
 - $L \cap \mathcal{C}T$
 - $L \setminus A$
 - $T \setminus (A \cup L)$

- e) $\mathbb{C}(A \cup L \cup T)$?
- (7) Onko lause tosi?
- $0 \in \{0, 1, 2\}$
 - $\{0\} \subset \{0, 1, 2\}$
 - $\emptyset \subset \{1, 2\}$
 - $\{\text{å, ä, ö}\} \subset \{\text{o, ä, ö}\}$
- (8) Luokan opiskelijoista kahdeksalla on läppäri, kymmenellä pöytäkone ja viidellä tabletti. Kahdella opiskelijalla on sekä läppäri että pöytäkone, kolmella sekä tabletti että pöytäkone, mutta kellekään ei ole sekä läppäriä että tablettia. Kahdella opiskelijalla ei ole mitään tietokonetta.
- Piirrä tilannetta kuvaava Venn-diagrammi.
 - Kuinka monella opiskelijalla on läppäri mutta ei pöytäkonetta?
 - Kuinka monella opiskelijalla on vain pöytäkone?
 - Kuinka monta opiskelijaa luokalla on?
- (9) Olkoot perusjoukko \mathbb{R} sekä joukot A ja B reaalilukuvälit $A =] - 1, 2[$ ja $B = [0, 4[$. Ilmaise välimerkintää käyttäen joukot
- $A \cup B$,
 - $A \cap B$,
 - $\mathbb{C}(A \cap B)$,
 - $B \setminus A$,
 - $B \setminus (A \cap B)$,
 - $A \cap \mathbb{C}B$.
- (10) Osoita Venn-diagrammin avulla, että
- $$X \setminus (A \cup B) = (X \setminus A) \cap (X \setminus B),$$
 - $$X \setminus (A \cap B) = (X \setminus A) \cup (X \setminus B).$$
- (11) Jos $A \subset B$ ja $B \subset C$, niin mitä voidaan päätellä joukoista A ja C ? Perustele
- Venn-diagrammin avulla,
 - osajoukon määritelmän avulla.
- (12) Onko lause tosi?
- $A \cap B \subset A$
 - $\mathbb{C}(\mathbb{C}A) = A$
 - $(A \cup B) \setminus B = A$
 - $A \cap \mathbb{C}B = A \setminus B$
 - $B \cap \mathbb{C}B = B$
- (13) Ilmaise joukkomerkitöjä käyttäen kuvan
- punainen alue,
 - sininen alue,
 - vihreä alue,
 - keltainen alue.



- (14) Tarkastellaan kaksinumeroisia luonnollisia lukuja $10, 11, \dots, 98, 99$.
- a) Kuinka monta kaksinumeroista luonnollista lukua on olemassa?
 - b) Kuinka moni niistä on jaollinen luvulla 4? Kuinka moni ei ole jaollinen luvulla 4?
 - c) Kuinka moni kaksinumeroisista luonnollisista luvuista on jaollinen luvulla 6?
 - d) Kuinka moni kaksinumeroisista luonnollisista luvuista on jaollinen luvuilla 4 ja 6?
 - e) Kuinka moni kaksinumeroisista luonnollisista luvuista on jaollinen luvulla 4 tai luvulla 6?
 - f) Kuinka moni kaksinumeroisista luonnollisista luvuista ei ole jaollinen luvulla 4 eikä luvulla 6?
 - g) Piirrä tilanteesta Venn-diagrammi.

3.2. Avoin lause ja konnektiivien joukko-opillinen tulkinta.

Tutkimustehtävä.

- 1) Ketkä seuraavista henkilöistä toteuttavat väitteen ”henkilö on entinen Suomen tasavallan presidentti”? a) Urho Kekkonen, b) Paavo Nurmi, c) Armi Kuusela, d) Tarja Halonen, e) Carl Gustaf Emil Mannerheim.
- 2) Lause $P(x)$ on ” $-10x = 100$ ”. Onko lause $P(-2)$, $P(5)$ tai $P(-10)$ tosi?
- 3) Millä kokonaisluvuilla lause $Q(x)$: ” $2x^2 - x - 1 = 0$ ” on tosi?

Avoin lause ja ratkaisujoukko. Lauselogiikassa asioiden tiloja ilmaisemaan käytetään atomilauseita, esimerkiksi lausetta S : ”sataa”. Tämän lauseen totuusarvo kuitenkin riippuu tarkastelijan olinpaikasta x . Onkin luonnollinen ajatus tarkastella loogista lausetta, jossa on *vapaa muuttuja*, tässä tapauksessa paikka x . Tällöin merkitään $S(x)$: ”paikassa x sataa”. Lauseen totuusarvo ratkeaa vasta, kun vapaan muuttujan arvo kiinnitetään. Siksi lausetta $S(x)$ kutsutaan *avoimeksi lauseeksi*. Avoimia lauseita kutsutaan myös *predikaateiksi*, ja avoimia lauseita käsittelevää logiikkaa sanotaan *predikaattilogiikaksi*.

Vapaa muuttuja saa arvoja annetusta perusjoukosta X . Perusjoukkoa ei ole tapana kirjoittaa näkyviin, jos se voidaan päätellä tilanteesta. Esimerkiksi yllä mainitussa avoimessa lauseessa $S(x)$ perusjoukkona ovat kaikki paikkakunnat. Avoimen lauseen *ratkaisujoukon* muodostavat puolestaan ne perusjoukon alkiot, joilla avoin lause on tosi. Esimerkiksi lauseen $S(x)$ ratkaisujoukkona ovat kaikki ne paikkakunnat, joilla sataa.

Avoimessa lauseessa voi olla useampiakin muuttujia, voitaisiin esimerkiksi tarkastella lausetta $S(x, t)$: ”paikassa x sataa hetkellä t ”. Monimutkaisempia avoimia lauseita voidaan muodostaa konnektiivien avulla.

Matematiikassa avoin lause on usein yhtälö tai epäyhtälö. Yhtälössä esiintyvät tuntemattomat voidaan tulkita vapaiksi muuttujiksi. Esimerkiksi voidaan merkitä $C(x)$: ” $\cos x + x^2 = 2$ ”. Avoimen lauseen ratkaisujoukko on niiden pisteiden x joukko, joilla kyseinen yhtälö toteutuu.

Esimerkki 1. Olkoon $P(x)$ avoin lause ” $2x - 10 = 0$ ”. Onko lause a) $P(5)$, b) $P(-5)$ tosi?

Ratkaisut:

a) Sijoitetaan luku 5 avoimeen lauseeseen muuttujan x paikalle. Koska $2 \cdot 5 - 10 = 10 - 10 = 0$, lause $P(5)$ on tosi.

b) Sijoitetaan luku -5 avoimeen lauseeseen muuttujan x paikalle. Koska $2 \cdot (-5) - 10 = -10 - 10 = -20 \neq 0$, lause $P(-5)$ on epätosi.

Vastaukset: a) On. b) Ei ole.

Esimerkki 2. Yhtälöiden ja epäyhtälöiden yhteydessä perusjoukkoa kutsutaan myös *määrittelyjoukoksi*. Ratkaise avoin lause $2x^2 + 5x - 3 < 0$, kun määrittelyjoukko on a) reaalilukujen joukko b) kokonaislukujen joukko.

Ratkaisut:

a) Tutkitaan polynomifunktion $2x^2 + 5x - 3$ merkkiä. Ratkaistaan funktion $2x^2 + 5x - 3$ nollakohdat toisen asteen yhtälön ratkaisukaavalla.

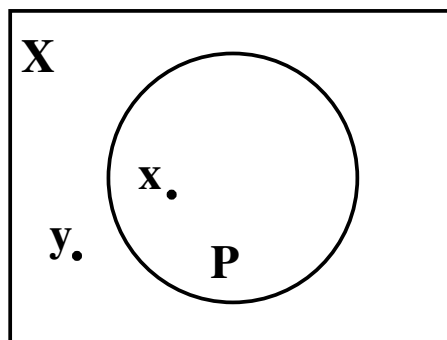
$$\begin{aligned} 2x^2 + 5x - 3 &= 0 \\ x &= \frac{-5 \pm \sqrt{5^2 - 4 \cdot 2 \cdot (-3)}}{2 \cdot 2} \\ x &= \frac{-5 \pm \sqrt{49}}{4} = \frac{-5 \pm 7}{4} \\ x &= -3 \text{ tai } x = \frac{1}{2}. \end{aligned}$$

Koska funktion $2x^2 + 5x - 3$ kuvaaja on ylöspäin aukeava paraabeli, avoin lause $2x^2 + 5x - 3 < 0$ toteutuu, kun $-3 < x < \frac{1}{2}$. Avoimen lauseen ratkaisujoukko on siis väli $] -3, \frac{1}{2}[$.

b) Kun määrittelyjoukko on kokonaislukujen joukko, a-kohdan ratkaisuihin kelpaavat vain $x = -2$, $x = -1$ ja $x = 0$. Avoimen lauseen ratkaisujoukko on siis $\{-2, -1, 0\}$.

Vastaukset: a) $-3 < x < \frac{1}{2}$, b) $x = -2$ tai $x = -1$ tai $x = 0$

Ominaisuudet ja osajoukot. Joukko-opin soveltamisen kannalta on usein hyödyllistä *samastaa* keskenään joukot ja perusjoukon X alkien ominaisuudet. Tällöin avoimelle lauseelle $P(x)$ käytetään myös merkintää $x \in P$. Jos $\neg P(y)$, voidaan merkitä $y \notin P$. Tätä voidaan havainnollistaa Venn-diagrammilla. Kuvassa $x \in P$ ja $y \notin P$.

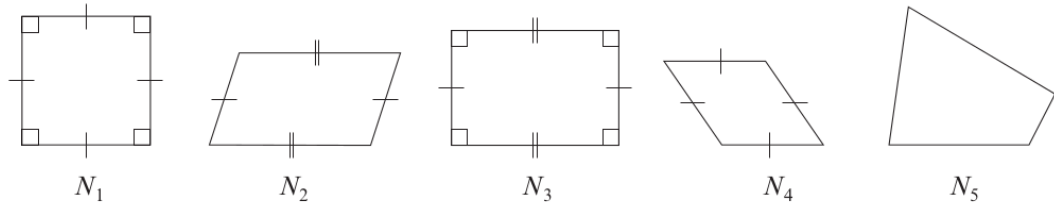


Jos predikaatit ajatellaan perusjoukon osajoukoiksi, niin joukko-opilliset operaatiot voidaan tulkita loogisina operaatioina. Kahden predikaatin P ja Q konjunktia $P \wedge Q$ vastaa joukko-opissa leikkaus $P \cap Q$, disjunktia $P \vee Q$ yhdiste $P \cup Q$ ja negaatiota $\neg P$ komplementtijoukko $\mathbb{C}P$. Tarkastellaan implikaation $P(x) \rightarrow Q(x)$ totuustaulua:

$x \in P$	$x \in Q$	$P(x) \rightarrow Q(x)$
1	1	1
1	0	0
0	1	1
0	0	1

Nähdään, että implikaatio on epätosi vain silloin, jos $x \in P$ mutta $x \notin Q$, toisin sanoen P ei ole Q :n osajoukko. Implikaatiota $P \rightarrow Q$ vastaa siis sisältymisrelaatio $P \subset Q$. Erityisesti periaatetta, että epätodesta lauseesta voidaan päätellä mitä tahansa, vastaa se, että tyhjä joukko \emptyset on minkä tahansa joukon osajoukko. Ekvivalenssia $P \leftrightarrow Q$ vastaava relaatio on joukko-opillinen yhtäsuuruus $P = Q$.

Esimerkki 3. Olkoon perusjoukko kuviossa olevien nelikulmioiden joukko. Olkoot avoin lause $K(x)$: ”nelikulmio x on suorakulmio” ja $S(x)$: ”nelikulmio x on suunnikas”. Ratkaise avoin lause. a) $K(x)$, b) $S(x)$, c) $\neg S(x)$, d) $\neg K(x) \wedge S(x)$ e) $K(x) \leftrightarrow S(x)$.



Ratkaisut:

a) Avoin lause $K(x)$ on tosi, kun nelikulmio on suorakulmio. Suorakulmioita ovat nelikulmiot N_1 ja N_3 , joten ratkaisujoukko on $\{N_1, N_3\}$.

b) Avoin lause $S(x)$ on tosi, kun nelikulmio on suunnikas. Suunnikkaita ovat nelikulmiot N_1 , N_2 , N_3 ja N_4 , joten ratkaisujoukko on $\{N_1, N_2, N_3, N_4\}$.

c) Negaatio $\neg S(x)$ on tosi, kun avoin lause $S(x)$ on epätosi eli kun nelikulmio ei ole suunnikas. Ehto toteutuu vain nelikulmiolla N_5 . Ratkaisujoukko on $\{N_5\}$.

d) Avoin lause $\neg K(x) \wedge S(x)$ on tosi, kun nelikulmio on suunnikas mutta ei suorakulmio. Ehto toteutuu nelikulmioilla N_2 ja N_4 , joten ratkaisujoukko on $\{N_2, N_4\}$.

e) Avoin lause $K(x) \leftrightarrow S(x)$ on tosi, kun nelikulmio on suorakulmio ja suunnikas tai ei kumpikaan. Ehto toteutuu nelikulmioilla N_1, N_3 ja N_5 , joten ratkaisujoukko on $\{N_1, N_3, N_5\}$.

Vastaukset: a) $\{N_1, N_3\}$, b) $\{N_1, N_2, N_3, N_4\}$, c) $\{N_5\}$, d) $\{N_2, N_4\}$, e) $\{N_1, N_3, N_5\}$.

Esimerkki 4. Heitetään kahta noppaa, punaista ja sinistä. Tuloksena saadaan lukupari (x, y) , missä x on punaisen nopan silmäluku ja y on sinisen nopan silmäluku. Perusjoukko X sisältää lukuparit

$(1, 1), (1, 2), (1, 3), (1, 4), (1, 5), (1, 6), (2, 1), (2, 2), \dots, (6, 5), (6, 6)$.

Olkoot avoimet lauseet $S(x, y)$: ” $x + y > 9$ ” ja $Y(x, y)$: ” $x = y$ ”. Määritä avoimen lauseen a) $S(x, y)$, b) $Y(x, y)$, c) $\neg S(x, y) \wedge Y(x, y)$, d) $\neg S(x, y) \rightarrow Y(x, y)$ ratkaisujoukko.

6						
5						
4						
3	(1,3)					
2	(1,2)	(2,2)				
1	(1,1)	(2,1)	(3,1)			
	1	2	3	4	5	6

Ratkaisu:

a) Avoin lause $S(x, y)$ on tosi, kun noppien silmälukujen summa on suurempi kuin 9 eli siis 10, 11 tai 12. Ehto toteutuu lukupareilla $(4, 6), (5, 5), (5, 6), (6, 4), (6, 5)$ ja $(6, 6)$. Ratkaisujoukko on

$$\{(4, 6), (5, 5), (5, 6), (6, 4), (6, 5), (6, 6)\}.$$

b) Avoin lause $Y(x, y)$ on tosi, kun noppien silmäluvut ovat samat. Ehto toteutuu lukupareilla $(1, 1), (2, 2), (3, 3), (4, 4), (5, 5)$ ja $(6, 6)$. Ratkaisujoukko on $\{(1, 1), (2, 2), (3, 3), (4, 4), (5, 5), (6, 6)\}$.

c) Avoin lause $\neg S(x, y) \wedge Y(x, y)$ on tosi, kun noppien silmälukujen summa on pienempi tai yhtä suuri kuin 9 ja kun silmäluvut ovat samat. Ehto toteutuu lukupareilla $(1, 1), (2, 2), (3, 3)$ ja $(4, 4)$. Ratkaisujoukko on $\{(1, 1), (2, 2), (3, 3), (4, 4)\}$.

d) Implikaatio $\neg S(x, y) \rightarrow Y(x, y)$ on tosi aina, kun avoin lause $\neg S(x, y)$ on epätosi eli kun $S(x, y)$ on tosi. Avoimen lauseen $S(x, y)$ ratkaisujoukko on määritetty a-kohdassa. Lisäksi implikaatio $\neg S(x, y) \rightarrow$

$Y(x, y)$ on tosi silloin, kun avoimet lauseet $\neg S(x, y)$ ja $Y(x, y)$ ovat molemmat tosia. Tämän tapauksen ratkaisujoukko on määritetty c -kohdassa. Implikaation $\neg S(x, y) \rightarrow Y(x, y)$ ratkaisujoukko on siis

$$\{(1, 1), (2, 2), (3, 3), (4, 4), (4, 6), (5, 5), (5, 6), (6, 4), (6, 5), (6, 6)\}.$$

Vastaukset: a) $\{(4, 6), (5, 5), (5, 6), (6, 4), (6, 5), (6, 6)\}$

b) $\{(1, 1), (2, 2), (3, 3), (4, 4), (5, 5), (6, 6)\}$

c) $\{(1, 1), (2, 2), (3, 3), (4, 4)\}$

d) $\{(1, 1), (2, 2), (3, 3), (4, 4), (4, 6), (5, 5), (5, 6), (6, 4), (6, 5), (6, 6)\}$

Esimerkki 5. Ratkaise reaalilukujen joukossa

a) yhtälö $(x + 4)(x^2 - 2) = 0$,

b) yhtälöpari

$$\begin{cases} x + 4 = 0, \\ x^2 - 2 = 0. \end{cases}$$

Ratkaisut:

a) Tulon nollasäännön perusteella yhtälö $(x + 4)(x^2 - 2) = 0$ toteutuu, kun $x + 4 = 0$ tai $x^2 - 2 = 0$.

Yhtälö $x + 4 = 0$ toteutuu, kun $x = -4$.

Yhtälö $x^2 - 2 = 0$ eli $x^2 = 2$ toteutuu, kun $x = \sqrt{2}$ tai $x = -\sqrt{2}$.

Siis yhtälö $(x + 4)(x^2 - 2) = 0$ toteutuu, kun $x = -4$ tai $x = -\sqrt{2}$ tai $x = \sqrt{2}$. Yhtälön ratkaisujoukko on $\{-4, -\sqrt{2}, \sqrt{2}\}$.

b) Yhtälöpari

$$\begin{cases} x + 4 = 0, \\ x^2 - 2 = 0, \end{cases}$$

toteutuu niillä reaaliluvuilla, jotka toteuttavat molemmat yhtälöt $x + 4 = 0$ ja $x^2 - 2 = 0$. a-kohdan perusteella tiedetään, että ensimmäinen yhtälö toteutuu, kun $x = -4$, ja jälkimmäinen, kun $x = -\sqrt{2}$ tai $x = \sqrt{2}$. Koska yhtälöparin

$$\begin{cases} x + 4 = 0, \\ x^2 - 2 = 0, \end{cases}$$

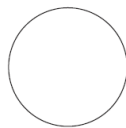
toteuttavat ne reaaliluvut, jotka toteuttavat sekä lauseen ” $x = -4$ ” että lauseen ” $x = -\sqrt{2}$ tai $x = \sqrt{2}$ ”, nähdään, että yhtälöparilla ei ole ratkaisuja. Yhtälöparin ratkaisujoukko on siis tyhjä joukko \emptyset .

Vastaukset:

a) $x = -4$ tai $x = -\sqrt{2}$ tai $x = \sqrt{2}$ b) Yhtälöparilla ei ole ratkaisuja.

Tehtäviä.

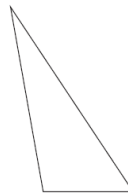
- (1) Olkoot $A(x)$ avoin lause ”paikkakunnalla x paistaa aurinko” ja $T(x)$ avoin lause ”paikkakunnalla x tuulee”. Suomenna lause.
 - a) $\neg T(x)$,
 - b) $A(x) \wedge T(y)$,
 - c) $\neg A(\text{Lempäälä})$,
 - d) $\neg(A(\text{Turku}) \rightarrow T(\text{Kuopio}))$.
- (2) Olkoot $S(x)$ avoin lause ” x on suomalainen formulakuljettaja” ja $E(x)$ avoin lause ” x on eurooppalainen formulakuljettaja, joka ei ole suomalainen”. Kuljettaja voi olla joko nykyinen tai entinen. Ratkaise avoin lause, kun perusjoukko on $\{\text{Räikkönen, Vettel, Senna}\}$.
 - a) $S(x)$,
 - b) $\neg S(x)$,
 - c) $E(x)$,
 - d) $\neg(S(x) \vee E(x))$.
- (3) Olkoon $Q(x)$ avoin lause ” $x^2 = 64$ ”. Onko lause a) $Q(-8)$ b) $Q(6)$ tosi?
- (4) Olkoon $P(x, y)$ avoin lause ” $x^2 + y \leq 0$ ”. Onko lause a) $P(0, 0)$ b) $P(-1, 1)$ c) $P(5, -100)$ tosi?
- (5) Ratkaise avoin lause $4x^2 + 7x - 2 = 0$, kun perusjoukko on a) reaalilukujen joukko b) kokonaislukujen joukko.
- (6) Olkoot perusjoukko $\{0, 1, 2, \dots, 10\}$, $A(x)$ avoin lause ” $x \leq 1$ ” ja $B(x)$ avoin lause ” $x > 5$ ”. Ratkaise avoin lause.
 - a) $A(x)$,
 - b) $\neg B(x)$,
 - c) $A(x) \wedge B(x)$,
 - d) $\neg A(x) \rightarrow B(x)$.



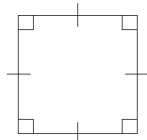
A



B



C



D



E



F

- (7) Olkoot $S(x)$ avoin lause ”kuvio x on symmetrinen jonkin suoran suhteen” ja $P(x)$ avoin lause ”kuvio x on symmetrinen jonkin pisteen suhteen”. Perusjoukon muodostavat oheiset kuviot. Ratkaise avoin lause.

- a) $S(x)$,
 - b) $P(x)$,
 - c) $\neg(S(x) \vee P(x))$,
 - d) $S(x) \leftrightarrow P(x)$.
- (8) Arvotaan kaksi lukua, joista molemmat voivat olla 1, 2 tai 3. Arvonnan tuloksena saadaan lukupari (x, y) , missä x on ensimmäisen arvonnän tulos ja y toisen arvonnän tulos. Olkoot avoimet lauseet $S(x, y)$: " $x \leq y$ " ja $T(x, y)$: "tulo xy on jaollinen luvulla 3". Ratkaise avoin lause, kun perusjoukon muodostavat arvonnän tuloksena saatavat mahdolliset lukuparit

$(1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (2, 3), (3, 1), (3, 2), (3, 3)$.

- a) $S(x, y)$,
 - b) $\neg T(x, y)$,
 - c) $\neg(S(x, y) \vee T(x, y))$,
 - d) $S(x, y) \rightarrow T(x, y)$.
- (9) Ratkaise reaalitylukujen joukossa
- a) epäyhtälö $x^2 \leq 4$,
 - b) epäyhtälöpari

$$\begin{cases} x^2 & \leq & 4 \\ x & > & -1. \end{cases}$$

- (10) Ratkaise reaalitylukujen joukossa epäyhtälö
- a) $|x| > 5$,
 - b) $|x| \leq 1$,
 - c) $|x - 4| > 5$,
 - d) $|2x - 6| \leq 1$.
- (11) Ratkaise avoin lause reaalitylukujen joukossa. Ilmaise ratkaisujoukko myös välimerkintää käyttäen.
- a) $(x^2 > 1) \vee (0 \leq x \leq 2)$,
 - b) $(x^2 > 1) \wedge (0 \leq x \leq 2)$,
 - c) $(x^2 > 1) \rightarrow (0 \leq x \leq 2)$.
- (12) Olkoot $P(x)$ avoin lause $(x < 10) \wedge (x^2 = 100)$ ja $Q(x)$ avoin lause $(x \geq 10) \leftrightarrow (x^2 = 100)$. Ratkaise avoin lause reaalitylukujen joukossa.
- a) $P(x)$,
 - b) $Q(x)$,
 - c) $P(x) \vee Q(x)$,
 - d) $P(x) \wedge Q(x)$.

Kotitehtäviä.

- (1) Olkoon $T(x, y)$ avoin lause " x lähettää tekstiviestin y :lle". Suomenna lause.
- a) $T(\text{Tiina}, \text{Elias})$,
 - b) $\neg T(\text{Elias}, \text{Tiina}) \wedge T(\text{Elias}, \text{Vilma})$,

- c) $T(x, x)$,
- d) $T(y, \text{Rasmus}) \leftrightarrow T(\text{Rasmus}, y)$.
- (2) Olkoot $E(x)$ avoin lause ” x on eurooppalainen pääkaupunki” ja $S(x)$ avoin lause ” x on suomalainen kaupunki”. Ratkaise avoin lause, kun perusjoukko on $\{\text{Helsinki}, \text{Rovaniemi}, \text{Praha}, \text{Milano}\}$.
 - a) $E(x)$,
 - b) $\neg S(x)$,
 - c) $S(x) \wedge \neg E(x)$,
 - d) $\neg(E(x) \wedge S(x))$,
 - e) $E(x) \leftrightarrow S(x)$.
- (3) Olkoon $R(x)$ avoin lause ” $x^2 - 100 > 0$ ”. Onko lause a) $R(10)$ b) $R(-15)$ tosi?
- (4) Olkoon $S(x, y)$ avoin lause ” $x^2 + y^2 = 5$ ”. Onko lause a) $S(2, 3)$ b) $S(2, -1)$ c) $S(-\sqrt{5}, 0)$ d) $S(-1, -1)$ tosi?
- (5) Ratkaise avoin lause $9x^2 + 30x + 25 \leq 0$, kun määrittelyjoukko on a) reaalilukujen joukko b) kokonaislukujen joukko.
- (6) Olkoot perusjoukko $\{1, 2, 3, \dots, 16\}$, $C(x)$ avoin lause ”luku 12 on jaollinen luvulla x ” ja $D(x)$ avoin lause ”luvun x neliöjuuri on kokonaisluku”. Ratkaise avoin lause.
 - a) $C(x)$,
 - b) $D(x)$,
 - c) $\neg C(x) \wedge D(x)$,
 - d) $C(x) \leftrightarrow D(x)$.
- (7) Arvotaan kolme lukua, joista jokainen voi olla 1 tai 2. Arvonnan tuloksena saadaan lukukolmikko (x, y, z) , missä x on ensimmäisen arvonnän tulos, y toisen arvonnän tulos ja z kolmannen arvonnän tulos. Olkoot avoimet lauseet $S(x, y, z)$: ” $x + y + z \geq 5$ ”, $T(x, y, z)$: ”tulo xyz on pariton” ja $U(x, y, z)$: ”summa $x + y + z$ on jaollinen luvulla 3”. Ratkaise avoin lause, kun perusjoukon muodostavat arvonnän tuloksena saatavat mahdolliset lukukolmikot

$(1, 1, 1), (1, 1, 2), (1, 2, 1), (1, 2, 2), (2, 1, 1), (2, 1, 2), (2, 2, 1), (2, 2, 2)$.

 - a) $S(x, y, z)$,
 - b) $T(x, y, z)$,
 - c) $U(x, y, z)$,
 - d) $S(x, y, z) \wedge T(x, y, z)$,
 - e) $S(x, y, z) \vee \neg U(x, y, z)$,
 - f) $\neg(S(x, y, z) \vee T(x, y, z) \vee U(x, y, z))$,
 - g) $S(x, y, z) \wedge (T(x, y, z) \leftrightarrow U(x, y, z))$.
- (8) Ratkaise reaalilukujen joukossa.
 - a) $x^2 = 1$ tai $x(x + 5)(x - 1) = 0$
 - b) $x^2 = 1$ ja $x(x + 5)(x - 1) = 0$
- (9) Ratkaise reaalilukujen joukossa
 - a) epäyhtälö $x^2 - 11x + 30 > 0$,

b) epäyhtälöpari

$$\begin{cases} x^2 - 11x + 30 > 0 \\ 2x > -6 - x. \end{cases}$$

(10) Ratkaise avoin lause reaalilukujen joukossa. Ilmaise ratkaisujoukko myös välimerkintää käyttäen.

- a) $(-4 < x) \vee (x < 8)$,
- b) $(-4 < x) \wedge (x < 8)$,
- c) $((-4 < x) \wedge (x < 8)) \wedge (-5 \leq x \leq -3)$,
- d) $(-4 < x) \leftrightarrow (-5 \leq x \leq -3)$.

(11) Olkoot $A(x)$ avoin lause $(x \geq 0) \rightarrow (x \geq 20)$ ja $B(x)$ avoin lause $\neg((x \leq 0) \vee (x \geq 20))$. Ratkaise avoin lause reaalilukujen joukossa.

- a) $A(x)$,
- b) $B(x)$,
- c) $A(x) \vee B(x)$.

3.3. Kvanttorit. *Kvanttorien* avulla voidaan ilmaista täsmällisesti yleisluontoisia väitteitä, kuten tämän kirjan ensimmäisessä luvussa annettu esimerkki: ”kaikki joutsenet ovat valkoisia”. Tavoitteena on muodostaa loogisesti päteviä päätelmiä, jotka koskevat esimerkiksi jonkin joukon kaikkia alkioita.

Tutkimustehtävä. Ovatko seuraavat väitteet tosia?

- (1) Kaikki koulumme opiskelijat opiskelevat englantia.
- (2) Kaikki koulumme opiskelijat opiskelevat pitkää matematiikkaa.
- (3) Koulussamme on opiskelija, joka harrastaa kilpaurheilua.
- (4) Koulussamme on opiskelija, joka on tämän vuoden Miss Suomi.
- (5) Kirjoita kohtien 1 ja 3 väitteiden negaatiot kahdella eri tavalla.

Predikaattilogiikassa määritellään kaksi kvanttoria, \exists ja \forall . Näistä ensimmäistä kutsutaan *eksistenssikvanttoriksi* eli *olemassalokvanttoriksi*. Lause

$$\exists x P(x)$$

tarkoittaa, että perusjoukossa X on ainakin yksi alkio, jolla on ominaisuus P . Toisin sanoen joukko P ei ole tyhjä joukko. Lause luetaan: ”On olemassa x siten, että $P(x)$ ”.

Kvanttoria \forall kutsutaan *universaalikvanttoriksi* eli *kaikkikvanttoriksi*. Lause

$$\forall x P(x)$$

tarkoittaa, että ominaisuus P on kaikilla perusjoukon X alkioilla. Lause luetaan: ”Kaikille x pätee $P(x)$ ”.

Kvanttorien avulla voidaan esittää matemaattisia väittämiä hyvin tiiviissä ja täsmällisessä muodossa. Tästä on hyötyä etenkin matemaattisessa logiikassa, jossa tutkimuskohteena ovat matemaattiset teoriat, tulokset ja todistukset.

Esimerkki 1. Liikuntailtapäivässä koulun opiskelijat harrastavat eri talviurheilulajeja. Olkoot perusjoukko koulun opiskelijat ja avoimet lauseet $H(x)$: ”opiskelija x hiihtää” ja $L(x)$: ”opiskelija x laskettelee lumilaudalla”.

Kirjoita suomen kielellä lauseet a) $\forall x H(x)$, b) $\exists x L(x)$. Milloin lause on tosi? Milloin lause on epätosi?

Ratkaisu: a) Lause tarkoittaa, että kaikki koulun opiskelijat hiihtävät. Lause on tosi silloin, kun kaikki opiskelijat hiihtävät. Lause on epätosi silloin, kun on ainakin yksi opiskelija, joka ei hiihdä.

b) Lause tarkoittaa, että joku koulun opiskelija laskettelee lumilaudalla. Lause on tosi silloin, kun ainakin yksi opiskelija laskettelee lumilaudalla. Lause on epätosi silloin, kun kukaan koulun opiskelijoista ei laskettele lumilaudalla.

Esimerkki 2. Olkoot perusjoukko reaalilukujen joukko \mathbb{R} ja avoimet lauseet $P(x)$: " $x^2 > 0$ " sekä $Q(x)$: " $x^2 \leq 0$ ". Suomennet lauseet a) $\forall x P(x)$, b) $\exists x Q(x)$. Ovatko lauseet tosia?

Ratkaisu: a) Lause tarkoittaa, että kaikkien reaalilukujen neliöt ovat positiivisia. Lause on epätosi, sillä luvun 0 neliö ei ole positiivinen: $0^2 = 0$.

Lauseen epätodeksi osoittamiseen siis riittää, että on olemassa yksikin alkio (niin sanottu *vastaesimerkki*), jolle avoin lause $P(x)$ on epätosi.

b) Lause tarkoittaa, että on olemassa reaaliluku, jonka neliö on pienempi tai yhtä suuri kuin nolla. Lause on tosi, sillä $0^2 = 0$.

Lauseen todeksi osoittamiseen siis riittää, että on olemassa yksikin alkio, jolle avoin lause $Q(x)$ on tosi.

Vastaus: a) Kaikkien reaalilukujen neliöt ovat positiivisia. Lause on epätosi.

b) On olemassa reaaliluku, jonka neliö on pienempi tai yhtä suuri kuin nolla. Lause on tosi.

Esimerkki 3. Onko lause tosi? Perustele.

- a) $\exists x \in \mathbb{Z}(4x - 3 = 0)$
- b) $\forall x \in \mathbb{R}(-x^2 + x \leq 2)$

Ratkaisu:

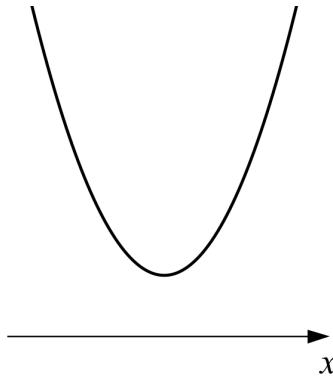
a) Yhtälön $4x - 3 = 0$ ratkaisu on $x = \frac{3}{4}$. Koska luku $\frac{3}{4}$ ei ole kokonaisluku, lause $\exists x \in \mathbb{Z}(4x - 3 = 0)$ on epätosi.

b) Epäyhtälö $-x^2 + x \leq 2$ on yhtäpitävä epäyhtälön $0 \leq x^2 - x + 2$ kanssa. Tutkitaan polynomifunktion $x^2 - x + 2$ merkkiä. Ratkaistaan funktion $x^2 - x + 2$ nollakohdat toisen asteen yhtälön ratkaisukaavalla.

$$x^2 - x + 2 = 0$$

$$x = \frac{-(-1) \pm \sqrt{(-1)^2 - 4 \cdot 1 \cdot 2}}{2 \cdot 1} = \frac{1 \pm \sqrt{-7}}{2}$$

Funktiolla ei ole nollakohtia, koska diskriminantti -7 on negatiivinen.



Koska funktion $x^2 - x + 2$ kuvaaja on ylöspäin aukeava paraabeli, funktio saa vain positiivisia arvoja. Siten epäyhtälö $0 \leq x^2 - x + 2$ toteutuu kaikilla muuttujan x arvoilla. Lause $\forall x \in \mathbb{R}(-x^2 + x \leq 2)$ on siis tosi.

Vastaus: a) Lause on epätosi. b) Lause on tosi.

Esimerkki 4. Suomenna lause

- a) $\forall x \in \mathbb{Z} \exists y \in \mathbb{Z}(x + y = 0)$
- b) $\exists y \in \mathbb{R} \forall x \in \mathbb{R}(x + y = x)$.

Onko lause tosi?

Ratkaisu:

a) Lause tarkoittaa, että jokaista kokonaislukua x kohden on olemassa sellainen kokonaisluku y , että lukujen summa on nolla.

Lause on tosi, sillä jokaisella kokonaisluvulla on vastaluku, joka on kokonaisluku. Luvun ja sen vastaluvun summa on nolla.

b) Lause tarkoittaa, että on olemassa sellainen reaaliluku y , että sen ja minkä tahansa reaaliluvun x summa on aina yhtä suuri kuin x .

Lause on tosi, sillä nolla on tällainen reaaliluku.

Vastaus: a) Jokaista kokonaislukua x kohden on olemassa sellainen kokonaisluku y , että lukujen summa on nolla. Lause on tosi.

b) On olemassa sellainen reaaliluku y , että sen ja minkä tahansa reaaliluvun x summa on aina x . Lause on tosi.

Kvanttorien negaatiot. Tutkitaan lausetta ”kaikki joutsenet ovat valkoisia”. Lause voidaan formalisoida kaikkikvanttorin avulla $\forall x V(x)$, missä perusjoukkona on joutsenten joukko J ja $V(x)$ on lause ” x on valkoinen”. Tämä lause osoittautui epätodeksi, kun Australiasta löydettiin mustia joutsenia. Lauseen $\forall x V(x)$ negaatio $\neg \forall x V(x)$ voidaan kirjoittaa $\exists x \neg V(x)$ ja suomentaa ”on olemassa (ainakin yksi) joutsen, joka ei ole valkoinen”. Vastaavasti lauseen $\exists x V(x)$ negaatio $\neg \exists x V(x)$ eli ”ei ole

olemassa valkoista joutsenta” voidaan lausua ekvivalentissa muodossa $\forall x \neg V(x)$. Tämä lause voidaan hieman kömpelösti kielentää ”kaikki joutsenet ovat ei-valkoisia”.

Kvanttorien negaatiot

Olkoon $P(x)$ avoin lause. Tällöin

- lause $\neg \forall x P(x)$ on loogisesti ekvivalentti lauseen $\exists x \neg P(x)$ kanssa, ja
- lause $\neg \exists x P(x)$ on loogisesti ekvivalentti lauseen $\forall x \neg P(x)$ kanssa.

Saatu kvanttorien negaatioita koskeva tulos muotoillaan joskus myös toisella tavalla. Koska lause $\neg \forall x V(x)$ on loogisesti ekvivalentti lauseen $\exists x \neg V(x)$ kanssa, voidaan päätellä, että lause $\forall x V(x)$ on loogisesti ekvivalentti lauseen $\neg \exists x \neg V(x)$ kanssa. Vastaava päättely voidaan tehdä myös eksistenssikvanttorin tapauksessa.

Esimerkki 5. Muodosta lauseen

- a) $\forall x \in \mathbb{R} (-x^2 \leq 0)$
- b) $\exists x \in \mathbb{N} (2x - 3 > 0)$

negaatio. Onko negaatio tosi?

Ratkaisu:

a) Lauseen $\forall x \in \mathbb{R} (-x^2 \leq 0)$ negaatio on loogisesti ekvivalentti lauseen $\exists x \in \mathbb{R} (-x^2 > 0)$ kanssa.

Lause $\exists x \in \mathbb{R} (-x^2 > 0)$ on epätosi, sillä tunnetusti x^2 on aina suurempi tai yhtä suuri kuin nolla. Siten $-x^2$ on aina pienempi tai yhtä suuri kuin nolla.

b) Lauseen $\exists x \in \mathbb{N} (2x - 3 > 0)$ negaatio on loogisesti ekvivalentti lauseen $\forall x \in \mathbb{N} (2x - 3 \leq 0)$ kanssa.

Lause $\forall x \in \mathbb{N} (2x - 3 \leq 0)$ on epätosi, sillä esimerkiksi tapauksessa $x = 5$ saadaan lausekkeen $2x - 3$ arvoksi $2 \cdot 5 - 3 = 7$, joka ei ole pienempi tai yhtä suuri kuin nolla.

Vastaus: a) $\exists x \in \mathbb{R} (-x^2 > 0)$. Negaatio on epätosi.

b) $\forall x \in \mathbb{N} (2x - 3 \leq 0)$. Negaatio on epätosi.

Tehtäviä.

- (1) Olkoon perusjoukko kaikki koulun opiskelijat. Olkoon lause $T(x)$: ”opiskelija x on täysi-ikäinen”. Suomenna lause.
 - a) $\forall x T(x)$
 - b) $\exists x T(x)$
 - c) $\exists x \neg T(x)$
 - d) $\forall x \neg T(x)$
- (2) Suomenna lause. Onko lause tosi? Perustele.
 - a) $\forall x \in \mathbb{R} (|x| > 0)$
 - b) $\forall x \in \mathbb{R} (|x| \geq 0)$
 - c) $\exists x \in \mathbb{N} (x^2 < 2)$
 - d) $\exists x \in \mathbb{N} (x^2 = 2)$
- (3) Formalisoi lause. Onko lause tosi? Perustele.
 - a) Jokainen kokonaisluku on joko positiivinen tai negatiivinen.
 - b) On olemassa sellainen kokonaisluku, jonka neliöjuuri on yhtä suuri kuin luku itse.
 - c) Minkään kokonaisluvun neliö ei ole 7.
- (4) Osoita, että yhtälö $\sqrt{x^2} = x$ ei pidä paikkaansa kaikilla reaali-luvuilla.
- (5) Jalkapallojoukkue on lähdössä turnausmatkalle. Olkoon $P(x, y)$ avoin lause ”pelaajalla x on pelaajan y puhelinnumero”. Suomenna lause.
 - a) $\forall x \exists y P(x, y)$
 - b) $\exists x \forall y P(x, y)$
 - c) $\exists y \forall x P(x, y)$
- (6) Formalisoi lause. Onko lause tosi?
 - a) Positiivisten kokonaislukujen joukossa on pienin alkio.
 - b) Negatiivisten kokonaislukujen joukossa on pienin alkio.
- (7) Onko lause tosi? Perustele.
 - a) $\forall x \in \mathbb{R} \exists y \in \mathbb{R} (xy = 1)$
 - b) $\exists y \in \mathbb{R} \forall x \in \mathbb{R} (xy = x)$
- (8) Olkoon $M(x)$: ” x on matemaatikko”. Formalisoi lause.
 - a) Kaikki eivät ole matemaatikkoja.
 - b) Joku ei ole matemaatikko.
 - c) Ei ole olemassa matemaatikkoa.
 - d) Kukaan ei ole matemaatikko.
- (9) Muodosta lauseen negaatio.
 - a) $\forall x \in \mathbb{Z} (x < 12)$
 - b) $\exists x \in \mathbb{Z} (x^2 = 12)$
 - c) $\exists x \in \mathbb{N} ((x^2 = 9) \wedge (x < 5))$
 - d) $\forall x \in \mathbb{N} ((x = 0) \vee (x \geq 1))$
- (10) Osoita, että lause $\exists a, b, c \in \mathbb{Z}_+ (a^2 + b^2 = c^2)$ on tosi.

- (11) (Lisämateriaalia) Olkoot $M(x)$: ” x on matemaatikko” ja $I(x)$: ” x on iloinen”. Formalisoi lause.
- Kaikki ovat iloisia matemaatikkoja.
 - Matemaatikot ovat iloisia.
 - Kukaan matemaatikko ei ole iloinen.
 - Kaikki matemaatikot eivät ole iloisia.
- (12) (Lisämateriaalia) Olkoot $K(x)$: ” x on kampaaja” ja $T(x, y)$: ” x tekee y :lle kampauksen”. Formalisoi lause.
- Kukaan kampaaja ei tee kampausta itselleen.
 - Joku kampaaja tekee kampauksen niille kampaajille, jotka eivät tee kampausta itselleen.

Kotitehtäviä.

- (1) Olkoon perusjoukko xy -tason suorien joukko. Olkoot lauseet $N(x)$: ”suora on nouseva” ja $L(x)$: ”suora on laskeva”. Suomena lause. Onko lause tosi?
- $\exists x L(x)$
 - $\forall x (N(x) \vee L(x))$
 - $\exists x (\neg N(x) \wedge \neg L(x))$
 - $\forall x \neg N(x)$
- (2) Onko lause tosi? Perustele.
- $\forall x \in \mathbb{R} (x^2 \geq 0)$
 - $\exists x \in \mathbb{N} (x^2 = -9)$
 - $\forall x \in \mathbb{R} ((x-1)(x-3) \geq 0)$
 - $\exists x \in \mathbb{Z} (-x^2 - 2 \leq 0)$
- (3) Onko lause tosi? Perustele.
- $\exists x \in \mathbb{R} (x^2 - 3x + 3 = 0)$
 - $\forall x \in \mathbb{R} (x^2 - 3x + 3 \geq 0)$
- (4)
- Osoita, että yhtälö $\sqrt{xy} = \sqrt{x}\sqrt{y}$ ei pidä paikkaansa kaikilla reaaliluvuilla x ja y .
 - Osoita, että on olemassa sellaiset reaaliluvut x ja y , että yhtälö $\sqrt{xy} = \sqrt{x}\sqrt{y}$ pitää paikkansa.
 - Millä ehdolla yhtälö $\sqrt{xy} = \sqrt{x}\sqrt{y}$ pitää yleisesti paikkansa?
- (5) Olkoon $S(x, y)$: ” x on suorittanut kurssin y ”. Formalisoi lause.
- Joku on suorittanut kaikki kurssit.
 - Jokainen on suorittanut ainakin yhden kurssin.
 - Kukaan ei ole suorittanut kaikkia kursseja.
 - On olemassa kurssi, jota kukaan ei ole suorittanut.
- (6) Onko lause tosi? Perustele.
- $\forall x \in \mathbb{Z}_+ \exists y \in \mathbb{Z}_+ (x = \sqrt{y})$
 - $\exists y \in \mathbb{R} \forall x \in \mathbb{R} (x^2 - 4 > y)$
- (7) Ilmaise suomen kielellä lauseen negaatio kahdella eri tavalla soveltamalla kvanttorien negaatioiden loogisesti ekvivalentteja muotoja.

- a) Jokainen opiskelija saa tästä kurssista arvosanan 10.
 b) On olemassa opiskelija, joka saa tästä kurssista arvosanan 10.
- (8) Kirjoita lause toisin.
 a) $\neg \forall x \neg P(x)$
 b) $\neg \exists x (P(x) \vee Q(x))$
- (9) Muodosta lauseen negaatio. Onko negaatio tosi?
 a) $\forall x \in]1, \infty[(\sqrt{x} < x)$
 b) $\exists x \in \mathbb{Q} (x^3 = 5)$
 c) $\forall n \in \mathbb{Z} \exists m \in \mathbb{Z} ((n = 2m) \vee (n = 2m + 1))$
- (10) Funktiota $f: X \rightarrow Y$ voidaan ajatella kahden muuttujan avoimen lauseena $P(x, y): "f(x) = y"$, missä x kuuluu määrittelyjoukkoon X ja y maalijoukkoon Y . Funktiolta edellytetään lisäksi, että
- $\forall x \exists y P(x, y)$, ja
 - $\neg (\exists x \exists y \exists z (P(x, y) \wedge P(x, z) \wedge (y \neq z)))$.
- Tulkitse sanallisesti tai kuvaa käyttäen, mitä tämä määritelmä tarkoittaa.
- (11) (Lisämateriaalia) Olkoot $S(x, y): "x$ on suorittanut kurssin $y"$ ja $L(x): "x$ on lukiolainen". Formalisoi lause.
 a) Joku lukiolainen on suorittanut kaikki kurssit.
 b) Kukaan lukiolainen ei ole suorittanut kaikkia kursseja.
- (12) (Lisämateriaalia) Olkoot $S(x, y): "x$ on suorittanut kurssin $y"$, $L(x): "x$ on lukiolainen" ja $M(y): "y$ on pitkän matematiikan kurssi". Formalisoi lause.
 a) Joku lukiolainen ei ole suorittanut yhtään pitkän matematiikan kurssia.
 b) Joku lukiolainen on suorittanut pitkän matematiikan kurssin.
 c) Jokaisella lukiolaisella on pitkän matematiikan kurssi suoritettuna.
 d) On olemassa pitkän matematiikan kurssi, jota kukaan lukiolainen ei ole suorittanut.
- (13) (Lisämateriaalia) Määritä kaikki funktiot $f: X \rightarrow Y$, kun $X = \{a, b, c\}$ ja $Y = \{1, 2\}$.
- (14) (Lisämateriaalia) Määritä kaikki funktiot $f: X \rightarrow Y$, kun $X = \emptyset$ ja $Y \neq \emptyset$.
- (15) (Lisämateriaalia) Määritä kaikki funktiot $f: X \rightarrow Y$, kun $X \neq \emptyset$ ja $Y = \emptyset$.
- (16) (Lisämateriaalia) Tutustu logiikkapohjaiseen Prolog-ohjelmointikieleen
<http://www.cs.helsinki.fi/u/wikla/OKP/OppaatK07/prolog.html>
 Lataa koneellesi Prolog-tulkki <http://www.gprolog.org/> ja kokeile Prolog-ohjelmointia.

4. MATEMAATTISEN VÄITTEEN TODISTAMINEN

Matematiikassa pyritään *todistamaan* matemaattisia tuloksia. Todistamisen ideana on, että tulos johdetaan loogisesti sitovalla päättelyllä, jossa voidaan vedota aikaisemmin todistettuihin tuloksiin, käsiteltävän teorian *aksioomiin* eli perusoletuksiin sekä loogisiin päättelysääntöihin. Matematiikassa tärkeimpiä tuloksia sanotaan yleensä *lauseiksi* eli *teoreemoiksi* (esim. Pythagoraan lause) ja pienempiä aputuloksia kutsutaan *apulauseiksi* eli *lemmoiksi*.

Kun tulos on todistettu matemaattisesti, se on kumoamaton. Matemaattiset tulokset eivät siksi vanhene. Toisaalta matemaattisten tulosten soveltamista rajoittavat niiden johtamisessa käytetyt oletukset, koska tulos ei sano mitään tilanteesta, jossa nämä oletukset eivät ole voimassa.

Tutkimustehtävä.

- (1) Mitä lukuja tarkoittaa merkintä $2n$, kun n käy läpi kaikki luonnolliset luvut? Entä mitä lukuja tarkoittaa merkintä $2n+1$, kun $n \in \mathbb{N}$?
- (2) Esitä luvut 6, 10 ja 26 muodossa $2n$.
- (3) Esitä luvut 7, 11 ja 35 muodossa $2n+1$.
- (4) Laske yhteen parittomia lukuja. Esimerkiksi $5+7=12$. Mitä havaitset summasta?
- (5) Todista havainto matemaattisesti. Kahdelle eri suurelle parittomalle luvulle voidaan käyttää yleisiä merkintöjä $2n+1$, $n \in \mathbb{N}$, ja $2m+1$, $m \in \mathbb{N}$.

Oletus, väite ja deduktio

Matemaattinen tulos muodostuu kolmesta osasta. Tulokseen liittyy *oletuksia*. Oletusten täytyy olla tosia, jotta tulosta voitaisiin käyttää. Tuloksen toinen osa on *väite*. Matematiikan lause sanoo, että oletusten vallitessa lauseen väite on myös tosi. Tuloksen kolmas osa on *todistus*. Matemaattinen todistus on deduktiivinen päättelyketju, jossa oletuksista johdetaan lauseen väite. Matemaattisen todistuksen loppuun merkitään yleensä pieni neliö merkiksi todistuksen päättymisestä.

Yksinkertaisin matemaattisen todistuksen tyyppi on *suora todistus*. Suorassa todistuksessa tulos saadaan suoralla päättelyllä, jossa voidaan vedota lauseen oletuksiin, aksioomiin, määritelmiin ja aikaisemmin todistettuihin tuloksiin, esimerkiksi laskusääntöihin. Suoralla todistuksella voidaan todistaa seuraavan esimerkin tulos.

Esimerkki 1. Todista lause.

Lause 1. Olkoot m ja n parillisia kokonaislukuja. Tällöin luku $m+n$ on parillinen.

Todistus. Koska m ja n ovat parillisia, voidaan kirjoittaa $m = 2a$ ja $n = 2b$, missä a ja b ovat kokonaislukuja.

Siten

$$m + n = 2a + 2b = 2(a + b).$$

Luku $2(a + b)$ on parillinen, joten väite on todistettu. \square

Esimerkki 2. Todista lause.

Lause 2. Kahden rationaaliluvun summa on rationaalinen.

Todistus. Olkoot q_1 ja q_2 kaksi rationaalilukua. Ne voidaan kirjoittaa muodossa

$$q_1 = \frac{m_1}{n_1}, \quad q_2 = \frac{m_2}{n_2},$$

ja missä m_1, m_2, n_1, n_2 ovat kokonaislukuja ja $n_1, n_2 \neq 0$.

Edelleen voidaan kirjoittaa

$$\begin{aligned} q_1 + q_2 &= \frac{m_1}{n_1} + \frac{m_2}{n_2} \\ &= \frac{m_1 n_2}{n_1 n_2} + \frac{m_2 n_1}{n_2 n_1} = \frac{m_1 n_2 + m_2 n_1}{n_1 n_2}. \end{aligned}$$

Nyt $m_1 n_2 + m_2 n_1$ sekä $n_1 n_2$ ovat kokonaislukuja ja $n_1 n_2 \neq 0$, joten summa $q_1 + q_2$ kuuluu rationaalilukujen joukkoon \mathbb{Q} . \square

Esimerkki 3. Todista lause.

Lause 3. Olkoot a ja b reaalilukuja. Tulo $ab < 0$, jos ja vain jos joko $a > 0$ ja $b < 0$ tai $a < 0$ ja $b > 0$.

Todistus. Ekvivalenssilauseen väite on muotoa ”jos ja vain jos”. Tällainen lause todistetaan usein kahdessa osassa.

Todistetaan aluksi lauseen ”jos”-osa: $ab < 0$, jos joko $a > 0$ ja $b < 0$ tai $a < 0$ ja $b > 0$.

Oletetaan aluksi, että $a > 0$ ja $b < 0$. Kertomalla epäyhtälö $b < 0$ luvulla a saadaan $ab < 0$.

Vastaavasti jos $a < 0$ ja $b > 0$, niin kertomalla epäyhtälö $a < 0$ luvulla b saadaan $ab < 0$. Siten lauseen ensimmäinen osa on todistettu.

Osoitetaan seuraavaksi lauseen toinen osa: $ab < 0$ vain, jos $a > 0$ ja $b < 0$ tai $a < 0$ ja $b > 0$.

Huomataan aluksi, että jos $ab < 0$, niin $a \neq 0$ ja $b \neq 0$. Jos $a > 0$, niin jakamalla epäyhtälö $ab < 0$ luvulla a saadaan $b < 0$. Toisaalta, jos $a < 0$, niin jaettaessa epäyhtälön $ab < 0$ suunta vaihtuu ja saadaan $b > 0$. Siis myös lauseen toinen osa on todistettu. \square

Epäsuora todistus Tärkeä esimerkki matemaattisesta todistusmenetelmästä on *epäsuora todistus*. Epäsuora todistus perustuu jo aikaisemmin tässä kurssissa esiintyneeseen kolmannen poissulkevan lakiin. Tämä laki sanoo, että kaikki väitteet ovat joko tosia tai epätosia.

Käänteisessä todistuksessa ajatuksena on, että väitteen $A \rightarrow B$ todistamiseksi riittää osoittaa, että väitteen B negaatio $\neg B$ eli niin sanottu *vastaoletus* johtaa oletuksen A negaatioon $\neg A$. Käänteinen todistus perustuu kappaleessa 2.3 esiteltyyn kontraposition lakiin, jonka mukaan lauseet $A \rightarrow B$ ja $\neg B \rightarrow \neg A$ ovat loogisesti ekvivalentit.

Käänteisessä todistuksessa täytyy siis olettaa väitteen negaatio ja päätellä siitä, että oletus on epätosi. Tällä tavoin voidaan osoittaa esimerkiksi seuraava tulos:

Lause 4. Olkoon $m \in \mathbb{N}$ siten, että m^2 on parillinen. Tällöin m on parillinen.

Todistus. Lauseen todistamiseksi tehdään vastaoletus, joka on lauseen väitteen ” m on parillinen” negaatio.

Vastaoletus: m on pariton.

Tästä seuraa, että on olemassa $k \in \mathbb{N}$, jolle $m = 2k + 1$.

Nyt

$$m^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1.$$

Siten m^2 on pariton. On päädytty ristiriitaan lauseen oletuksen kanssa. Siten lauseen väite on tosi. \square

Ristiriitatodistuksessa pyritään todistamaan muotoa $A \rightarrow B$ oleva väite tekemällä ensin vastaoletus $\neg B$ ja päätymällä johonkin ristiriitaan, ei kuitenkaan välttämättä oletuksen A negaatioon.

Ehkä kuuluisin esimerkki epäsuorasta todistuksesta on todistus sille, että luku $\sqrt{2}$ on irrationaalinen. Todistuksessa tarvitaan seuraava lisätietoa rationaaliluvuista. Sanotaan, että kokonaisluku a on kokonaisluvun b tekijä, jos on olemassa sellainen kokonaisluku c , että $b = a \cdot c$. Rationaaliluku $q \in \mathbb{Q}$ voidaan aina esittää *supistetussa muodossa* $q = m/n$, missä m ja n ovat kokonaislukuja, joilla ei ole yhteisiä tekijöitä, ja $n \neq 0$. Esimerkiksi murtoluku $2/5$ on supistetussa muodossa, koska luvuilla 2 ja 5 ei ole yhteisiä tekijöitä. Sen sijaan murtoluku $6/9$ ei ole supistetussa muodossa, koska luku 3 on sekä osoittajan että nimittäjän tekijä. Murtoluvun $6/9$ esitys supistetussa muodossa on $2/3$.

Lause 5. Luku $\sqrt{2}$ on irrationaalinen.

Todistus. Vastaoletus: Luku $\sqrt{2}$ on rationaalinen.

On siis olemassa luku $q \in \mathbb{Q}$ siten, että $q^2 = 2$.

Kirjoitetaan luku q supistetussa muodossa $q = m/n$, missä kokonaisluvuilla m ja n ei ole yhteisiä tekijöitä. Nyt $q^2 = 2$, jos ja vain jos

$$\left(\frac{m}{n}\right)^2 = 2.$$

Kertomalla puolittain luvulla n^2 saadaan yhtälö

$$m^2 = 2n^2.$$

Koska luku $2n^2$ on parillinen, on m^2 parillinen. Lauseen 4 perusteella myös m on parillinen.

Siten on olemassa $k \in \mathbb{Z}$, jolle $m = 2k$.

Koska

$$n^2 = m^2/2 = (2k)^2/2 = 2k^2,$$

luku n^2 on parillinen. Lauseen 4 nojalla myös n on parillinen.

Näin ollen luku 2 on lukujen m ja n yhteinen tekijä. Tämä on ristiriita, koska oletettiin, ettei näillä luvuilla ole yhteisiä tekijöitä. \square

Tehtäviä.

- (1) a) Laske neljän peräkkäisen kokonaisluvun summa. Toista lasku useilla neljän peräkkäisen kokonaisluvun joukoilla. Mitä havaitset summasta? b) Jos neljän peräkkäisen kokonaisluvun joukon pienin luku on m , niin millainen esitysmuoto on kolmella muulla luvulla? c) Todista a-kohdan tulos matemaattisesti käyttäen hyväksi b-kohdan esitysmuotoja.
- (2) Todista, että parillisen ja parittoman kokonaisluvun summa on pariton.
- (3) Todista, että kahden parillisen kokonaisluvun tulo on parillinen.
- (4) Todista, että kahden rationaaliluvun tulo on rationaalinen.
- (5) Olkoot a ja b kokonaislukuja. Todista, että luku $a + b$ on parillinen silloin ja vain silloin, kun luku $a - b$ on parillinen.
- (6) Olkoon m sellainen kokonaisluku, että m^2 on pariton. Todista, että tällöin m on pariton.
- (7) Todista väite todeksi tai epätodeksi: Kahden irrationaaliluvun summa on aina irrationaaliluku.
- (8) Luku $\sqrt{3}$ on irrationaaliluku. Todista, että $\sqrt{3} + 1/2$ on irrationaaliluku. Vihje: Käytä epäsuoraa todistusta.
- (9) Todista, että irrationaaliluvun ja nollasta poikkeavan rationaaliluvun tulo on irrationaaliluku.
- (10) Todista, että luku $\sqrt{6}$ on irrationaaliluku.
- (11) Todista: Jos luku a on irrationaaliluku, niin myös luku

$$\frac{2a - 5}{3a - 11}$$

on irrationaaliluku. Vihje: Käytä symbolisen laskimen solve-toimintoa.

- (12) Tarkastellaan suorakulmaista kolmiota, jonka kateettien pituudet ovat a ja b ja hypotenuusan pituus c . Todista väite todeksi tai epätodeksi.
 - a) On olemassa sellainen suorakulmainen kolmio, jonka sivujen pituudet a , b ja c ovat kaikki parillisia kokonaislukuja.
 - b) On olemassa sellainen suorakulmainen kolmio, jonka sivujen pituudet a , b ja c ovat kaikki parittomia kokonaislukuja.
- (13) Kokonaisluvut $0, 1, 2, \dots, 12$ asetetaan mielivaltaiseen järjestykseen ympyrän kehälle. Todista, että joidenkin neljän peräkkäisen luvun summa on vähintään 26.

Kotitehtäviä.

- (1) a) Laske luonnollisten lukujen $1, 2, 3, \dots, 10$ neliöt.
 b) Esitä väite luonnollisten lukujen neliöiden parillisuudesta tai parittomuudesta.
 c) Todista väitteesi matemaattisesti.

- (2) Todista, että kolmen parittoman kokonaisluvun summa on pariton.
- (3) Todista, että kolmen peräkkäisen kokonaisluvun summa on jaollinen luvulla 3.
- (4) Todista, että kahden parittoman kokonaisluvun tulo on pariton.
- (5) Olkoot a ja b reaalilukuja. Todista, että tulo $ab = 0$, jos ja vain jos $a = 0$ tai $b = 0$.
- (6) Olkoon n kokonaisluku. Todista, että luku $n^2 + 3n + 1$ on aina pariton. Käytä a) suoraa b) epäsuoraa todistusta.
- (7) Todista, että ei ole olemassa sellaisia positiivisia kokonaislukuja x ja y , jotka toteuttavat yhtälön $4^x = 7^y$.
- (8) Todista väite todeksi tai epätodeksi: Kahden irrationaaliluvun tulo voi olla rationaaliluku.
- (9) Todista, että luku $\sqrt{5}$ on irrationaaliluku. Tarvitset seuraavaa lisätietoa: jos kahden kokonaisluvun tulo on jaollinen luvulla 5, niin ainakin toinen tulon tekijöistä on jaollinen luvulla 5.
- (10) Tarkastellaan paritonta määrää parittomia kokonaislukuja. Todista, että lukujen keskiarvo ei voi olla nolla.
- (11) Tarkastellaan kolmiota, jonka sivujen pituudet ovat a , b ja c . Niin sanotun *Heronin kaavan* mukaan kolmion pinta-alalle pätee $A = \sqrt{p(p-a)(p-b)(p-c)}$, missä $p = \frac{1}{2}(a+b+c)$. Todista, että jos kolmion sivujen pituudet ovat luvulla 4 jaollisia kokonaislukuja, niin kolmion pinta-alan neliö on jaollinen luvulla 16.
- (12) Niin sanotun *Fermat'n suuren lauseen* mukaan ei ole olemassa sellaisia positiivisia kokonaislukuja x , y ja z , jotka toteuttaisivat yhtälön $x^n + y^n = z^n$, missä n on lukua 2 suurempi kokonaisluku. Erityisesti siis yhtälöllä $x^3 + y^3 = z^3$ ei ole ratkaisua, jos x , y ja z ovat positiivisia kokonaislukuja.
 - a) Todista, että ei ole olemassa sellaisia positiivisia rationaalilukuja x , y ja z , jotka toteuttavat yhtälön $x^3 + y^3 = z^3$.
 - b) Todista väite todeksi tai epätodeksi: ei ole olemassa sellaisia keskenään eri suuria kokonaislukuja x , y ja z , jotka toteuttavat yhtälön $x^3 + y^3 = z^3$.
- (13) Olkoot a ja b reaalilukuja, joille pätee $0 \leq a \leq 1$ ja $0 \leq b \leq 1$. Todista, että tällöin $0 \leq \frac{a+b}{1+ab} \leq 1$.

5. JOHDANTO LUKUTEORIAAN

Kurssin loppuosassa perehdytään lukuteoriaan. Lukuteoria on matematiikan ala, joka tutkii kokonaislukuja. Lukuteorialla on nykyään paljon sovelluksia mm. tietotekniikassa ja digitaalisessa tiedonsiirrossa. Esimerkiksi yleisesti käytetty RSA-salakirjoitusmenetelmä perustuu lukuteorian tuloksiin. Lukuteoria tarjoaa myös havainnollisen johdannon moniin matemaattisiin ajattelutapoihin, joita käytetään myös muiden matemaattisten teorioiden yhteydessä.

Kuva: pankkiautomaatti.

5.1. Jaollisuus ja jakojäännös. Kokonaislukujen jaollisuus on lukuteoriassa keskeinen käsite, johon on tutustuttu jo alakoulussa.

Tutkimustehtävä.

- (1) Laske jakokulmassa a) $905/11$ b) $540/12$. Ilmoita jakolaskun tulos kokonaisosan ja jakojäännöksen avulla.
- (2) Kirjoita kummankin jakolaskun perusteella yhtälö, joka kertoo, kuinka jaettava saadaan ilmaistua osamäärän, jakajan ja jakojäännöksen avulla.

Alakoulun matematiikassa esimerkiksi kokonaislukujen jakolasku $17/3$ ratkaistaan seuraavasti: $17/3 = 5$, jää 2. Tämä tarkoittaa, että luku 3 menee 5 kertaa lukuun 17 ja jää 2. Yleisesti kokonaislukujen a ja $b \neq 0$ jakolaskusta a/b saadaan tulokseksi *osamäärä* ja *jakojäännös*. Edellisessä jakolaskussa osamäärä on 5 ja jakojäännös on 2. Mikäli jakojäännös on nolla eli jako menee tasan, sanotaan, että luku a on *jaollinen* luvulla b tai että luku b *jakaa* luvun a . Tällöin merkitään $b|a$. Jos $b|a$, niin luku a voidaan kirjoittaa osamäärän q ja luvun b avulla $a = qb$. Itse asiassa nämä ehdot ovat yhtäpitäviä. Jos luku a ei ole jaollinen luvulla b , merkitään $b \nmid a$.

Esimerkki 1. Tutki, onko totta, että a) $3|6$ b) $2|5$ c) $-4|12$.

Ratkaisu:

a) Tapa 1: Suoritetaan jakolasku $6/3 = 2$. Jako menee tasan, joten luku 6 on jaollinen luvulla 3. Siis $3|6$.

Tapa 2: Koska $6 = 2 \cdot 3$, luku 3 on luvun 6 tekijä. Siis $3|6$.

b) Tapa 1: Suoritetaan jakolasku $5/2 = 2$, jää 1. Jako ei mene tasan, joten luku 5 ei ole jaollinen luvulla 2. Siis $2 \nmid 5$.

Tapa 2: Lukua 5 ei voida kirjoittaa muodossa $2q$, missä $q \in \mathbb{Z}$, sillä luku 5 ei ole parillinen. Siis $2 \nmid 5$.

c) Tapa 1: Suoritetaan jakolasku $12/(-4) = -12/4 = -3$. Jako menee tasan, joten luku 12 on jaollinen luvulla -4 . Siis $-4|12$.

Tapa 2: Koska $12 = -3 \cdot (-4)$, luku -4 on luvun 12 tekijä. Siis $-4 \mid 12$.

Vastaus: a) On. b) Ei ole. c) On.

Jaollisuuden tutkimisessa tärkeä tulos on seuraava lause, jonka todistus on melko vaativa:

Lause (Jakoyhtälö). Jos a ja b ovat kokonaislukuja ja $b > 0$, niin on olemassa sellaiset yksikäsitteiset kokonaisluvut q ja r , että

$$a = qb + r, \quad 0 \leq r < b.$$

Jakoyhtälössä esiintyvää lukua q sanotaan lukujen a ja b (vaillinaiseksi) osamääräksi ja lukua r jakojäännökseksi.

Todistus. (Lisämateriaali) Todistetaan väite tapauksessa $a \geq 0$. Tutkitaan aluksi joukkoja

$$S = \{a - nb \mid n \in \mathbb{Z}\}.$$

Koska $a \in S$, tässä joukossa on ainakin yksi epänegatiivinen alkio. Olkoon $r = a - qb$ joukon S pienin epänegatiivinen alkio. Nyt $r < b$, koska muuten luku

$$0 \leq r - b = a - qb - b = a - (q + 1)b$$

olisi lukua r pienempi joukon S epänegatiivinen alkio.

Yksikäsitteisyyden toteamiseksi tehdään vastaoletus, että

$$a = q_1b + r_1 = q_2b + r_2.$$

Voidaan olettaa, että $q_2 > q_1$. Nyt

$$r_1 - r_2 = q_2b - q_1b = (q_2 - q_1)b \geq b.$$

Toisaalta $r_1 - r_2 < b$, koska $0 \leq r_1 < b$ ja $0 \leq r_2 < b$, mikä on ristiriita. Siten ainoa mahdollisuus on, että $q_1 = q_2$ ja $r_1 = r_2$. \square

Esimerkki 2. Määritä jakolaskun osamäärä ja jakojäännös sekä kirjoita vastaava jakoyhtälö, kun a) luku 23 jaetaan luvulla 5, b) luku -19 jaetaan luvulla 6.

Ratkaisu: a) Vaillinaisen osamäärän voidaan selvittää päässälaskulla tai laskinta käyttäen. Laskinta käytettäessä lasketaan jakolasku normaalisti ja otetaan lopputuloksen kokonaisosa.

Laskin antaa $23/5 = 4,6$, joten vaillinaiseksi osamääräksi saadaan 4.

Jakojäännös saadaan nyt selville vähentämällä luku $4 \cdot 5$ jaettavasta 23, siis $23 - 4 \cdot 5 = 3$. Siten jakojäännökseksi saadaan 3. Jakoyhtälö on

$$23 = 4 \cdot 5 + 3.$$

b) Laskin antaa $-19/6 \approx -3,167$. Vaillinaiseksi osamääräksi on valittava -4 , jotta jakojäännös olisi epänegatiivinen.

Jakojäännös saadaan jälleen selville vähentämällä luku $-4 \cdot 6$ jaettavasta -19 , siis $-19 - (-4) \cdot 6 = -19 + 24 = 5$. Siten jakojäännökseksi saadaan 5. Jakoyhtälö on

$$-19 = -4 \cdot 6 + 5.$$

Vastaus: a) $23 = 4 \cdot 5 + 3$, b) $-19 = -4 \cdot 6 + 5$.

Esimerkki 3. Jussi tavoittelee Cooperin testissä tulosta 3050 metriä. Testi juostaan 400 metriä pitkällä radalla. Kuinka monta kokonaista kierrosta Jussin pitää juosta? Kuinka pitkä matka hänen pitää juosta vielä kokonaisten kierrosten lisäksi?

Ratkaisu: Jaetaan ensin tavoiteltava tulos yhden rata kierroksen pituudella: $3050/400 = 7,625$. Jussin pitää siis juosta 7 kokonaista kierrosta. Koska $3050 - 7 \cdot 400 = 3050 - 2800 = 250$, Jussin pitää juosta kokonaisten kierrosten lisäksi 250 metriä.

Vastaus: Jussin on juostava 7 kokonaista kierrosta ja 250 metriä.

Esimerkki 4. Olkoot a , b ja c kokonaislukuja ja $a \neq 0$. Osoita, että jos $a|b$ ja $a|c$, niin $a|(b+c)$.

Ratkaisu: Jos $a|b$, niin on olemassa sellainen kokonaisluku q , että $b = qa$. Jos $a|c$, niin on olemassa sellainen kokonaisluku r , että $c = ra$. Tällöin $b + c = qa + ra = (q + r)a$, missä $q + r$ on kokonaisluku. Siis $a|(b + c)$.

Tehtäviä.

- (1) Onko luku a) 50 b) 48 c) -72 d) -34 jaollinen luvulla 6?
- (2) Jakaako luku 13 luvun a) 117 b) -65 c) 160 d) -81 ?
- (3) Osoita, että a) $3|66$ b) $7 \nmid 120$ c) $15|(-330)$ d) $11 \nmid (-619)$.
- (4) Onko väite tosi? a) $3|53$ b) $-9|108$ c) $12 \nmid (-158)$ d) $-7|175$ e) $-17 \nmid (-646)$
- (5) Kirjoita jakoyhtälö, kun
 - a) luku 7 jaetaan luvulla 3
 - b) luku 51 jaetaan luvulla 4
 - c) luku 1000 jaetaan luvulla 125
 - d) luku 3858 jaetaan luvulla 97.
- (6) Kirjoita jakoyhtälö, kun
 - a) luku -22 jaetaan luvulla 7
 - b) luku -2844 jaetaan luvulla 36
 - c) luku -3858 jaetaan luvulla 97.
- (7) Kirjoita jakoyhtälö jakolaskulle a) $9/25$ b) $-9/25$ c) $124/120$ d) $-124/120$.
- (8) Päättele, mikä on jakojäännös, kun
 - a) luku 1967 jaetaan luvulla 5
 - b) luku -426 jaetaan luvulla 5
 - c) luku 67876 jaetaan luvulla 50
 - d) luku -30509 jaetaan luvulla 50.
- (9) Leipomossa on pakattavana 260 sämpylää. Kuinka monta täyttä pussia saadaan ja kuinka monta sämpylää jää yli, jos käytetään vain a) 24 b) 10 c) 6 d) 4 sämpylän pusseja?
- (10) Jos kello on nyt 13.05, niin mitä kello oli 2012 tuntia ja 45 minuuttia sitten?
- (11)
 - a) Mikä luku jaettuna luvulla 17 antaa osamääräksi 98 ja jakojäännökseksi 5?
 - b) Mikä luku jaettuna luvulla 12 antaa osamääräksi -91 ja jakojäännökseksi 0?
 - c) Millä positiivisella kokonaisluvulla luku 146 on jaettava, jotta osamäärä olisi 3 ja jakojäännös 2?
 - d) Millä positiivisella kokonaisluvulla luku 72 on jaettava, jotta jakojäännös olisi 7?
- (12) Määritä osamäärä ja jakojäännös sekä kirjoita jakoyhtälö, kun
 - a) luku $2^{18} + 10$ jaetaan luvulla $2^{15} + 1$ b) luku $3^{100} + 100$ jaetaan luvulla $3^{98} + 10$.
- (13) Olkoot a , b , c , r ja s kokonaislukuja ja $a \neq 0$. Osoita, että jos $a|b$ ja $a|c$, niin $a|(rb + sc)$.
- (14) Olkoot a , b , c ja d kokonaislukuja ja $a, b \neq 0$. Osoita, että jos $a|c$ ja $b|d$, niin $(ab)|(cd)$.
- (15) Osoita, että jos a ja b ovat parittomia kokonaislukuja, niin $4|(a^2 - b^2)$.

- (16) Olkoot a ja b nollasta eroavia kokonaislukuja. Mitä voidaan päätellä, jos $a|b$ ja $b|a$?
- (17) Olkoon n positiivinen kokonaisluku. Määritä osamäärä ja jakojäännös sekä kirjoita jakoyhtälö, kun
- luku $5n + 3$ jaetaan luvulla 5
 - luku $n^2 + 2n + 2$ jaetaan luvulla $n + 1$
 - luku $n^3 + 3n^2 - n - 3$ jaetaan luvulla $n + 3$
 - luku $2n^3 + 3n^2 + 4n + 9$ jaetaan luvulla $2n + 3$.
- (18) a) Muodosta jakoyhtälö luvuille $0, 1, 2, \dots, 7$, kun jakajana on luku 3. Mitä arvoja jakojäännös voi saada?
- b) Osoita, että jos kahden kokonaisluvun tulo on jaollinen luvulla 3, niin ainakin toinen luvuista on jaollinen luvulla 3. Vihje: Käytä epäsuoraa todistusta.

Kotitehtävät.

- Onko luku a) 42 b) -75 c) 102 d) -98 jaollinen luvulla 7?
- Jakaako luku 11 luvun a) -165 b) 21 c) -101 d) 209?
- Osoita, että a) $2|234$ b) $-17|408$ c) $14 \nmid 223$ d) $6 \nmid (-472)$.
- Onko väite tosi? a) $8 \nmid 168$ b) $13 \nmid (-95)$ c) $-5|777$ d) $29 \nmid 2583$
e) $-4|(-924)$
- Kirjoita jakoyhtälö, kun
 - luku 9 jaetaan luvulla 6
 - luku 576 jaetaan luvulla 19
 - luku 3712 jaetaan luvulla 32.
- Kirjoita jakoyhtälö, kun
 - luku -12 jaetaan luvulla 5
 - luku -147 jaetaan luvulla 6
 - luku -875 jaetaan luvulla 35.
- Kirjoita jakoyhtälö jakolaskulle a) $3/17$ b) $-3/17$ c) $88/80$ d) $-88/80$.
- Päättele, mikä on jakojäännös, kun
 - luku 5555 jaetaan luvulla 4
 - luku -555 jaetaan luvulla 4
 - luku 123456 jaetaan luvulla 100
 - luku -654321 jaetaan luvulla 100.
- Tänään on keskiviikko. Mikä viikonpäivä a) on 1000 päivän kuluttua b) oli 500 päivää sitten?
- Kello on 17.28 ja on tiistai. Mitä kello on 2073 tunnin kuluttua? Mikä viikonpäivä silloin on?
- Tarkastellaan kirjainjonoa ABCDEFGABCDEFGFGABCDEFGFG...
 - Mikä on jonon 12742. kirjain? b) Kuinka monta A-kirjainta on jonossa ennen sitä?
- a) Mikä luku jaettuna luvulla 19 antaa osamääräksi 6 ja jakojäännökseksi 13?

- b) Mikä luku jaettuna luvulla 7 antaa osamääräksi -23 ja jakojäännökseksi 5?
- c) Millä positiivisella kokonaisluvulla luku 1263 on jaettava, jotta osamäärä olisi 114 ja jakojäännös 9?
- d) Millä positiivisella kokonaisluvulla luku -140 on jaettava, jotta jakojäännös olisi 3?
- (13) Olkoon n kokonaisluku. Osoita, että luku $(3n+1)^4 - (3n+1)^3$ on jaollinen luvulla 3. Vihje: Käytä symbolisen laskimen **expand**-toimintoa.
- (14) Olkoon n kokonaisluku. Osoita, että luku $(2n+1)^5 - (2n-1)^4 - 2n$ on jaollinen luvulla 16.
- (15) Määritä osamäärä ja jakojäännös sekä kirjoita jakoyhtälö, kun
 - a) luku $7^{50} + 1$ jaetaan luvulla $7^{48} - 1$
 - b) luku $7^{50} - 1$ jaetaan luvulla $7^{25} + 1$.
- (16) Olkoot a , b ja c kokonaislukuja ja $a \neq 0$. Osoita, että jos $a|b$ ja $a|(b+c)$, niin $a|c$.
- (17) Olkoot p , q ja r positiivisia kokonaislukuja. Osoita, että jos p on luvun q tekijä ja q on luvun r tekijä, niin p on luvun r tekijä.
- (18) Olkoot a , b ja c kokonaislukuja ja $a, c \neq 0$. Osoita, että jos $(ac)|(bc)$, niin $a|b$.
- (19) Olkoot a ja b kokonaislukuja. Osoita, että luku $a+b$ on jaollinen luvulla 3 silloin ja vain silloin, kun luku $a - 2b$ on jaollinen luvulla 3.
- (20) Olkoon n positiivinen kokonaisluku. Määritä osamäärä ja jakojäännös sekä kirjoita jakoyhtälö, kun
 - a) luku $2n^2 - n - 2$ jaetaan luvulla $n + 1$
 - b) luku $n^3 + n^2 + 6$ jaetaan luvulla $n + 2$
 - c) luku $n^2 + 2n - 1$ jaetaan luvulla n .
 Vihje: Voit laskea polynomien jakolaskun symbolisen laskimen avulla.
- (21) (Lisämateriaalia.) Todista jakoyhtälö, kun $a < 0$.
- (22) (Lisämateriaalia.) *Lukujärjestelmä* tarkoittaa tapaa, jolla luvut kirjoitetaan numeroiden avulla. *Kantaluku* kertoo, kuinka monta eri numeroa lukujärjestelmän luvuissa voi esiintyä. Esimerkiksi *kymmenjärjestelmässä* kantaluku on 10 ja käytössä ovat numerot 0, 1, 2, 3, 4, 5, 6, 7, 8 ja 9. Kymmenjärjestelmän luku 3258 muodostuu numeroista 3, 2, 5 ja 8 kantaluvun 10 potenssien avulla seuraavasti:

$$\begin{aligned} 3258 &= 3 \cdot 1000 + 2 \cdot 100 + 5 \cdot 10 + 8 \\ &= 3 \cdot 10^3 + 2 \cdot 10^2 + 5 \cdot 10^1 + 8 \cdot 10^0. \end{aligned}$$

Kymmenjärjestelmässä siis luvun viimeinen numero on luvun 10^0 kerroin, toiseksi viimeinen luvun 10^1 kerroin, kolmanneksi viimeinen luvun 10^2 kerroin jne.

Kaksijärjestelmän eli binäärijärjestelmän luvut taas muodostuvat numeroista 0 ja 1. Esimerkiksi binääriluku 101101 voidaan ilmaista kymmenjärjestelmässä kirjoittamalla luku kantaluvun 2 potenssien avulla seuraavasti:

$$\begin{aligned} 101101 &= 1 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 \\ &= 1 \cdot 32 + 0 \cdot 16 + 1 \cdot 8 + 1 \cdot 4 + 0 \cdot 2 + 1 = 45. \end{aligned}$$

Kaksijärjestelmässä siis luvun viimeinen numero on luvun 2^0 kerroin, toiseksi viimeinen luvun 2^1 kerroin, kolmanneksi viimeinen luvun 2^2 kerroin jne.

Kymmenjärjestelmän lukuja voidaan muuntaa binääriluvuiksi jakoyhtälöiden avulla. Muunnetaan luku 18 binääriluvuksi. Jaetaan ensin kymmenjärjestelmän luku 18 kaksijärjestelmään kantaluvulla 2 ja kirjataan ylös jakojäännös. Tämän jälkeen jaetaan edellisen jakolaskun osamäärä kantaluvulla 2 ja kirjataan taas jakojäännös muistiin. Näin jatketaan, kunnes osamääräksi jää luku 0.

$$\begin{aligned} 18 &= 9 \cdot 2 + 0 \\ 9 &= 4 \cdot 2 + 1 \\ 4 &= 2 \cdot 2 + 0 \\ 2 &= 1 \cdot 2 + 0 \\ 1 &= 0 \cdot 2 + 1 \rightarrow \text{lopetetaan} \end{aligned}$$

Kirjoittamalla nyt jakojäännökset lopusta alkuun saadaan luku 10010. Se on kymmenjärjestelmän luvun 18 binääriesitys.

- Muunna binäärijärjestelmän luvut 1001 ja 110110100 kymmenjärjestelmään.
- Muunna kymmenjärjestelmän luvut 25 ja 520 binäärijärjestelmään.
- Etsi laskimesi ohjekirjasta, miten muunnokset voidaan toteuttaa laskimella.
- Ohjelmoi laskimesi ohjelmointikielellä ohjelma, joka suorittaa muunnoksen kymmenjärjestelmästä binäärijärjestelmään.

5.2. Kongruenssi. Luonnonilmiöitä mallinnettaessa tulee usein vastaan tilanteita, joissa on hyödyllistä samastaa keskenään jaksollisesti toistuvat ilmiöt. Tällaisia ilmiöitä ovat esimerkiksi vuodenajat, viikonpäivät ja kellonajat. Samaan tapaan kokonaislukujen jonossa esimerkiksi parilliset tai yhdellätoista jaolliset luvut esiintyvät jaksollisesti. Lukujonossa toistuvien ominaisuuksien tutkimisessa käytetään *kongruenssin* käsitettä.

Tutkimustehtävä.

- (1) Ryhmittele luvut 16, 59, 12, 3, 177, 21, 47, 65, 222, -17 , -100 ja -1 niin, että samaan joukkoon kuuluvat ne luvut, joilla on sama jakojäännös, kun ne jaetaan luvulla 5.
- (2) Valitse ensin kaksi lukua, jotka ovat samassa kohdan 1 joukossa. Laske niiden erotus. Toista kaksi kertaa. Valitse sitten kaksi lukua, jotka ovat eri joukoissa kohdassa 1. Laske niiden erotus. Toista kaksi kertaa. Miten erotuksen arvosta näkee, kuuluvatko vähenevä ja vähentäjä samaan kohdan 1 joukkoon?
- (3) Miten voit esittää yleisessä muodossa kaikki ne kokonaisluvut, jotka ovat jaollisia luvulla 5? Entä ne luvut, joiden jakojäännös on 1, 2, 3 tai 4, kun jaetaan luvulla 5?
- (4) Todista kohdan 2 havaintosi.

Kokonaislukujen a ja b kongruenssi tarkoittaa, että niillä on sama jakojäännös jaettaessa positiivisella kokonaisluvulla k . Kongruenssille on käytännöllistä antaa seuraava matemaattinen määritelmä.

Kongruenssi

Kokonaisluvut a ja b ovat *kongruentteja modulo k* , jos erotus $a - b$ on jaollinen positiivisella kokonaisluvulla k . Tällöin merkitään

$$a \equiv b \pmod{k}.$$

Jos a ja b eivät ole kongruentteja modulo k , merkitään

$$a \not\equiv b \pmod{k}.$$

Merkintää $(\text{mod } k)$ ei ole tapana kirjoittaa, jos luku k on asiayhteydestä selvä.

Kongruenssiyhtälön

$$a \equiv b \pmod{k}$$

kanssa on yhtäpitävää, että $a - b = nk$ eli $a = b + nk$ vähintään yhdellä luvulla $n \in \mathbb{Z}$.

Esimerkki 1. Osoita, että a) $27 \equiv 19 \pmod{4}$ b) $13 \equiv -82 \pmod{5}$.

Ratkaisu:

a) Tapa 1

Koska $27 - 19 = 8 = 2 \cdot 4$, niin erotus $27 - 19$ on jaollinen luvulla 4. Siten $27 \equiv 19 \pmod{4}$.

Tapa 2

Kun luku 27 jaetaan luvulla 4, saadaan jakoyhtälö $27 = 6 \cdot 4 + 3$. Vastaavasti $19 = 4 \cdot 4 + 3$. Luvuilla 27 ja 19 on siis sama jakojäännös, 3, kun jaetaan luvulla 4. Siten $27 \equiv 19 \pmod{4}$.

b) Koska $13 - (-82) = 95 = 19 \cdot 5$, niin $5 \mid (13 - (-82))$. Siten $13 \equiv -82 \pmod{5}$.

Esimerkki 2. Hannalla on kaksi lasta, Aaro ja Mirkku. Hanna laski, että Aaron syntymäpäivä on 38 päivän kuluttua ja Mirkun 59 päivän kuluttua äidin syntymäpäivästä. Ovatko Aaron ja Mirkun syntymäpäivät samana viikonpäivänä?

Ratkaisu: Tutkitaan, ovatko luvut 38 ja 59 kongruentteja modulo 7. Koska $59 - 38 = 21 = 3 \cdot 7$, niin $59 \equiv 38 \pmod{7}$. Aaron ja Mirkun syntymäpäivät ovat siis samana viikonpäivänä.

Vastaus: Ovat.

Esimerkki 3.

- a) Määritä pienin epänegatiivinen kokonaisluku, joka on kongruentti luvun 45 kanssa modulo 7.
- b) Jos tänään on perjantai ja loman alkuun on 45 päivää, niin minä viikonpäivänä loma alkaa?

Ratkaisu:

a) Kun luku 45 jaetaan luvulla 7, saadaan jakoyhtälö $45 = 6 \cdot 7 + 3$. Koska voidaan kirjoittaa $45 - 3 = 6 \cdot 7$, nähdään, että jakojäännös 3 on kongruentti luvun 45 kanssa modulo 7. Luku 3 on myös pienin epänegatiivinen kokonaisluku, joka on kongruentti luvun 45 kanssa modulo 7.

b) a-kohdan perusteella luku 3 on kongruentti luvun 45 kanssa modulo 7. Kysytty viikonpäivä saadaan selville laskemalla perjantaista 3 päivää eteenpäin, jolloin on maanantai. Siis loma alkaa maanantaina.

Vastaus: a) 3 b) Loma alkaa maanantaina.

Kongruenssin laskusääntöjä. Kongruensseilla on monia ominaisuuksia, jotka muistuttavat yhtälöiden ratkaisemisessa käytettäviä laskusääntöjä.

Lause. Olkoot $a, b, c, d \in \mathbb{Z}$ ja $k, n \in \mathbb{Z}_+$ sekä $a \equiv c, b \equiv d \pmod{k}$. Tällöin:

- (1) $a + b \equiv c + d \pmod{k}$,
- (2) $a - b \equiv c - d \pmod{k}$,

$$\begin{aligned}(3) \quad ab &\equiv cd \pmod{k}, \\(4) \quad a^n &\equiv c^n \pmod{k}.\end{aligned}$$

Todistus. Todistetaan kohdat 1 ja 3. Kohdan 2 todistus on kotitehtävänä, ja potenssisääntö 4 todistetaan lisämateriaalina olevan kappaleen 5.4 tehtävässä XX.

Kongruenssin määritelmän perusteella $a = c + mk$ ja $b = d + nk$, missä $m, n \in \mathbb{Z}$.

Siten

$$\begin{aligned}a + b - (c + d) &= c + mk + d + nk - c - d \\&= mk + nk = (m + n)k,\end{aligned}$$

missä $(m + n)$ on kokonaisluku. Siis erotus $a + b - (c + d)$ on jaollinen luvulla k , joten ensimmäinen väite pätee.

Samaan tapaan saadaan

$$\begin{aligned}ab - cd &= (c + mk)(d + nk) - cd \\&= cd + cnk + dm + mnk^2 - cd \\&= (cn + dm + mnk)k,\end{aligned}$$

missä $(cn + dm + mnk)$ on kokonaisluku. Siten erotus $ab - cd$ on jaollinen luvulla k , joten kolmas väite pätee. \square

Erityisesti tuloksesta seuraa, että jos $a \equiv b \pmod{k}$, niin $na \equiv nb \pmod{k}$ kaikilla $n \in \mathbb{Z}$.

Esimerkki 4.

Määritä pienin epänegatiivinen luku, jonka kanssa luku a) $350 - 7778$, b) $65 \cdot 141$, c) $16^{10} + 82$ on kongruentti modulo 7.

Ratkaisu:

Korvataan luvut mahdollisimman yksinkertaisilla luvuilla, jotka ovat kongruentteja modulo 7, ja sovelletaan kongruenssin laskusääntöjä.

a) Koska $350 \equiv 0$ ja $7778 \equiv 1 \pmod{7}$, niin säännön 2 mukaan $350 - 7778 \equiv 0 - 1 = -1 \equiv 6 \pmod{7}$.

b) Koska $65 \equiv 2$ ja $141 \equiv 1 \pmod{7}$, niin säännön 3 mukaan $65 \cdot 141 \equiv 2 \cdot 1 = 2 \pmod{7}$.

c) Koska $16 \equiv 2$ ja $82 \equiv 5 \pmod{7}$, niin säännön 1 ja potenssisäännön 4 mukaan $16^{10} + 82 \equiv 2^{10} + 5 = 1024 + 5 = 1029 \equiv 0 \pmod{7}$.

Vastaus: a) 6 b) 2 c) 0

Esimerkki 5. Osoita, että luku $n^4 + 2n^3 + n^2$ on jaollinen luvulla 4, kun n on kokonaisluku.

Ratkaisu: Kun kokonaisluku jaetaan luvulla 4, jakojäännös voi olla 0, 1, 2 tai 3. Siten jokainen kokonaisluku n on jotakin seuraavaa muotoa: $4q$, $4q+1$, $4q+2$ tai $4q+3$, missä $q \in \mathbb{Z}$. Tutkitaan luvun $n^4 + 2n^3 + n^2$ jaollisuutta luvulla 4 erikseen kussakin näistä osajoukoista.

Tapa 1: Kirjoitetaan lauseke $n^4 + 2n^3 + n^2$ muotoon

$$n^4 + 2n^3 + n^2 = n^2(n^2 + 2n + 1) = n^2(n + 1)^2.$$

1) Kun $n = 4q$, niin

$$\begin{aligned} n^4 + 2n^3 + n^2 &= (4q)^2(4q + 1)^2 = 4^2 \cdot q^2(4q + 1)^2 \\ &= 4 \cdot 4q^2(4q + 1)^2. \end{aligned}$$

Koska $4q^2(4q + 1)^2 \in \mathbb{Z}$, niin luku $n^4 + 2n^3 + n^2$ on jaollinen luvulla 4.

2) Kun $n = 4q + 1$, niin

$$\begin{aligned} n^4 + 2n^3 + n^2 &= (4q + 1)^2(4q + 2)^2 = (4q + 1)^2(2(2q + 1))^2 \\ &= (4q + 1)^2 \cdot 2^2 \cdot (2q + 1)^2 = 4(4q + 1)^2(2q + 1)^2, \end{aligned}$$

joten luku $n^4 + 2n^3 + n^2$ on jaollinen luvulla 4.

3) Kun $n = 4q + 2$, niin

$$\begin{aligned} n^4 + 2n^3 + n^2 &= (4q + 2)^2(4q + 3)^2 = (2(2q + 1))^2(4q + 3)^2 \\ &= 2^2 \cdot (2q + 1)^2(4q + 3)^2 = 4(2q + 1)^2(4q + 3)^2, \end{aligned}$$

joten luku $n^4 + 2n^3 + n^2$ on jaollinen luvulla 4.

4) Kun $n = 4q + 3$, niin

$$\begin{aligned} n^4 + 2n^3 + n^2 &= (4q + 3)^2(4q + 4)^2 = (4q + 3)^2(4(q + 1))^2 \\ &= (4q + 3)^2 \cdot 4^2 \cdot (q + 1)^2 = 4(4q + 3)^2 \cdot 4 \cdot (q + 1)^2, \end{aligned}$$

joten luku $n^4 + 2n^3 + n^2$ on jaollinen luvulla 4.

Siis luku $n^4 + 2n^3 + n^2$ on jaollinen luvulla 4, kun n on kokonaisluku.

Tapa 2:

1) Kun $n = 4q$, niin $n \equiv 0 \pmod{4}$. Siten

$$n^4 + 2n^3 + n^2 \equiv 0^4 + 2 \cdot 0^3 + 0^2 = 0 \pmod{4}$$

ja luku $n^4 + 2n^3 + n^2$ on jaollinen luvulla 4.

2) Kun $n = 4q + 1$, niin $n \equiv 1 \pmod{4}$. Siten

$$n^4 + 2n^3 + n^2 \equiv 1^4 + 2 \cdot 1^3 + 1^2 = 1 + 2 + 1 = 4 \equiv 0 \pmod{4}$$

ja luku $n^4 + 2n^3 + n^2$ on jaollinen luvulla 4.

3) Kun $n = 4q + 2$, niin $n \equiv 2 \pmod{4}$. Siten

$$n^4 + 2n^3 + n^2 \equiv 2^4 + 2 \cdot 2^3 + 2^2 = 16 + 16 + 4 = 36 \equiv 0 \pmod{4}$$

ja luku $n^4 + 2n^3 + n^2$ on jaollinen luvulla 4.

4) Kun $n = 4q + 3$, niin $n \equiv 3 \pmod{4}$. Siten

$$n^4 + 2n^3 + n^2 \equiv 3^4 + 2 \cdot 3^3 + 3^2 = 81 + 54 + 9 = 144 \equiv 0 \pmod{4}$$

ja luku $n^4 + 2n^3 + n^2$ on jaollinen luvulla 4.

Siis luku $n^4 + 2n^3 + n^2$ on jaollinen luvulla 4, kun n on kokonaisluku.

Tehtäviä.

- (1) Osoita, että a) $23 \equiv 8 \pmod{5}$ b) $1326 \equiv -546 \pmod{8}$ c) $403 \equiv 0 \pmod{13}$.
- (2) Määritä pienin epänegatiivinen luku, jonka kanssa luku a) 56 b) -72 c) 3857 on kongruentti modulo 6.
- (3) Määritä kaikki kokonaisluvut x , joille $x \equiv 7 \pmod{12}$ ja $18 < x < 130$.
- (4) Pitkäkestoiset kynttilät sytytettiin samaan aikaan. Toinen paloi 128 tuntia ja toinen 181 tuntia. Sammuivatko kynttilät samaan kellonaikaan?
- (5) Aaron syntymäpäiväjuhlat alkavat 912 tunnin kuluttua ja Mirkun syntymäpäiväjuhlat 1419 tunnin kuluttua.
 - a) Mihin kellonaikaan Mirkun juhlat alkavat, kun Aaron juhlat alkavat kello 12.00?
 - b) Aaron juhlat ovat lauantaina. Mikä viikonpäivä nyt on?
- (6) Määritä pienin epänegatiivinen luku, jonka kanssa luku
 - a) $234 - 15$
 - b) $79 \cdot 650$
 - c) $19^{12} + 772$
 on kongruentti modulo 4.
- (7) Tiedetään, että jakojäännös on 2, kun kokonaisluku n jaetaan luvulla 5. Mikä on jakojäännös, kun luku $3n^2 + 8n + 7$ jaetaan luvulla 5?
- (8) Kokonaisluvut voidaan jakaa osajoukkoihin esimerkiksi niin, että kussakin osajoukossa ovat ne luvut, jotka ovat kongruentteja keskenään jaettaessa luvulla 3. Näihin osajoukkoihin kuuluvia lukuja voidaan merkitä $3q$, $3q + 1$ ja $3q + 2$, missä $q \in \mathbb{Z}$. Miten voidaan merkitä lukuja osajoukoissa, jotka syntyvät, kun kokonaisluvut jaetaan luvulla a) 4 b) 5 c) 2?
- (9) Olkoon n kokonaisluku. Osoita, että $n^2 - n \equiv 0 \pmod{2}$.
- (10) Olkoon n kokonaisluku. Osoita, että luku $n(n+5)$ on parillinen.
- (11) Osoita, että luku $n(n+1)(n+8)$ on jaollinen luvulla 3, kun n on kokonaisluku.
- (12) Osoita, että luku $n^5 - n$ on jaollinen luvulla 5, kun n on kokonaisluku.
- (13) Osoita, että luku $n^3 + 2$ ei ole jaollinen luvulla 4 millään kokonaisluvun n arvolla.
- (14) Jokainen kokonaisluku on joko parillinen tai pariton. Osoita erikseen näissä osajoukoissa, että luku $n^4 + 2n^3 + n^2$ on jaollinen luvulla 4, kun n on kokonaisluku. (Vrt. esimerkki 5 s. XX.)
- (15) Etsi kaikki kokonaisluvut x , jotka toteuttavat kongruenssin $5x \equiv 1 \pmod{3}$.
- (16) Olkoon k positiivinen kokonaisluku. Osoita, että kokonaisluvut a ja b ovat kongruentteja modulo k eli erotus $a - b$ on jaollinen

luvulla k , jos ja vain jos luvuilla a ja b on sama jakojäännös, kun jaetaan luvulla k .

- (17) Julius Caesar käytti erästä vanhimista tunnetuista salakirjoitusmenetelmistä. Hän muutti viestin salaiseksi korvaamalla jokaisen kirjaimen toisella kirjaimella, joka sijaitsi aakkosissa kolme kirjainta myöhemmin. Viimeisten kirjainten jälkeen palattiin taas aakkosten alkuun. Suomen kielessä on 28 kirjainta, jos W-kirjainta ei lasketa mukaan. Siten esimerkiksi viesti AVAIN ON ÖLJYRUUKUSSA kirjoitettaisiin Caesarin menetelmällä DZDLQ RQ COMÄUYNYVVD. Suomenna viestit
- KÄCNNBÄV NHVNLÄCOOB
 - BOB VÄC UÄSBOHLXB.
- (18) Caesarin salakirjoitusmenetelmää voidaan kuvata funktiolla $f(n) = n + 3 \pmod{28}$, missä n on kunkin kirjaimen järjestysnumero aakkosissa. Koodattavan kirjaimen järjestysnumeroon lisätään luku 3 ja näin saatu funktion arvo tulkitaan takaisin kirjaimeksi.
- Kirjoita viesti AVAIN ON ÖLJYRUUKUSSA käyttäen salakirjoitusta, jota kuvaa funktio
- $f(n) = n + 13 \pmod{28}$
 - $f(n) = 3n + 7 \pmod{28}$.
 - Määritä funktiot, joiden avulla a- ja b-kohtien salakirjoitus voidaan purkaa.

Kotitehtäviä.

- Osoita, että a) $34 \equiv 10 \pmod{3}$ b) $-128 \equiv 274 \pmod{6}$ c) $1053 \equiv 0 \pmod{27}$.
- Määritä pienin epänegatiivinen luku, jonka kanssa luku a) 25 b) -121 c) 5777 on kongruentti modulo 5.
- Määritä kaikki kokonaisluvut x , joille $x \equiv 3 \pmod{8}$ ja $-50 < x < 51$.
- Neptunus-planeetan pyörähdysaika on noin 16 tuntia. Onko Neptunuksella sama kellonaika 223 tunnin kuluttua kuin 49 tuntia sitten?
- Maijan isoäiti on syntynyt 7.3. eräänä karkausvuonna. Maijan äiti on syntynyt 9525 päivää isoäitiä myöhemmin ja Maija itse 10229 päivää äitiään myöhemmin. Tutki, ovatko jotkut henkilöistä syntyneet samana viikonpäivänä.
- Nyt on tammikuu. Mikä kuukausi
 - on 76 kuukauden kuluttua
 - oli 555 kuukautta sitten?
- Määritä pienin epänegatiivinen luku, jonka kanssa luku
 - $17 - 930 + 452$
 - $19 \cdot 30 + 183 \cdot 11$
 - $5 \cdot 26^{15} + 493$

on kongruentti modulo 9.

- (8) Tiedetään, että jakojäännös on 5, kun kokonaisluku n jaetaan luvulla 11. Mikä on jakojäännös, kun luku $2n^3 - 6n - 9$ jaetaan luvulla 11?
- (9) Osoita kongruenssin laskusääntöjä koskevan lauseen kohta 2: Jos $a \equiv c$ ja $b \equiv d \pmod{k}$, niin $a - b \equiv c - d \pmod{k}$.
- (10) Olkoon n kokonaisluku. Osoita, että luku $n^2 + n$ on jaollinen kahdella.
- (11) Osoita, että luku $n(n+1)(4n-1)$ on jaollinen luvulla 6, kun n on kokonaisluku.
- (12) Osoita, että luku $n(4n^2 - 1)$ on jaollinen luvulla 3, kun n on kokonaisluku.
- (13) Osoita, että luku $n^2 - 3$ ei ole jaollinen luvulla 5 millään kokonaisluvun n arvolla.
- (14) Etsi kaikki kokonaisluvut x , jotka toteuttavat kongruenssin $4x + 1 \equiv 3 \pmod{7}$.
- (15) Olkoot a ja b kokonaislukuja. Osoita väite todeksi tai epätodeksi: jos $ab \equiv 0 \pmod{m}$, niin $a \equiv 0$ tai $b \equiv 0 \pmod{m}$.
- (16) Olkoot a ja b kokonaislukuja. Osoita väite todeksi tai epätodeksi: jos $a^2 \equiv b^2 \pmod{m}$, niin $a \equiv b \pmod{m}$.
- (17) (Lisämateriaalia) Luvun a määräämä *jäännösluokka modulo m* on luvun a kanssa kongruenttien lukujen joukko. Luvun a jäännösluokkaa merkitään \underline{a} . Siis $\underline{a} = \{a + km \mid k \in \mathbb{Z}\}$. Esimerkiksi jäännösluokat modulo 4 ovat $\underline{0} = \{4k \mid k \in \mathbb{Z}\}$, $\underline{1} = \{1 + 4k \mid k \in \mathbb{Z}\}$, $\underline{2} = \{2 + 4k \mid k \in \mathbb{Z}\}$ ja $\underline{3} = \{3 + 4k \mid k \in \mathbb{Z}\}$.
- a) Määritä jäännösluokat modulo 5.
- b) Jäännösluokkien yhteenlasku ja kertolasku määritellään seuraavasti: $\underline{a} + \underline{b} = \underline{a + b}$ ja $\underline{a} \cdot \underline{b} = \underline{a \cdot b}$. Täydennä seuraavat jäännösluokkien yhteen- ja kertolaskutaulut modulo 5.

+	<u>0</u>	<u>1</u>	<u>2</u>	<u>3</u>	<u>4</u>
<u>0</u>					
<u>1</u>					
<u>2</u>					
<u>3</u>					
<u>4</u>					

·	<u>0</u>	<u>1</u>	<u>2</u>	<u>3</u>	<u>4</u>
<u>0</u>					
<u>1</u>					
<u>2</u>					
<u>3</u>					
<u>4</u>					

- c) Jäännösluokan vasta-alkio määritellään seuraavasti: \underline{b} on alkion \underline{a} vasta-alkio, jos $\underline{a} + \underline{b} = \underline{0}$. Määritä b-kohdan taulukoiden avulla kunkin jäännösluokan vasta-alkiot modulo 5.
- d) Jäännösluokan käänteisalkio määritellään seuraavasti: \underline{c} on alkion \underline{a} käänteisalkio, jos $\underline{a} \cdot \underline{c} = \underline{1}$. Määritä b-kohdan taulukoiden avulla käänteisalkiot niille jäännösluokkien modulo 5 alkioille, joilla sellainen on olemassa.
- e) Ratkaise jäännösluokissa modulo 5 yhtälö $\underline{x} + \underline{x} = \underline{1}$.
- f) Ratkaise jäännösluokissa modulo 5 yhtälö $\underline{x} \cdot \underline{x} = \underline{4}$.

5.3. Kongruenssin sovelluksia. Kongruenssi on hyödyllinen työkalu lukuteoriassa. Kongruenssin laskusääntöjä käyttämällä voidaan esimerkiksi tutkia lukujen jaollisuutta. Näin saadaan johdettua monia klassisia tuloksia, esimerkiksi helpot testit sille, onko kokonaisluku jaollinen luvuilla 3 ja 9.

Esimerkki 1. Määritä jakojäännös, kun

- a) luku 7^{650} jaetaan luvulla 6
- b) luku $7^{650} - 194$ jaetaan luvulla 8
- c) luku $0 + 1 + 2 + 3 + \dots + 68 + 69$ jaetaan luvulla 7.

Ratkaisu:

Riittää määrittää pienin epänegatiivinen kokonaisluku, joka on kongruentti jaettavan kanssa, sillä edellisen kappaleen esimerkissä 3 huomattiin, että kyseinen luku on sama kuin jakojäännös.

a) Koska $7 \equiv 1 \pmod{6}$, niin $7^{650} \equiv 1^{650} = 1 \pmod{6}$. Jakojäännös on siis 1.

b) Koska $7 \equiv -1$ ja $194 \equiv 2 \pmod{8}$, niin $7^{650} - 194 \equiv (-1)^{650} - 2 = 1 - 2 = -1 \equiv 7 \pmod{8}$. Jakojäännös on siis 7.

c) Jokainen kokonaisluku on kongruentti jonkin luvuista 0, 1, 2, 3, 4, 5 tai 6 kanssa modulo 7. Saadaan, että

$$\begin{aligned} &0 + 1 + 2 + 3 + 4 + 5 + 6 + 7 + \dots + 63 + 64 + 65 + 66 + 67 + 68 + 69 \\ &\equiv (0+1+2+3+4+5+6) + (0+1+2+3+4+5+6) + \dots + (0+1+2+3+4+5+6) \\ &= 10 \cdot (0 + 1 + 2 + 3 + 4 + 5 + 6) = 10 \cdot 21 \equiv 3 \cdot 0 = 0 \pmod{7}. \end{aligned}$$

Jakojäännös on siis 0.

Vastaus: a) 1 b) 7 c) 0

Esimerkki 2. Mikä on luvun a) 2^{120} , b) 3^{100} viimeinen numero?

Ratkaisu:

a) Positiivisen kokonaisluvun viimeinen numero on sama kuin sen jakojäännös jaettaessa luvulla 10. Tutkitaan, onko luvulla 2 sellaisia potensseja, jotka voisivat olla hyödyllisiä sievennettäessä kongruenssilausekkeita modulo 10. Esimerkiksi $2^2 = 4$, $2^3 = 8$, $2^4 = 16$ ja $2^5 = 32$. Havaitaan, että $2^5 = 32 \equiv 2 \pmod{10}$. Tällöin

$$\begin{aligned} 2^{120} = (2^5)^{24} &\equiv 2^{24} = 2^{20} \cdot 2^4 = (2^5)^4 \cdot 2^4 \\ &\equiv 2^4 \cdot 2^4 = 2^8 = 2^5 \cdot 2^3 \\ &\equiv 2 \cdot 2^3 = 2^4 = 16 \\ &\equiv 6 \pmod{10}. \end{aligned}$$

Luvun 2^{120} jakojäännös jaettaessa luvulla 10 on 6. Sen viimeinen numero on siis 6.

b) Tapa 1

Tutkitaan luvun 3 potensseja: $3^2 = 9$, $3^3 = 27$, $3^4 = 81$. Havaitaan, että $3^4 = 81 \equiv 1 \pmod{10}$. Nyt $3^{100} = (3^4)^{25} \equiv 1^{25} = 1 \pmod{10}$. Luvun 3^{100} jakojäännös jaettaessa luvulla 10 on 1. Sen viimeinen numero on siis 1.

Tapa 2

Koska $3^2 = 9 \equiv -1 \pmod{10}$, niin $3^{100} = (3^2)^{50} \equiv (-1)^{50} = 1 \pmod{10}$. Luvun 3^{100} viimeinen numero on 1.

Vastaus: a) 6, b) 1.

Esimerkki 3.

Olkoon n luonnollinen luku. Osoita, että luku $498 \cdot 16^n + 104^{2n+1} + 3$ on jaollinen luvulla 5.

Ratkaisu:

Koska $498 \equiv 3$, $16 \equiv 1$ ja $104 \equiv -1 \pmod{5}$, niin

$$\begin{aligned} 498 \cdot 16^n + 104^{2n+1} + 3 &\equiv 3 \cdot 1^n + (-1)^{2n+1} + 3 \\ &= 3 \cdot 1 + (-1)^{2n} \cdot (-1) + 3 \\ &= 3 + 1 \cdot (-1) + 3 \\ &= 3 - 1 + 3 = 5 \equiv 0 \pmod{5}. \end{aligned}$$

Jakojäännös on 0, kun luku $498 \cdot 16^n + 104^{2n+1} + 3$ jaetaan luvulla 5. Luku $498 \cdot 16^n + 104^{2n+1} + 3$ on siis jaollinen luvulla 5.

Esimerkki 4. Tutki, onko a) luku 16 783 jaollinen luvulla 3, b) luku 295 542 jaollinen luvulla 9.

Ratkaisu:

a) Luku 16 783 voidaan esittää muodossa

$$16\,783 = 1 \cdot 10^4 + 6 \cdot 10^3 + 7 \cdot 10^2 + 8 \cdot 10 + 3.$$

Koska $10 \equiv 1 \pmod{3}$, niin $10^2 \equiv 1^2 = 1 \pmod{3}$. Samoin $10^3 \equiv 1$ ja $10^4 \equiv 1 \pmod{3}$.

Tällöin

$$\begin{aligned} 16\,783 &= 1 \cdot 10^4 + 6 \cdot 10^3 + 7 \cdot 10^2 + 8 \cdot 10 + 3 \\ &\equiv 1 \cdot 1 + 6 \cdot 1 + 7 \cdot 1 + 8 \cdot 1 + 3 \\ &= 1 + 6 + 7 + 8 + 3 = 25 \\ &\equiv 1 \pmod{3}. \end{aligned}$$

Luvun 16 783 jakojäännös on 1, kun jaetaan luvulla 3. Luku 16 783 ei siis ole jaollinen luvulla 3.

b) Koska $10 \equiv 1 \pmod{9}$, niin

$$\begin{aligned} 295\,542 &= 2 \cdot 10^5 + 9 \cdot 10^4 + 5 \cdot 10^3 + 5 \cdot 10^2 + 4 \cdot 10 + 2 \\ &\equiv 2 \cdot 1 + 9 \cdot 1 + 5 \cdot 1 + 5 \cdot 1 + 4 \cdot 1 + 2 \\ &= 2 + 9 + 5 + 5 + 4 + 2 = 27 \\ &\equiv 0 \pmod{9}. \end{aligned}$$

Luvun 295 542 jakojäännös on 0, kun jaetaan luvulla 9. Luku 295 542 on siis jaollinen luvulla 9.

Vastaus: a) Ei ole. b) On.

Edellisessä esimerkissä havaittiin, että luku 16 783 on kongruentti numeroidensa summan $1 + 6 + 7 + 8 + 3$ kanssa modulo 3. Samoin luku 295 542 on kongruentti summan $2 + 9 + 5 + 5 + 4 + 2$ kanssa modulo 9. Nämä ovat esimerkkejä yleisestä säännönmukaisuudesta:

Jaollisuussääntöjä

Kokonaisluku on jaollinen luvulla 3, jos ja vain jos sen numeroiden summa on jaollinen luvulla 3. Vastaavasti kokonaisluku on jaollinen luvulla 9, jos ja vain jos sen numeroiden summa on jaollinen luvulla 9.

Muillakin luvuilla on samantapaisia jaollisuussääntöjä, joista esi-merkkinä on lukuun 11 liittyvä sääntö harjoitustehtävissä.

Tehtäviä.

- (1) Määritä jakojäännös, kun
 - a) luku $80 \cdot 30 - 352$ jaetaan luvulla 7
 - b) luku 2^{140} jaetaan luvulla 3
 - c) luku $0 + 1 + 2 + 3 + \dots + 79 + 80$ jaetaan luvulla 4.
- (2) Määritä jakojäännös, kun
 - a) luku $5 \cdot 11^{99} + 20$ jaetaan luvulla 6
 - b) luku $6^{120} \cdot 4^{301}$ jaetaan luvulla 5
 - c) luku $3^{60} + 55$ jaetaan luvulla 8
 - d) luku 2^{151} jaetaan luvulla 14.
- (3) Näytä, että luku $7^{2502} + 2^{1573}$ on jaollinen kolmella. [Ylioppilas-tehtävä K99 10b kohta 2]
- (4) Määritä jakojäännös, kun summa $(1^3 + 2^3 + 3^3 + \dots + 105^3)$ jaetaan luvulla 3.
- (5) Mikä on luvun a) 2^{77} b) 3^{33} viimeinen numero?
- (6) Olkoon n luonnollinen luku. Osoita, että luku $4 \cdot 7^{n+1} + 2$ on jaollinen luvulla 3.
- (7) Olkoon n luonnollinen luku. Osoita, että luku $13^{2n} + 2^{3n+4} - 10$ on jaollinen luvulla 7.
- (8) Tutki, onko luku jaollinen luvulla 3.
 - a) 123 456 789
 - b) 987 654 321 233
- (9) Määritä jakojäännös, kun luku jaetaan luvulla 9.
 - a) 999 000 000 800
 - b) 111 111 111 111
- (10) Todista, että $(n+1)$ -numeroinen kokonaisluku $a_n a_{n-1} a_{n-2} \dots a_2 a_1 a_0$ on kongruentti numeroidensa summan kanssa modulo 9. Ohje: Esitä luku kymmenen potenssien avulla:

$$\begin{aligned}
 a_n a_{n-1} a_{n-2} \dots a_2 a_1 a_0 \\
 = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + a_{n-2} \cdot 10^{n-2} + \\
 \dots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0.
 \end{aligned}$$

- (11) a) Ajattele jotakin kolminumeroista lukua ja kirjoita se paperille. Vaihda lukusi numeroiden järjestystä ja kirjoita uusi luku paperille. Laske lukujen erotus, jaa erotus luvulla 3 ja kirjoita jakojäännös paperille. Lisää jakojäännökseen luku 7, kerro näin saatu luku luvulla 2 ja vähennä tuloksesta luku 4. Tulos on 10, eikö vain? Miten se voidaan tietää?
- b) Keksi oma algoritmisi, jonka tulos tiedetään etukäteen.

Kotitehtäviä.

- (1) Määritä jakojäännös, kun
 - a) luku $700 - 22 \cdot 185$ jaetaan luvulla 6

- b) luku 2799^{2799} jaetaan luvulla 7
- c) luku $1 + 2 + 3 + 4 + \dots + 36 + 37$ jaetaan luvulla 8.
- (2) Määritä jakojäännös, kun
 - a) luku 2^{256} jaetaan luvulla 5
 - b) luku $12^{10} \cdot 13^3 - 114 \cdot 552$ jaetaan luvulla 11
 - c) luku $34^3 - 966$ jaetaan luvulla 9
 - d) luku 6^{57} jaetaan luvulla 15.
- (3) Tutki, onko luku $46^{78} + 89^{67}$ jaollinen viidellä. (Yo-koe, kevät 2011)
- (4) Määritä jakojäännös, kun summa $(2^0 + 2^1 + 2^2 + 2^3 + 2^4 + 2^5 + \dots + 2^{244})$ jaetaan luvulla 5.
- (5) Mikä on luvun a) 2^{103} b) 4^{111} viimeinen numero?
- (6) Mitkä ovat luvun 5^{30} kaksi viimeistä numeroa?
- (7) Osoita, että
 - a) luku $10^n - 1$ on jaollinen luvulla 9 kaikilla positiivisilla kokonaisluvuilla n
 - b) luku $11^n + 1$ on jaollinen luvulla 12 kaikilla parittomilla positiivisilla kokonaisluvuilla n .
- (8) Olkoon n luonnollinen luku. Määritä jakojäännös, kun luku $501 \cdot 4^{2n} + 2^{2n}$ jaetaan luvulla 5.
- (9) Tutki, onko luku jaollinen luvulla 9.
 - a) 182 736 451
 - b) 18 273 645 144
- (10) Määritä jakojäännös, kun luku jaetaan luvulla 3.
 - a) 222 333 445
 - b) 101 010 101 111
- (11) Osoita luvun 11 jaollisuussääntö: Kokonaisluku on jaollinen luvulla 11, jos ja vain jos sen numeroiden vuorotteleva summa on jaollinen luvulla 11. Vuorotteleva summa lasketaan siten, että luvun viimeisestä numerosta vähennetään toiseksi viimeinen numero, lisätään kolmanneksi viimeinen numero, vähennetään neljänneksi viimeinen numero jne. Vihje: $10 \equiv -1 \pmod{11}$.
- (12) Tutki, onko luku jaollinen luvulla 11.
 - a) 24 927
 - b) 928 072 618
 - c) 7 000 000 000 000 007
 - d) 7 000 000 000 000 070
- (13) Todista, että $a^3b - b^3a$ on tasan jaollinen 3:lla, jos a ja b ovat kokonaislukuja ja $a > b$. [YO 1896 tehtävä 3]

5.4. Luonnolliset luvut ja induktioperiaate (lisämateriaalia).
Käytännön tilanteissa luonnollisia lukuja käytetään yleensä ilmaise-
maan lukumääriä.

Tutkimustehtävä.

- (1) Hyvin suuri määrä ihmisiä seisoo jonossa. Jonossa toteutuu pe-
riaate: jos jollakin jonon henkilöllä on siniset silmät, niin myös
seuraavalla henkilöllä on siniset silmät. Ensimmäisellä jonos-
sa seisovalla henkilöllä on siniset silmät. Mitä voidaan päätellä
muista jonon henkilöistä?
- (2) Tarkastellaan positiivisten kokonaislukujen jonoa $1, 2, 3, 4, 5, 6, \dots$.
Voidaan osoittaa, että jos jollakin positiivisella kokonaisluvulla
 k pätee $3^k \geq 1 + 2k$, niin silloin pätee myös $3^{k+1} \geq 1 + 2(k+1)$.
Tiedetään, että $3^1 \geq 1 + 2 \cdot 1$. Mitä voidaan päätellä? Vertaa
tämän ja edellisen kohdan tilanteita.

Lukuteorian yhteydessä on tarpeellista määritellä täsmällisesti, mitä
luonnolliset luvut ovat. Tämä johtaa matemaattiseen *induktioperiaat-
teeseen*. Asetetaan seuraavat ehdot:

- (1) Luvut 0 ja 1 ovat luonnollisia lukuja.
- (2) Jos n on luonnollinen luku, niin luku $n+1$ on myös luonnollinen
luku.

Kohtaa (2) kutsutaan induktioperiaatteenksi. Vaikka joukko

$$\mathbb{N} = \{0, 1, 2, \dots\}$$

on ääretön, jokainen luku $n \in \mathbb{N} \setminus \{0\}$ on kuitenkin muotoa $n = 1 + \dots + 1$, missä yhteenlaskettavia lukuja on äärellisen monta.

Luonnollisten lukujen määrittelemine induktioperiaatteen avulla joh-
taa tärkeään todistustyyppiin, jota sanotaan *induktiotodistukseksi*. In-
duktiotodistuksen ideana on palauttaa luonnollista lukua $n+1$ kos-
keva väite luonnollista lukua n koskevaksi väitteeksi. Jos lukua $n+1$
koskevan väitteen totuus voidaan päätellä lukua n koskevan väitteen
totuudesta, väite pätee edelleen kaikille luonnollisille luvuille, mikäli se
pätee luvulle 0.

Induktiotodistuksen muoto on yleensä seuraava.

1. Osoitetaan, että tulos pätee, kun $n = 0$. Tämä vaihe on yleensä
yksinkertainen lasku. Induktio voidaan aloittaa myös esimer-
kiksi luvusta $n = 1$.
2. Kiinnitetään $k \in \mathbb{N}$. Oletetaan, että tulos on tosi luvulla $n = k$.
Osoitetaan, että tulos on tosi luvulla $n = k+1$.
3. Nyt induktioperiaatteen seurauksena, että tulos on tosi kaikilla $n \in \mathbb{N}$.

Todistuksen toista vaihetta kutsutaan *induktioaskeleeksi*, siinä esiintyvää oletusta *induktio-oletukseksi* ja väitettä *induktioväitteeksi*.

Esimerkki 1. Olkoon n luonnollinen luku. Osoita induktiolla, että luku $n^2 - n$ on jaollinen luvulla 2.

Ratkaisu: Kun $n = 0$, saadaan $n^2 - n = 0$, joka on jaollinen luvulla 2.

Induktioaskel: Oletetaan, että tulos on tosi jollakin kiinteällä $n = k$. Toisin sanoen $k^2 - k = 2m$ jollakin luonnollisella luvulla m .

Induktioväite: Tulos on tosi, kun $n = k + 1$, eli $(k + 1)^2 - (k + 1)$ on jaollinen luvulla 2.

Lasketaan

$$(k+1)^2 - (k+1) = k^2 + 2k + 1 - k - 1 = k^2 - k + 2k = 2m + 2k = 2(m+k),$$

missä $(m+k)$ on kokonaisluku. Siis $(k+1)^2 - (k+1)$ on jaollinen luvulla 2, joten induktioväite on todistettu.

Nyt induktioperiaatteesta seuraa, että väite on tosi kaikilla $n = 0, 1, 2, \dots$ □

Esimerkki 2. Osoita, että $2^n \geq n^2$, kun n on kokonaisluku ja $n \geq 4$.

Ratkaisu:

Aloitetaan induktio luvusta $n = 4$. Lasketaan aluksi $2^4 = 16$ ja $4^2 = 16$. Epäyhtälö on tosi, kun $n = 4$.

Induktioaskel: Olkoon $k \geq 4$ kiinteä. Oletetaan, että tulos on tosi, kun $n = k$, eli $2^k \geq k^2$.

Induktioväite: Tulos pätee tapauksessa $n = k + 1$ eli $2^{k+1} \geq (k + 1)^2$.

Huomataan aluksi, että induktio-oletuksen perusteella $2^{k+1} = 2 \cdot 2^k \geq 2 \cdot k^2$. Pitää vielä osoittaa, että kaikilla $k \geq 4$ pätee $2k^2 \geq (k + 1)^2$. Tutkitaan, millä muuttujan x arvoilla epäyhtälö $2x^2 \geq (x + 1)^2$ on tosi.

$$\begin{aligned} 2x^2 &\geq (x + 1)^2 \\ 2x^2 &\geq x^2 + 2x + 1. \\ x^2 - 2x - 1 &\geq 0. \end{aligned}$$

Polynomin $x^2 - 2x - 1$ nollakohdat ovat $x = 1 - \sqrt{2} \approx -0,414$ ja $x = 1 + \sqrt{2} \approx 2,414$, ja sen kuvaaja on ylöspäin aukeava paraabeli. Siten epäyhtälö $2k^2 \geq (k + 1)^2$ on tosi, kun $k \geq 4$. Näin ollen myös epäyhtälö $2^{k+1} \geq 2k^2 \geq (k + 1)^2$ on tosi, kun $k \geq 4$.

Siis induktioperiaatteen perusteella $2^n \geq n^2$ kaikilla $n = 4, 5, 6, \dots$ □

Esimerkki 3. Osoita induktiolla, että positiivisille kokonaisluvuille $n = 1, 2, \dots$ pätee

$$\sum_{m=1}^n m = 1 + 2 + 3 + \dots + n = \frac{n(n+1)}{2}.$$

Ratkaisu: Tarkistetaan kaava tapauksessa $n = 1$. Kaavan vasen puoli on

$$\sum_{m=1}^1 m = 1$$

ja kaavan oikea puoli

$$\frac{1 \cdot (1+1)}{2} = \frac{2}{2} = 1.$$

Siten kaava on tosi, kun $n = 1$.

Induktioaskel: Oletetaan, että kaava on todistettu oikeaksi luvun $n = k$ tapauksessa. Toisin sanoen, induktio-oletus on

$$\sum_{m=1}^k m = 1 + 2 + 3 + \dots + k = \frac{k(k+1)}{2}.$$

Induktioväite: Kaava pätee, kun $n = k + 1$, eli

$$\sum_{m=1}^{k+1} m = \frac{(k+1)((k+1)+1)}{2} = \frac{(k+1)(k+2)}{2}.$$

Ottamalla huomioon induktio-oletus saadaan suoralla laskulla

$$\begin{aligned} \sum_{m=1}^{k+1} m &= 1+2+3+\dots+k+(k+1) = \frac{k(k+1)}{2} + (k+1) = \frac{k(k+1)}{2} + \frac{2(k+1)}{2} \\ &= \frac{k(k+1) + 2(k+1)}{2} = \frac{(k+1)(k+2)}{2}, \end{aligned}$$

eli kaava pätee myös, kun $n = k + 1$.

Induktioperiaatteen nojalla väite on siis tosi kaikilla $n = 1, 2, \dots$ \square

Esimerkki 4. Monikulmion sanotaan olevan *kupera* eli *konvekssi*, jos sen kaikki kulmat ovat pienempiä kuin 180° .

Osoita matemaattisella induktiolla, että n -sivuisen kuperan monikulmion lävistäjien lukumäärä on

$$\frac{n(n-3)}{2},$$

kun $n \geq 3$.

Ratkaisu: Kun $n = 3$, kyseessä on kolmio. Kolmio on aina kupera, mutta sillä ei ole yhtään lävistäjää. Kaava antaa

$$\frac{3(3-3)}{2} = \frac{3 \cdot 0}{2} = 0,$$

joten se on tosi tapauksessa $n = 3$.

Induktioaskel: Olkoon $k \geq 3$ kiinteä. Oletetaan, että tulos on tosi, kun $n = k$ eli k -sivuisen kuperan monikulmion lävistäjien lukumäärä on

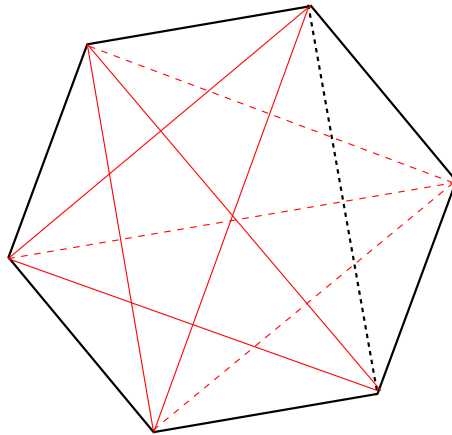
$$\frac{k(k-3)}{2}.$$

Osoitetaan, että tulos on tosi, kun $n = k + 1$, eli $(k + 1)$ -sivuisella kuperalla monikulmiolla on

$$\frac{(k+1)((k+1)-3)}{2}$$

lävistäjää.

Huomataan aluksi, että $(k + 1)$ -sivuisessa monikulmiossa on yksi kärki enemmän kuin k -sivuisessa. Jos $(k + 1)$ -sivuisesta kuperasta monikulmiosta poistetaan yksi kärki ja yhdistetään poistetun kärjen viereiset kärjet janalla, saadaan kupera k -kulmio. Kaikki näin saadun k -kulmion lävistäjät ovat myös alkuperäisen $(k + 1)$ -kulmion lävistäjiä. Poistetusta pisteestä voidaan piirtää $k - 2$ lävistäjää. Lisäksi poistetun pisteen viereisiä pisteitä yhdistävä jana on $(k + 1)$ -kulmion lävistäjä. Siten k -kulmiossa on $k - 1$ lävistäjää vähemmän kuin $(k + 1)$ -kulmiossa.



Siten $(k + 1)$ -sivuisen monikulmion lävistäjien lukumäärä on

$$\frac{k(k-3)}{2} + k - 1 = \frac{k(k-3)}{2} + \frac{2k-2}{2} = \frac{k(k-3) + 2k-2}{2} = \frac{k^2 - k - 2}{2}.$$

Polynomilla $k^2 - k - 2$ on nollakohdat $k = -1$ ja $k = 2$. Polynomi tekijöihinsä jaettuna on $k^2 - k - 2 = (k + 1)(k - 2)$. Siis $(k + 1)$ -sivuisen

monikulmion lävistäjien lukumäärä

$$\frac{(k+1)(k-2)}{2} = \frac{(k+1)((k+1)-3)}{2}.$$

Kaava pätee siis myös kuperille $(k+1)$ -sivuiselle monikulmiolle.

Induktioperiaatteen nojalla kaava on tosi, kun $n = 3, 4, 5, \dots$

□

Tehtäviä.

- (1) Osoita induktiolla, että luku $n^2 + n$ on jaollinen luvulla 2, kun n on luonnollinen luku.
- (2) Osoita induktiolla, että luku $n^3 + 2n$ on jaollinen luvulla 3, kun n on luonnollinen luku.
- (3) Osoita induktiolla, että $2^n > n$, kun n on positiivinen kokonaisluku.
- (4) Osoita induktiolla, että $n^2 > 2n + 1$, kun n on kokonaisluku ja $n \geq 3$.
- (5) Osoita, induktiolla, että luku $7^n + 5$ on jaollinen luvulla 6, kun n on positiivinen kokonaisluku.
- (6) Osoita induktiolla, että luku $10^n - 3^n$ on jaollinen luvulla 7, kun n on positiivinen kokonaisluku.
- (7) Osoita induktiolla, että luku $7^n - 6n + 8$ on jaollinen luvulla 9, kun n on positiivinen kokonaisluku.
- (8) Osoita induktiolla, että $n! > n^2$, kun n on kokonaisluku ja $n \geq 4$. Merkintä $n!$ tarkoittaa luvun n *kertomaa*. Se on tulo $n! = n \cdot (n-1) \cdot (n-2) \cdot \dots \cdot 3 \cdot 2 \cdot 1$.
- (9) Olkoot n positiivinen kokonaisluku ja r reaaliluku, jolle pätee $r \neq 1$. Osoita induktiolla, että

$$1 + r + r^2 + r^3 + \dots + r^{n-1} = \frac{1 - r^n}{1 - r}.$$

- (10) Olkoon n positiivinen kokonaisluku. Osoita induktiolla, että

$$1 \cdot 1! + 2 \cdot 2! + 3 \cdot 3! + \dots + n \cdot n! = (n+1)! - 1.$$

- (11) Osoita induktiolla, että

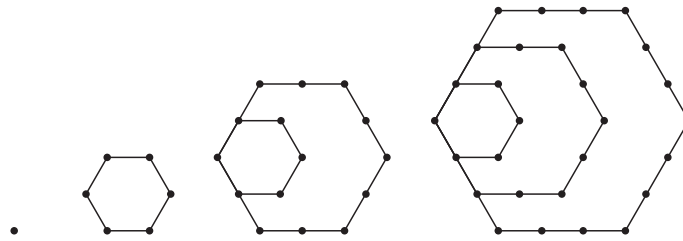
$$\sum_{m=1}^n m^2 = \frac{n(n+1)(2n+1)}{6}, \text{ kun } n = 1, 2, \dots$$

- (12) Osoita induktiolla, että n -alkioisessa joukossa on

$$\frac{n(n-1)}{2}$$

kahden alkion osajoukkoa, kun $n \geq 2$.

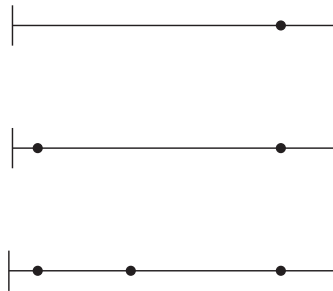
- (13) Todista kappaleessa 5.2 esitetyjen kongruenssin laskusääntöjä koskevan lauseen kohta 4: Olkoot $a, b \in \mathbb{Z}$ ja $k, n \in \mathbb{Z}_+$ sekä $a \equiv b \pmod{k}$. Tällöin $a^n \equiv b^n \pmod{k}$.
- (14) Tarkastellaan kuviojonoa, joka muodostuu säännöllisen kuusikulmion muotoisista pistejoukoista. Jonon neljä ensimmäistä kuviota ovat seuraavat:



- a) Laske, kuinka monta pistettä on kuviojonon kussakin neljässä ensimmäisessä kuviossa.
- b) Muodosta kaava, jolla voidaan laskea, kuinka monta pistettä on n . kuviossa. Tarpeen vaatiessa voit hyödyntää laskimesi polynomisovitus toimintoja.
- c) Todista kaava induktiolla.

Kotitehtäviä.

- (1) Osoita induktiolla, että n jakopisteellä jana voidaan jakaa enintään $n + 1$ janaksi.



- (2) Osoita induktiolla, että luku $n^3 + 5n$ on jaollinen luvulla 6, kun n on luonnollinen luku.
- (3) Osoita, että $3^n > 2n$, kun n on positiivinen kokonaisluku.
- (4) Osoita induktiolla, että $3^n < n!$, kun n on kokonaisluku ja $n \geq 7$.
- (5) Osoita induktiolla, että luku $6^n - 1$ on jaollinen luvulla 5, kun n on positiivinen kokonaisluku.
- (6) Osoita induktiolla, että luku $8^n - 5^n$ on jaollinen luvulla 3, kun n on positiivinen kokonaisluku.
- (7) Osoita induktiolla, että luku $27^{2n} + 3 \cdot 13^n$ on jaollinen luvulla 4, kun n on positiivinen kokonaisluku.
- (8) Osoita induktiolla, että

$$\sum_{m=1}^n m^3 = \frac{n^2(n+1)^2}{4}, \text{ kun } n = 1, 2, \dots$$

- (9) Osoita induktiolla, että $(1+2+3+\dots+n)^2 = 1^3+2^3+3^3+\dots+n^3$, kun n on positiivinen kokonaisluku.
- (10) Tasoon piirretään n suoraa ($n \geq 2$). Osoita, että suorilla voi olla korkeintaan $n(n-1)/2$ leikkauspistettä.
- (11) Tarkastele seuraavia luvun 2 peräkkäisistä potensseista muodostuvia summia:

$$\begin{aligned} 1 &= 1 \\ 1+2 &= 3 \\ 1+2+4 &= 7 \\ 1+2+4+8 &= 15 \\ 1+2+4+8+16 &= 31 \\ 1+2+4+8+16+32 &= 63 \\ 1+2+4+8+16+32+64 &= 127. \end{aligned}$$

Muodosta kaava, jolla voidaan laskea summa $2^0+2^1+2^2+\dots+2^n$, missä n on luonnollinen luku. Todista kaava induktiolla.

- (12) Olkoot n luonnollinen luku ja x reaaliluku, jolle pätee $x > -1$. Osoita, että $(1+x)^n \geq 1+nx$. Kyseessä on niin sanottu *Bernoullin epäyhtälö*.
- (13) Olkoon n positiivinen kokonaisluku. Todista, että

$$\frac{1}{2} \leq \frac{1}{n+1} + \frac{1}{n+2} + \dots + \frac{1}{n+n} < 1.$$

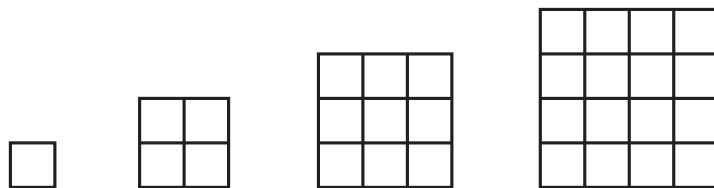
[YO syksy 1971 tehtävä 7]

- (14) Osoita, että kaikilla positiivisilla kokonaisluvuilla n on

$$1^2 + 3^2 + 5^2 + \dots + (2n-1)^2 = \frac{n(4n^2-1)}{3}.$$

[Ylioppilastehtävä K98 8b]

- (15) Tarkastellaan ruudukoista muodostuvaa kuviojonoa, jonka neljä ensimmäistä kuviota ovat seuraavat:



- a) Laske, kuinka monta neliötä kaikkiaan on kuviojonon kussakin neljässä ensimmäisessä ruudukossa.
- b) Muodosta kaava, jolla voidaan laskea, kuinka monta neliötä on n . ruudukossa. Tarpeen vaatiessa voit hyödyntää laskimesi polynomisovitus toimintoja.
- c) Todista kaava induktiolla.
- (16) Eräs keino, jolla voi tarkastaa onko yhteenlasku oikein suoritettu, perustuu seuraavaan lausemaan:

Jos useampien kokonaislukujen summa ja samoin näiden lukujen numerosummien summa jaetaan 9:llä, niin tulevat jäännökset yhtä suuriksi. Todista tämä lauselema. [YO 1895 tehtävä 2]

6. LUKUTEORIAN TULOKSIA

Tässä luvussa käsitellään joitakin lukuteorian tunnetuimpia tuloksia ja niiden todistuksia.

6.1. Suurin yhteinen tekijä ja Eukleideen algoritmi. Seuraavaksi käsitellään kahden positiivisen kokonaisluvun yhteisiä tekijöitä ja esitetään käytännöllinen menetelmä *suurimman yhteisen tekijän* etsimiseksi.

Tutkimustehtävä.

- (1) Määritä lukujen 45 ja 75 kaikki positiiviset tekijät.
- (2) Mitkä ovat lukujen yhteiset positiiviset tekijät?
- (3) Mikä on lukujen suurin yhteinen tekijä?
- (4) Supista murtoluku $\frac{45}{75}$.

Esimerkki 1. Määritä lukujen 30 ja 84 kaikki positiiviset tekijät. Mitkä ovat niiden yhteiset positiiviset tekijät? Mikä on niiden suurin yhteinen tekijä?

Ratkaisu: Luvun 30 positiiviset tekijät ovat 1, 2, 3, 5, 6, 10, 15 ja 30. Luvun 84 positiiviset tekijät ovat 1, 2, 3, 4, 6, 7, 12, 14, 21, 28, 42 ja 84.

Lukujen 30 ja 84 yhteiset positiiviset tekijät ovat 1, 2, 3 ja 6. Yhteisistä tekijöistä suurin on 6.

Vastaus: Yhteiset positiiviset tekijät ovat 1, 2, 3 ja 6. Suurin yhteinen tekijä on 6.

Suurin yhteinen tekijä

Olkoot a ja b positiivisia kokonaislukuja. Positiivista kokonaislukua d sanotaan lukujen a ja b suurimmaksi yhteiseksi tekijäksi, jos seuraavat ehdot ovat voimassa:

- (1) Luku d on lukujen a ja b tekijä, eli $d|a$ ja $d|b$.
- (2) Luku d on suurin lukujen a ja b tekijöistä.

Lukujen a ja b suurinta yhteistä tekijää merkitään $\text{syt}(a, b)$ tai joskus $\text{gcd}(a, b)$. Lyhenne gcd tulee englanninkielisestä ilmaisusta *greatest common divisor*.

Kahden luvun suurin yhteinen tekijä voidaan ainakin periaatteessa aina löytää luettelemalla näiden lukujen tekijät, etsimällä lukujen yhteiset tekijät ja valitsemalla lopuksi yhteisistä tekijöistä suurin. Tämä menettelytapa muuttuu kuitenkin hankalaksi suurten lukujen kohdalla, vaikka käytössä olisi tietokone.

Tehokkaan algoritmin suurimman yhteisen tekijän etsimiseksi esitti aleksandrialainen matemaatikko Eukleides (n. 300 eaa.) teoksessaan *Stoikheia* (Alkeet, latinaksi *Elementa*). Alkeet on yksi matematiikan

historian tärkeimmistä teoksista, ja se säilyi käytetyimpänä geometrian oppikirjana aina 1800-luvulle saakka. Teoksessa esitettyä algoritmia kutsutaan *Eukleideen algoritmiksi*, ja se perustuu seuraavaan lemmaan:

Lemma. Olkoot a ja b sellaisia positiivisia kokonaislukuja, että

$$a = qb + r,$$

missä q sekä r ovat kokonaislukuja ja $0 < r < b$. Tällöin kokonaisluku c on lukujen a ja b yhteinen tekijä, jos ja vain jos c on lukujen b ja r yhteinen tekijä.

Todistus. Oletetaan aluksi, että c on jokin lukujen a ja b yhteinen tekijä. Osoitetaan, että se on myös lukujen b ja r yhteinen tekijä.

Kirjoitetaan $r = a - qb$. Luvun c täytyy olla luvun r tekijä, koska se on lukujen a ja b tekijä. Siten c on lukujen b ja r yhteinen tekijä.

Oletetaan, että c on jokin lukujen b ja r yhteinen tekijä. Koska $a = qb + r$, luvun c täytyy olla myös luvun a tekijä. Siten c on lukujen a ja b yhteinen tekijä.

□

Seuraus. Jos a ja b ovat positiivisia kokonaislukuja ja $a = qb + r$, missä q sekä r ovat kokonaislukuja ja $0 < r < b$, niin $\text{syt}(a, b) = \text{syt}(b, r)$.

Todistus. Lemman perusteella lukujen a ja b yhteiset tekijät ovat samat kuin lukujen b ja r yhteiset tekijät. Erityisesti siis lukujen a ja b suurimman yhteisen tekijän täytyy olla sama kuin lukujen b ja r suurimman yhteisen tekijän. □

Eukleideen algoritmin idea on seuraava: Lähdetään liikkeelle kahdesta positiivisesta kokonaisluvusta a ja b , $a \geq b$, joiden yhteistä tekijää etsitään. Ensimmäinen askel on esittää luku a luvun b avulla jakoyhtälönä:

$$a = q_1b + r_1, \quad 0 \leq r_1 < b.$$

Jos jakojäännös $r_1 = 0$, niin $b|a$ ja $\text{syt}(a, b) = b$. Jos $r_1 \neq 0$, jaetaan b luvulla r_1 , jolloin saadaan esitys

$$b = q_2r_1 + r_2, \quad 0 \leq r_2 < r_1,$$

missä q_2 on jakolaskun b/r_1 osamäärä ja r_2 jakojäännös.

Jos $r_2 = 0$, niin r_1 on suurin yhteinen tekijä ja voidaan lopettaa. Mikäli näin ei ole, jatketaan jakamalla luku r_1 luvulla r_2 , jolloin saadaan

$$r_1 = q_3r_2 + r_3, \quad 0 \leq r_3 < r_2.$$

Näin jatkamalla päädytään lopulta jakolaskuun, joka menee tasan. Lukujen a ja b suurin yhteinen tekijä on viimeinen nollasta eroava jakojäännös. Koska algoritmissa esiintyy laskeva jono $b > r_1 > r_2 > \dots \geq 0$, tarvitaan enintään b askelta. Algoritmissa tarvittavat jakolaskut kannattaa yleensä tehdä laskimella.

Esimerkki 2. Määritä $\text{syt}(84, 30)$ Eukleideen algoritmia käyttäen.

Ratkaisu:

$84 = 2 \cdot 30 + 24$	Jaetaan luku 84 luvulla 30 ja esitetään luku 84 luvun 30 avulla. Jakojäännös ei ole nolla.
$30 = 1 \cdot 24 + 6$	Jaetaan luku 30 saadulla jakojäännöksellä 24 ja esitetään luku 30 luvun 24 avulla. Jakojäännös ei ole nolla.
$24 = 4 \cdot 6$	Esitetään luku 24 jakojäännöksen 6 avulla. Nyt jako menee tasan.

(Kuvioon tulee nuolet luvusta 30 lukuun 30 ja luvusta 24 lukuun 24, sekä luvusta 24 lukuun 24 ja luvusta 6 lukuun 6.)

Suurin yhteinen tekijä on viimeinen nollasta eroava jakojäännös, 6. Siis $\text{syt}(84, 30) = 6$. Saatiin sama tulos kuin esimerkissä 1.

Vastaus: $\text{syt}(84, 30) = 6$.

Esimerkki 3. Määritä $\text{syt}(16515, 3951)$ Eukleideen algoritmia käyttäen.

Ratkaisu: Eukleideen algoritmi johtaa yhtälöihin:

$$\begin{aligned}
 16515 &= 4 \cdot 3951 + 711, \\
 3951 &= 5 \cdot 711 + 396, \\
 711 &= 1 \cdot 396 + 315, \\
 396 &= 1 \cdot 315 + 81, \\
 315 &= 3 \cdot 81 + 72, \\
 81 &= 1 \cdot 72 + 9, \\
 72 &= 8 \cdot 9.
 \end{aligned}$$

Suurin yhteinen tekijä on viimeinen nollasta eroava jakojäännös, siis tässä tapauksessa 9. Siten

$$\text{syt}(16515, 3951) = 9.$$

Vastaus: $\text{syt}(16515, 3951) = 9$.

Tehtäviä.

- (1) Määritä lukujen suurin yhteinen tekijä.
 - a) 15 ja 20
 - b) 9 ja 36
 - c) 4 ja 7
- (2) Määritä Eukleideen algoritmia käyttäen
 - a) $\text{sy}(184, 152)$
 - b) $\text{sy}(227, 143)$.
- (3) Määritä Eukleideen algoritmia käyttäen
 - a) $\text{sy}(272, 1479)$
 - b) $\text{sy}(4719, 18207)$.
- (4) Esitä murtoluku a) $\frac{143}{605}$ b) $\frac{5989}{30899}$ supistetussa muodossa. Vihje: Määritä osoittajan ja nimittäjän suurin yhteinen tekijä.
- (5) Osoita, että murtoluku $\frac{8788}{13475}$ ei supistu.
- (6) Leirille osallistui 780 tyttöä ja 612 poikaa. Osallistujat jaettiin keskenään yhtä suuriin ryhmiin siten, että kussakin ryhmässä oli vain tyttöjä tai poikia. Mikä oli suurin mahdollinen ryhmäkoko?
- (7) Määritä lukujen 188 000 100 ja 188 suurin yhteinen tekijä.
- (8) Olkoon a positiivinen kokonaisluku. Määritä
 - a) $\text{sy}(a, a)$
 - b) $\text{sy}(a, 1)$
 - c) $\text{sy}(a^2, a)$
 - d) $\text{sy}((a+1)!, a!)$.
 Merkintä $a!$ tarkoittaa luvun a *kertomaa*. Se on tulo $a! = a \cdot (a-1) \cdot (a-2) \cdot \dots \cdot 3 \cdot 2 \cdot 1$.
- (9) Olkoon n positiivinen kokonaisluku. Osoita Eukleideen algoritmia käyttäen, että $\text{sy}(n+1, n) = 1$.
- (10) Olkoon n positiivinen kokonaisluku. Määritä lukujen $n^2 + 2n$ ja $n+1$ suurin yhteinen tekijä.
- (11) Olkoon n positiivinen kokonaisluku. Osoita, että $\text{sy}(3^{n+1} + 10, 3^n + 2) = 1$.

Kotitehtäviä

- (1) Määritä lukujen suurin yhteinen tekijä.
 - a) 63 ja 7
 - b) 64 ja 33
 - c) 45 ja 60
- (2) Määritä Eukleideen algoritmia käyttäen
 - a) $\text{sy}(657, 306)$
 - b) $\text{sy}(2197, 4641)$
 - c) $\text{sy}(15787, 4111)$.
- (3) Esitä murtoluku a) $\frac{182}{299}$ b) $\frac{7697}{32041}$ supistetussa muodossa.

- (4) Leipomo suljettiin remontin ajaksi. Ennen sulkemista laskettiin, että leipomon varastossa oli 4896 vehnäsämpylää ja 1408 grahamsämpylää. Sämpylät pakattiin kuljetusta varten keskenään samankokoisiin pusseihin siten, että kuhunkin pussiin tuli vain vehnä- tai grahamsämpylöitä. Mikä oli suurin mahdollinen pussikoko? Oletetaan, että vehnäsämpylä oli samankokoinen kuin grahamsämpylä ja että yksikään pussi ei jäänyt vajaaksi.
- (5) Määritä lukujen 468 468 468 108 ja 234 suurin yhteinen tekijä.
- (6) Olkoot a , b ja c positiivisia kokonaislukuja. Lukujen a , b ja c suurin yhteinen tekijä eli $\text{sy}(a, b, c)$ voidaan määrittää siten, että ensin määritetään kahden luvun suurin yhteinen tekijä ja sitten tämän ja kolmannen luvun suurin yhteinen tekijä. Määritä
 - a) $\text{sy}(15, 30, 40)$
 - b) $\text{sy}(6, 9, 11)$
 - c) $\text{sy}(171, 456, 665)$.
- (7) Olkoot a ja b positiivisia kokonaislukuja ja $\text{sy}(a, b) = 9$. Voiko tällöin yhtälö $a + b = 186$ olla tosi?
- (8) Olkoon n positiivinen kokonaisluku. Tutki, mitä arvoja $\text{sy}(n + 4, n)$ voi saada.
- (9) Olkoon n positiivinen kokonaisluku. Määritä lukujen $n^2 + 3n$ ja $n + 2$ suurin yhteinen tekijä.
- (10) Olkoot a ja b positiivisia kokonaislukuja. Osoita, että $\text{sy}(a, b)$ on jaollinen kaikilla lukujen a ja b yhteisillä tekijöillä.

6.2. Diofantoksen yhtälöt. Noin vuoden 250 tienoilla elänyt Diofantos oli yksi viimeisistä antiikin Aleksandriassa vaikuttaneista suurista matemaatikoista. Aleksandrian suuruuden ajan oppineisuuden keskukseksi katsotaan yleisesti päättyneen noin sata vuotta myöhemmin pakonaksi ja noidaksi syytetyn naismatemaatikko Hypatian murhaan vuonna 415. Vaikka Diofantos kirjoitti kreikaksi ja häntä usein kutsutaan kreikkalaiseksi matemaatikoksi, Diofantos oli todennäköisesti kreikkalaistunut babylonialainen.

Tutkimustehtävä.

- (1) Missä sijaitsevat ne xy -tason pisteet, joiden koordinaatit toteuttavat yhtälön $x + 3y = 6$?
- (2) Etsitään seuraavaksi kokonaislukuratkaisuja kahden muuttujan yhtälölle $x + 3y = 6$. Määritä yhtälölle jokin kokonaislukuratkaisu.
- (3) Määritä yhtälölle vielä ainakin kolme muuta kokonaislukuratkaisua. Kuinka monta ratkaisua yhtälöllä on kaiken kaikkiaan?
- (4) Määritä kaikki yhtälön $x + 3y = 6$ kokonaislukuratkaisut.
- (5) Etsi vastaava kokonaislukukertoimen kahden muuttujan yhtälö, jolla ei ole yhtään kokonaislukuratkaisua.

Marginaaliin: Diofantoksesta ei tiedetä kovinkaan paljon, mutta hänen tarkka elinikänsä tunnetaan kuitenkin hautakiveen ikuistetusta matemaattisesta ongelmasta: Diofantoksen poikavuodet kestivät $1/6$ hänen elämästään, parta alkoi kasvaa $1/12$ tämän jälkeen, $1/7$ kuluttua hän meni naimisiin ja hänen poikansa syntyi 5 vuotta myöhemmin. Poika eli puolet siitä, mitä isänsä, ja isä kuoli neljä vuotta poikansa kuoleman jälkeen. Ongelma johtaa yhtälöön

$$\frac{1}{6}x + \frac{1}{12}x + \frac{1}{7}x + 5 + \frac{1}{2}x + 4 = x,$$

josta Diofantoksen elinvuodet voidaan ratkaista. Ratkaisu on $x = 84$.

Diofantoksen yhtälöiksi kutsutaan muotoa

$$ax + by = c$$

olevia yhtälöitä, missä x ja y ovat kokonaislukuja. Yhtälössä esiintyvät vakiot a, b ja c ovat myös kokonaislukuja ja ainakin toinen luvuista a, b on nollasta poikkeava. Tässä kurssissa käsitellään vain kyseistä muotoa olevia yhtälöitä, mutta nykyään matematiikassa sanotaan Diofantoksen yhtälöiksi myös muita yhtälöitä, joissa ratkaistavana on yksi tai useampi kokonaisluku. Diofantos ei itse tutkinut tällaisia yhtälöitä.

Diofantoksen yhtälöllä voi olla useita ratkaisuja tai ei yhtään ratkaisua. Esimerkiksi yhtälölle

$$3x + 6y = 18$$

voidaan löytää ainakin seuraavat ratkaisut:

$$18 = 3 \cdot 4 + 6 \cdot 1 = 3 \cdot (-6) + 6 \cdot 6 = 3 \cdot 10 + 6 \cdot (-2).$$

Toisaalta esimerkiksi yhtälöllä $2x + 10y = 17$ ei ole ratkaisua.

Ratkaisujen etsimisessä on hyötyä tiedosta, että jos on annettu positiiviset kokonaisluvut a ja b , niin on aina olemassa kokonaisluvut x ja y siten, että

$$\text{syt}(a, b) = ax + by.$$

Käytännössä kertoimien etsiminen ei ole vaikeaa, sillä siinä voidaan käyttää hyväksi Eukleideen algoritmia.

Esimerkki 1. Ratkaise Diofantoksen yhtälö $\text{syt}(84, 30) = 84x + 30y$.

Ratkaisu: Lukujen 84 ja 30 suurin yhteinen tekijä ratkaistiin edellisen kappaleen esimerkissä 2. Eukleideen algoritmi johti yhtälöihin

$$\begin{aligned} 84 &= 2 \cdot 30 + 24, \\ 30 &= 1 \cdot 24 + 6, \\ 24 &= 4 \cdot 6, \end{aligned}$$

joten $\text{syt}(84, 30) = 6$. Ratkaistavana on siis yhtälö $6 = 84x + 30y$.

Pyritään nyt ilmaisemaan luku 6 lukujen 84 ja 30 avulla. Kuljetaan Eukleideen algoritmia lopusta alkuun ja ratkaistaan jakoyhtälöistä jakojäännökset. Viimeinen nollasta eroava jakojäännös on 6. Lausutaan se lukujen 30 ja 24 avulla: $6 = 30 - 1 \cdot 24$. Saadussa lausekkeessa luku 24 on edellisen yhtälön jakojäännös, joka puolestaan voidaan lausua lukujen 84 ja 30 avulla: $24 = 84 - 2 \cdot 30$. Yhdistämällä tulokset saadaan luku 6 ilmaistua lukujen 84 ja 30 avulla:

$$6 = 30 - 1 \cdot 24 = 30 - 1 \cdot (84 - 2 \cdot 30) = 30 - 1 \cdot 84 + 2 \cdot 30 = -1 \cdot 84 + 3 \cdot 30.$$

Siis $6 = 84 \cdot (-1) + 30 \cdot 3$, joten yhtälön $6 = 84x + 30y$ ratkaisu on $x = -1$ ja $y = 3$.

Vastaus: $x = -1$ ja $y = 3$.

Diofantoksen yhtälöitä voidaan usein ratkaista esimerkiksi tietokoneella, mutta se onnistuu myös seuraavaa tulosta käyttämällä.

Lause. Diofantoksen yhtälöllä

$$ax + by = c$$

on ratkaisu, jos ja vain jos $d|c$, kun $d = \text{syt}(a, b)$.

Todistus. Osoitetaan aluksi epäsuoraa todistusta käyttämällä, että ratkaisun olemassaolosta seuraa $d|c$. Tehdään vastaoletus, että $d \nmid c$. Tällöin yhtälöllä ei voi olla ratkaisua, koska $d|a$ ja $d|b$, joten d jakaa yhtälön vasemman puolen mutta ei oikeaa puolta.

On vielä osoitettava ekvivalenssiväitteen toinen suunta: Jos $d|c$, niin kyseisellä Diofantoksen yhtälöllä on ratkaisu. Jos $d|c$, niin $c = dt$ jollakin kokonaisluvulla t . Aikaisemmin todettiin, että lukujen a ja b suurin yhteinen tekijä voidaan kirjoittaa muodossa

$$d = \text{syt}(a, b) = ax_1 + by_1$$

joillekin luvuille x_1 ja y_1 . Koska

$$c = dt = (ax_1 + by_1)t = a(tx_1) + b(ty_1),$$

saadaan pari $x = tx_1$ ja $y = ty_1$, joka toteuttaa alkuperäisen yhtälön. \square

Lause. Jos

$$ax + by = c$$

on ratkeava Diofantoksen yhtälö, sen yksi ratkaisu on $x = tx_1$ ja $y = ty_1$, missä kertoimet x_1 ja y_1 määräytyvät yhtälöstä

$$d = \text{syt}(a, b) = ax_1 + by_1 \text{ ja } t = c/d.$$

Todistus. Edellisen lauseen nojalla Diofantoksen yhtälöllä

$$d = ax + by,$$

missä $d = \text{syt}(a, b)$, on ratkaisu. Merkitään jotakin kyseisen yhtälön ratkaisua x_1, y_1 .

On osoitettava, että tämän ratkaisun avulla voidaan löytää haluttua muotoa oleva ratkaisu alkuperäiselle yhtälölle

$$ax + by = c.$$

Edellisen lauseen perusteella Diofantoksen yhtälöllä on ratkaisu, jos ja vain jos $d|c$. Siten $t = c/d$ on kokonaisluku.

Kerrotaan yhtälön

$$d = ax_1 + by_1$$

molemmat puolet luvulla $t = c/d$. Tällöin saadaan

$$c = td = t(ax_1 + by_1) = a(tx_1) + b(ty_1).$$

Tämä osoittaa, että $x = tx_1$ ja $y = ty_1$ on alkuperäisen Diofantoksen yhtälön ratkaisu. \square

Itse asiassa jos x_0 ja y_0 ovat yhtälön $ax + by = c$ jokin ratkaisu, niin sen kaikki ratkaisut saadaan kaavoista

$$x = x_0 + n\frac{b}{d}, \text{ ja } y = y_0 - n\frac{a}{d}, \text{ missä } n \in \mathbb{Z} \text{ ja } d = \text{syt}(a, b).$$

Erityisesti siis jokaisella ratkeavalla Diofantoksen yhtälöllä on äärettömän monta ratkaisua. Ratkaisussa esiintyvät kertoimet saattavat kuitenkin olla negatiivisia lukuja.

Esimerkki 2. Määritä Diofantoksen yhtälön

$$172x + 20y = 1000$$

jokin ratkaisu.

Ratkaisu: Tutkitaan ensin, onko Diofantoksen yhtälöllä $172x + 20y = 1000$ ratkaisua. Määritetään $\text{sy}(172, 20)$ Eukleideen algoritmia käyttäen:

$$172 = 8 \cdot 20 + 12,$$

$$20 = 1 \cdot 12 + 8,$$

$$12 = 1 \cdot 8 + 4,$$

$$8 = 2 \cdot 4.$$

Siten $\text{sy}(172, 20) = 4$. Koska $4 \mid 1000$, Diofantoksen yhtälöllä on ratkaisu.

Ratkaisun löytämiseksi täytyy esittää luku 4 lukujen 172 ja 20 avulla muodossa

$$4 = 172 \cdot x_1 + 20 \cdot y_1.$$

Soveltamalla Eukleideen algoritmin askelia käänteisessä järjestyksessä saadaan

$$\begin{aligned} 4 &= 12 - 8 \\ &= 12 - (20 - 12) \\ &= 2 \cdot 12 - 20 \\ &= 2 \cdot (172 - 8 \cdot 20) - 20 \\ &= 2 \cdot 172 + (-17) \cdot 20. \end{aligned}$$

Kertomalla tämä lauseke luvulla $1000/4 = 250$ saadaan viimein

$$\begin{aligned} 1000 = 250 \cdot 4 &= 250 \cdot (2 \cdot 172 + (-17) \cdot 20) \\ &= 500 \cdot 172 + (-4250) \cdot 20. \end{aligned}$$

Siten yhtälön $172x + 20y = 1000$ ratkaisu on $x = 500$ ja $y = -4250$.

Vastaus: $x = 500$ ja $y = -4250$

Esimerkki 3. Määritä Diofantoksen yhtälön $172x + 20y = 1000$ kaikki ratkaisut. Mitkä niistä toteuttavat ehdon $|x| + |y| \leq 50$?

Ratkaisu: Diofantoksen yhtälön $ax + by = c$ kaikki ratkaisut saadaan kaavoista

$$x = x_0 + n \frac{b}{d} \text{ ja } y = y_0 - n \frac{a}{d},$$

missä x_0 ja y_0 ovat yhtälön jokin ratkaisu, $d = \text{sy}(a, b)$ ja n on mikä tahansa kokonaisluku. Diofantoksen yhtälössä $172x + 20y = 1000$ on $a = 172$, $b = 20$, ja edellisen esimerkin nojalla $x_0 = 500$, $y_0 = -4250$ ja $d = 4$. Sijoittamalla kaavoihin saadaan yhtälön $172x + 20y = 1000$ ratkaisuiksi

$$x = 500 + n \frac{20}{4} \text{ ja } y = -4250 - n \frac{172}{4}$$

eli $x = 500 + 5n$ ja $y = -4250 - 43n$, $n \in \mathbb{Z}$.

Jotta ehto $|x| + |y| \leq 50$ toteutuisi, pitää muuttujien x ja y olla itseisarvoiltaan pieniä. Tutkitaan yhtälöitä $x = 500 + 5n = 0$ ja $y = -4250 - 43n = 0$ ja ratkaistaan kummastakin parametri n .

$$\begin{aligned} 500 + 5n &= 0 \\ 5n &= -500 \\ n &= -100 \\ -4250 - 43n &= 0 \\ -43n &= 4250 \\ n &\approx -98,8 \end{aligned}$$

Osoittautuu siis, että molempien yhtälöiden mukaan n on lähellä arvoa -100 tai -99 . Taulukoidaan myös muutamia muita näitä arvoja lähellä olevia parametrin n arvoja ja tutkitaan kussakin tapauksessa, toteutuuko ehto $|x| + |y| \leq 50$.

n	x	y	$ x + y $
-97	15	-79	94
-98	10	-36	46
-99	5	7	12
-100	0	50	50
-101	-5	93	98
-102	-10	136	146

Taulukosta nähdään, että $|x| + |y| \leq 50$, kun $x = 10$ ja $y = -36$, kun $x = 5$ ja $y = 7$ tai kun $x = 0$ ja $y = 50$. Muita ratkaisuja ei ole, sillä kun n pienenee tai suurenee taulukon arvoista, niin sekä $|x|$ että $|y|$ suurenevät.

Vastaus: Kaikki ratkaisut ovat $x = 500 + 5n$ ja $y = -4250 - 43n$, $n \in \mathbb{Z}$. Näistä ehdon $|x| + |y| \leq 50$ toteuttavat ratkaisut $x = 10$ ja $y = -36$, $x = 5$ ja $y = 7$ sekä $x = 0$ ja $y = 50$.

Esimerkki 4. (Kexleruksen viiniongelmä) (Lisämateriaalia) Suomen ensimmäinen matematiikan professori, Turun akatemiassa vaikuttanut Simon Kexlerus (1602–1669) jätti jälkeensä seuraavan ongelman.



Markan kolikko vuodelta 1983.

Sinulla on viinejä, jotka maksavat 3, 5, 8 ja 10 markkaa pullolta. Ota yhteensä kymmenen täyttää pulloa ja tee niistä sekoitus, joka maksaa 6 markkaa pullolta. Kuinka monta pulloa kutakin viinilajia on otettava?

Ratkaisu: Merkitään tarvittavien pullojen määrää a, b, c ja d . Ongelma johtaa kahteen Diofantoksen yhtälöön,

$$a + b + c + d = 10$$

ja

$$3a + 5b + 8c + 10d = 60.$$

Selvästi tehtävän ratkaisut ovat kokonaislukuja välillä $0, \dots, 10$. Tehtävä ei ole aikaisemmin esitettyä muotoa. Siitä kuitenkin saadaan sellainen, jos oletetaan, että käytetään vain kahta eri viiniä. Toisin sanoen, asetetaan kaksi kertoimista a, b, c, d nolaksi.

Kahden ensimmäisen viinin hinta on tavoitehintaa alhaisempi ja kahden jälkimmäisen vastaavasti tavoitehintaa korkeampi. Siksi ongelma voi ratketa kahta viiniä käyttämällä vain, jos toinen valitaan seokseen kahdesta edullisemmasta ja toinen kahdesta kalliimmasta viinistä. Kokeillaan aluksi kertoimia $a = c = 0$. Nyt saadaan

$$5b + 10d = 60.$$

Koska $\text{sy}(5, 10) = 5$ ja $5 \mid 60$, ratkaisu on olemassa. Esitetään aluksi luku 5 lukujen 10 ja 5 avulla:

$$5 = -1 \cdot 5 + 1 \cdot 10.$$

Kertomalla luvulla 12 saadaan

$$60 = -12 \cdot 5 + 12 \cdot 10,$$

joten yhtälöllä $5b + 10d = 60$ on ratkaisu $b = -12$ ja $d = 12$. Tätä ratkaisua ei kuitenkaan voida hyväksyä, koska siinä esiintyy negatiivinen kerroin, -12 , eikä se myöskään toteuta toista vaadittua yhtälöä, $b + d = 10$.

Yhtälöllä on kuitenkin muitakin ratkaisuja. Ne saadaan kaavoista

$$b = -12 + (10/5)n, \quad d = 12 - (5/5)n,$$

eli

$$b = -12 + 2n, \quad d = 12 - n,$$

missä n on mikä tahansa kokonaisluku. Sijoittamalla yhtälöön $b + d = 10$ saadaan

$$-12 + 2n + 12 - n = 10,$$

eli $n = 10$. Ratkaisu on siis $b = -12 + 2 \cdot 10 = 8$ ja $d = 12 - 10 = 2$.

Vastaus: On otettava esimerkiksi 8 pulloa 5 markan viiniä ja 2 pulloa 10 markan viiniä.

Esimerkiksi tietokonetta käyttämällä voidaan löytää ongelman kaikki ratkaisut. Niitä on yhteensä seitsemän. Ei ole tiedossa, miten Kexlerus itse ratkaisi ongelmansa.

Tehtäviä.

- (1) Tutki, onko Diofantoksen yhtälöllä ratkaisua.
 - (a) $7x + 5y = 3$
 - (b) $5x + 85y = 42$
 - (c) $6x + 51y = 100$
- (2) Leirille osallistui 364 nuorta. Oliko mahdollista majoittaa osallistujat 24 ja 16 hengen parakkeihin siten, että yksikään parakki ei jäänyt vajaaksi?
- (3) Määritä Diofantoksen yhtälön jokin ratkaisu.
 - (a) $14x + 49y = \text{syt}(14, 49)$
 - (b) $56x + 72y = \text{syt}(56, 72)$
- (4) Määritä Diofantoksen yhtälön jokin ratkaisu.
 - (a) $56x + 72y = 40$
 - (b) $24x + 138y = -24$
- (5) Tutki, onko suoralla
 - (a) $26x + 91y + 10 = 0$
 - (b) $529x + 621y - 92 = 0$
 pisteitä, joiden molemmat koordinaatit ovat kokonaislukuja.
- (6) Määritä Diofantoksen yhtälön kaikki ratkaisut.
 - (a) $2x + 3y = 1$
 - (b) $2x + 3y = 7$
- (7) Määritä Diofantoksen yhtälön $45x + 21y = -6$ kaikki ratkaisut.
- (8) Määritä Diofantoksen yhtälön $13\,509x + 10\,203y = 228$ kaikki ratkaisut.
- (9) Etsi Diofantoksen yhtälö, jolla a) ei ole ratkaisua b) on äärettömän monta ratkaisua.
- (10) Määritä Diofantoksen yhtälön $63x + 279y = 450$ kaikki ratkaisut. Mitkä niistä toteuttavat ehdon $|x| + |y| < 25$?
- (11) Käytettävissä on 8 gramman ja 12 gramman punnuksia. Kuinka monta kummankinlaista punnusta tarvitaan, jotta punnusten kokonaismassaksi tulisi 100 grammaa? Selvitä kaikki vaihtoehdot.
- (12) Ruhtinas jakoi 63 yhtä suurta kekoa hedelmiä sekä 7 erillistä hedelmää tasan 23 matkalaiselle. Kuinka monta hedelmää kussakin keossa oli? Vihje: Tutki yhtälöä $63x + 7 = 23y$. (Mahavira, v. 850)
- (13) Olkoot a, b, c ja d positiivisia kokonaislukuja. Osoita, että yhtälöllä $ax + by + cz = d$ on kokonaislukuratkaisu, jos ja vain jos luku d on jaollinen lukujen a, b ja c suurimmalla yhteisellä tekijällä.

Kotitehtäviä

- (1) Tutki, onko Diofantoksen yhtälöllä ratkaisua.
 - (a) $9x + 6y = 72$
 - (b) $12x + 10y = 323$

- (c) $14x + 35y = -91$
- (2) Emilia sai valmistujaislahjaksi 200 euron lahjakortin erääseen keramiikkapajaan. Hän osti pajasta 27 euron hintaisia kynttilänjalkoja ja 15 euron hintaisia jälkiruokalautasia. Hän maksoi ostoksensa lahjakortilla ja sai rahaa takaisin 12 euroa. Laskiko myyjä oikein?
- (3) Määritä Diofantoksen yhtälön jokin ratkaisu.
(a) $59x + 12y = \text{syt}(59, 12)$
(b) $119x + 272y = \text{syt}(119, 272)$
- (4) Määritä Diofantoksen yhtälön jokin ratkaisu.
(a) $36x + 16y = 28$
(b) $221x + 35y = 2$
- (5) Määritä Diofantoksen yhtälön kaikki ratkaisut.
(a) $2x + 6y = 2$
(b) $2x + 6y = -10$
- (6) Määritä Diofantoksen yhtälön $35x + 84y = 14$ kaikki ratkaisut.
- (7) Määritä Diofantoksen yhtälön $11\,925x + 3\,843y = -117$ kaikki ratkaisut.
- (8) Määritä Diofantoksen yhtälön $168x + 204y = 24$ kaikki ratkaisut. Mille ratkaisuille pätee $-50 \leq x \leq 0$ ja $y > 10$?
- (9) Esitä luku 100 kahden positiivisen kokonaisluvun summana niin, että toinen luvuista on jaollinen luvulla 7 ja toinen luvulla 11. (Euler, v. 1770)
- (10) Yhtiön kauppavoitto 150 mk on jaettava tasan osakkaille. Jos osakkaita olisi ollut 5 enemmän, olisi jokainen saanut 5 mk vähemmän. Montako osakasta oli yhtiössä? [YO 1874 tehtävä 6]
- (11) Sata lyhdettä viljaa jaetaan sadalle henkilölle niin, että kukin mies saa 3 lyhdettä, nainen 2 lyhdettä ja lapsi puoli lyhdettä. Kuinka monta miestä, naista ja lasta on? (Alcuin Yorkilainen, v. 775)
- (12) (Lisämateriaalia.) Osoita suoralla sijoituksella, että $a = 2$, $b = 4$, $c = 3$ ja $d = 1$ on yksi Kexleruksen viiniongelman ratkaisuisia.
- (13) (Lisämateriaalia.) Ratkaise Kexleruksen viiniongelma, kun asetetaan $b = 0$ ja $d = 0$.
- (14) (Lisämateriaalia.) Osoita, että Kexleruksen viiniongelmallalla ei ole ratkaisuja, jos asetetaan $a = 0$ ja $d = 0$.

6.3. Alkuluvut ja aritmetiikan peruslause.

Tutkimustehtävä.

- (1) Millä positiivisilla kokonaisluvuilla luku 60 on jaollinen?
- (2) Millä positiivisilla kokonaisluvuilla luku 29 on jaollinen?
- (3) Esitä luku 60 mahdollisimman pienten positiivisten kokonaislukujen tulona.

Alkuluvuksi sanotaan luonnollista lukua $p \geq 2$, joka ei ole jaollinen muilla positiivisilla kokonaisluvuilla kuin itsellään sekä luvulla 1. Esimerkiksi luku 13 on alkuluku. Luku 14 ei ole alkuluku, koska se on jaollinen myös luvuilla 2 ja 7.

Esimerkki 1. Tutki, onko luku a) 23, b) 357 alkuluku.

Ratkaisu:

a) Luku 23 ei ole jaollinen luvulla 2, sillä se ei ole parillinen. Luku 23 ei ole jaollinen luvulla 3, sillä

$$\frac{23}{3} = 7\frac{2}{3},$$

joka ei ole kokonaisluku. Luku 23 ei ole jaollinen luvulla 4 eikä millään muullakaan parillisella luvulla, sillä se ei ole jaollinen luvulla 2. Luku 23 ei ole jaollinen luvulla 5, sillä se ei pääty numeroon 0 tai 5. Luku 23 ei ole jaollinen luvulla 7, sillä

$$\frac{23}{7} = 3\frac{2}{7}.$$

Luku 23 ei ole jaollinen luvulla 9, sillä se ei ole jaollinen luvulla 3. Luku 23 ei ole jaollinen luvulla 11, sillä

$$\frac{23}{11} = 2\frac{1}{11}.$$

Seuraava kokeiltava luku olisi 13. Se on kuitenkin jo liian suuri, sillä se on yli puolet luvusta 23. Osoittautuu, että luku 23 on jaollinen ainoastaan itsellään ja luvulla 1. Se on siis alkuluku.

b) Luku 357 ei ole jaollinen luvulla 2, sillä se ei ole parillinen. Se ei siis myöskään ole jaollinen millään muulla parillisella luvulla. Koska $357 = 119 \cdot 3$, niin luku 357 on jaollinen luvuilla 3 ja 119. Jaollisuus luvulla 3 nähdään myös siitä, että luvun 357 numeroiden summa $3 + 5 + 7 = 15$ on jaollinen luvulla 3. Luku 357 ei ole alkuluku.

Vastaus: a) On. b) Ei ole.

Alkulukuja voidaan etsiä helpommin esimerkiksi yksinkertaisella algoritmilla, joka tunnetaan *Eratostheneen seulana*. Eratosthenes oli kreikkalainen matemaatikko, filosofi, runoilija, tähtitieteilijä ja historioitsija. Bysanttilaisten historioitsijoiden mukaan hän syntyi vuonna 276 eaa.

nykyisessä Libyassa ja kuoli 81-vuotiaana vuonna 195 eaa. Eratosthenes vaikutti tuon ajan sivistyksen keskuksessa Aleksandriassa. Hänen kuuluisin keksintönsä lienee menetelmä maapallon ympärysmittan laskemiseksi.

Algoritmin idea on seuraava. Halutaan löytää alkuluvut välillä $2, \dots, n$.

- (1) Tehdään aluksi lista tutkittavista luvuista.
- (2) Listan ensimmäinen luku 2 on alkuluku. Aluksi poistetaan listasta kaikki lukua 2 suuremmat luvut, jotka ovat jaollisia luvulla 2.
- (3) Edetään seuraavaan listassa jäljellä olevaan lukuun k . Se ei ole jaollinen millään itseään pienemmällä alkuluvulla, joten sekin on alkuluku.
- (4) Poistetaan listasta kaikki lukua k suuremmat luvut, jotka ovat jaollisia luvulla k .
- (5) Toistetaan vaiheita (3) ja (4) niin kauan, kun luku $k \leq \sqrt{n}$.

Nyt listassa on jäljellä vain alkulukuja. Tämä voidaan nähdä seuraavasti: Olkoon välillä $]\sqrt{n}, n]$ jokin luku z , joka ei ole alkuluku. Tällöin voidaan kirjoittaa $z = qm$, missä q ja m ovat positiivisia kokonaislukuja. Nyt pätee $q \leq \sqrt{n}$ tai $m \leq \sqrt{n}$, sillä jos $q > \sqrt{n}$ ja $m > \sqrt{n}$, niin $z = qm > \sqrt{n} \cdot \sqrt{n} = n$, mikä ei ole mahdollista. Koska $q \leq \sqrt{n}$ tai $m \leq \sqrt{n}$, niin z ei enää voi olla mukana listassa. Välillä $]\sqrt{n}, n]$ ei siis enää ole muita kuin alkulukuja.

Eratostheneen seula on käyttökelpoinen etsittäessä suhteellisen pieniä alkulukuja. Suurempien alkulukujen etsimiseen on kehitetty monenlaisia matemaattisia algoritmeja. Suurten alkulukujen löytäminen on joskus tarpeellista etenkin lukuteoriaan pohjaavia salakirjoitusmenetelmiä käytettäessä.

Esimerkki 2. Etsi Eratostheneen seulaa käyttäen alkuluvut välillä $2, \dots, 60$.

Ratkaisu: Tehdään aluksi lista tutkittavista luvuista.

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60

Luku 2 on alkuluku. Poistetaan listasta muut luvulla 2 jaolliset luvut. Seuraava jäljellä oleva luku on 3. Se on myös alkuluku. Poistetaan muut luvulla 3 jaolliset luvut. Seuraava jäljellä oleva luku on 5. Se on alkuluku. Poistetaan muut luvulla 5 jaolliset luvut. Seuraava jäljellä

oleva luku on 7. Sekin on alkuluku. Poistetaan kaikki muut luvulla 7 jaolliset luvut. Seuraava jäljellä oleva luku on 11. Koska kuitenkin $\sqrt{60} \approx 7,75 < 11$, niin algoritmi päättyy ja kaikki listassa jäljellä olevat luvut ovat alkulukuja. Luvuista $2, \dots, 60$ alkulukuja ovat siis 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53 ja 59.

Vastaus: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53 ja 59

Alkutekijä. Kokonaisluvun n *alkutekijöiksi* sanotaan niitä alkulukuja, joilla n on jaollinen. Toisin sanoen, p on luvun n alkutekijä, jos ja vain jos $p|n$ ja p on alkuluku. Esimerkiksi luvun 12 tekijät ovat 1, 2, 3, 4, 6 ja 12. Näistä alkutekijöitä ovat 2 ja 3.

Lukuteorian keskeisimpiä tuloksia on aritmetiikan peruslause, jonka todistuksen esitti ensimmäisenä Eukleides pääteoksensa *Elementa* (Alkeet) seitsemännessä kirjassa. Eukleideen esittämä todistus ei kuitenkaan ole täysin riittävä. Ensimmäisen täydellisen ja virheettömän todistuksen esitti Carl Friedrich Gauss.

Aritmetiikan peruslause. Jokainen kokonaisluku $n > 1$ voidaan kirjoittaa (tekijöiden järjestystä vaille) yksikäsitteisesti alkutekijöidensä tulona:

$$n = p_1^{m_1} \cdot p_2^{m_2} \cdot \dots \cdot p_k^{m_k},$$

missä p_1, \dots, p_k ovat luvun n alkutekijät ja m_1, \dots, m_k ovat positiivisia kokonaislukuja.

Esitystä kutsutaan luvun n *alkutekijähajotelmaksi*. Esimerkiksi luvun 750 alkutekijähajotelma on $2 \cdot 3 \cdot 5^3$.

Aritmetiikan peruslauseen todistuksessa tarvitaan seuraavaa aputulosta.

Eukleideen lemma. Jos $n = a \cdot b$ ja p on sellainen alkuluku, että $p|n$, niin $p|a$ tai $p|b$.

Eukleideen lemmän todistus. Oletetaan, että $p \nmid a$. Osoitettavaksi jää, että $p|b$.

Koska p on alkuluku ja $p \nmid a$, pätee $\text{syte}(p, a) = 1$. Aikaisemmin osoitettiin, että tällöin on olemassa kokonaisluvut x, y siten, että

$$ax + py = 1.$$

Kertomalla yhtälön molemmat puolet luvulla b , saadaan

$$abx + bpy = b.$$

Oletuksen nojalla $p|n$ eli $p|(ab)$. Nyt p jakaa molemmat yhtälön vasemalla puolella olevat luvut, ja siten yhtälön perusteella $p|b$. \square

Aritmetiikan peruslauseen todistus. Aloitetaan osoittamalla ristiriita-argumentilla, että tällainen hajotelma on aina olemassa.

Tehdään vastaoletus, että n on pienin sellainen luku, jolla kyseistä hajotelmaa ei ole. Koska luvulla n ei ole alkutekijähajotelmaa, n ei voi olla alkuluku. Siten $n = a \cdot b$ joillakin kokonaisluvuilla $a, b > 1$.

Nyt kuitenkin $a, b < n$, ja siten luvuilla a ja b on kummallakin alkutekijähajotelmat, koska n oli oletuksen mukaan pienin luku, jolla kyseistä hajotelmaa ei ole. Tämä on ristiriita, joten jokaisella kokonaisluvulla $n > 1$ on alkutekijähajotelma.

Osoitetaan vielä, että hajotelma on yksikäsitteinen. Tämä seuraa Eukleideen lemmasta seuraavalla päättelyllä. Oletetaan, että n on alkuluku, jolla on kaksi eri esitystä alkutekijähajotelmana:

$$n = p_1^{m_1} \cdot p_2^{m_2} \cdot \dots \cdot p_k^{m_k}$$

ja

$$n = q_1^{r_1} \cdot q_2^{r_2} \cdot \dots \cdot q_j^{r_j}.$$

Voidaan olettaa, että jokin luvuista p_i esiinny ainakin kerran jälkimmäisessä hajotelmassa. Koska p_i on alkuluku, se ei jaa lukua q_1 . Koska $p_i | n$, Eukleideen lemmän perusteella

$$p_i | (q_2^{r_2} \cdot \dots \cdot q_j^{r_j}).$$

Samasta syystä p_i ei voi myöskään jakaa lukua q_2 . Näin voidaan jatkaa aina lukuun q_j asti, mistä seuraa, että $p_i | 1$. Tämä on ristiriita, joten alkutekijähajotelma on yksikäsitteinen. \square

Esimerkki 3. Määritä luvun 4200 alkutekijähajotelma.

Ratkaisu:

4200	2	Jaetaan luku 4200 ensin luvulla 2 niin
2100	2	monta kertaa kuin jako menee tasan.
1050	2	
525	3	Siirrytään tutkimaan osamäärän jaollisuutta seuraavalla alkuluvulla eli luvulla 3. Jaetaan osamäärä luvulla 3 niin monta kertaa kuin jako menee tasan.
175	5	Jatketaan samoin seuraavilla alkuluvuilla
35	5	niin kauan, että osamääräksi tulee 1.
7	7	
1		

Kirjoittamalla nyt kaikkien jakajien tulo ja käyttämällä potenssimerkintää saadaan luvun 4200 alkutekijähajotelmaksi

$$4200 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 5 \cdot 5 \cdot 7 = 2^3 \cdot 3 \cdot 5^2 \cdot 7.$$

Vastaus. $4200 = 2^3 \cdot 3 \cdot 5^2 \cdot 7$.

Alkutekijähajotelma voidaan määrittää myös symbolisen laskimen tekijöihin jakoon tarkoitetulla komennolla. Esimerkiksi edellinen esimerkki voidaan ratkaista komennolla `factor(4200)`.

Esimerkki 4. Tutki, onko luku 457 alkuluku.

Ratkaisu:

Eratostheneen seulan esittelyn yhteydessä osoitettiin, että jos tutkitaan, onko positiivinen kokonaisluku n alkuluku, luku riittää jakaa kokonaisluvuilla, jotka ovat pienempiä tai yhtä suuria kuin luku \sqrt{n} . Koska toisaalta jokainen positiivinen kokonaisluku voidaan esittää alkutekijöidensä tulona, riittää, kun jaollisuutta tutkitaan alkuluvuilla, jotka ovat pienempiä tai yhtä suuria kuin luku \sqrt{n} . Kun siis tutkitaan, onko luku 457 alkuluku, luku riittää jakaa alkuluvuilla, jotka ovat pienempiä tai yhtä suuria kuin $\sqrt{457} \approx 21,4$. Näitä ovat alkuluvut 2, 3, 5, 7, 11, 13, 17 ja 19. Luku 457 ei ole jaollinen millään näistä luvuista. Se on siis alkuluku.

Vastaus: On.

Lukuteorian kuuluisimpia tuloksia on seuraava lause, jonka todisti ensimmäisenä Eukleides noin 300 eaa. Tässä esitettävä todistus on idealtaan sama kuin Eukleideen alkuperäinen todistus.

Eukleideen lause. Alkulukuja on äärettömän monta.

Todistus. Tehdään vastaoletus, että alkulukuja olisi äärellisen monta. Olkoot listassa $p_1, p_2, p_3, \dots, p_n$ kaikki alkuluvut. Tarkastellaan lukua

$$m = p_1 \cdot p_2 \cdot p_3 \cdots p_{n-1} \cdot p_n.$$

Merkitään $q = m + 1$.

Nyt joko q on alkuluku tai q ei ole alkuluku. Mikäli q on alkuluku, on päädytty ristiriitaan, koska luku q ei ollut listassa $p_1, p_2, p_3, \dots, p_n$, jonka piti sisältää kaikki alkuluvut.

Voidaan siis olettaa, että q ei ole alkuluku. Tällöin on olemassa jokin alkuluku p siten, että $1 < p < q$ ja $p|q$. Toisaalta $p|m$, koska m on kaikkien alkulukujen tulo. Edelleen, koska $p|q$ ja $p|m$, täytyy päteä $p|(q - m)$ eli $p|(m + 1 - m)$. Siten $p|1$, mikä on ristiriita. Alkulukuja on siis äärettömän monta. \square

Pienin yhteinen jaettava. Olkoot a ja b positiivisia kokonaislukuja. Lukujen a ja b *pienin yhteinen jaettava* $\text{pyj}(a, b)$ on pienin positiivinen kokonaisluku, joka on jaollinen molemmilla luvuista a ja b . Esimerkiksi luvulla 12 jaollisia lukuja ovat 12, 24, 36, 48, 60, 72, 84, 96, 108, 120, ... ja luvulla 15 jaollisia lukuja ovat 15, 30, 45, 60, 75, 90, 105, 120, ... Huomataan, että luku 60 on pienin positiivinen kokonaisluku, joka on jaollinen sekä luvulla 12 että luvulla 15. Siten $\text{pyj}(12, 15) = 60$.

Lukujen a ja b pienintä yhteistä jaettavaa kutsutaan toisinaan *pienimmäksi yhteiseksi monikerraksi*, jota merkitään $\text{pym}(a, b)$. Voidaan käyttää myös merkintää $\text{lcm}(a, b)$, joka tulee englanninkielisistä sanoista *least common multiple*.

Lukujen a ja b suurin yhteinen tekijä sekä pienin yhteinen jaettava voidaan määrittää lukujen alkutekijähajotelmien avulla. Suurimman yhteisen tekijän alkutekijöitä ovat kaikki lukujen a ja b yhteiset alkutekijät. Kunkin yhteisen alkutekijän eksponentiksi valitaan lukujen a ja b alkutekijähajotelmissa esiintyvistä eksponenteista pienempi. Vastaavasti pienimmän yhteisen jaettavan alkutekijöitä ovat kaikki ne alkuluvut, jotka ovat luvun a tai luvun b tekijöitä. Kunkin alkutekijän eksponentiksi valitaan lukujen a ja b alkutekijähajotelmissa esiintyvistä eksponenteista suurempi.

Esimerkki 5. Määritä alkutekijähajotelmien avulla lukujen 280 ja 500 suurin yhteinen tekijä $\text{syt}(280, 500)$ ja pienin yhteinen jaettava $\text{pyj}(280, 500)$.

Ratkaisu: Lukujen 280 ja 500 alkutekijähajotelmat ovat $280 = 2^3 \cdot 5 \cdot 7$ ja $500 = 2^2 \cdot 5^3$. Lukujen suurimman yhteisen tekijän alkutekijöitä ovat kaikki lukujen yhteiset alkutekijät eli 2 ja 5. Valitsemalla alkutekijöiden 2 ja 5 eksponenteiksi alkutekijähajotelmissa esiintyvistä eksponenteista pienempi saadaan

$$\text{syt}(280, 500) = 2^2 \cdot 5 = 20.$$

Lukujen 280 ja 500 pienimmän yhteisen jaettavan alkutekijöitä ovat kaikki ne alkutekijät, jotka ovat jommankumman luvun alkutekijähajotelmassa, siis tekijät 2, 5 ja 7. Valitsemalla alkutekijöiden 2, 5 ja 7 eksponenteiksi alkutekijähajotelmissa esiintyvistä eksponenteista suurempi saadaan

$$\text{pyj}(280, 500) = 2^3 \cdot 5^3 \cdot 7 = 7000.$$

Vastaus: $\text{syt}(280, 500) = 20$ ja $\text{pyj}(280, 500) = 7000$.

Lause. Olkoot a ja b positiivisia kokonaislukuja ja $\text{syt}(a, b) = 1$. Jos c on sellainen luku, että $a|c$ ja $b|c$, niin $(ab)|c$.

Todistus. Tutkitaan aluksi tapausta, että a ja b ovat alkulukuja. Koska $\text{syt}(a, b) = 1$, välttämättä $a \neq b$.

Kirjoitetaan luvulle c alkutekijähajotelma

$$c = p_1^{m_1} \cdot p_2^{m_2} \cdot \dots \cdot p_k^{m_k}.$$

Koska $a|c$ ja $b|c$, seuraa alkutekijähajotelman yksikäsitteisyydestä sekä Eukleideen lemmasta, että $a = p_i$ ja $b = p_j$ jollakin indekseillä i, j . Nyt $p_i \neq p_j$, koska $a \neq b$, ja siten luku $ab = p_i p_j$ jakaa luvun c .

Todistetaan lopuksi yleinen tapaus. Kirjoitetaan luvuille a ja b alkutekijähajotelmat

$$a = q_1^{s_1} \cdot q_2^{s_2} \cdot \dots \cdot q_u^{s_u}$$

ja

$$b = r_1^{t_1} \cdot r_2^{t_2} \cdot \dots \cdot r_v^{t_v}.$$

Koska $\text{sy}(a, b) = 1$, täytyy päteä $q_i \neq r_j$ kaikilla indekseillä i, j . Kuten ensimmäisessä kohdassa, nähdään, että kaikkien lukujen $q_i^{s_i}$ ja $r_j^{t_j}$ täytyy esiintyä luvun c alkutekijähajotelmassa. Siten $(ab)|c$. \square

Edellisen lauseen tulos pätee siis erityisesti silloin, kun luvut a ja b ovat alkulukuja. Jos esimerkiksi luku on jaollinen alkuluvuilla 3 ja 5, niin se on myös jaollinen niiden tulolla 15. Lausetta ei voida kuitenkaan soveltaa tilanteessa, jossa lukujen a ja b suurin yhteinen tekijä ei ole yksi. Esimerkiksi luku 12 on jaollinen sekä luvulla 4 että luvulla 6, mutta se ei ole jaollinen niiden tulolla 24.

Esimerkki 6. Osoita väite todeksi tai epätodeksi: Luku $n^3 - n$ on jaollinen luvulla 6, kun n on kokonaisluku.

Ratkaisu:

Lauseke $n^3 - n$ voidaan kirjoittaa muotoon $n^3 - n = n(n^2 - 1) = n(n+1)(n-1) = (n-1)n(n+1)$. Nähdään, että luku $n^3 - n$ on kolmen peräkkäisen kokonaisluvun tulo. Ainakin yksi luvuista on parillinen, joten luku $n^3 - n$ on jaollinen kahdella. Täsmälleen yksi luvuista on jaollinen luvulla 3, joten myös luku $n^3 - n$ on jaollinen luvulla 3. Luvut 2 ja 3 ovat alkulukuja. Tällöin luku $n^3 - n$ on jaollinen tulolla $2 \cdot 3 = 6$. Väite on tosi.

Fermat'n pieni lause. *Fermat'n pieni lause* sanoo, että jos $a \in \mathbb{Z}$ ja p on alkuluku, niin

$$a^p \equiv a \pmod{p}.$$

Lauseen esitti Pierre de Fermat vuonna 1640 kirjeessään, valittaen kuitenkin väitteen todistusta liian pitkäksi. Ensimmäisen todistuksen julkaisi Leonhard Euler, mutta käytännössä sama todistus oli esiintynyt Gottfried Leibnizin julkaisemattomissa muistiinpanoissa.

Kiinalainen alkulukutesti. Useat matemaatikot ovat toisistaan riippumatta esittäneet virheellisen *otaksuman* eli *konjektuurin*, jonka mukaan luku p on alkuluku, jos ja vain jos

$$2^p \equiv 2 \pmod{p}.$$

Väitteessä esiintyvä kaava on sama kuin Fermat'n pienessä lauseessa, kun $a = 2$. Väitettä kutsutaan usein *kiinalaiseksi alkulukutestiksi*. Sen on väitetty esiintyneen jo filosofi Kungfutseen liitettyissä matemaattisissa teksteissä noin 2500 vuotta sitten. Kysymyksessä on kuitenkin ilmeisesti 1800-luvulla syntynyt väärinkäsitys, joka johtui käänkösvirheestä.

Pienin vastaesimerkki konjektuurille on suhteellisen suuri luku $p = 341 = 11 \cdot 31$. Tämä esimerkki valaisee sitä, miksi matemaattista todistamista tarvitaan eikä pelkkä lukujen kokeileminen edes laskimella tai tietokoneella riitä osoittamaan tulosta.

Goldbach (Lisämateriaalia). *Goldbachin konjektuuri* on yksi lukuteorian ja samalla matematiikan vanhimmista sekä kuuluisimmista avoimista ongelmista. Konjektuurin esitti vuonna 1742 saksalainen matemaatikko Christian Goldbach. Konjektuuri sanoo, että jokainen parillinen kokonaisluku, joka on suurempi kuin 2, voidaan esittää kahden alkuluvun summana.

Lukuja voidaan esittää kahden alkuluvun summana useilla eri tavoilla. Esimerkiksi

$$4 = 2 + 2,$$

$$6 = 3 + 3,$$

$$8 = 3 + 5,$$

$$10 = 7 + 3 \text{ tai } 10 = 5 + 5,$$

$$12 = 5 + 7$$

$$14 = 3 + 11 \text{ tai } 14 = 7 + 7, \text{ jne.}$$

Eulerin φ -funktio. (Lisämateriaalia) Olkoot n ja k positiivisia kokonaislukuja. Funktio $\varphi(n)$ ilmaisee niiden kokonaislukujen k lukumäärän, joille pätee $\text{syt}(n, k) = 1$, kun $1 \leq k \leq n$. Sen laskemisessa voidaan käyttää esimerkiksi *Eulerin tulokaavaa*

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right),$$

missä p on alkuluku. Funktiolla $\varphi(n)$ on monia teoreettisia ja käytännöllisiä sovelluksia, kuten seuraavaksi esiteltävä RSA-algoritmi.

RSA-algoritmi. (Lisämateriaalia) Tällä hetkellä ehkä merkittävin lukuteorian käytännöllinen sovellus on niin kutsuttu *julkisen avaimen salakirjoitus*. Julkisen avaimen salakirjoituksen esittelivät MIT:n (Massachusetts Institute of Technology) tutkijat Ron Rivest, Adi Shamir ja Leonard Adleman vuonna 1978. Algoritmia kutsutaan sitä koskevan alkuperäisen tutkimusartikkelin kirjoittajien sukunimien alkukirjaimista muodostetulla lyhenteellä RSA. Aihepiiri on edelleen aktiivisen tutkimuksen kohteena, mutta algoritmin teoreettinen perusta on klassisissa lukuteorian tuloksissa. Siksi RSA-algoritmi osoittaa, että puhtaan matematiikan tutkimuksella voi olla uusia yllättäviä ja merkittäviä sovelluksia jopa satoja vuosia tutkimuksen julkaisemisen jälkeenkin.

RSA-algoritmi perustuu lukuteoriaan ja alkulukujen ominaisuuksiin. Algoritmin keskeisiä käsitteitä ovat *julkinen avain* ja *salainen avain*. Julkista avainta käytetään viestin salakirjoittamisessa, mutta sen avulla salakirjoitusta ei voi purkaa. Salakirjoituksen purkamisessa käytetään

salaista avainta, jonka vain viestin vastaanottaja tietää. Julkisen avaimen salakirjoitusmenetelmät poistavat siten kaikkien aikaisempien salakirjoitusmenetelmien keskeisen heikkouden. Niitä käytettäessä viestin lähettäjän ei koskaan tarvitse saada viestin purkamisessa tarvittavaa tietoa.

Salakirjoituksessa käytetään hyväksi kappaleen 5.2 lisämateriaalissa esiteltyjen jäännösluokkien ominaisuuksia, erityisesti *multiplikatiivista käänteislukua*. Luvun a multiplikatiivisella käänteisluvulla modulo m tarkoitetaan sellaista kokonaislukua a^{-1} , jolle pätee $a \cdot a^{-1} \equiv 1 \pmod{m}$.

RSA-algoritmin matemaattinen idea on seuraava:

1. Valitaan kaksi alkulukua p ja q .
2. Lasketaan luku $n = pq$. Lukua n käytetään laskettaessa jakojäännöksiä, joita tarvitaan viestin salaamisessa ja salauksen purkamisessa.
3. Lasketaan $\varphi(n) = (p-1)(q-1)$.
4. Valitaan kokonaisluku e siten, että $1 < e < \varphi(n)$ ja $\text{syty}(e, \varphi(n)) = 1$.
5. Etsitään kokonaisluku $d = e^{-1} \pmod{\varphi(n)}$. Toisin sanoen d on luvun e multiplikatiivinen käänteisluku modulo $\varphi(n)$ eli

$$d \cdot e \equiv 1 \pmod{\varphi(n)}$$

Salakirjoituksessa julkinen avain on lukupari (n, e) . Salainen avain on lukupari (n, d) .

Viesti voidaan lähettää turvallisesti seuraavasti. Olkoon lähetettävä viesti kokonaisluku m , jolle $0 < m < n$. Lasketaan

$$c = m^e \pmod{n}.$$

Luku c on salakirjoitettu viesti. Viesti puretaan laskemalla

$$m = c^d \pmod{n}.$$

Pidempiä viestejä voidaan lähettää katkaisemalla ne sopivan mittaisiksi paloiksi (bittijonoiksi), jotka vuorollaan salakirjoitetaan samalla tavalla. Tehokkaita algoritmeja salakirjoitusprosessin eri vaiheiden käsittelemiseksi kehitellään jatkuvasti.

Esimerkki 7. Salakirjoita RSA-algoritmia käyttäen viesti 65, joka vastaa ASCII-koodausjärjestelmässä kirjainta A. Käytä algoritmista tarvittavina alkulukuina lukuja 47 ja 59. Pura lopuksi koodaamasi viesti.

Ratkaisu: Nyt $p = 47$ ja $q = 59$. Siten $n = pq = 2773$ ja kaavalla $\varphi(n) = (p-1)(q-1)$ saadaan

$$\varphi(2773) = (47-1)(59-1) = 46 \cdot 58 = 2668.$$

Seuraavaksi valitaan jokin luku e siten, että $1 < e < 2668$ ja $\text{syte}(e, 2668) = 1$. Esimerkiksi $e = 13$ käy.

Salaisen avaimen d löytämiseksi on laskettava multiplikatiivinen käänteisluku $13^{-1} \pmod{2668}$. Käyttämällä esimerkiksi niin kutsuttua *laajennettua Eukleideen algoritmia* tai tietokonetta saadaan $d = 821$. Tuloksen voi tarkistaa laskemalla:

$$d \cdot e = 821 \cdot 13 = 10673 = 4 \cdot 2668 + 1 \equiv 1 \pmod{2668},$$

kuten pitääkin. Siten julkinen avain on pari $(n = 2773, e = 13)$ ja salainen avain pari $(n = 2773, d = 821)$.

Koska lähetettävä viesti on luku $m = 65$, niin salakirjoitetuksi viestiksi saadaan

$$c = 65^{13} \pmod{2773} = 660.$$

Puretaan vielä viesti. Laskemalla saadaan

$$m = 660^{821} \pmod{2773} = 65,$$

eli päädyttiin alkuperäiseen viestiin, kuten pitääkin.

Näin isoilla luvuilla laskeminen on luonnollisesti hankalaa laskimenkin avulla. Tuloksen voi tarkastaa symbolisen laskennan ohjelmistoa tai esim. Wolfram Alphaa käyttäen.

Vastaus: Salakirjoitettu viesti on 660. Purettu viesti on 65.

Tehtäviä.

- (1) Mitkä ovat kymmenen pienintä alkulukua?
- (2) Onko luku a) 37 b) 77 c) 87 d) 101 alkuluku?
- (3) Määritä Eratostheneen seulan avulla kaikki välillä $75, \dots, 100$ olevat alkuluvut.
- (4) Pitääkö väite paikkansa? Perustele.
 - a) Jos tulo mn on jaollinen luvulla 97, niin ainakin toinen kokonaisluvusta m ja n on jaollinen luvulla 97.
 - b) Jos tulo mn on jaollinen luvulla 55, niin ainakin toinen kokonaisluvusta m ja n on jaollinen luvulla 55.
- (5) Määritä luvun alkutekijähajotelma. a) 42 b) 600 c) 4410
- (6) Määritä luvun $8!$ alkutekijähajotelma.
- (7) Millä luvuilla on luvun 241 jaollisuus vähintään tutkittava, jotta saadaan selville, onko se alkuluku?
- (8) Onko luku a) 187, b) 197, c) 299, d) 601 alkuluku?
- (9) Luvut 2 ja 3 ovat kaksi peräkkäistä kokonaislukua, jotka molemmat ovat alkulukuja. Osoita, että muita peräkkäisiä alkulukuja ei ole olemassa.
- (10) Mikä on lukujen suurin yhteinen tekijä?
 - a) $2^3 \cdot 3^2 \cdot 5^5 \cdot 7^5$ ja $2^5 \cdot 3^2 \cdot 5^2$
 - b) $2 \cdot 3 \cdot 5 \cdot 11$ ja $2 \cdot 3 \cdot 5 \cdot 11$
- (11) Mikä on lukujen pienin yhteinen jaettava?
 - a) $3^7 \cdot 5^3 \cdot 7^3$ ja $2^9 \cdot 3^6 \cdot 5^9$
 - b) 19^{31} ja 19^{17}
- (12) Määritä alkutekijähajotelman avulla lukujen
 - a) 15 ja 42
 - b) 20 ja 75
 - c) 2250 ja 30 800suurin yhteinen tekijä ja pienin yhteinen jaettava.
- (13) Jokamiesluokan kilpa-auto A kiertää radan 55 sekunnissa ja B 65 sekunnissa. Kuinka pitkän ajan kuluttua lähdöstä autot ovat uudestaan yhtä aikaa lähtölinjalla?
- (14) Olkoot x ja y kokonaislukuja. Ratkaise yhtälö $(3x+2y)(x+y) = 21$.
- (15) Perustele väite todeksi tai epätodeksi.
 - a) Jos luku on jaollinen luvuilla 6 ja 25, niin se on jaollinen myös luvulla 150.
 - b) Jos luku on jaollinen luvuilla 6 ja 9, niin se on jaollinen myös luvulla 54.
- (16) Olkoon n kokonaisluku. Osoita, että luku $n(n+1)(n+2)$ on jaollinen luvulla 6.
- (17) Osoita, että jos n on kokonaisluku, niin luku $7n^3 - 7n$ on jaollinen luvulla 42.

- (18) Osoita, että jos n on kokonaisluku, niin luku $n^4 - n^2$ on jaollinen luvulla 12.
- (19) Määritä jakojäännös, kun luku 9^{13} jaetaan luvulla 13.
- (20) Toisinaan Fermat'n pieni lause esitetään seuraavassa muodossa: jos p on alkuluku ja a on kokonaisluku, joka ei ole luvun p monikerta, niin tällöin

$$a^{p-1} \equiv 1 \pmod{p}.$$

Osoita lauseen tämän muodon avulla, että $n^{19} \equiv n \pmod{19}$ kaikilla luonnollisilla luvuilla n .

- (21) Muotoa $F_n = 2^{2^n} + 1$, $n = 0, 1, 2, \dots$ olevia lukuja sanotaan *Fermat'n luvuiksi*. Euler tutki 1700-luvulla, ovatko kaikki Fermat'n luvut alkulukuja. Ratkaise tämä Eulerin ongelma laskinta käyttäen.
- (22) Päättelä, kuinka monta nollaa on luvun $50!$ lopussa.

Kotitehtäviä.

- (1) Onko luku a) 43 b) 39 c) 79 d) 221 alkuluku?
- (2) Pitääkö väite paikkansa? Perustele.
- a) Jos tulo mn on jaollinen luvulla 171, niin ainakin toinen kokonaisluvusta m ja n on jaollinen luvulla 171.
- b) Jos tulo mn on jaollinen luvulla 149, niin ainakin toinen kokonaisluvusta m ja n on jaollinen luvulla 149.
- (3) Määritä luvun alkutekijähajotelma. a) 126 b) 13200 c) 1 000 000
- (4) Millä luvuilla on luvun 267 jaollisuus vähintään tutkittava, jotta saadaan selville, onko se alkuluku?
- (5) Onko luku a) 229, b) 251, c) 707, d) 2827 alkuluku?
- (6) Tutki laskimen **factor**-toiminnolla, onko luku
- a) 72 222 222 227
- b) 7 222 222 227
- c) 722 222 227
- alkuluku.
- (7) Etsi Internetistä, mikä on tällä hetkellä suurin tunnettu alkuluku.
- (8) Jos luvut n ja $n+2$ ovat alkulukuja, niin kyseistä lukuparia kutsutaan alkulukukaksosiksi. Se, onko alkulukukaksosia äärettömän monta, on vielä ratkaisematon lukuteorian ongelma. Etsi kymmenen alkulukukaksosta. Käytä laskinta tai tietokonetta apunasi.
- (9) Mikä on lukujen suurin yhteinen tekijä?
- a) $2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$ ja $2^{11} \cdot 3^8 \cdot 11 \cdot 17^{10}$
- b) $5 \cdot 7^3 \cdot 19^2$ ja $3 \cdot 11^2 \cdot 41$
- (10) Mikä on lukujen pienin yhteinen jaettava?
- a) $7^3 \cdot 11^2$ ja $2^4 \cdot 7^2 \cdot 11$
- b) $41 \cdot 43$ ja $41 \cdot 43$

- c) $2 \cdot 7$ ja $5 \cdot 13$
- (11) Määritä alkutekijähajotelman avulla lukujen
- 70 ja 385
 - 240 ja 4900
 - 2310 ja 17 199
- suurin yhteinen tekijä ja pienin yhteinen jaettava.
- (12) Määritä $\text{sy}(117325, 16625)$ ja $\text{pyj}(117325, 16625)$.
- (13) Pulsarit ovat nopeasti pyöriviä ja rytmisiä radiopulsseja säteileviä tähtiä. Pulsari X lähettää radiopulssin 510 millisekunnin välein, pulsari Y taas 357 millisekunnin välein.
- Eräänä ajanhetkenä molempien pulsarien lähettämä pulssi havaitaan yhtä aikaa. Kuinka pitkän ajan kuluttua molempien pulsarien pulssit havaitaan yhtä aikaa seuraavan kerran?
 - Kuinka monta kierrosta pulsarit pyörähtävät kyseisenä aikana?
- (14) Perustele väite todeksi tai epätodeksi.
- Jos luku on jaollinen luvuilla 15 ja 12, niin se on jaollinen myös luvulla 180.
 - Jos luku on jaollinen luvuilla 36 ja 5, niin se on jaollinen myös luvulla 180.
- (15) Osoita, että luku $5n^3 - 5n$ on jaollinen luvulla 30, kun n on luonnollinen luku.
- (16) Osoita, että muotoa $p^2 - 1$ oleva luku on jaollinen luvulla 12, kun p on alkuluku ja suurempi kuin 3. [YO 2010 tehtävä 12]
- (17) Erään maan olympiajoukkueessa oli vain yleisurheilijoita ja purjehtijoita. Yleisurheilijoita oli neljä kertaa niin paljon kuin purjehtijoita. Naisia oli kaksi kertaa niin paljon kuin miehiä. Kun joukkue matkusti 100-paikkaisella lentokoneella kisoihin, oli koneen matkustajista noin puolet joukkueen urheilijoita ja loput valmentajia, huoltajia ja median edustajia. Kuinka monta urheilijaa joukkueessa oli?
- (18) Olkoon n kokonaisluku. Osoita, että luku $n^5 + 10n^4 + 35n^3 + 50n^2 + 24n$ on jaollinen luvulla 120. Vihje: Käytä symbolisen laskimen **factor**-toimintoa.
- (19) Määritä jakojäännös, kun luku $51 \cdot 31^{94} + 102$ jaetaan luvulla 47. Voit käyttää Fermat'n pientä lausetta apunasi.
- (20) Osoita, että $2^{341} = 2^{11 \cdot 31} \equiv 2 \pmod{341}$. Tulos osoittaa, että kiinalaiseen alkulukutestiin liittyvä otaksuma on epätosi eikä testi siten toimi kaikilla luvuilla.
- (21) Alkulukujen lukumääräfunktio $\pi(x)$ kertoo välillä $[0, x]$ olevien alkulukujen lukumäärän. Alkulukujen tiheys välillä $[0, x]$ saadaan jakamalla $\pi(x)$ välin pituudella x .
- Laske $\pi(10^n)$, kun $n = 1, 2, 3, 4, 5$.

- b) Mitä alkulukujen määrälle $\pi(x)$ näyttää tapahtuvan, kun x kasvaa? Miksi?
- c) Laske alkulukujen tiheys väleillä $[0, 10^n]$, kun $n = 1, 2, 3, 4, 5$.
- d) Mitä alkulukujen tiheydelle

$$\frac{\pi(x)}{x}$$

näyttää tapahtuvan, kun x kasvaa?

Käytä tehtävässä laskinta tai matemaattisia ohjelmistoja, kuten verkosta ilmaiseksi ladattavissa olevaa Maxima-ohjelmistoa. Esimerkiksi Texas Instrumentsin TI-Nspire CX CAS -laskin sisältää toiminnon `numtheory\primecount(a,b)`, joka antaa alkulukujen määrän välillä $[a, b]$.

- (22) *Mersennen alkulukuja* ovat alkuluvut, jotka ovat muotoa $2^p - 1$, missä p on alkuluku.

- a) Etsi neljä pienintä Mersennen alkulukua.
 - b) Ovatko kaikki muotoa $2^p - 1$ olevat luvut alkulukuja?
 - c) Osoita, että jos $2^p - 1$ on alkuluku, myös p on alkuluku.
- Vihje: Käytä epäsuoraa todistusta ja sovelleta kaavaa

$$x^n - 1 = (x - 1)(x^{n-1} + \dots + x + 1).$$

- (23) a) Selvitä kokeilemalla pienillä luvuilla, mitä on $\text{sy}(a, b) \cdot \text{pyj}(a, b)$.
- b) Todista saamasi tulos.
 - c) Miten Eukleideen algoritmia ja saamaasi tulosta voidaan hyödyntää pienimmän yhteisen jaettavan määrittämisessä?
 - d) Määritä Eukleideen algoritmin ja saamasi tuloksen avulla $\text{pyj}(496125, 9450)$.
 - e) Texas Instrumentsin TI-Nspire CX CAS -laskimesta löytyy ohjelma `numtheory\gcdstep(a,b)`, joka määrittää lukujen a ja b suurimman yhteisen tekijän Eukleideen algoritmilla välivaiheet näyttäen. Tutustu ohjelman toimintaan ja määritä sen avulla $\text{pyj}(7856, 678)$. Kirjoita ylös Eukleideen algoritmin välivaiheet käyttäen tämän oppikirjan mukaisia merkintöjä.

- (24) (Lisämateriaalia.) Salakirjoita RSA-algoritmia käyttäen viesti 66, joka vastaa ASCII-koodausjärjestelmässä kirjainta B. Käytä esimerkin 7 avainta ja esim. **Wolfram Alpha**. Tarkasta tuloksesi purkamalla viesti.

Vihje: Voit antaa syötteen Wolfram Alphalle muodossa $\text{Mod}[a^p, n]$, esim. $\text{Mod}[660^{821}, 2773]$.

- (25) (Lisämateriaalia.) Osoita, että Eulerin φ -funktio on *multiplikaatiivinen* eli $\varphi(mn) = \varphi(m)\varphi(n)$, kun $\text{sy}(m, n) = 1$.

Vihje: Tutki Eulerin tulokaavaa. Mitä tapahtuu, kun $\text{sy}(m, n) = 1$?

7. HARJOITUSTEHTÄVIEN RATKAISUJA

Kaavan

$$\sum_{k=1}^n k^2 = \frac{n(n+1)(2n+1)}{6}$$

todistus.

Todistus. 1. Lasketaan

$$1^2 = \frac{1(1+1)(2 \cdot 1 + 1)}{6} = \frac{6}{6} = 1.$$

Väite siis pätee luvulla $n = 1$.

2. Tehdään induktioaskel, eli osoitetaan väite luvulle $n + 1$. Oletuksena on, että väite pätee luvulla n :

$$1^2 + 2^2 + 3^2 + \dots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

Lisätään yhtälön molemmille puolille $(n+1)^2$:

$$\begin{aligned} 1^2 + 2^2 + 3^2 + \dots + n^2 + (n+1)^2 &= \frac{n(n+1)(2n+1)}{6} + (n+1)^2 \\ &= \frac{n(n+1)(2n+1) + 6(n+1)^2}{6} \\ &= \frac{(n+1)(n(2n+1) + 6(n+1))}{6} \\ &= \frac{(n+1)(2n^2 + 7n + 6)}{6}. \end{aligned}$$

Toisaalta

$$\begin{aligned} ((n+1) + 1)(2(n+1) + 1) &= (n+2)(2n+3) \\ &= 2n^2 + 3n + 4n + 6 = 2n^2 + 7n + 6. \end{aligned}$$

Siten

$$\frac{(n+1)(2n^2 + 7n + 6)}{6} = \frac{(n+1)((n+1) + 1)(2(n+1) + 1)}{6},$$

ja siis

$$1^2 + 2^2 + 3^2 + \dots + n^2 + (n+1)^2 = \frac{(n+1)((n+1) + 1)(2(n+1) + 1)}{6}.$$

Väite on todistettu. \square

8. LOOGINEN ALGEBRA JA BOOLEN ALGEBRA (LISÄMATERIAALIA)

8.1. Looginen algebra. Tutkimustehtävä Määritellään joukossa $B = \{0, 1\}$ kolme operaatiota, $+$, \cdot ja $-$ seuraavasti:

$0 + 0 = 0$	$0 \cdot 0 = 0$	$-0 = 1$
$0 + 1 = 1$	$0 \cdot 1 = 0$	$-1 = 0$
$1 + 0 = 1$	$1 \cdot 0 = 0$	
$1 + 1 = 1$	$1 \cdot 1 = 1$	

- (1) Miten nämä operaatiot eroavat kokonaislukujen yhteenlaskusta, kertolaskusta ja vastaluvusta?
- (2) Vertaa operaatioita logiikan konnektiiveihin. Mitä konnektiiveja operaatiot $+$, \cdot ja $-$ vastaavat?

Määritellään joukossa $B = \{0, 1\}$ kolme operaatiota, yhteenlasku ($+$), kertolasku (\cdot) ja komplementti ($-$) seuraavan taulukon avulla:

$0 + 0 = 0$	$0 \cdot 0 = 0$	$-0 = 1$
$0 + 1 = 1$	$0 \cdot 1 = 0$	$-1 = 0$
$1 + 0 = 1$	$1 \cdot 0 = 0$	
$1 + 1 = 1$	$1 \cdot 1 = 1$	

Yhteenlasku vastaa disjunktiota, kertolasku konjunktiota ja komplementti negaatiota. Näin määritellyn *loogisen algebran* avulla monimutkaisten yhdistettyjen lauseiden totuusarvoja voidaan laskea nopeammin kuin totuustauluja käyttämällä. Pitää vain muistaa, milloin laskusäännöt eroavat kokonaisluvulla 0 ja 1 laskemisesta ja milloin taas voidaan suoraan soveltaa kokonaislukulaskentaa.

Esimerkki 1. Määritä lauseen a) $\neg A \vee (B \wedge A)$, b) $A \vee (\neg B \wedge A)$ totuusarvo, kun A on tosi ja B on epätosi.

Ratkaisu:

a) Sijoittamalla $A = 1$ ja $B = 0$ sekä käyttämällä loogisen algebran merkintöjä ja laskusääntöjä saadaan $-1 + (0 \cdot 1) = 0 + 0 = 0$, joten lause on epätosi.

Huomaa, että sulkeita ei välttämättä tarvitsisi käyttää, koska kertolasku suoritetaan ennen yhteenlaskua. Tämä vastaa konnektiivien suoritusjärjestystä (konjunktio ennen disjunktiota).

b) Sijoittamalla $A = 1$ ja $B = 0$ saadaan $1 + ((-0) \cdot 1) = 1 + 1 \cdot 1 = 1 + 1 = 1$, joten lause on tosi.

Vastaus: a) epätosi, b) tosi

Esimerkki 2. Esitä De Morganin laki

$$\neg(A \vee B) \leftrightarrow \neg A \wedge \neg B$$

loogisen algebran merkinnöin ja osoita laki päteväksi.

Ratkaisu: De Morganin laki saa loogisessa algebrassa muodon

$$-(A + B) = (-A) \cdot (-B).$$

Loogisen algebran laskusäännöillä saadaan seuraava totuustaulu:

A	B	$-(A + B)$	$(-A) \cdot (-B)$
1	1	$-(1 + 1) = -1 = 0$	$(-1) \cdot (-1) = 0 \cdot 0 = 0$
1	0	$-(1 + 0) = -1 = 0$	$(-1) \cdot (-0) = 0 \cdot 1 = 0$
0	1	$-(0 + 1) = -1 = 0$	$(-0) \cdot (-1) = 1 \cdot 0 = 0$
0	0	$-(0 + 0) = -0 = 1$	$(-0) \cdot (-0) = 1 \cdot 1 = 1$

Koska lausekkeet $-(A + B)$ ja $(-A) \cdot (-B)$ saavat samat totuusarvot kaikilla lauseiden A ja B totuusarvoilla, De Morganin laki on pätevä.

Tehtäviä.

- (1) Määritä lauseen a) $\neg(B \wedge A) \vee (A \wedge \neg B)$, b) $(B \vee \neg A) \wedge (A \vee \neg B)$ totuusarvo, kun A on tosi ja B on epätosi.
- (2) Esitä a) kaksoisnegaation laki $\neg\neg A \leftrightarrow A$ b) De Morganin laki $\neg(A \wedge B) \leftrightarrow \neg A \vee \neg B$ loogisen algebran merkinnöin. Laadi totuustaulu laskemalla loogisen algebran laskusäännöillä ja osoita laki päteväksi.
- (3) Esitä a) implikaatio $A \rightarrow B$, b) ekvivalenssi $A \leftrightarrow B$ käyttäen loogisen algebran merkintöjä. Laske lauseen totuusarvot atomilauseiden A ja B eri totuusarvoilla käyttäen loogisen algebran laskusääntöjä.

8.2. Boolean algebra. Olkoon B joukko, jossa on määritelty operaatiot $+$, \cdot ja $-$. Joukko B operaatioineen on *Boolean algebra*, jos seuraavat ehdot ovat voimassa kaikille $x, y, z \in B$:

1. $x + y = y + x$	6. $x \cdot (y \cdot z) = (x \cdot y) \cdot z$
2. $x + (y + z) = (x + y) + z$	7. $x \cdot 1 = x$
3. $x + 0 = x$	8. $x \cdot (-x) = 0$
4. $x + (-x) = 1$	9. $x + (y \cdot z) = (x + y) \cdot (x + z)$
5. $x \cdot y = y \cdot x$	10. $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$

Alkiota 0 kutsutaan nolla-alkioksi ja alkiota 1 ykkösalkioksi. Voidaan osoittaa, että looginen algebra (joukko $B = \{0, 1\}$ ja operaatiot $+$, \cdot sekä $-$) on Boolean algebra.

Esimerkki 1. Osoita, että looginen algebra toteuttaa Boolean algebran ehdot 3, 4 ja 9.

Ratkaisu:

Koska $0 + 0 = 0$ ja $1 + 0 = 1$, toteutuu ehto 3.

Koska $0 + (-0) = 0 + 1 = 1$ ja $1 + (-1) = 1 + 0 = 1$, toteutuu ehto 4.

Esitetään ehto 9 lauselogiikan merkinnöillä. Ehto $x + (y \cdot z) = (x + y) \cdot (x + z)$ on sama kuin $x \vee (y \wedge z) \leftrightarrow (x \vee y) \wedge (x \vee z)$ eli lauselogiikan osittelulaki, joten ehto toteutuu.

Esimerkki 2. Osoita, että Boolean algebrassa $x + x = x$.

Ratkaisu: Sovelletaan Boolean algebran ehtoja lausekkeeseen $x + x = x$.

$$\begin{array}{ll}
 x + x & \text{ehto 7} \\
 = (x + x) \cdot 1 & \text{ehto 4} \\
 = (x + x) \cdot (x + (-x)) & \text{ehto 9} \\
 = x + (x \cdot (-x)) & \text{ehto 8} \\
 = x + 0 & \text{ehto 3} \\
 = x &
 \end{array}$$

Loogisen algebran lisäksi voidaan määritellä myös muita Boolean algebroita. Esimerkiksi joukon X potenssijoukko eli sen kaikkien osajoukkojen joukko $\mathcal{P}(X)$ yhdessä operaatioiden yhdiste \cup , leikkaus \cap ja komplementti $\bar{}$ kanssa muodostavat Boolean algebran. Näin saadun Boolean algebran nolla-alkio on tyhjä joukko \emptyset ja ykkösalkio on joukko X itse. Esimerkissä 2 johdettu tulos $x + x = x$ vastaa tällöin joukko-opin tulosta $A \cup A = A$. Kun tulos on johdettu Boolean algebroiden teorias-
sa, se voidaan ottaa suoraan käyttöön joukko-opissa. Boolean algebroja tutkimalla saadaan siten tuloksia, joita voidaan hyödyntää sekä logi-
kassa että joukko-opissa. Koska Boolean algebra on määritelty hyvin
yleisellä tasolla, se on käsitteenä abstrakti. Tämä näkyy esimerkiksi

tuloksen $x + x = x$ todistamisessa: todistaminen erikseen sekä logiikassa että joukko-opissa on helppoa, mutta todistus Boolean algebrassa vaatii varsin abstraktia ajattelua.

Tehtäviä.

- (1) Osoita, että looginen algebra toteuttaa Boolean algebran ehdot 1,2, 5-8 ja 10.
- (2) Osoita, että seuraavat laskusäännöt ovat voimassa loogisessa algebrassa.

- a) $x + x = x$
- b) $x \cdot x = x$
- c) $x + 1 = 1$
- d) $x \cdot 0 = 0$
- e) $x + x \cdot y = x$
- f) $x \cdot (x + y) = x$
- g) $x + (-x) \cdot y = x + y$
- h) $x \cdot (-x + y) = x \cdot y$
- i) $-(-x) = x$
- j) $-(x + y) = (-x) \cdot (-y)$
- k) $-(x \cdot y) = (-x) + (-y)$

- (3) Tulkitse, mitä Boolean algebran tulokset

- a) $x \cdot x = x$
- b) $x + 1 = 1$
- c) $x \cdot 0 = 0$
- d) $-(-x) = x$
- e) $x + x \cdot y = x$
- f) $x \cdot (x + y) = x$

tarkoittavat joukko-opissa. Perustele tulokset myös käyttäen Venn-diagrammeja.

- (4) Sievennä lausekkeet Boolean algebran määritelmän ja tehtävän 2 laskusääntöjen avulla.

- a) $x \cdot x + x \cdot x$
- b) $x \cdot x \cdot x \cdot y \cdot y \cdot y$
- c) $(a + b) \cdot (a + c)$
- d) $a + b \cdot a + b$
- e) $(a + (-b)) \cdot b$
- f) $a + b + (-(a \cdot b))$

- (5) Piirrä Boolean algebran lauseketta

- a) $(x + y) \cdot (x + z)$
- b) $(x + y) \cdot (x + (-y))$
- c) $x + (-x) \cdot y$

vastaava looginen piiri. Sievennä lauseke Boolean algebran säännöillä ja piirrä sievennettyä muotoa vastaava piiri. Loogisia piirejä on käsitelty kappaleessa 2.1 tehtävissä xx ja yy.

- (6) Osoita, että tehtävän 2 säännöt ovat voimassa kaikissa Boolean algebroissa. **Vain todellisille matemaatikoille.**

- (7) Reaalilukujen joukossa \mathbb{R} määritellään yhteenlaskua muistuttava laskutoimitus $x \circ y$ seuraavasti: $x \circ y = x + y - 2$ kaikilla $x, y \in \mathbb{R}$. Osoita, että laskutoimitus toteuttaa seuraavat ehdot:
- i $(x \circ y) \circ z = x \circ (y \circ z)$ kaikilla $x, y, z \in \mathbb{R}$.
 - ii $x \circ y = y \circ x$ kaikilla $x, y \in \mathbb{R}$.
 - iii On olemassa sellainen luku $\omega \in \mathbb{R}$, että $x \circ \omega = \omega \circ x = x$ kaikilla $x \in \mathbb{R}$. Mikä ω on?
 - iv Jokaisella $x \in \mathbb{R}$ on vasta-alkio x^* , jolle $x \circ x^* = x^* \circ x = \omega$.
- [Ylioppilastehtävä s97 9b]