

Ollin  
Opas  
Olympiatason  
Ongelmanratkaisuun

Olli Järviniemi

## Sisältö

1	Lue tämä ensin	3
2	Johdantotehtäviä	7
3	Kehäkulmalause ja jännenelikulmiot (Geometria)	10
4	Geometrian lisämenetelmiä (Geometria)	25
5	Projektiivinen geometria (Geometria)	46
6	Lisätehtäviä (Geometria)	60
7	Aritmetiikan peruslause (Lukuteoria)	78
8	Kongruenssit (Lukuteoria)	87
9	Eksponenttifunktiot ja neliönjäännökset (Lukuteoria)	96
10	Primitiivijuuret (Lukuteoria)	109
11	Lisätehtäviä (Lukuteoria)	123
12	Polynomit (Algebra)	142
13	Arviointi ja epäyhtälöt (Algebra)	151
14	Summia (Algebra)	169
15	Lineaariset rekursiot (Algebra)	180
16	Funktionaaliyhtälöt (Algebra)	197
17	Lisätehtäviä (Algebra)	208
18	Pelit (Kombinatoriikka)	220
19	Laskennallista kombinatoriikkaa (Kombinatoriikka)	229
20	Prosessit (Kombinatoriikka)	250

<b>21 Verkot (Kombinatoriikka)</b>	<b>257</b>
<b>22 Lisätehtäviä (Kombinatoriikka)</b>	<b>270</b>
<b>23 Esitietoja</b>	<b>286</b>
<b>24 Lisämateriaaleja</b>	<b>308</b>
<b>25 Kevyempää luettavaa</b>	<b>312</b>
<b>26 Kiitokset</b>	<b>322</b>

# 1 Lue tämä ensin

## Mistä tässä on kyse?

Tämän materiaalin päätavoite on opettaa lukiolaisten matematiikkakilpailuissa tarvittavaa ongelmanratkaisua, kuten kirjan nimikin kertoo. Tähän pyritään esittämällä lukuisia esimerkkitehtäviä, jotka sisältävät erilaisia lähestymistapoja vaikeiden ongelmien ratkomiseen.

Kovatasoinen ongelmanratkaisija ”näkee” tehtävän kohdatessaan hyvin erilaisia asioita kuin aloittelija. Tässä kirjassa selitän, millaisia asioita minä näen tehtäviä ratkoessani. Tarkoitus on, että tästä tarttuu jotain myös lukijalle.

Kirja sisältää myös kilpailumatematiikassa tarvittavaa teoriaa, koska useat tehtävät olisi käytännössä mahdotonta ratkaista suoraan peruskoulu- ja lukiomatematiikan pohjalta.

## Miten matematiikkakilpailut toimivat Suomessa?

Suomessa kilpailuvuoden aloittaa syksyllä järjestettävä valtakunnallinen Lukion matematiikkakilpailun alkukilpailu, jonka järjestää MAOL. Syksyllä on myös marraskuussa järjestettävä kansainvälinen Baltian tie -joukkumatematiikkakilpailu, jonka viisihenkinen joukkue valitaan syksyn alussa valmennusviikonlopussa.

MAOLin loppukilpailu pidetään alkukilpailua seuraavan vuoden alussa. Huhtikuussa pidetään Pohjoismainen matematiikkakilpailu, johon valitaan 20 edustajaa Suomesta. Samoihin aikoihin pidetään Euroopan tyttöjen matematiikkaolympialaiset eli EGMO. Heinäkuussa järjestettävät Kansainväliset matematiikkaolympialaiset (International Mathematical Olympiad, IMO) ovat kilpailuvuoden kohokohta. Suomen kuusihenkinen joukkue valitaan toukokuussa pidettävällä valintaviikolla.

IMO-valintaviikon lisäksi valmennus järjestää kuusi kertaa vuodessa kaikille avoimia valmennusviikonloppuja. Lisätietoa kilpailuista ja valmennustoiminnasta löytyy Suomen matemaattisen yhdistyksen valmennusjaoston eli matematiikkavalmennuksen sivuilta osoitteesta <https://matematiikkakilpailut.fi/>.

Vaikka suurin osa kilpailuista on suunnattu lukiolaisille, myös peruskoululaisille on kilpailuja. Seitsemäsluokkalaisille on alueellisia kilpailuja (katso <https://matematiikkakilpailut.fi/seiskat/>), ja MAOL järjestää myös peruskoululaisille valtakunnallisen matematiikkakilpailun. Myös peruskoululaisten kilpailussa on alku- ja loppukilpailu, ja myös peruskoululaisille on valmennusta (ja peruskoululaiset saavat tietysti osallistua ”lukiolaisten” valmennusviikonloppuihin). Tästäkin saa lisätietoa matematiikkavalmennuksen sivuilta.

## Kenelle kirja on suunnattu?

Kirjoittaessani kirjaa ajattelin kohdeyleisön olevan kilpailumatematiikasta kiinnostuneet nuoret (noin lukioikäiset), koska he ovat kilpailuja ajatellen sopivan ikäisiä. Kirja soveltuu kuitenkin yleisesti kenelle vain, jolla on peruskoulutaidot matematiikasta ja jota kiinnostaa kilpailumatematiikka ja siihen liittyvä ongelmanratkaisu.

*Kirja ei kuitenkaan ole kevyttä luettavaa.* Esimerkiksi kyky seurata monimutkaisia

todistuksia (tai ylipäättään todistuksia) ei ole itsestäänselvyys, mutta kirjan lukemista varten tämä taito on välttämätön. Lisäksi monet kirjan tehtävistä ovat hyvin vaikeita. Lukeminen siis vaatii lukijalta merkittävää panostusta.

Tästä huolimatta myös nuoremmille lukijoille on pyritty tarjoamaan mahdollisuus kirjan sisällön ymmärtämiseksi. Esitietoja-lukuun on koottu kirjan kannalta oleellisia simpia esitietoja. Tarkoituksena on, että materiaali on itsenäinen ja että kiinnostunut ja päättäväinen yläkouluikäinen pystyy saamaan siitä jotakin irti.

### **Kattaako kirja kaiken kilpailumatematiikasta?**

*Ehdottomasti tärkein asia kilpailumatematiikan oppimiseksi on tehtävien tekeminen.* Tämä kirja ainoastaan tukee harjoittelua. Jalkapalloa tai viulunsoittoa ei opita katsomalla, kun muut pelaavat tai soittavat. Vastaavasti matematiikkaa ei opi pelkästään lukemalla, miten muut tekevät matematiikkaa, vaan sitä pitää itse tehdä.

Lukemalla voi kuitenkin oppia joitain hyödyllisiä asioita. Kilpailutehtävissä oletetaan tunnetuksi, että kisaja tietää tiettyjä asioita (lukion oppimäärän ulkopuolisesta) matematiikasta. Tällaisia yleisesti tunnettuja menetelmiä on koottu tämän kirjan lukuihin kohtuu kattavasti.

Tiedon lisäksi kilpailutehtävät vaativat tietysti ongelmanratkaisutaitoja. Nämä tietysti kehittyvät parhaiten tekemällä tehtäviä. Toivon, että tästä kirjasta löytyvät ajatukset omista ratkaisuprosesseistani ovat kuitenkin hyödyllisiä ja kiinnostavia.

Vaikka tässä kirjassa pyritään esittämään kattavasti tärkeimmät menetelmät kilpailutehtäviä ajatellen, on tietysti olemassa valtava määrä sekalaisia temppuja ja ideoita, jotka soveltuvat vähintään yhteen kilpatehtävään. Ei ole kuitenkaan mielekasta tehdä listaa kaikista kikoista, joita voi yrittää soveltaa tehtäviin. *Harjoittelun tuoma intuitio on paljon tehokkaampi väline ongelmanratkaisuun kuin mikään lista erinäisistä jipoista.*

### **Eikö tällaista materiaalia ole olemassa jo ennestään?**

Kilpailumatematiikkaan liittyvää materiaalia on tietysti paljon, mutta mielestäni monessa materiaalissa on puutteita. Suurin ongelma on sisältö: monissa teksteissä käydään läpi tehtävien ratkaisuja, mutta niissä ei opeteta, miten ratkaisuihin voisi päätyä itse. Tämän kirjan tekstistä suuri osa kuvaa sitä, miten olen itse ratkaissut jonkin tehtävän.

Toinen merkittävä ongelma on aloittelijaystävällisyys: ei ole helppoa löytää materiaalia tai kokoelmaa materiaaleja, jotka lähtisivät perusteista (kilpailumatematiikan kannalta) ja joista voisi oppia suunnilleen kaiken tarvittavan. Lisäksi monet materiaalit käsittelevät matematiikkaa mielestäni aivan liian formaalisti – tyyli ei sovi harrastelijalle, joka ei ole törmännyt matematiikkaan koulun ulkopuolella. Näiden ongelmien korjaamiseksi tämä materiaali lähtee perusteista ja tekstin tyyli on rennompi kuin monissa muissa materiaaleissa. Mutta kuten jo mainittiinkin, käsiteltävät asiat ovat silti vaikeita ja niiden ymmärtäminen vaatii lukijalta työtä.

### **Miten kirjaa kannattaa lukea?**

*Kirjan tehtävät eivät ole vaikeusjärjestyksessä.* Suuressa osassa lukuja viimeinen tehtävä on tarkoituksellisesti muita vaikeampi, ja esimerkiksi lisätehtäväluvuissa

kaikki tehtävät ovat haastavia. Kirjaa ei siis välttämättä kannata lukea luku kerrallaan, vaan tarvittaessa kannattaa hypätä vaikeimpien kohtien yli ja palata niihin myöhemmin.

*Suosittelen oikeastaan, että lukija yrittää ratkaista tehtäviä, joiden ratkaisut hän on joskus aiemmin lukenut.* Tätä kautta pääsee kokeilemaan, mitä kirjassa esittämistäni ongelmanratkaisumenetelmistä on tarttunut itselle.

Yleisesti kirjan ajatuksista saa paremmin kiinni, jos tietoisesti miettii, miten ne eroavat omista. Tehtävän ratkaisun luettua suosittelen lukijaa miettimään esimerkiksi seuraavia asioita: Mikä oli ratkaisun pääidea? Mikä oli ratkaisun vaikein kohta, ja mitkä osat olivat vain rutiininomaisia yksityiskohtia? Miten ratkaisuun voisi päätyä? Olisinko itse voinut keksiä ratkaisun? Miksi tai miksi en?

Aihealueiden sisällä luvut kannattaa lukea järjestyksessä ainakin lukuteorian ja geometrian kohdalla, koska seuraavat luvut rakentuvat pitkälti edellisten päälle. Algebrassa järjestyksellä ei ole niin paljoa väliä ja kombinatoriikassa ei käytännössä ollenkaan. Aihealueiden välisiä riippuvuuksia ei ole yksittäisiä tehtäviä enempää, vaikkakin jotkin yksityiskohdat saattavat aueta vasta sen jälkeen, kun on lukenut toisen osion materiaalia.

Kirjassa on paikoittain kohtia, joissa on verrattain paljon teoriaa. Pitääkseni painotuksen riittävästi ongelmanratkaisussa ja esittääkseni joitain mielestäni hyviä tehtäviä olen kirjoittanut jokaiseen osa-alueeseen lisätehtäviä sisältävän luvun. Lisätehtävät ovat keskimäärin vaikeampia kuin muissa luvuissa vastaan tulevat tehtävät, joten ne eivät välttämättä sovellu perheen pienimmille.

Kirjaa lukiessa kannattaa muistaa, että matematiikan lukeminen ei toimi niin, että joko on tai ei ole lukenut jotain asiaa. Vaikka osa ajatuksista menisi ohi, niin monesti lukemisesta silti oppii jotain. Lisäksi vaikeisiin kohtiin voi ja kannattaa palata myöhemmin.

**Tekstin seassa esiintyy erilaisia lyhenteitä, kuten IMO. Mitä nämä tarkoittavat?**

IMO eli Kansainväliset matematiikkaolympialaiset mainittiin jo aiemmin Suomen kilpailutoiminnan yhteydessä. Muita tekstissä esiintyviä kilpailujen lyhenteitä ovat MAOL (Matemaattisten Aineiden Opettajien Liitto), EGMO (Euroopan tyttöjen matematiikkaolympialaiset), ELMO (Ex-Lincoln Math Olympiad: tämä on eräs Yhdysvaltojen vuosittainen harjoituskilpailu) ja APMO (Asian Pacific Mathematics Olympiad). Lisäksi kilpailun yhteydessä voidaan mainita, että tehtävä on kilpailun lyhytlistalta, mikä tarkoittaa sitä, että tehtävä on ollut ehdolla kilpailun tehtäväksi, mutta sitä ei ole valittu itse kilpailuun.

Mainittujen kilpailuiden tehtävät toimivat hyvänä harjoittelumateriaalina. Harjoittelumateriaaleista on kerrottu lisää Lisämateriaaleja-luvussa.

**Mistä kirjan nimi tulee?**

Motivaatio kirjan kirjoittamiseen tuli Suomen kisakoodausvalmennuksen puolelta. Antti Laaksonen on kirjoittanut opetusmateriaalin nimeltä ”Kisakoodarin käsikirja”, joka lyhennetään usein KKKK. Kirja on tarkoitukseensa toimiva, ja ajattelin, että

myös matematiikan puolelle voisi tehdä vastaavan materiaalin. Aluksi kirja kulki työnimellä ”Matematiikkamittelijän mittava manuaali” eli MMMM.

Kun mietin kirjan nimeä uudelleen, halusin painottaa ongelmanratkaisua jo sen nimessä. Lyhenteeksi pitäisi siis tulla OOOO. Tästä muodostui nykyinen nimi, joka on kuvaava monestakin syystä:

- Sana ”Ollin” kuvaa kirjan persoonallista tyyliä: Kerron nimenomaan omista ajatuksistani ja ideoistani, ja tehtävien ratkaisut vastaavat omaa ratkaisuprosessiani. Lisäksi kirjan lopussa on kirjoittamiani kilpailumatematiikkaa koskevia henkilökohtaisia tekstejä, jotka voivat olla kiinnostavia ja opettavaisia.
- Kirja on vähän niin kuin oppikirja, mutta rennompi, joten se on opas.
- Materiaali soveltuu olympiatasoon tähtääville. Monet esimerkkitehtävät ovat vaikeita.
- Toistetaan vielä kerran, että kirjan pääpaino on ongelmanratkaisussa.

## 2 Johdantotehtäviä

Kilpailumatematiikka jakautuu neljään osa-alueeseen: algebraan, geometriaan, kombinatoriikkaan ja lukuteoriaan. Tässä luvussa annetaan pieni maistiainen jokaisesta osa-alueesta esittämällä yksi kuhunkin aihealueeseen liittyvä tehtävä. Kaikki näistä eivät ole helppoja, ainakaan jos ei ole harrastanut kilpailumatematiikkaa aiemmin. Tehtävät onkin valittu itse tehtävän tai sen ratkaisun mielenkiintoisuuden vuoksi. Lukija voi halutessaan pohtia tehtäviä ennen ratkaisujen lukemista.

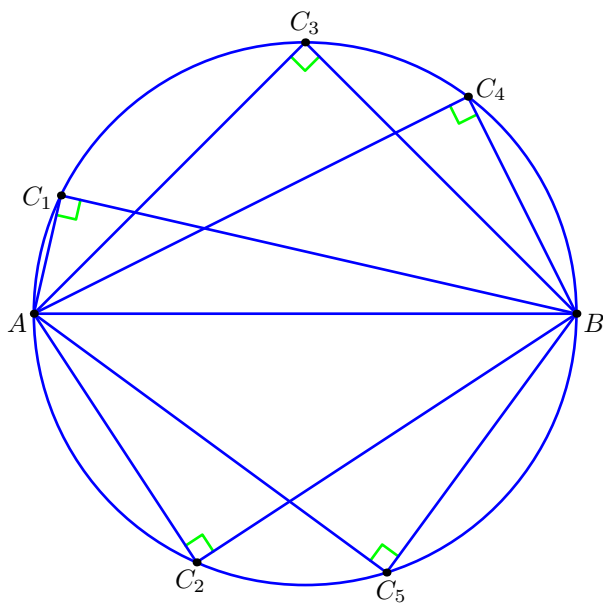
### 2.1 Geometria

Tehtävänä on osoittaa seuraava tulos, joka tunnetaan nimellä Thaleen lause.

#### Lause (Thaleen lause)

Tasoon on piirretty ympyrä, jonka halkaisija on jana  $AB$ . Ympyrältä valitaan jokin piste  $C$ . Osoita, että  $\angle ACB = 90^\circ$ .

Tässä kuvassa tilannetta on havainnollistettu viidellä eri pisteen  $C$  valinnalla.



Kuvien suorat kulmat todella näyttävät suorilta kulmilta, mutta mistä se johtuu? Todistus näytetään ensimmäisessä geometrian kappaleessa.

### 2.2 Lukuteoria

#### Tehtävä

Etsi kaikki positiiviset kokonaisluvut  $x$  ja  $y$ , joilla  $|3^x - 2^y| = 1$ .



Listaamalla kakkosen potensseja  $2, 4, 8, 16, \dots$  ja kolmosen potensseja  $3, 9, 27, 81, \dots$  huomataan, että parit  $(2, 3)$ ,  $(4, 3)$  ja  $(8, 9)$  ovat sellaisia, joissa luvut ovat yhden päässä toisistaan. Ovatko tässä kaikki kakkosen ja kolmosen potenssien parit, jotka ovat yhden etäisyydellä toisistaan? Ratkaisu ongelmaan löytyy lukuteorian kappaleesta Eksponenttifunktiot ja neliönjäännökset.

## 2.3 Algebra

### Tehtävä

Yhtälöllä  $x^3 + 2x^2 + 3x + 4 = 0$  on kolme ratkaisua. Merkitään niitä kirjaimin  $a$ ,  $b$  ja  $c$ . Laske  $a^2 + b^2 + c^2$ .

Kolmannen asteen yhtälön ratkaiseminen on vaikeaa (mutta ratkaiseminen on mahdollista). Olisi hyvin työlästä etsiä yhtälölle kaikki kolme ratkaisua, laskea ratkaisujen neliöt ja summata nämä yhteen. Tehtävään on kuitenkin elegantti ratkaisu, jossa vastauksen laskeminen on ovelien havaintojen vuoksi hyvin helppoa. Ratkaisu löytyy kappaleesta Polynomit.

## 2.4 Kombinatoriikka

### Tehtävä

Anna ja Berg pelaavat dominopalikoilla  $(2 \times 1)$  peliä  $n \times 1$  ruudun laudalla. Pelissä pelaajat laittavat vuorotellen yhden dominopalikan laudalle niin, että palikka peittää täsmälleen kaksi ruutua eikä mene yhdenkään muun palikan päälle. Peli loppuu, kun tällaisia siirtoja ei pystytä enää tekemään. Viimeisen siirron tehnyt pelaaja voittaa pelin. Osoita, että jos Anna ja Berg pelaavat yhden pelin jokaisella luvun  $n$  arvolla  $2, 3, \dots, 2007$ , Anna aloittaa jokaisen pelin ja molemmat pelaajat pelaavat optimaalisesti, niin Anna voittaa ainakin 1505 peliä.

Käydään läpi esimerkkipeli arvolla  $n = 9$  eli  $9 \times 1$ -laudalla.

Anna voi laittaa dominopalikan ruutujen 4 ja 5 kohdalle.



Berg voi laittaa palikan kohtien 6 ja 7 kohdalle, jolloin tilanne näyttää tältä:



Pelaa Anna miten tahansa, voi Berg tehdä vielä yhden siirron Annan jälkeen. Berg saa tehtyä viimeisen siirron ja voittaa pelin. Olisiko Anna voinut voittaa pelaamalla alussa jotenkin muuten?

Usein pelejä käsittelevissä tehtävissä oletetaan, että pelaajat pelaavat parhaalla mahdollisella tavalla, ja yleensä kysytään pelin voittajaa. Tämä tehtävä on hieman epätavallinen, koska tehtävässä ei pyydetä osoittamaan mitään koskien tiettyä luvun  $n$  arvoa. Halutaan vain todistaa, että aloittava Anna voittaa suurimman osan peleistä, tarkemmin sanoen vähintään 1505 peliä. Tehtävän ratkaisu löytyy kombinatoriikan luvusta Pelit.

### 3 Kehäkulmalause ja jännenelikulmiot (Geometria)

Tässä luvussa esitetään kilpailuissa esiintyvän geometrian perusteet.

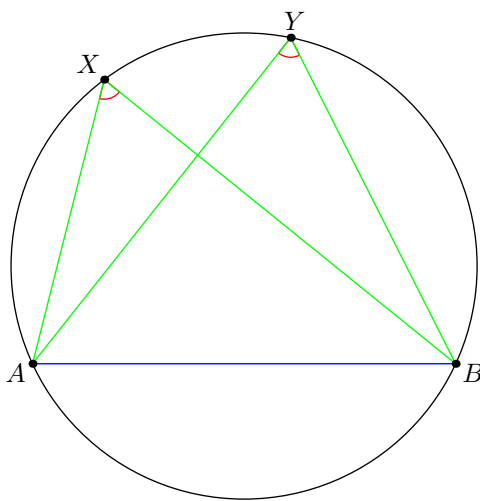
Lukijan oletetaan muistavan koulusta seuraavat perusasiat:

- Kolmion kulmien summa on  $180^\circ$ .<sup>1</sup> (Oleellista ei tietenkään ole se, että summa on jokin sovittu asteluku, vaan se, että kolmion kulmien summa on yhtä suuri kuin oikokulma.)
- Jos kolmiossa on kaksi yhtä pitkää sivua, niin siinä on kaksi yhtä suurta kulmaa, ja toisin päin. Tällaisia kolmioita kutsutaan tasakylkiseksi kolmioiksi.

Seuraavaksi käsitellään kehäkulmalausetta, joka myös on koulusta tuttu. Tulos on kuitenkin tärkein kilpailugeometriassa käytettävistä välineistä, joten se kannattaa käydä läpi huolella.

#### 3.1 Kehäkulmalause

Tutkitaan seuraavaa kuvaa.



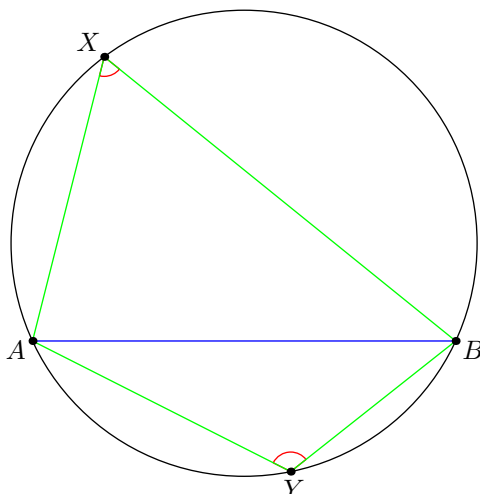
Pisteet  $A, B, X$  ja  $Y$  ovat siis mielivaltaisia pisteitä ympyrän kehällä. Kehäkulmalause sanoo, että punaisella merkityt kulmat ovat yhtä suuret.

#### Lause (Kehäkulmalause)

Olkoot  $A, B, X$  ja  $Y$  mielivaltaiset (eri) pisteet ympyrän kehällä. Oletetaan, että  $X$  ja  $Y$  ovat samalla puolella janaa  $AB$ . Tällöin  $\angle AXB = \angle AYB$ .

Huomaa lauseen oletus pisteiden  $X$  ja  $Y$  sijainnista. Tämä oletus on välttämätön, kuten seuraavasta kuvasta nähdään – toinen kulmista näyttää olevan tylppä ja toinen terävä.

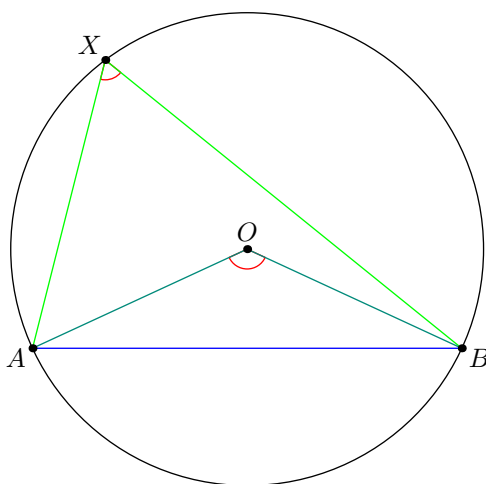
<sup>1</sup>Osaatko todistaa tämän?



Ennen kuin tutkitaan tilannetta pidemmälle, esitetään kehäkulmalauseen yleistys. Tämä yleistys on oikeastaan helpompi siksi, että se antaa vinkin siitä, miten lause todistetaan.

**Lause (Kehäkulmalauseen keskuskulmaversio)**

Olkoot  $A$ ,  $B$  ja  $X$  (eri) pisteitä ympyrän kehällä, ja olkoon  $O$  ympyrän keskipiste. Tällöin pätee  $\angle AOB = 2\angle AXB$ .

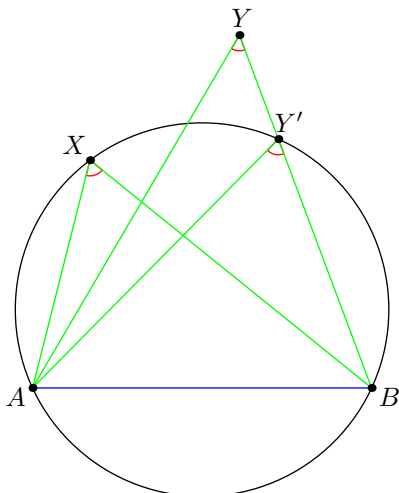


Huomaa, että tämä lause todistaa kehäkulmalauseen: lausehan osoittaa, että  $\angle AXB$  on aina puolet kulmasta  $\angle AOB$  riippumatta siitä, miten piste  $X$  valitaan. Siis  $\angle AXB$  on aina sama kaikilla pisteen  $X$  valinnoilla. Paitsi...

Myös tässä lauseessa tulee huomioida se mahdollisuus, että  $X$  on ”väärällä puolella” janaa  $AB$ . Tällöin kulma  $\angle AOB$  tulee mitata niin, että se kiertää pisteen  $O$  eri puolelta kuin kuvassa.

Lauseen voi todistaa käyttäen pelkästään tietoa siitä, että kolmion kulmien summa on 180 astetta ja että jos kolmiossa on kaksi yhtä pitkää sivua, niin siinä on kaksi yhtä suurta kulmaa.





Nyt kehäkulmalauseen nojalla  $\angle AY'B$  on sama kuin  $\angle AXB$ , joka puolestaan on oletuksen nojalla sama kuin kulma  $\angle AYB$ . Nyt kolmiossa  $AYY'$  kulma  $\angle AY'Y$  on  $180^\circ - \angle AYY'$ , ja koska kolmion kulmien summa on  $180^\circ$ , tulisi kulman  $\angle YAY'$  olla  $0^\circ$ . Tämä on mahdotonta, joten  $Y$  ei voi olla ympyrän ulkopuolella.

Vastaavasti käsitellään tapaus, jossa piste  $Y$  on ympyrän sisäpuolella.

### 3.2 Jännelikulmiot

Aiemmin tutkittiin tilannetta, jossa pisteet  $X$  ja  $Y$  ovat eri puolilla janaa  $AB$ . Kehäkulmalauseen keskuskulmaversioiden nojalla tällöin  $\angle AXB$  vastaa puolta kulmasta  $\angle AOB$  ja  $\angle AYB$  on puolet kulmasta  $\angle AOB$ , missä kulma kiertää pisteen  $O$  toista kautta kuin kulman  $\angle AXB$  tapauksessa. Yhteensä näiden keskuskulmien summa on täysi kulma, eli pätee  $\angle AXB + \angle AYB = 180^\circ$ . Siis jos nelikulmion  $AYBX$  kaikki pisteet ovat samalla ympyrällä, niin sen vastakkaisten kulmien  $\angle AXB$  ja  $\angle AYB$  summa on  $180^\circ$ .

Toisaalta jos nelikulmion  $AYBX$  vastakkaisten kulmien  $\angle AXB$  ja  $\angle AYB$  summa on  $180^\circ$ , niin kehäkulmalauseen vain jos -puolella ja keskuskulmaversiolla saadaan, että pisteet  $A, Y, B$  ja  $X$  todella ovat kaikki samalla ympyrällä.

Edelliset huomiot antavat seuraavan hyvin tärkeän lauseen koskien jännelikulmioita, eli nelikulmioita, joiden kaikki kärkipisteet ovat samalla ympyrällä.

#### Lause (Jännelikulmioiden peruslause)

Olkoon  $AYBX$  nelikulmio. Tällöin pisteet  $A, Y, B$  ja  $X$  ovat samalla ympyrällä jos ja vain jos nelikulmion vastakkaisten kulmien  $\angle AYB$  ja  $\angle AXB$  summa on  $180$  astetta.

Sillä ei tietenkään ole väliä, kumpi pari vastakkaisia kulmia ehtoon otetaan, koska nelikulmion kulmien summa on  $360^\circ$  (joten  $\angle AYB + \angle AXB$  on  $180^\circ$  täsmälleen silloin, kun  $\angle XAY + \angle XBY = 180^\circ$ ).

Huomaa, että lausetta käyttäessä tulee ottaa nimenomaan vastakkaiset kulmat

nelikulmiosta. Tämän vuoksi lauseessa tulee tietää, missä järjestyksessä pisteet  $A, Y, B$  ja  $X$  ovat toisiinsa nähden. Puhuttaessa nelikulmiosta  $ABCD$  oletetaan aina, että  $A, B, C$  ja  $D$  sijaitsevat tässä järjestyksessä toisiinsa nähden eli että sen sivut eivät leikkaa toisiaan.

Kehäkulmalauseella ja sen vain jos -puolella saadaan toinen ekvivalentti ehto jännenelikulmiolauseen väitteen kanssa: nelikulmio  $AYBX$  on jännenelikulmio jos ja vain jos  $\angle YAB = \angle YXB$ .

### 3.3 Huomautus: suunnatut kulmat

Edellä esitetyt tulokset tuntuvat epäkäytännöllisiltä: miltei jokaista tulosta käytettäessä tulisi varmistaa, että jotkin pisteet ovat oikealla puolella jotain janaa tai että pisteet ovat oikeassa järjestyksessä.

Yllättävää kyllä, tämä ongelma on paljon lievempi kuin mitä edellisen tekstin perusteella luulisi. Suuressa osassa kilpailutehtäviä ei esiinny tällaisia ns. konfiguraatio-ongelmia, ja niissä, joissa esiintyy, käsiteltävät tapaukset monesti ratkeavat käytännössä katsoen samalla todistuksella. Usein riittääkin vain alussa olettaa, että tehtävän pisteet ovat siinä järjestyksessä, missä ne ovat itse piirretyissä kuvassa, ja lopuksi mainita, että muut tapaukset ratkeavat samalla tavalla (olettaen, että näin todella on – muuten voi tulla ongelmia).

Edellinen ”ratkaisu” ongelmaan voi tuntua epäilyttävältä (ja onhan se). Ongelmaan on kuitenkin myös ”oikea” ratkaisu: suunnatut kulmat. Suunnatut kulmat perustuvat siihen ideaan, että merkitessä  $\angle ABC$  tarkoitetaan kulman vastaavan aluetta, joka saadaan kiertämällä janaa  $BC$  vastapäivään, kunnes se kohtaa janan  $BA$ . Lisäksi ajatellaan, että kulmat lasketaan ”modulo 180 astetta”<sup>2</sup>. Täten esimerkiksi  $\angle ABC = 360^\circ - \angle CBA \equiv -\angle CBA \pmod{180^\circ}$ . En ole itse tarvinnut suunnattuja kulmia kilpailutehtäviä ratkoessani, minkä vuoksi niitä ei käytetä tässä materiaalissa.

Oli ratkaisu ongelmaan mikä hyvänsä, tulee kilpailuissa aina piirtää mallikuva geometrian tehtäviin – tällöin on selvää, mitä konfiguraatiota tarkastellaan.

### 3.4 Esimerkkitehtäviä

Pelkästään kehäkulmalause ja jännenelikulmioita koskevat tulokset riittävät ratkomaan suuren osan geometrian tehtävistä, kunhan niitä osaa soveltaa hyvin. Tässä esitetään muutama esimerkki. (Ja vaikka tehtävä ei ratkeaisikaan pelkästään näillä menetelmillä, on niiden soveltaminen usein iso osa ratkaisua. Tästä nähdään esimerkkejä seuraavissa luvuissa.)

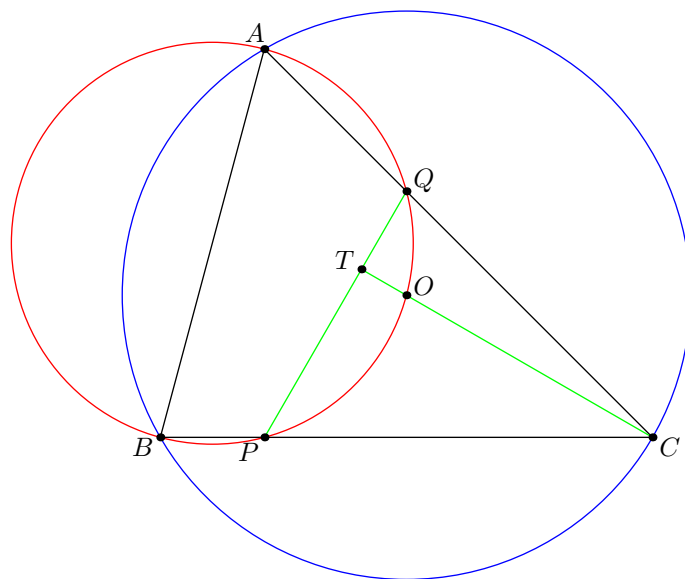
Ensimmäinen esimerkkitehtävä on ollut MAOLin loppukilpailussa vuonna 2014.

<sup>2</sup>Modulo on määritelty lukuteorian kappaleessa Kongruenssit. Lukija ei kuitenkaan jää paljosta paitsi, vaikka hän ei vielä olisikaan lukenut kongruensseista.

**Tehtävä**

Olkoon  $O$  teräväkulmaisen kolmion  $ABC$  ympärysympyrän keskipiste. Pisteiden  $A, B$  ja  $O$  kautta kulkeva ympyrä leikkaa sivut  $BC$  ja  $AC$  pisteissä  $P$  ja  $Q$ . Osoita, että janan  $CO$  jatke leikkaa kohtisuorasti janaa  $PQ$ .

Minkä tahansa kolmion kärkipisteiden kautta voidaan piirtää ympyrä (tämä todistetaan hieman myöhemmin). Tehtävässä  $O$  on tämän ns. ympärysympyrän keskipiste.



Merkitään kyseistä leikkauspistettä kirjaimella  $T$ . Haluamme siis todistaa, että  $\angle PTC = 90^\circ$ . Yksi lähestymistapa voisi olla yrittää laskea, mitä ovat  $\angle TPC$  ja  $\angle TCP$ : jos näiden kulmien summa on  $90^\circ$ , niin tällöin pätee  $\angle PTC = 90^\circ$ .

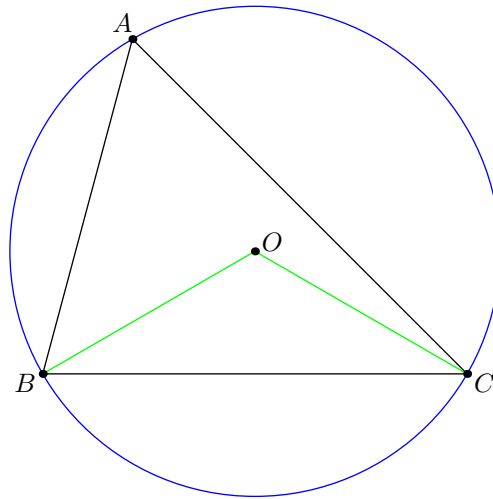
Yritetään ensiksi laskea, mitä  $\angle TPC$  on. Yleinen ajatus kulmanjahtauksessa on aina yrittää esittää kulmia ”tunnettujen” kulmien avulla. Esimerkiksi tässä (ja käytännössä kaikissa tehtävissä, jotka käsittelevät kolmiota) tunnetuiksi kulmiksi voi ajatella kulmat  $\angle BAC$ ,  $\angle ACB$  ja  $\angle CBA$ . Nämä kulmat lyhennetään usein kirjoittamalla  $\angle A$ ,  $\angle B$  ja  $\angle C$ , koska niitä käytetään ratkaisuissa hyvin paljon.

Ei ole kovin vaikeaa nähdä ”polkua”, jonka kautta  $\angle TPC$  saadaan palautettua kolmion  $ABC$  kulmiin: Ensinnäkin  $\angle TPC = 180^\circ - \angle BPT$ . Koska  $ABPQ$  on jännelikulmio, on sen vastakkaisten kulmien summa  $180^\circ$ . Täten  $\angle BPQ + \angle BAQ = 180^\circ$ , eli  $\angle BPT = 180^\circ - \angle A$ . Yhdistämällä saadut tiedot saadaan  $\angle TPC = \angle A$ .

Olemme saaneet laskettua, mitä  $\angle TPC$  on. Vielä pitää laskea kulma  $\angle PCT$ , jonka haluamme olevan  $90^\circ - \angle A$ . Nyt on hyvä ensiksi huomata, että  $\angle PCT = \angle BCO$ . Pelkästään kuvaa katsomalla voisi ajatella, että tämä sievennys on triviaali, mutta toisaalta pisteet  $P$  ja  $T$  ovat paljon ”vaikeampia” kuin piste  $O$ . Tämän takia kannattaa mieluummin keskittyä kulmaan  $\angle BCO$ .

Voimme nyt unohtaa kokonaan pisteet  $P, T$  ja  $Q$ , ja ongelma palautuu muotoon ”Todista, että  $\angle BCO = 90^\circ - \angle A$ ”. Tämä on selvästi edistystä. Tutkittava konfiguraatio on jo niin yksinkertainen, että tehtävän luulisi ratkeavan.

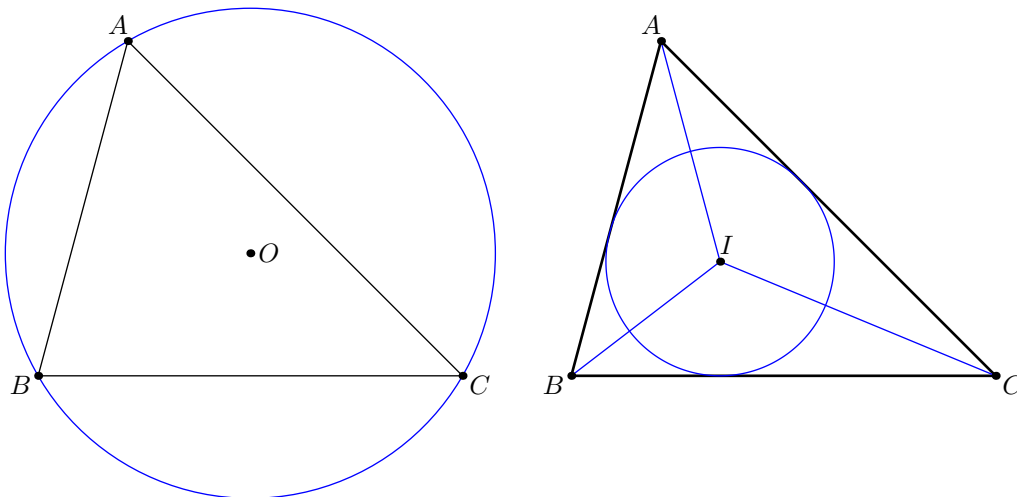




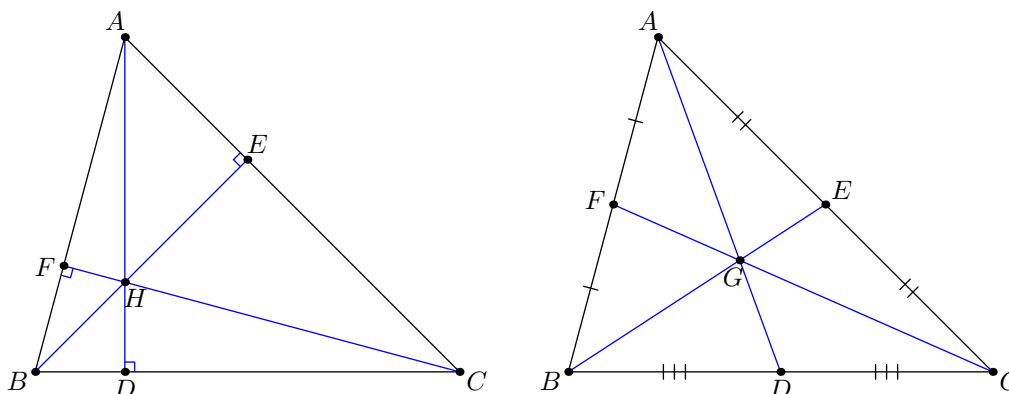
Kuvaan on piirretty apujana  $BO$ . Soveltamalla kehäkulmalauseen keskuskulmaversiota saadaan  $\angle BOC = 2\angle A$ , ja koska  $BOC$  on tasakylkinen kolmio, saadaan kantakulmat laskettua:  $\angle OBC = \angle OCB = 90 - \angle A$ . Olemme siis valmiit.

Huomattiin siis, että tehtävä palautuu yhtälön  $\angle BCO = 90^\circ - \angle A$  todistamiseen. Huomaamme, että pystymme oikeastaan laskemaan minkä tahansa kulman, jotka muodostetaan valitsemalla jotkin kolme pisteistä  $A, B, C$  ja  $O$ . Onkin tärkeää tietää, miten yleiset konfiguraatiot käyttäytyvät.

Ympärysympyrän keskipiste  $O$  ei ole ainoa kolmion tärkeä piste. Seuraavaksi esitetään neljä yleisimmin esiintyvää kolmion merkillistä pistettä.<sup>3</sup>



<sup>3</sup>Kilpailutehtävissä tarvitsee harvemmin tietää monia eksoottisia pisteitä. Seuraavassa luvussa käydään vielä läpi sivuympyröiden keskipisteitä ja yhdeksän pisteen ympyrää koskevia ominaisuuksia. Täällä on lueteltu kymmeniä tuhansia kolmion merkillisiä pisteitä: <https://faculty.evansville.edu/ck6/encyclopedia/ETC.html>.



Vasemmalta oikealle ja ylhäältä alas: ympärysympyrän keskipiste  $O$ , sisäympyrän keskipiste  $I$ , korkeusjanojen leikkauspiste (ortokeskus)  $H$  ja mediaanien leikkauspiste (painopiste)  $G$ . (Kirjainten valinnat tulevat englannista.) Ensi luvussa todistetaan, miksi esimerkiksi korkeusjanat leikkaavat samassa pisteessä.

Ympärysympyrän keskipistettä koskevia ominaisuuksia on jo käyty läpi. Mainitaan vielä yksi asia: piste  $O$  on janojen  $AB$ ,  $BC$  ja  $CA$  keskinormaalien leikkauspiste. (Kerataan, että janan normaali on suora, joka leikkaa sitä kohtisuorasti ja keskinormaali on normaali, joka jakaa janan kahteen yhtä pitkään osaan.)

Sisäympyrän keskipistettä  $I$  koskien mainitaan aluksi seuraavat asiat:

1.  $I$  määritellään olemaan sellaisen ympyrän (ns. sisäympyrän) keskipiste, joka sivuaa jokaista kolmion  $ABC$  sivuista.
2.  $I$  on kolmion  $ABC$  kulmanpuolittajien leikkauspiste. (Kulmanpuolittaja on nimensä mukaisesti suora, joka puolittaa jonkin kulman. Siis esimerkiksi  $\angle BAI = \angle CAI = \frac{1}{2}\angle A$ .)

Välillä sisäympyrän yhteydessä esiintyvät kolmion  $ABC$  sivuamispisteet sisäympyrän kanssa ja janat kolmion kärkipisteistä näihin sivuamispisteisiin. Huomaa, että nämä janat eivät ole kulmanpuolittajia. (Ne kuitenkin leikkaavat samassa pisteessä. Leikkauspiste ei kuitenkaan ole sisäympyrän keskipiste.)

Konfiguraatiosta, jossa on kolmion kärjet  $A$ ,  $B$  ja  $C$ , kulmanpuolittajat  $AD$ ,  $BE$  ja  $CF$  sekä näiden leikkauspiste  $I$ , voidaan laskea osa kulmista varsin suoraviivaisesti, mutta aivan kaikkea ei saada laskettua. Esimerkiksi kulmaa  $\angle AEF$  ei saa laskettua kulmien  $\angle A$ ,  $\angle B$  ja  $\angle C$  avulla.

Kolmion ortokeskus  $H$  on sen korkeusjanojen leikkauspiste. Ei ole ilmeistä, miksi korkeusjanat leikkaavat samassa pisteessä (tämä todistetaan myöhemmin). Kyseessä on jälleen konfiguraatio, josta voi laskea kaikki kulmat. Seuraava lemma on tärkeä tulos tähän liittyen.

**Lemma**

Olkoon  $ABC$  kolmio, ja olkoot  $AD$ ,  $BE$  ja  $CF$  sen korkeusjanat. Olkoon  $H$  kolmion  $ABC$  ortokeskus. Tällöin  $AFHE$  ja  $BFEC$  ovat jännelikulmioita.

Lemman todistus on triviaali käyttämällä tuloksia kehäkulmalauseesta ja jännelikulmioista. Tarvitsemme oikeastaan vain erikoistapausta suorille kulmille, joka tunnetaan Thaleen lauseena, joka esiteltiin jo johdantokappaleessa.

Huomaa, että lemmassa mainitut jännelikulmiot on ”otettu pisteen  $A$  suhteen”. Konfiguraatiossa on oikeastaan kuusi kappaletta jännelikulmioita, kaksi jokaista kärkeä  $A$ ,  $B$  ja  $C$  kohti.

Nyt ei ole vaikeaa laskea kulmia kuvasta. Ehkäpä vaikein kulma laskea on  $\angle FED$ . Ensiksi huomataan, että  $\angle FED = \angle FEH + \angle HED$ . Lemmaa käyttämällä tämä saadaan muotoon  $\angle FAH + \angle HCD$ . Molemmat näistä kulmista ovat  $90^\circ - \angle B$ , mikä nähdään katsomalla suorakulmaisia kolmioita  $BAD$  ja  $BCF$ .

Ortokeskusta koskeva konfiguraatio on myös siitä näppärä, että sivujen pituuksia voi laskea suhteellisen helposti trigonometrian avulla.

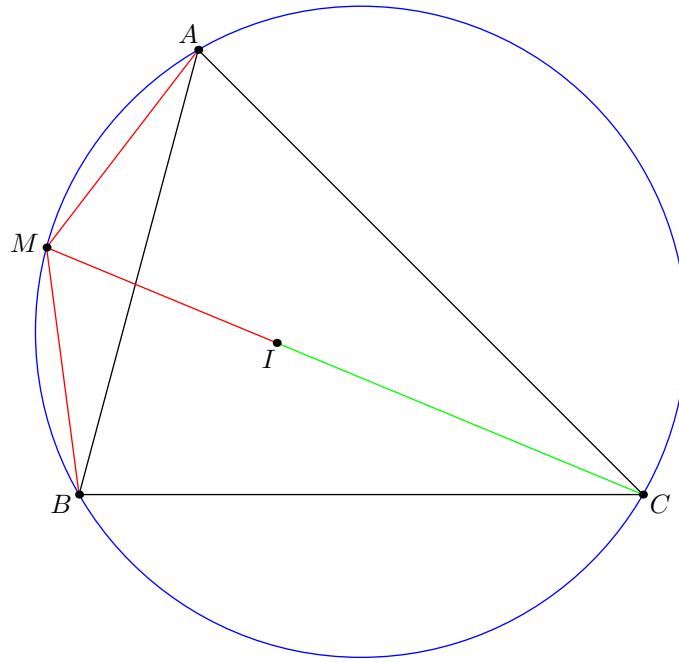
Kolmion mediaaneiksi tai keskijanoiksi kutsutaan niitä janoja, joiden toinen pää on kolmion yksi kärkipiste ja toinen pää on kolmion vastakkaisen sivun keskipiste. Näiden janojen leikkauspistettä  $G$  kutsutaan kolmion painopisteeksi.

Jos  $AD$  on kolmion mediaani, niin kulmia  $\angle BAD$  ja  $\angle DAC$  ei saa laskettua pelkästään kulmien  $\angle A$ ,  $\angle B$  ja  $\angle C$  avulla (käyttämättä trigonometrisia funktioita). Kolmio  $DEF$  on kuitenkin yhdenmuotoinen kolmion  $ABC$  kanssa. Tämä seuraa huomaamalla, että kolmioilla  $FAE$  ja  $BAC$  on yhteinen kulma  $\angle A$  ja että tämän kulman vieressä olevien sivujen suhteet ovat samat, nimittäin  $1 : 2$ . Täten pätee  $FE : BC = 1 : 2$ . Vastaava pätee myös muille sivuille. Huomataan vielä, että janat  $BC$  ja  $FE$  ovat yhdensuuntaiset.

Seuraava tehtävä on hieman samantyylinen kuin aiempi MAOLin tehtävä. Tehtävän konfiguraatio esiintyy usein kilpailutehtävissä, joten se kannattaa opetella tunnistamaan.

**Tehtävä**

Olkoon  $ABC$  kolmio, ja olkoon  $I$  sen sisäympyrän keskipiste. Olkoon  $M$  kulman  $\angle C$  puolittajan leikkauspiste kolmion  $ABC$  ympärysympyrän kanssa. Osoita, että  $M$  on kolmion  $AIB$  ympärysympyrän keskipiste.



Haluamme osoittaa, että  $MA = MB = MI$ . Todistetaan ensin helpompi osuus  $MA = MB$ .

Kehäkulmalauseen nojalla pätee  $\angle MAB = \angle MCB$ . Vastaavasti  $\angle MBA = \angle MCA$ . Oletuksen nojalla  $MC$  on kulman  $\angle C$  puolittaja, joten  $\angle MCB = \angle MCA$ . Täten  $\angle MBA = \angle MAB$ , eli  $MBA$  on tasakylkinen kolmio, eli  $MA = MB$ . Yleisesti pätee, että yhtä suuria kulmia vastaavat kaaret ovat yhtä pitkiä.

Todistetaan sitten, että  $MA = MI$ . Toisin sanoen halutaan, että  $MAI$  on tasakylkinen kolmio. Yritetään laskea kolmion  $MAI$  kulmat. Helpoin kulma on  $\angle AMI$ : tämä on vain  $\angle AMC = \angle B$ .

Seuraavaksi lasketaan vaikkapa kulma  $\angle MAI$ . Saadaan

$$\angle MAI = \angle MAB + \angle BAI = \angle MCB + \frac{1}{2}\angle A = \frac{1}{2}\angle C + \frac{1}{2}\angle A.$$

Nyt saadaan laskettua  $\angle MIA$ :

$$\angle MIA = 180^\circ - \angle AMI - \angle MAI = 180^\circ - \angle B - \frac{1}{2}\angle A - \frac{1}{2}\angle C.$$

Tämän voi sieventää kirjoittamalla  $180^\circ = \angle A + \angle B + \angle C$ , jolloin jäljelle jää  $\frac{1}{2}\angle A + \frac{1}{2}\angle C = \angle MAI$ . Tämä todistaa väitteen.

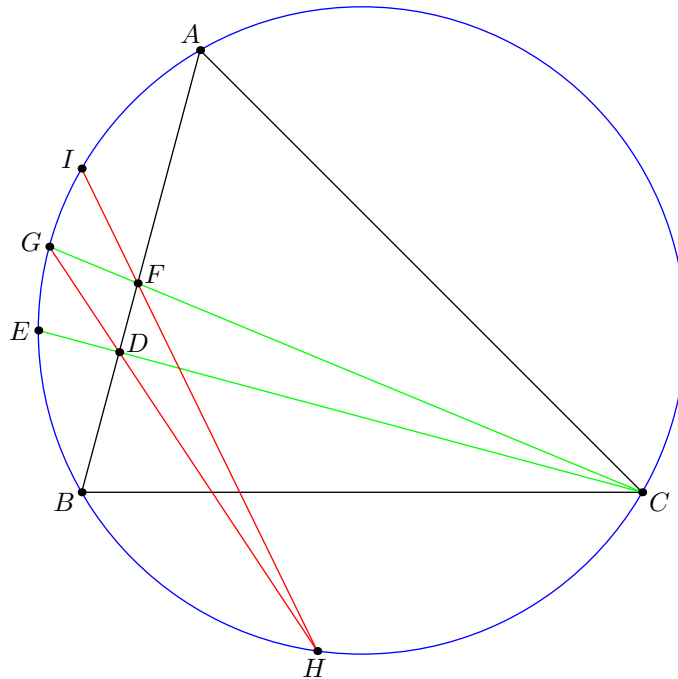
Kommentti: Todistus vaatii pienen määrän laskemista, mutta siinä ei ole mitään erityisen vaikeaa: lasketaan vain rutiininomaisesti kaikki kulmat, mitä nähdään, ja tulos seuraa.

Väitteelle on myös seuraava lyhyempi todistus, mutta tämä on hieman vaikeampi nähdä. Huomataan, että  $\angle AIB = 180^\circ - \frac{1}{2}\angle A - \frac{1}{2}\angle B$ , mikä sievennyy muotoon  $90^\circ + \frac{1}{2}\angle C$ . Lisäksi  $\angle AMB = 180^\circ - \angle C$ . Nyt sen kulman  $\angle AMB$ , joka on kuvassa yli  $180^\circ$ , koko on  $180^\circ + \angle C = 2\angle AIB$ , joten väite seuraa kehäkulmalauseen keskuskulma- ja vain jos -versioista.

Seuraava esimerkkitehtävä on vuoden 2014 Baltian tie -kilpailusta.

### Tehtävä

Olkoon  $\Gamma$  teräväkulmaisen kolmion  $ABC$  ympärysympyrä. Pisteiden  $C$  kautta kulkeva sivun  $AB$  normaali leikkaa sivun  $AB$  pisteessä  $D$  ja ympyrän  $\Gamma$  uudelleen pisteessä  $E$ . Kulman  $C$  puolittaja leikkaa sivun  $AB$  pisteessä  $F$  ja ympyrän  $\Gamma$  uudelleen pisteessä  $G$ . Suora  $GD$  leikkaa ympyrän  $\Gamma$  uudelleen pisteessä  $H$ , ja suora  $HF$  leikkaa ympyrän  $\Gamma$  uudelleen pisteessä  $I$ . Osoita, että  $AI = EB$ .



Ensinnäkin todetaan, että  $AI = EB$  täsmälleen silloin, kun janoja  $AI$  ja  $EB$  vastaavat ympärysympyrän kaaret ovat yhtä pitkät, mikä puolestaan tapahtuu täsmälleen silloin, kun  $\angle ICA = \angle ECB$ .<sup>4</sup> Tämä kulmaehto on paljon lähestyttävämpi kuin pituuksia koskeva ehto, joten käytetään sitä.

Kaaret  $\widehat{AI}$  ja  $\widehat{BE}$  eivät vielä ole kovin helppoja käsitellä. Huomataan kuitenkin, että  $\widehat{BE} = \widehat{BG} - \widehat{EG}$  ja  $\widehat{AI} = \widehat{GA} - \widehat{GI}$ , missä vähennyslaskulla tarkoitetaan kaarien pituuksien vähennyslaskua. Kulmanpuolittajaominaisuuden vuoksi kaarien  $\widehat{BG}$  ja  $\widehat{AG}$  pituudet ovat samat.

Riittää siis todistaa, että kaarien  $\widehat{EG}$  ja  $\widehat{GI}$  pituudet ovat samat. Kaari  $EG$  vastaa kulmaa  $\angle ECG$ , ja kaari  $GI$  vastaa kulmaa  $\angle GHI$ . Haluamme siis, että  $\angle GHI = \angle ECG$ .

Pääsemme nyt helposti eroon osasta konfiguraation pisteitä: Koska  $\angle GHI = \angle DHF$  ja  $\angle ECG = \angle DCF$ , voimme unohtaa pisteet  $I$  ja  $E$ . Nyt riittää siis todistaa, että  $\angle DHF = \angle DCF$ . (Pistettä  $G$  ei voi unohtaa, koska sitä käytettiin pisteen  $H$  määrittämiseen.)

<sup>4</sup>Formaalin todistuksen saa esimerkiksi käyttämällä sinilauseetta, joka esitetään luvun lopussa.

Ehto  $\angle DHF = \angle DCF$  vastaa tietysti sitä, että  $DCHF$  on jännelikulmio. Mitä kautta tämä kannattaa todistaa? Hyvä idea on lähteä siitä, mitä kulmia pystyy laskemaan. Ainakin  $\angle DCF$  pystyttäisiin laskemaan erotuksena  $\angle BCF - \angle BCD$ . Tämä ei kuitenkaan ole kovin hyödyllistä: jotta tätä tietoa pystyisi hyödyntämään, pitäisi osata laskea myös  $\angle DHF$ , mutta tästähän me lähdimme.

Toinen kulma, joka pystytään laskemaan, on  $\angle DFC$ :

$$\angle DFC = 180^\circ - \angle AFC = \angle FAC + \angle FCA = \angle A + \frac{1}{2}\angle C.$$

Jotta tätä voitaisiin hyödyntää, haluttaisiin laskea  $\angle DHC$ . Huomataan, että tämäkin onnistuu:

$$\angle DHC = \angle GHC = \angle GHA + \angle AHC = \angle GCA + \angle ABC = \frac{1}{2}\angle C + \angle B.$$

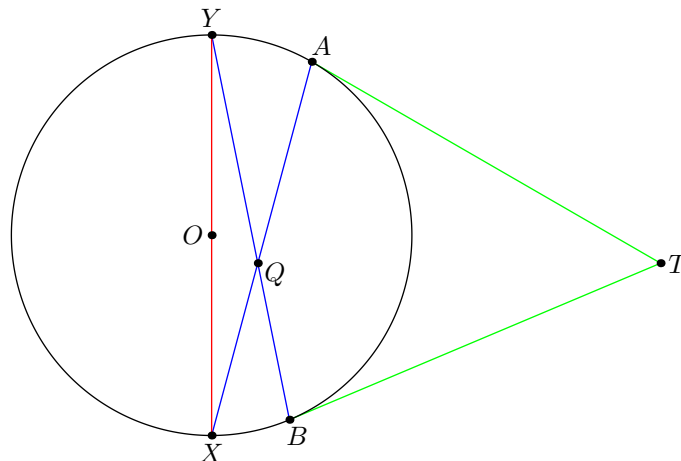
Siispä  $\angle DFC + \angle DHC = \angle A + \angle B + \angle C = 180^\circ$ , eli  $DHCF$  todella on jännelikulmio, ja olemme valmiit.

Kommentti: Välillä on hyvä yrittää ”kuoria” tehtävänantoa eli muotoilla ekvivalentteja muotoja tehtävästä. Helpommissa tehtävissä, kuten tässä, tehtävä voi lähes ratketa tällaisilla muunnoksilla, ja vaikeammissakin tehtävissä tällä pääsee usein alkuun.

Viimeinen tehtävä on MAOLin loppukilpailusta vuodelta 2017.

### Tehtävä

Valitaan ympyrän kehältä mielivaltaisesti kaksi sellaista pistettä  $A$  ja  $B$ , että  $AB$  ei ole ympyrän halkaisija. Pisteisiin  $A$  ja  $B$  piirretty ympyrän tangentit kohtaavat pisteessä  $T$ . Seuraavaksi valitaan halkaisija  $XY$  niin, että janat  $AX$  ja  $BY$  leikkaavat: olkoon tämä leikkauspiste  $Q$ . Osoita, että pisteet  $A$ ,  $B$  ja  $Q$  ovat ympyrällä, jonka keskipiste on  $T$ .



On yleisesti tunnettu fakta, että  $TA = TB$  – toisin sanoen ympyrälle piirretyt tangentit ovat yhtä pitkät. Todistetaan tämä pikaisesti. Huomaa, että tämän todistuksen kannalta pisteet  $X$ ,  $Y$  ja  $Q$  eivät ole oleellisia.

Olkoon  $O$  ympyrän keskipiste. Huomataan seuraavat faktat:

- $\angle OAT = 90^\circ$  tangenttiominaisuuden nojalla.
- $\angle OBT = 90^\circ$  samoin tangenttiominaisuuden nojalla.
- $OA = OB$ , koska nämä janaat ovat ympyrän säteitä.

Näillä huomioilla nähdään, että  $OAT$  ja  $OBT$  ovat suorakulmaisia kolmioita, joilla on yhtä pitkät hypotenuusat ( $OT$ ) ja yhtä pitkät kateetit ( $OA = OB$ ). Täten ne ovat yhteneviä, eli pätee  $TA = TB$ .

Yritetään sitten todistaa, että  $TA = TQ$ , eli kulmaehdoilla muotoiltuna  $\angle QAT = \angle AQT$ . Helpomman oloinen kulma on  $\angle QAT = \angle XAT$ , koska tämä ei vaadi vaikean pisteen  $Q$  käsittelemistä.

Kulma  $\angle XAT$  voidaan kirjoittaa helpommin muotoon

$$\angle XAT = \angle OAT - \angle OAX = 90^\circ - \angle OAX = 90^\circ - \angle OXA = 90^\circ - \angle YXA.$$

Tämän voi vielä kirjoittaa muotoon  $\angle AYZ$  kolmion  $AXY$  kautta. Lauseke ei kuitenkaan tästä enää sievene: voidaan ajatella, että ”tiedämme” kulman  $\angle AYZ$  suuruuden, aivan kuten kolmiotekävissä ”tiedämme” kulmien  $\angle A$ ,  $\angle B$  ja  $\angle C$  suuruudet.

Seuraavaksi pitäisi laskea  $\angle AQT$ . Tämä ei kuitenkaan vaikuta helpolta: emme tiedä, miten pisteet  $Q$  ja  $T$  liittyvät toisiinsa. Ainoat pisteeseen  $Q$  liittyvät kulmat, jotka tiedämme, ovat

$$\angle YQA = 180^\circ - \angle YAQ - \angle AYQ = 90^\circ - \angle AYB$$

ja

$$\angle AQB = 180^\circ - \angle YQA = 90^\circ + \angle AYB,$$

sekä tietysti  $\angle XQB = \angle YQA$ .

Vaikuttaa siltä, ettemme saa laskettua kulmaa  $\angle AQT$ . Olisi kannattanut miettiä vaikeampaa kulmaa ennen helppoa kulmaa  $\angle XAT$ , koska  $\angle XAT$  on aivan turha ilman tietoa kulmasta  $\angle AQT$ .

Mitä nyt tehdään? Pitäisi keksiä jokin toinen tapa saada todistettua, että  $A, Q$  ja  $B$  ovat  $T$ -keskisellä ympyrällä. Ei ole olemassa montaa tapaa todistaa tämän tyyppistä väitettä. Edellisen lisäksi yksi tulee kuitenkin mieleen: kehäkulmalauseen keskuskulmaversio.

Edellä laskimme, että  $\angle AQB = 90^\circ + \angle AYB$ . Haluamme vielä laskea kulman  $\angle ATB$ : kulmista  $\angle ATB$  sen, joka on yli  $180^\circ$ , tulisi olla  $180^\circ + 2\angle AYB$ , eli pienemmän tulee olla  $180^\circ - 2\angle AYB$ .

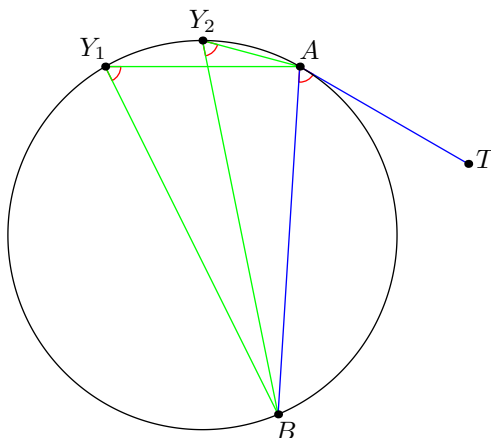
Kolmio  $ABT$  on tasakylkinen, eli jotta  $\angle ATB = 180^\circ - 2\angle AYB$ , tulee olla  $\angle BAT = \angle AYB$ . Huomataan, että tämä väite riippuu enää vain pisteistä  $A, B, Y$  ja  $T$ , eli pisteet  $X$  ja  $Q$  voidaan unohtaa. Lisäksi pisteen  $T$  tarkalla sijainnilla ei ole väliä: oleellista on, että se on pisteeseen  $A$  piirretyllä tangentilla. Todetaan vielä,

että yhtälön  $\angle BAT = \angle AYB$  vasen puoli ei riipu pisteen  $Y$  sijainnista, mutta oikea riippuu.

Käytännössä haluamme todistaa seuraavan tuloksen:

#### Lause (Kehäkulmalauseen tangenttiversio)

Olkoot  $A, B$  ja  $Y$  mielivaltaisia pisteitä ympyrällä. Olkoon  $T$  pisteeseen  $A$  piirretyllä tangentilla. Tällöin pätee  $\angle BAT = \angle BYA$ .



(Tässä pitää jälleen olettaa, että pisteet ovat oikeassa järjestyksessä toisiinsa nähden.)

Väite on uskottavan kuuloinen: jos annamme pisteen  $Y$  mennä lähemmäs ja lähemmäs pistettä  $A$  (kuten  $Y_1$  ja  $Y_2$  kuvassa), niin  $AY$  on lähempänä ja lähempänä yhdensuuntaista tangentin  $AT$  kanssa. Tangenttiversio vastaa siis kehäkulmalauseen tapausta, jossa  $Y = A$ . Tarkka todistaminen sivuutetaan. Väitteen voi kuitenkin todistaa samaan tapaan kuin normaalin kehäkulmalauseen, eikä todistus ole merkittävästi normaalia tapausta vaikeampi. Tämä ratkaisee tehtävän.

### 3.5 Sinilause

Lukiosta tuttu sinilause sanoo seuraavaa.

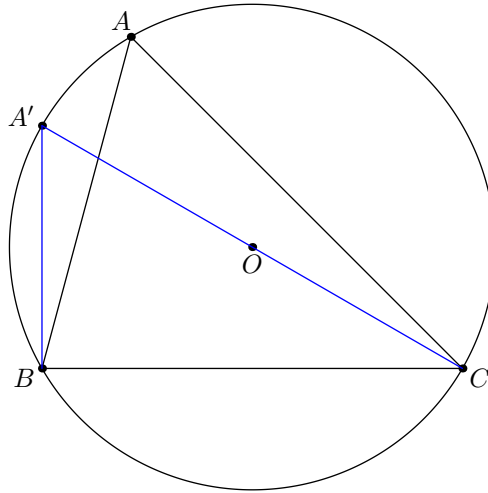
#### Lause (Sinilause)

Olkoon  $ABC$  kolmio, ja olkoon  $R$  sen ympärysympyrän säde. Päte

$$\frac{BC}{\sin(\angle A)} = \frac{AC}{\sin(\angle B)} = \frac{AB}{\sin(\angle C)} = 2R.$$

Usein sinilauseesta ei tarvita sitä tietoa, että nämä kaikki suhteet ovat juurikin  $2R$ . Tämä versio lauseesta on kuitenkin siitä kätevä, että se antaa helpon tavan todistaa lauseen. Tutkitaan alla olevaa kuvaa.





Piste  $A'$  on valittu niin, että  $A'C$  on ympyrän halkaisija. Nyt  $\angle A'BC = 90^\circ$ , joten suorakulmaisesta kolmiosta  $A'BC$  saadaan

$$\sin(\angle BA'C) = \frac{BC}{A'C} = \frac{BC}{2R}.$$

Koska kehäkulmalauseen nojalla  $\angle BA'C = \angle A$ , saadaan nyt  $\frac{BC}{\sin(\angle A)} = 2R$ . Vastavasti saadaan muut sinilauseen yhtälöt.

Sinilause on kätevä silloin, kun halutaan muuttaa kulmia koskevia tietoja sivujen pituuksia koskeviksi tiedoiksi, tai toisin päin. Tästä tullaan näkemään esimerkkejä myöhemmissä geometrian ratkaisuissa. Tässä on toinen näppärä seuraus sinilauseesta: Olkoot  $A, B, X$  ja  $Y$  pisteitä saman ympyrän kehällä. Tällöin janat  $AB$  ja  $XY$  ovat yhtä pitkät täsmälleen silloin, kun kaaria  $\widehat{AB}$  ja  $\widehat{XY}$  vastaavat kulmat ovat yhtä suuret. (Tämä tulos mainittiin jo aiemmin.)

## 4 Geometrian lisämenetelmiä (Geometria)

Tässä luvussa esitetään kehäkulmalauseen ja jännelikulmioiden jälkeen hyödyllisimpiä ja yleisimpiä geometrian menetelmiä. Lisäksi luvussa käydään läpi parin vaativamman tehtävän ratkaisut.

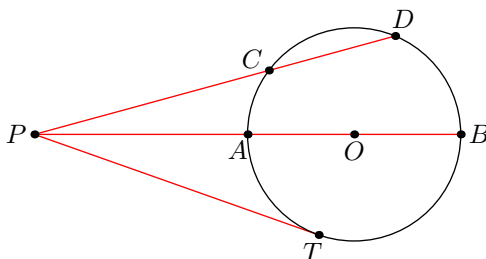
Luku koostuu kahdentyypisistä aiheista: itsenäisistä tuloksista (pisteen potenssi, radikaaliakselit, homotetia, Cevan lause) sekä tietyistä konfiguraatioista (sivuympyrät, yhdeksän pisteen ympyrä). Molemmat ovat tärkeitä kilpailutehtäviä ratkoessa: Monesti tehtävissä tulee ensiksi tehdä (usein melko vaikeita) huomioita kuviosta. Tätä tietysti auttaa, jos on hyvä ote yleisimmistä konfiguraatioista. Erilaisten huomioiden todistamisessa puolestaan tulevat apuun edellä mainitut menetelmät.

### 4.1 Pisteen potenssi ja radikaaliakselit

#### Lause (Pisteen potenssi)

Olkoon  $\Gamma$  ympyrä, ja olkoon  $P$  piste, joka ei ole ympyrän  $\Gamma$  kehällä. Olkoon  $\ell$  suora, joka kulkee pisteen  $P$  kautta ja joka leikkaa ympyrää  $\Gamma$  pisteissä  $A$  ja  $B$ . Pituuksien  $PA$  ja  $PB$  tulo  $PA \cdot PB$  ei riipu suorasta  $\ell$ .

Tätä tuloa  $PA \cdot PB$  kutsutaan pisteen  $P$  potenssiksi.



Kuvassa on esitetty kolme eri tapausta. Yksi tapaus on sellainen, jossa jana  $AB$  on ympyrän halkaisija. Toinen on satunnainen tapaus (pisteet  $C$  ja  $D$ ), ja kolmas tapaus on sellainen, jossa suoraan valitaan ympyrän tangentti. Tulo on siis sama myös silloin, kun valitaan ympyrälle tangentti: tällöin tulo on  $PT \cdot PT$ . Tämän voi perustella intuitiivisesti samaan tapaan kuin kehäkulmalauseen tangenttiversion: Tangentti saadaan valitsemalla jokin ympyrää leikkaava suora  $\ell$  ja kääntämällä se kulkemaan pisteen  $T$  kautta. Suoran  $\ell$  lähestyessä pistettä  $T$  myös suoran ja ympyrän leikkauspisteet  $A$  ja  $B$  lähestyvät pistettä  $T$ . Mitä lähempänä  $A$  ja  $B$  ovat pistettä  $T$ , sitä lähempänä etäisyydet  $PA$  ja  $PB$  ovat etäisyyttä  $PT$ .

Merkitään pisteen  $P$  potenssia ympyrän  $\Gamma$  suhteen merkinnällä  $\text{Pow}_\Gamma(P)$ , jolloin siis  $\text{Pow}_\Gamma(P) = PA \cdot PB$ . Kun  $AB$  on ympyrän  $\Gamma$  halkaisija, niin pätee  $PA = OP - r$  ja  $PB = OP + r$  (tässä  $r$  on ympyrän säde). Siispä

$$\text{Pow}_\Gamma(P) = (OP - r)(OP + r) = OP^2 - r^2.$$

Tämä antaa suoraviivaisen tavan laskea pisteen potenssin.

Pisteen potenssilla saadaan myös todistus Pythagoraan lauseelle: Pätee  $PT^2 = OP^2 - r^2$  eli  $PT^2 + OT^2 = OP^2$ . Pythagoraan lause on todistettu suorakulmaiselle kolmiolle  $POT$ , ja on selvää, että  $POT$  voi olla minkä tahansa suorakulmaisen kolmion muotoinen, eli väite on todistettu kaikille suorakulmaisille kolmioille.

Todistetaan sitten pisteen potenssia koskevat väitteet. Teemme tämän kahdessa osassa.

1. Jos  $C$  ja  $D$  ovat eri pisteitä ympyrän  $\Gamma$  kehällä ja  $AB$  on ympyrän halkaisija, niin  $PA \cdot PB = PC \cdot PD$ .
2. Jos  $PT$  on ympyrän tangentti ja  $AB$  on ympyrän halkaisija, niin  $PA \cdot PB = PT \cdot PT$ .

Todistamalla nämä väitteet saadaan, että kaikki tulot  $PX \cdot PY$  ovat yhtä suuria kuin tulo  $PA \cdot PB$ , mikä todistaa väitteen.

Aloitetaan kohdasta 1. Ideana on, että neljä pistettä ympyrällä antaa paljon tietoa kulmista, ja tämä tieto voidaan muuttaa pituuksia koskevaksi tiedoksi kolmioiden yhdenmuotoisuutta käyttäen. Tämän vuoksi onkin hyödyllistä kirjoittaa haluttu väite muodossa

$$\frac{PA}{PC} = \frac{PD}{PB}.$$

Aiomme siis todistaa, että kolmiot  $PAC$  ja  $PDB$  ovat yhdenmuotoiset.

Ensin huomataan, että kolmioissa  $PAC$  ja  $PDB$  on ainakin yksi sama kulma, nimittäin kärjestä  $P$  lähtevä. Lisäksi jännekelikulmioiden ominaisuuksilla saadaan suoraan

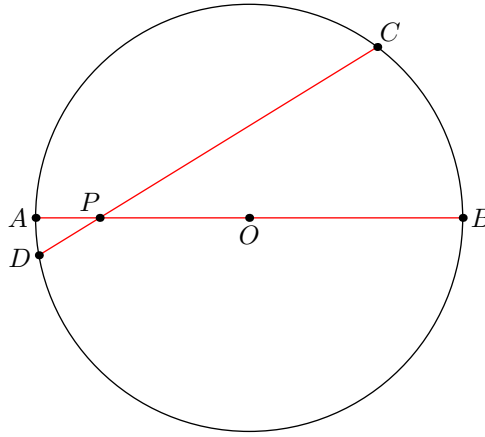
$$\angle PCA = 180^\circ - \angle ACD = 180^\circ - (180^\circ - \angle ABD) = \angle PBD.$$

Siis kolmion  $PAC$  kulma  $\angle C$  vastaa kolmion  $PDB$  kulmaa  $\angle B$ . Kolmioissa  $PAC$  ja  $PDB$  on täten kaksi samaa kulmaparia, joten ne ovat yhdenmuotoiset, mikä todistaa väitteen.

Todistetaan sitten kohta 2. Kuten aiemmin perusteltiin, tämä on tavallaan vain erikoistapaus kohdasta 1, ja siksi myös todistus etenee vastaavalla tavalla. Todistamme, että kolmiot  $PAT$  ja  $PTB$  ovat yhdenmuotoiset. Kuten edellä, kolmioilla on samat kulmat kärjessä  $P$ . Lisäksi kehäkulmalauseen tangenttiversiolla saadaan  $\angle PTA = \angle PBT$ , joka todistaa toisen yhteisen kulmaparin olemassaolon. Väite seuraa kuten yllä.

Todistus demonstroi hyvin, miten yhdenmuotoisilla kolmioilla voi muuttaa kulmaehtoja pituusehdoiksi. Tämä toimii tietysti myös toiseen suuntaan.

Pisteen potenssi toimii myös silloin, kun piste  $P$  on ympyrän sisällä.



Todistus sille, että tulot ovat aina samat, on tässä tapauksessa helpompi kuin aiemmin käsitellyssä tapauksessa (koska eri tapauksia on vähemmän): kehäkulmalauseen perusteella  $\angle ADP = \angle PBC$ , ja lisäksi pätee  $\angle APD = \angle CPB$ . Siis kolmiot  $PAD$  ja  $PCB$  ovat yhdenmuotoiset, ja väite seuraa. Tässä emme tarvitse edes sitä tietoa, että  $AB$  on ympyrän halkaisija.

Tässä tapauksessa on kuitenkin pieni yksityiskohta, joka kannattaa huomioida: jos määrittelemme edelleen pisteen potenssiksi  $\text{Pow}_\Gamma(P) = OP^2 - r^2$ , niin nyt  $\text{Pow}_\Gamma(P)$  on negatiivinen. Tämä on ehkä hieman epäintuitiivista: miksi pituuksien tulo  $PA \cdot PB$  olisi negatiivinen? Yksi selitys on, että mentäessä pisteestä  $P$  pisteisiin  $A$  ja  $B$  joudutaan nyt kulkemaan ”eri suuntiin”, joten jos tutkisimme ns. suunnattuja pituuksia, niin pituuksien  $PA$  ja  $PB$  merkit olisivat vastakkaismerkkiset, ja tulo olisi negatiivinen. Toinen syy sille, miksi määritelmästä  $\text{Pow}_\Gamma = OP^2 - r^2$  kannattaa pitää kiinni, tulee ilmi seuraavaksi radikaaliakseleita käsiteltäessä.

Valitaan tasosta kaksi ympyrää  $\Gamma_1$  ja  $\Gamma_2$ . Missä sijaitsevat ne pisteet  $P$ , joiden pisteen potenssit molempien ympyröiden suhteen ovat samat?

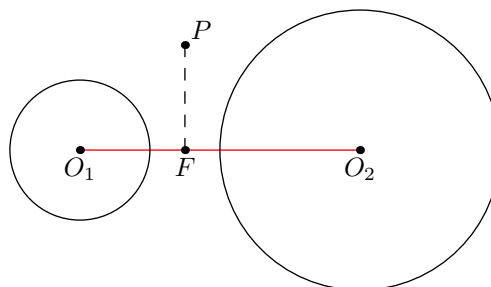
Olko  $r_1$  ja  $r_2$  ympyröiden  $\Gamma_1$  ja  $\Gamma_2$  säteet, ja olko  $O_1$  ja  $O_2$  näiden ympyröiden keskipisteet. Haluamme, että

$$O_1P^2 - r_1^2 = \text{Pow}_{\Gamma_1}(P) = \text{Pow}_{\Gamma_2}(P) = O_2P^2 - r_2^2$$

eli että

$$O_1P^2 - O_2P^2 = r_1^2 - r_2^2.$$

Pituuksien neliöt houkuttelevat käyttämään Pythagoraan lausetta. Tutkitaan seuraavaa kuvaa.



Olkoon siis  $P$  jokin tason piste, ja olkoon  $F$  pisteen  $P$  projektio suoralle  $O_1O_2$ . Olkoot  $x = O_1F$ ,  $y = FO_2$  ja  $PF = h$ . Pythagoraan lauseella voidaan kirjoittaa  $O_1P^2 = x^2 + h^2$  ja  $O_2P^2 = y^2 + h^2$ . Täten yhtälö  $\text{Pow}_{\Gamma_1}(P) = \text{Pow}_{\Gamma_2}(P)$  voidaan kirjoittaa muodossa

$$x^2 - y^2 = r_1^2 - r_2^2.$$

Huomaamme, että  $x^2 - y^2$  on jokin vakio. Mutta  $x^2 - y^2 = (x - y)(x + y)$  ja  $x + y = O_1O_2$  on vakio, joten  $x - y$  on vakio. Tästä seuraa, että pisteen  $F$  sijainti on vakio, eli kaikki pisteet  $P$  sijaitsevat jollain suoralla. Toisaalta kaikki pisteet  $P$ , joiden projektio suoralle  $O_1O_2$  on tämä sopiva  $F$ , toteuttavat ehdon  $\text{Pow}_{\Gamma_1}(P) = \text{Pow}_{\Gamma_2}(P)$ .

Edellinen todistus vaatisi hieman teknisiä yksityiskohtia, jotka on lakaistu maton alle. Todistuksessa ensinnäkin oletettiin, että  $F$  on pisteiden  $O_1$  ja  $O_2$  välissä, jotta saatiin  $x + y = O_1O_2$ . Toiseksi todistuksessa ei missään kohtaa todistettu, että löydetty kelpaava  $F$  on pisteiden  $O_1$  ja  $O_2$  välissä. (Näin ei oikeastaan edes aina ole: jos  $\Gamma_2$  on kokonaan ympyrän  $\Gamma_1$  sisällä, niin radikaaliakseli sijaitsee ympyröiden ulkopuolella.) Nämä yksityiskohdat saa käsiteltyä helposti sijoittamalla pisteet koordinaatistoon ja tätä kautta selvittämällä kelpaavien  $P$  sijainnit. Mitään uusia ideoita todistus ei kuitenkaan vaadi, joten yksityiskohdat sivuutetaan.

Niiden pisteiden  $P$  joukkoa, joilla pätee  $\text{Pow}_{\Gamma_1}(P) = \text{Pow}_{\Gamma_2}(P)$ , kutsutaan ympyröiden  $\Gamma_1$  ja  $\Gamma_2$  radikaaliakseliksi. Todistimme edellä seuraavan tuloksen.

#### Lause (Radikaaliakseli on suora)

Olkoot  $\Gamma_1$  ja  $\Gamma_2$  ympyröitä, joilla on eri keskipisteet. Tällöin niiden radikaaliakseli on suora.

Lauseen oletus siitä, että keskipisteet eivät ole samat, ei aiheuta tehtäviä ratkoessa käytännössä mitään ongelmia. Se on kuitenkin tarpeellinen oletus: jos keskipisteet ovat samat, niin radikaaliakseli joko sisältää kaikki pisteet (jos ympyröiden säteet ovat samat) tai ei mitään pisteitä (jos ympyröiden säteet eivät ole samat).

Mitä radikaaliakselista voidaan sanoa? Ensinnäkin se on kohtisuorassa ympyröiden keskipisteiden  $O_1$  ja  $O_2$  välistä janaa kohden, mikä on selvää symmetrian vuoksi (ja seuraa myös todistuksesta). Lisäksi jos  $\Gamma_1$  ja  $\Gamma_2$  leikkaavat kahdessa pisteessä  $P_1$  ja  $P_2$ , niin  $P_1$  ja  $P_2$  ovat tietysti radikaaliakselilla, koska niiden pisteen potenssit ovat nollia molempien ympyröiden suhteen. Tällöin radikaaliakseli on suora, joka kulkee pisteiden  $P_1$  ja  $P_2$  kautta.

Lopuksi mainitaan vielä yksi radikaaliakseleita koskeva tulos.

#### Lause (Radikaalikeskuksen olemassaolo)

Olkoot  $\Gamma_1, \Gamma_2$  ja  $\Gamma_3$  ympyröitä, joilla on eri keskipisteet. Olkoon  $\ell_1$  ympyröiden  $\Gamma_2$  ja  $\Gamma_3$  radikaaliakseli,  $\ell_2$  ympyröiden  $\Gamma_1$  ja  $\Gamma_3$  radikaaliakseli ja  $\ell_3$  ympyröiden  $\Gamma_1$  ja  $\Gamma_2$  radikaaliakseli. Suorat  $\ell_1, \ell_2$  ja  $\ell_3$  joko ovat kaikki yhdensuuntaisia tai leikkaavat samassa pisteessä.

Lauseen mukaista leikkauspistettä kutsutaan ympyröiden  $\Gamma_1, \Gamma_2$  ja  $\Gamma_3$  radikaalikeskukseksi. Tapaus, jossa  $\ell_1, \ell_2$  ja  $\ell_3$  ovat yhdensuuntaisia, voidaan mieltää niin,

että suorat  $\ell_i$  leikkaavat toistensa kanssa ”äärettömän kaukana” tavallisista pisteistä. Tällaisia tilanteita käsitellään tarkemmin projektiivisen geometrian luvussa. Ideana on, ettei tämä tapaus oikeastaan eroa yleisestä tapauksesta.

Lauseen todistusta varten tutkitaan seuraavia väitteitä:

1. Kolmion  $ABC$  sivujen keskinormaalit leikkaavat samassa pisteessä (kolmion ympärysympyrän keskipiste).
2. Kolmion  $ABC$  kulmanpuolittajat leikkaavat samassa pisteessä (kolmion sisäympyrän keskipiste).
3. Kolmen ympyrän radikaaliakselit leikkaavat samassa pisteessä.

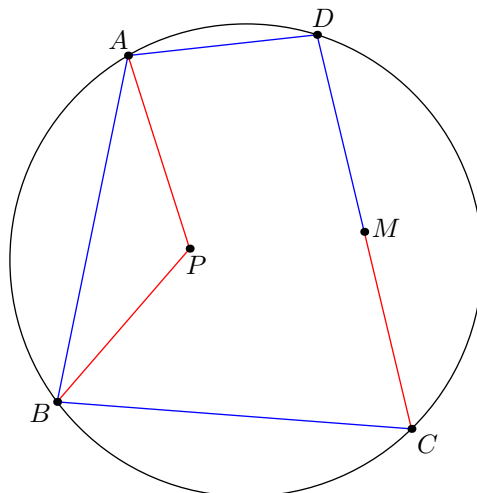
Jokainen näistä tuloksista voidaan todistaa samalla idealla.

1. Olkoon  $P$  sivujen  $AB$  ja  $BC$  keskinormaalien leikkauspiste. Koska  $P$  on sivun  $AB$  keskinormaalilla, pätee  $PA = PB$ . Vastaavasti  $PB = PC$ . Täten  $PA = PC$ , eli  $P$  on sivun  $AC$  keskinormaalilla.
2. Olkoon  $P$  kärkien  $A$  ja  $B$  kulmanpuolittajien leikkauspiste. Koska  $P$  on kulman  $A$  puolittajalla, on  $P$  yhtä kaukana sivuista  $AB$  ja  $AC$ . Vastaavasti  $P$  on yhtä kaukana sivuista  $BA$  ja  $BC$ . Täten  $P$  on yhtä kaukana sivuista  $CA$  ja  $CB$ , eli se on kulman  $C$  puolittajalla.
3. Olkoon  $P$  radikaaliakselien  $\ell_1$  ja  $\ell_2$  leikkauspiste. Koska  $P$  on radikaaliakselilla  $\ell_1$ , pätee  $\text{Pow}_{\Gamma_2}(P) = \text{Pow}_{\Gamma_3}(P)$ . Vastaavasti  $\text{Pow}_{\Gamma_1}(P) = \text{Pow}_{\Gamma_3}(P)$ . Täten  $\text{Pow}_{\Gamma_1}(P) = \text{Pow}_{\Gamma_2}(P)$ , eli  $P$  on radikaaliakselilla  $\ell_3$ .

Ensimmäinen esimerkkitehtävä on vuoden 2016 Baltian tie -kilpailusta.

### Tehtävä

Olkoon  $ABCD$  jännelikulmio, jonka sivut  $AB$  ja  $CD$  eivät ole yhdensuuntaisia. Olkoon  $M$  sivun  $CD$  keskipiste. Olkoon  $P$  sellainen piste jännelikulmion  $ABCD$  sisällä, että  $PA = PB = CM$ . Todista, että  $AB$ ,  $CD$  ja janan  $MP$  keskinormaali kulkevat saman pisteen kautta.



Tehtävän ratkaisu on hyvin yksinkertainen: Olkoon  $\Gamma_1$  jännenelikulmion  $ABCD$  ympärysympyrä,  $\Gamma_2$  ympyrä, jonka säde on  $AP$  ja keskipiste  $P$ , ja  $\Gamma_3$  ympyrä, jonka keskipiste on  $M$  ja säde  $CM$ . Tällöin ympyröiden  $\Gamma_1$  ja  $\Gamma_2$  radikaaliakseli on  $AB$  (koska  $A$  ja  $B$  ovat ympyröiden leikkauspisteet), ja vastaavasti ympyröiden  $\Gamma_1$  ja  $\Gamma_3$  radikaaliakseli on  $CD$ . Täten ympyröiden  $\Gamma_2$  ja  $\Gamma_3$  radikaaliakseli kulkee suorien  $AB$  ja  $CD$  leikkauspisteen kautta radikaalikeskuksen olemassaolon nojalla. Koska ympyröiden  $\Gamma_2$  ja  $\Gamma_3$  säteet ovat samat, on niiden radikaaliakseli nimenomaan janan  $PM$  keskinormaali.

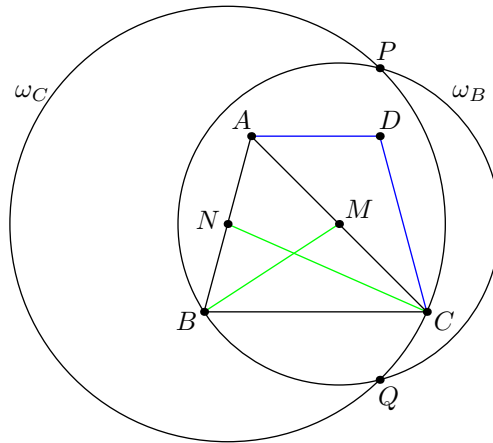
Huomaa, että ratkaisu ei missään kohdassa käyttänyt tietoa siitä, että  $P$  on nelikulmion  $ABCD$  sisällä. Väite pätee myös pisteen  $P$  ollessa nelikulmion ulkopuolella.

Kommentti: Miten tehtävän ratkaisuun voi päätyä? Tehtävässä on monta tekijää, jotka vihjaavat käyttämään radikaaliakseleita: paljon yhtä pitkiä janoja (mistä saadaan ympyröitä) ja kolmen suoran leikkaaminen samassa pisteessä. Lisäksi konfiguraatiossa ei ole paljoakaan asioita, mitä voi tehdä – melkeinpä ainoa lähestymistapa on lisätä  $P$ - ja  $M$ -keskiset ympyrät. Ratkaisu seuraa tämän jälkeen hyvinkin suoraviivaisesti.

Seuraava tehtävä on vuoden 2017 Pohjoismaisesta matematiikkakilpailusta.

### Tehtävä

Olkoot  $M$  ja  $N$  teräväkulmaisen kolmion  $ABC$  sivujen  $AC$  ja  $AB$  keskipisteet, missä  $AB \neq AC$ . Olkoon  $\omega_B$   $M$ -keskinen ympyrä, joka kulkee pisteen  $B$  kautta, ja olkoon  $\omega_C$   $N$ -keskinen ympyrä, joka kulkee pisteen  $C$  kautta. Olkoon  $D$  sellainen piste, että  $ABCD$  on tasakylkinen puolisuunnikas ja  $AD$  on  $BC$ :n suuntainen. Oletetaan, että  $\omega_B$  ja  $\omega_C$  leikkaavat kahdessa (eri) pisteessä  $P$  ja  $Q$ . Osoita, että  $D$  sijaitsee suoralla  $PQ$ .



Heti nähdään, että haluamme pisteen  $D$  olevan ympyröiden  $\omega_B$  ja  $\omega_C$  radikaaliakselilla. On mahdollista<sup>5</sup> laskea suoraan  $\text{Pow}_{\omega_B}(D) = MD^2 - MB^2$  ja  $\text{Pow}_{\omega_C}(D)$ , jolloin tehtävä ratkeaa. Etenemme kuitenkin toisella tavalla.

Mitä radikaaliakselista voidaan sanoa? Kuvasta näyttää siltä, että se on kohtisuorassa suoria  $AD$ ,  $NM$  ja  $BC$  vasten. Todistetaan tämä. Muistetaan, että radikaaliakseli on kohtisuorassa ympyröiden keskipisteiden välistä suoraa vasten, eli tässä tapauksessa  $PQ$  ja  $NM$  ovat kohtisuoria. Koska  $N$  ja  $M$  ovat sivujen  $AB$  ja  $AC$  keskipisteet, pätee  $NM \parallel BC$ . Tämä todistaa aputuloksen.

Jäljellä on enää radikaaliakselin  $PQ$  ”sijainnin” määrittäminen: onko  $PQ$  vaakasuuntaan nähden samassa kohdassa kuin  $D$  (kun jana  $BC$  on  $x$ -akselin suuntainen)? Yksi tapa ratkaista ongelma on käyttää analyyttistä geometriaa eli asetella pisteet koordinaatistoon ja laskea pisteiden koordinaatteja. Tämä idea johtaa ratkaisuun, eikä lähestymistapa edes vaadi kovin raskaita laskuja.<sup>6</sup> Vältämme kuitenkin jälleen mekaanista laskemista ja esitämme erilaisen lähestymistavan.

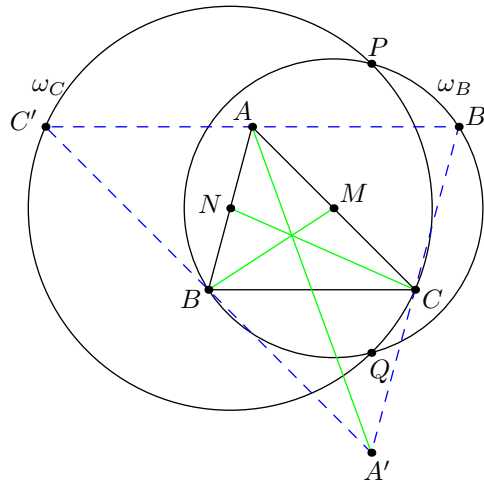
Kuten aiemmin todettiin, pisteen  $D$   $y$ -koordinaatilla ei ole väliä, vaan ainoastaan sen  $x$ -suuntaisella sijainnilla on väliä. Tämän vuoksi on luontevaa korvata  $D$  hieman helpommin käsiteltävällä pisteellä, nimittäin pisteen  $A$  peilauksella sivun  $BC$  keskipisteen yli. Olkoon tämä peilattu piste  $A'$ .

Nyt voidaan huomata mielenkiintoinen kuvio: suora  $AA'$  kulkee mediaanien  $BM$  ja  $CN$  leikkauspisteen kautta. Lisäksi jos määrittelemme ympyrän  $\omega_A$  samaan tapaan kuin ympyrät  $\omega_B$  ja  $\omega_C$ , niin  $AA'$  on sen halkaisija. Tästä motivoituneena peilataan myös pisteet  $B$  ja  $C$  pisteiden  $M$  ja  $N$  yli, jotta saadaan ympyröiden  $\omega_B$  ja  $\omega_C$  halkaisijat.

<sup>5</sup>Ratkaisusta tulee kuitenkin hyvin laskennallinen.

<sup>6</sup>Aivoja ei kuitenkaan kannata heittää narikkaan. Yksi hyvä tapa valita pisteiden koordinaatit on sijoittaa  $B$  origoon  $(0, 0)$ ,  $C$  pisteeseen  $(2c, 0)$  ja  $A$  pisteeseen  $(2a, 2)$ . Nyt  $N = (a, 1)$ ,  $M = (a + c, 1)$  ja  $D = (2c - 2a, 2)$ . Pisteiden  $P$  ja  $Q$  sijainnit saadaan kahden ympyrän leikkauspisteinä. Voimme huijata hieman: tiedämme, että leikkauspisteiden  $x$ -koordinaatit ovat  $2c - 2a$  (tämähän pyydettiin todistamaan), jolloin vähällä vaivalla saadaan myös  $y$ -koordinaatit. Voimme siis kirjoittaa ”Huomataan, että leikkauspisteet ovat  $P = \dots$  ja  $Q = \dots$ ” ja vain sijoittamalla tarkistaa, että nämä pisteet todella ovat ympyröillä  $\omega_B$  ja  $\omega_C$ .

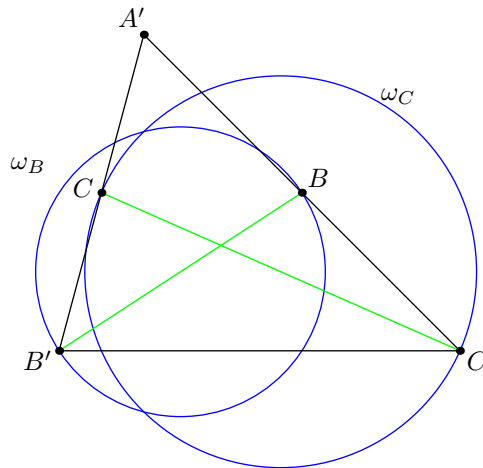




Nyt on hyvä hetki pysähtyä ja tarkastella ongelmaa kolmion  $A'B'C'$  näkökulmasta. Ongelma muuttuu seuraavaan muotoon: ”Janat  $BB'$  ja  $CC'$  ovat kolmion  $A'B'C'$  mediaaneja. Olkoot  $\omega_B$  ja  $\omega_C$  ympyröitä, joiden halkaisijat ovat  $BB'$  ja  $CC'$ . Osoita, että  $A'$  on ympyröiden  $\omega_B$  ja  $\omega_C$  radikaaliakselilla”.

Ongelma ei ehkä vielä ole triviaali, eikä se äkkiseltään edes näytä juurikaan helpommalta kuin alkuperäinen ongelma. Tässä muotoilussa on kuitenkin yksi selvä etu: ongelma koskee pelkästään yhtä kolmiota ja sen mediaaneja, kun taas alkuperäinen ongelma vaati lisäksi pisteen  $D$  tasakylkisen puolisuunnikkaan muodostamiseksi. Tämä muotoilu ongelmosta on siten paljon yksinkertaisempi ja myös luultavasti helpompi.

Tässä on uusi, selkeämpi kuva ongelmosta.



Konfiguraatio alkaa näyttää varsin yksinkertaiselta.

Jotta  $A'$  olisi radikaaliakselilla, tulisi sen pisteen potenssien olla samat molempien ympyröiden  $\omega_B$  ja  $\omega_C$  suhteen. Yksi tapa osoittaa tämä olisi käyttää kaavaa  $\omega_\Gamma(P) = OP^2 - r^2$ . Tässä tapauksessa tämä kaava ei kuitenkaan ole kovin hyödyllinen, koska ei ole helppoa laskea mediaanien pituuksia tai pisteen  $A'$  etäisyyttä mediaanin  $CC'$

keskipisteeseen.<sup>7</sup> Toinen idea on yrittää valita ympyrältä pisteet  $X$  ja  $Y$  siten, että  $A$  on suoralla  $XY$ , ja laskea  $AX \cdot AY$ . Ympyrällä  $\omega_B$  ainoat järkevät kandidaatit pisteeksi  $X$  ovat  $B$  ja  $B'$ . Tästä pääsemme seuraavaan ratkaisuun.

Olkoon  $E$  kärjen  $B'$  korkeusjanan kantapiste. Koska  $\angle B'EB = 90^\circ$ , on  $E$  ympyrällä  $\omega_B$ . Määritellään  $F$  vastaavasti, jolloin  $F$  on ympyrällä  $\omega_C$ . Halutaan osoittaa, että  $A'F \cdot A'C = A'E \cdot A'B$  eli että

$$\frac{A'F}{A'E} = \frac{A'B}{A'C}.$$

Jälkimmäinen osamäärä on sama kuin  $\frac{A'C'}{A'B'}$ , koska kolmiot  $A'BC$  ja  $A'C'B'$  ovat yhdenmuotoisia. Riittää siis osoittaa, että

$$\frac{A'F}{A'E} = \frac{A'C'}{A'B'}.$$

Ortokeskusta koskevista konfiguraatioista tiedämme, että  $B'FEC'$  on jännene-likulmio, joten pisteen potenssilla saadaan  $A'F \cdot A'B' = A'E \cdot A'C'$ , joka voidaan kirjoittaa muodossa

$$\frac{A'F}{A'E} = \frac{A'C'}{A'B'}.$$

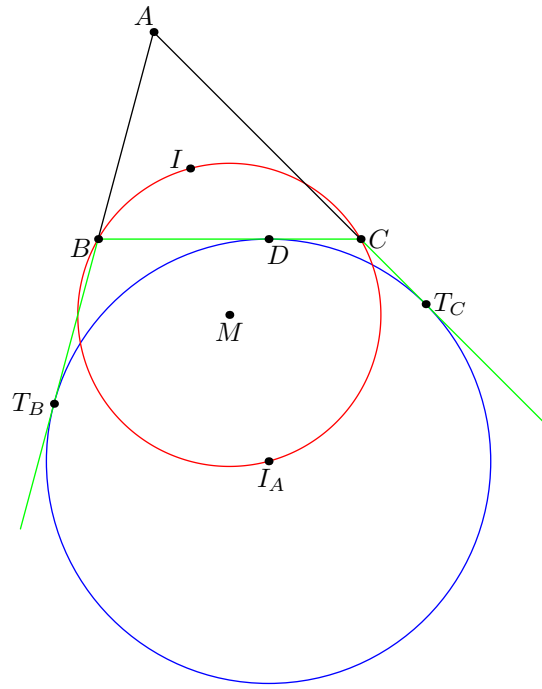
Tämä ratkaisee ongelman.

Kommentti: Ratkaisun vaikein osio vaikuttaisi olevan pisteiden  $A'$ ,  $B'$  ja  $C'$  lisääminen kuvioon. Mistä tämän voisi keksiä? Yksi ajatus on, etteivät tehtävässä valmiiksi olevat pisteet oikein tahdo riittää ongelman ratkaisemiseksi, joten tehtävään on hyvä lisätä uusia pisteitä ("Mitä muutakaan tässä voi tehdä?"). Jos taas ajatuksena on lisätä pisteitä, niin esitetty lisäykset ovat varsin luonnollisia: ongelma pyörii sivujen keskipisteiden ympärillä, joten peilaukset näiden pisteiden yli ovat luonteva idea (varsinkin kun näin saadaan ympyröiden halkaisijoita). Mainittakoon vielä, että usein ensimmäinen yritys ei onnistu, vaan ratkaisua etsiessä täytyy kokeilla monia erilaisia ideoita.

## 4.2 Sivuympyrät ja yhdeksän pisteen ympyrä

Olkoon annettuna kolmio  $ABC$ . Tutkitaan sellaista ympyrää, joka sivuaa sivua  $BC$  sekä sivujen  $AB$  ja  $AC$  jatkeita. Seuraavassa kuvassa on esitetty tämä konfiguraatio.

<sup>7</sup>Mediaanin pituuden voi tosin laskea seuraavasti: Peilataan  $C'$  pisteen  $C$  yli pisteeseen  $C''$ , jolloin  $C''A'C'B'$  on suunnikas. Niin sanottu suunnikaslause sanoo, että suunnikkaan lävistäjien pituuksien neliöiden summa on yhtä suuri kuin suunnikkaan sivujen pituuksien neliöiden summa: tulos seuraa kohtuu suoraviivaisesti kosinilauseesta. Kosinilause opetetaan lukiossa ja sen voi myös etsiä netistä.



Kuvassa siis  $I_A$  on määritellyn ympyrän keskipiste. Tämä ympyrä sivuaa janaa  $BC$  pisteessä  $D$  ja sivujen  $AC$  ja  $AB$  jatkeita pisteissä  $T_B$  ja  $T_C$ . Lisäksi kuvaan on piirretty kolmion  $ABC$  sisäympyrän keskipiste  $I$ .

Entä piste  $M$ ?  $M$  on määritelty olemaan kolmion  $BIC$  ympäri piirretyn ympyrän keskipiste. Edellisessä luvussa huomasimme, että tämä  $M$  on kolmion  $ABC$  ympärysympyrän kaaren  $BC$  keskipiste. Kuten kuvasta nähdään, myös seuraava tulos pätee.

### Lemma

Nelikulmio  $BICI_A$  on jännenelikulmio, jonka ympärysympyrän keskipiste on  $M$ . Lisäksi  $II_A$  on halkaisija tälle ympyrälle.

Mietitään hetki pisteen  $I_A$  ominaisuuksia. Samoin kuin todistimme ympärysympyrän keskipisteen, sisäympyrän keskipisteen ja radikaalikeskuksen olemassaolot, voimme myös todistaa, että  $I_A$  on kulmien  $\angle BAC$ ,  $\angle T_BBC$  ja  $\angle BCT_C$  puolittajien leikkauspiste.

Sitten lemmän todistukseen. Haluamme siis osoittaa, että  $BICI_A$  on jännenelikulmio. Tämän voi tehdä hyvin monella eri tavalla, tässä on yksi: Osoitetaan, että  $\angle I_ABC = \angle I_AIC$ . Ensimmäinen kulma saadaan laskettua edellä esitetyn huomion avulla:

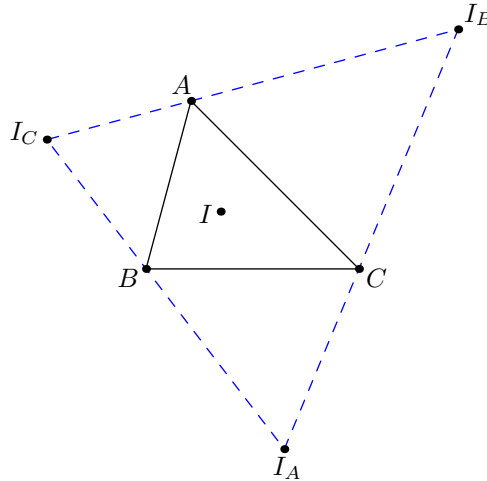
$$\angle I_ABC = \frac{1}{2}\angle T_BBC = \frac{1}{2}(180^\circ - \angle B) = 90^\circ - \frac{1}{2}\angle B.$$

Toista kulmaa varten huomataan ensiksi, että  $\angle I_AIC = \angle MIC$ . Tämä pätee, koska pisteet  $I, M$  ja  $I_A$  ovat kulman  $\angle A$  puolittajalla. Nyt koska  $M$  on kolmion  $BIC$  ympärysympyrän keskipiste, pätee

$$\angle MIC = \frac{1}{2}(180^\circ - \angle IMC) = \frac{1}{2}(180^\circ - 2\angle IBC) = \frac{1}{2}(180^\circ - \angle B) = 90^\circ - \frac{1}{2}\angle B.$$

Täten  $BICI_A$  on jännelikulmio. Lisäksi  $M$  on tietysti sen ympärysympyrän keskipiste ja  $II_A$  on ympyrän halkaisija.

Lemmasta seuraa, että  $\angle IBI_A = \angle ICI_A = 90^\circ$  (mikä seuraa myös suuremmin kulmanpuolittajaominaisuuksista). Tutkitaan seuraavaa konfiguraatiota, johon on merkitty kärkiä  $B$  ja  $C$  vastaavien sivuympyröiden keskipisteet  $I_B$  ja  $I_C$ .



Pätee  $\angle IBI_A = 90^\circ$  ja vastaavasti  $\angle ICI_A = 90^\circ$ . Siis  $\angle I_CBI_A = 180^\circ$ , eli pisteet  $I_C, B$  ja  $I_A$  ovat samalla suoralla. Eikä siinä vielä kaikki: pätee  $\angle I_BBI_C = \angle IBI_C = 90^\circ$ , eli  $I_BB$  on kolmion  $I_AI_BI_C$  korkeusjana. Pisteet  $A, B$  ja  $C$  ovat täten kolmion  $I_AI_BI_C$  korkeusjanojen kantapisteet, ja piste  $I$  on kolmion ortokeskus. Konfiguraatio on siis jo edellisestä luvusta tuttu.

Kehitellään tuloksia vielä eteenpäin. Tutkitaan kolmioita  $I_AI_BI_C$  ja  $ABC$ . Tiedämme, että janan  $II_A$  keskipiste (eli jännelikulmion  $BICI_A$  ympärysympyrän keskipiste)  $M_A$  on  $ABC$ :n ympärysympyrällä. Määritellään  $M_B$  ja  $M_C$  vastaavasti.

Olkoon  $N_A$  janan  $I_BI_C$  keskipiste, jolloin  $N_A$  on jännelikulmion  $I_BCB I_C$  ympärysympyrän keskipiste. Suora lasku antaa

$$\angle AN_AB = \angle I_CN_AB = 2\angle I_CCB = 2\angle ICB = \angle C,$$

eli  $N_A$  on kolmion  $ABC$  ympärysympyrällä.<sup>8</sup> Määritellään  $N_B$  ja  $N_C$  vastaavasti.

Olemme siis todistaneet, että pisteet  $A, B, C, M_A, M_B, M_C, N_A, N_B$  ja  $N_C$  ovat kaikki samalla ympyrällä. Tähän asti kaikkea on tutkittu kolmion  $I_AI_BI_C$  näkökulmasta. Katsomalla tilannetta kolmion  $ABC$  silmin saadaan seuraava tulos.

#### Lause (Yhdeksän pisteen ympyrä)

Olkoon  $ABC$  kolmio. Olkoot  $H_A, H_B$  ja  $H_C$  kolmion  $ABC$  korkeusjanojen kantapisteet ja  $N_A, N_B$  ja  $N_C$  kolmion  $ABC$  sivujen keskipisteet. Olkoon  $H$  kolmion  $ABC$  ortokeskus, ja olkoot  $M_A, M_B$  ja  $M_C$  janojen  $HA, HB$  ja  $HC$  keskipisteet. Tällöin pisteet  $H_A, H_B, H_C, N_A, N_B, N_C, M_A, M_B$  ja  $M_C$  ovat kaikki samalla ympyrällä.

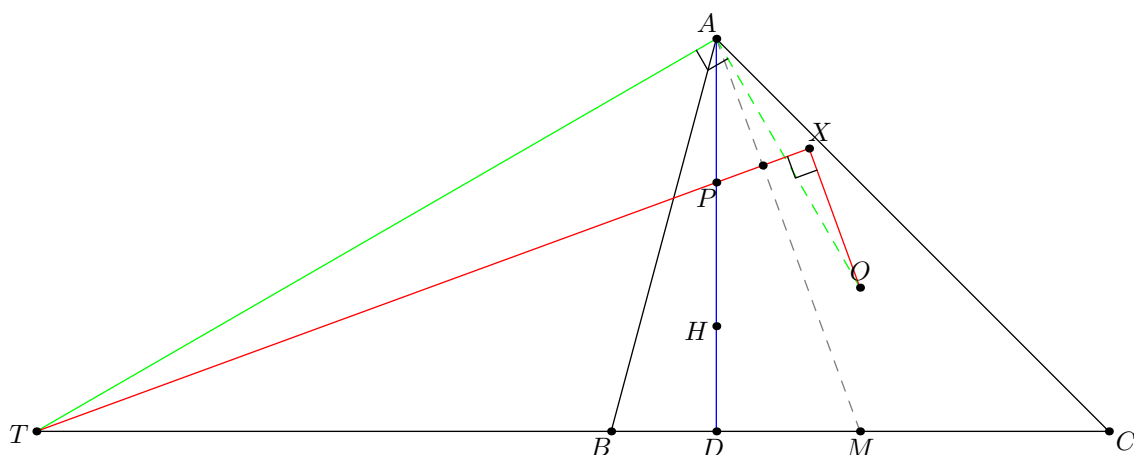
<sup>8</sup>Lisäksi pätee, että  $N_AM_A$  on kolmion  $ABC$  ympärysympyrän halkaisija.

Seuraava vaikea esimerkkitehtävä demonstroi loistavasti, miten tähän asti esiteltyjä geometrian menetelmiä voidaan soveltaa. Tehtävä on vuoden 2018 ELMO-lyhytlistalta.

### Tehtävä

Olkoon  $ABC$  kolmio, ja olkoot  $H$  ja  $O$  sen ortokeskus ja ympärysympyrän keskipiste. Olkoon  $P$  janan  $AH$  keskipiste, ja olkoon  $T$  se piste suoralla  $BC$ , jolla  $\angle TAO = 90^\circ$ . Olkoon  $X$  pisteen  $O$  projektio suoralle  $TP$ . Osoita, että janan  $PX$  keskipiste on kolmion  $ABC$  yhdeksän pisteen ympyrällä.

Tässä on tehtävän konfiguraatiosta kuva, johon on lisätty pari hyödylliseksi osoittautuvaa pistettä.



Olkoon  $Q$  janan  $PX$  keskipiste.

Miten todistetaan, että jokin piste on yhdeksän pisteen ympyrällä? Valitsemalla kyseiseltä ympyrältä jotkin kolme pistettä  $S, T$  ja  $U$  ja osoittamalla, että valitut pisteet ja annettu piste muodostavat yhdessä jännelikulmion. On tietysti monta tapaa valita pisteet  $S, T$  ja  $U$ . Millainen olisi hyvä valinta?

Piste  $P$  on yhdeksän pisteen ympyrällä ja se esiintyy valmiiksi tehtävässä, joten se voisi olla hyvä valinta. Mikään muu tehtävänannon pisteistä ei ole yhdeksän pisteen ympyrällä, joten mietitään muita kriteerejä. Haluamme, että pisteiden  $S, T, U$  ja  $Q$  väliset kulmat ovat laskettavissa. Montaa kandidaattia ei tule mieleen, mutta kärjen  $A$  korkeusjanan kantapiste  $D$  vaikuttaa lupaavalta, koska  $\angle QPD$  liittyy vahvasti tehtävän pisteisiin.

Jos kerran tiedämme, mitä  $\angle QPD$  on, niin haluaisimme neljännen pisteen  $U$  olevan sellainen, että voimme laskea kulman  $\angle DUQ$  suuruuden. Käymällä läpi vaihtoehtoja (korkeusjanojen kantapisteet, sivujen keskipisteet sekä janojen  $BH$  ja  $CH$  keskipisteet) huomataan, että sivun  $BC$  keskipiste  $M$  näyttäisi olevan samalla suoralla kuin pisteet  $A$  ja  $Q$ . Lisäksi huomataan, että tämä suora näyttäisi olevan kohtisuorassa suoraa  $TX$  kohti. Täten piste  $M$  vaikuttaa todella hyvältä valinnalta.

Saimme aikaan edistystä: saimme lisätietoa siitä, mitä tehtävässä tapahtuu ja miten tehtävänannon väitteen voisi todistaa. Toisaalta olemme ongelmissa: mediaanit

ja kulmat ovat haastava yhdistelmä, joten tehtävä ei tule ratkeamaan suoralla kulmanjahtauksella. Saamme kuitenkin jonkinlaisen otteen pisteestä  $M$ . Tiedämme, että  $\angle TMO = \angle BMO = 90^\circ = \angle TXO = \angle TAO$ . Pisteet  $T, A, X, O$  ja  $M$  ovat siis kaikki samalla ympyrällä (jonka halkaisija on jana  $TO$ ).

Työn alla on siis seuraavien väitteiden todistaminen.

1. Pisteet  $A, Q$  ja  $M$  ovat samalla suoralla.
2. Suorat  $AM$  ja  $TX$  ovat kohtisuorassa toisiaan vasten.
3. Kulmien  $\angle DPQ$  ja  $\angle DMQ$  summa on  $180^\circ$ . Olettamalla, että kohta 1 pätee, tämä saadaan muotoon  $\angle DPX + \angle DMA = 180^\circ$ .

Kohtien 1 ja 2 väitteet kannattaa yhdistää seuraavaksi väitteeksi: ”Jana  $AM$  puolittaa janan  $PX$  ja leikkaa tätä kohtisuorasti”. Tämä liittyy aiemmin mainittuun tehtävän ”kuorimiseen”: ongelmat kannattaa aina esittää mahdollisimman lähestyttävässä muodossa. Motivaatio muotoilun takana on se, että on usein helpompaa osoittaa, että jokin jana puolittaa jonkin toisen janan, kuin että kolme pistettä ovat samalla suoralla.

Kohdan 2 väitteestä seuraa, että nelikulmio  $TAQD$  on jännenelikulmio ja että suorat  $AQ$  ja  $XO$  ovat yhdensuuntaiset.

Olettaen kohtien 1 ja 2 väitteet saadaan

$$\angle PTD = \angle QTD = \angle QAD = \angle MAD = \angle AMO = \angle ATO.$$

Kohta 3 seuraa tästä. Kohdan 3 yhtälö  $\angle DPX + \angle DMA = 180^\circ$  voidaan nimittäin muotoilla uudelleen: Ensinnäkin  $\angle DPX = 180 - \angle TPD = 90 + \angle PTD$ . Toiseksi  $\angle DMA = \angle TMA = \angle TOA = 90^\circ - \angle ATO$ , eli haluamme  $\angle PTD = \angle ATO$ . Tämä todistettiin edellä.

Todistettavana on siis seuraava väite: ”Jana  $AM$  puolittaa janan  $PX$  ja leikkaa tätä kohtisuorasti”. Kohtisuoruus on helpompi ehto kuin pituuksia koskeva väite, joten aloitetaan siitä. Tässä vaiheessa voimme unohtaa pisteen  $X$ .

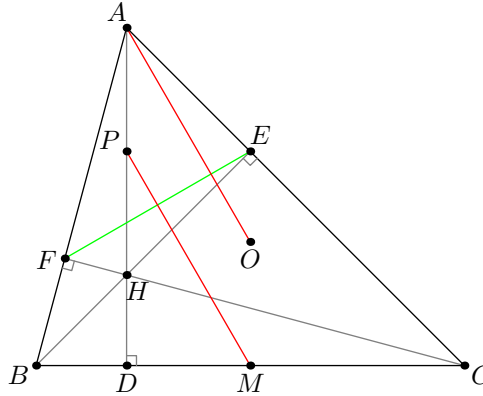
Mitä johtopäätöksiä voitaisiin vetää, jos pätsisi  $AM \perp TP$ ? Huomataan<sup>9</sup>, että tällöin  $P$  olisi kolmion  $AMT$  ortokeskus. Tämä on joustavampi ehto kuin  $AM \perp TP$ , joten käytetään sitä.

Ortokeskusominaisuus seuraa, jos osoitamme, että  $MP \perp AT$ , mikä puolestaan on ekvivalenttia sen kanssa, että suorat  $AO$  ja  $PM$  ovat yhdensuuntaisia. Tämä on hyvä muotoilu ongelmallemme: olemme päässeet kokonaan eroon pisteestä  $T$ . Tutkitaan siis pisteitä  $A, P, M$  ja  $O$ .

Tiedämme, että suorat  $AP$  ja  $MO$  ovat molemmat kohtisuorassa sivua  $BC$  kohden, joten  $AP \parallel MO$ . Ehto  $AO \parallel PM$  tarkoittaisi siis sitä, että nelikulmio  $APMO$  olisi suunnikas. Kulman  $\angle PAO$  voi laskea melko helposti, mutta kulma  $\angle PMO$  on paljon vaikeampi.

<sup>9</sup>Tätä ei tosin ole kovin helppo huomata.

Mietitään hetki ennen kuin jatketaan: mitä pisteistä  $P$  ja  $M$  voidaan sanoa? Ne ovat kyllä joidenkin janojen keskipisteitä, mutta tämä ei ole mielenkiintoisin asia, mitä pisteistä voidaan sanoa. Jos nimittäin  $E$  ja  $F$  ovat kärjistä  $B$  ja  $C$  lähtevien korkeusjanojen kantapisteet,<sup>10</sup> niin  $P$  on jännelikulmion  $AEHF$  ympärysympyrän keskipiste. Vastaavasti  $M$  on jännelikulmion  $BFEC$  ympärysympyrän keskipiste.



Ympyröiden keskipisteiden välinen jana  $PM$  on kohtisuorassa radikaaliakselia vasten. Tässä tapauksessa ympyrät leikkaavat kahdessa pisteessä  $E$  ja  $F$ , joten jana  $PM$  on kohtisuorassa janaa  $EF$  kohden. Enää tulee siis osoittaa, että  $AO$  on kohtisuorassa janaa  $EF$  kohden. Olemme päässeet eroon vaikeasta pisteestä  $P$ , mikä on hyvää edistystä.

Tämä ongelma on jo varsin helppo: pätee

$$\angle OAE = \angle OAC = \frac{1}{2}(180^\circ - \angle AOC) = 90^\circ - \angle B,$$

ja koska  $BCFE$  on jännelikulmio, niin

$$\angle FEA = \angle B,$$

joten väite seuraa.

---

Olemme nyt saaneet todistettua, että  $AM \perp TP$ , ja olemme huomanneet, että tästä seuraa, että  $P$  on kolmion  $TAM$  ortokeskus. Enää halutaan puolittajaominaisuus. Tutkitaan hetki tehtävää kolmion  $TAM$  näkökulmasta: Nyt  $O$  on sellainen piste kolmion  $TAM$  ympärysympyrällä, että  $TO$  on tämän ympyrän halkaisija. Tärkeämpi kysymys on kuitenkin ”mikä piste  $X$  on?”. Myös piste  $X$  on, kuten olemme jo aiemmin todenneet, kolmion  $TAM$  ympärysympyrällä. Lisäksi nyt tiedämme, että se saadaan jatkamalla kärjestä  $T$  lähtevää kolmion  $TAM$  korkeusjanaa tämän kolmion ympärysympyrälle.

Tehtävä on käytännössä palautettu tuttuun tilanteeseen, jossa tutkitaan kolmiota, sen ortokeskusta ja joitain pisteitä tähän liittyen. Tämän ongelman ratkaiseminen ei enää ole vaikeaa.

---

<sup>10</sup>On luontevaa lisätä nämä pisteet konfiguraatioon, koska kuvio sisältää jo ortokeskuksen  $H$ .

Saadaan

$$\angle MAX = \angle MTX = 90^\circ - \angle TMA = 90^\circ - (90^\circ - \angle MAD) = \angle MAP,$$

eli suora  $AM$  on kulman  $\angle PAX$  puolittaja. Täten kolmion  $PAX$  kärjestä  $A$  lähtevä korkeusjana ja kulmanpuolittaja ovat sama suora, joten kolmio on tasakylkinen. Väite on näin todistettu.

Kommentti: Tehtävä on vaikea, ja ratkaisu vaatii monia erilaisia huomioita. Vaikeita tehtäviä ratkoessa korostuu se, että pystyy välillä katsomaan ongelmaa kauempaa: on vaikea kuvitella, että yllä esitettyyn ratkaisuun voisi päätyä ”vahingossa” eli vain tekemällä sokeasti erilaisia havaintoja, vaan ratkaisua keksiessä pitää olla selkeä suunnitelma.

Tehtävässä tuli hyvin ilmi parikin asiaa, jotka ovat tärkeitä geometrian tehtäviä ratkoessa. Ensinnäkin on hyvä keksiä ensin kelvollinen suunnitelma, jota lähtee toteuttamaan.<sup>11</sup> Toiseksi tehtävän ratkaiseminen voi vaatia hyvinkin vaikeita huomioita konfiguraatiosta. Tässä tehtävässä mielestäni vaikeimmin keksittävä huomio oli se, että piste  $P$  on kolmion  $TAM$  ortokeskus. Kolmanneksi: On hyvä olla käsitys siitä, mikä on edistystä eli mitä kannattaa tavoitella. Tässä ratkaisussa tärkeimpiä edistysaskelia olivat vaikeiden pisteiden eliminointi sekä ehtojen kirjoittaminen joustavampaan muotoon.

Tämän tehtävän ratkaisussa korostui vielä ortokeskusten perusominaisuuksien hyödyllisyys.<sup>12</sup> Tähän on nostettu pari hyödyllistä ortokeskusta koskevaa tulosta, jotka tulivat edellisessä ratkaisussa ilmi, mutta joita ei ole mainittu aiemmin. Todistaminen jätetään lukijalle.

### Lemma

Olkoon  $H$  kolmion  $ABC$  ortokeskus. Olkoon  $H'$  pisteen  $H$  peilaus sivun  $BC$  yli, ja olkoon  $H''$  pisteen  $H$  peilaus sivun  $BC$  keskipisteen yli. Tällöin

1. Piste  $H'$  on kolmion  $ABC$  ympärysympyrällä
2. Piste  $H''$  on kolmion  $ABC$  ympärysympyrällä
3. Jana  $AH''$  on kolmion  $ABC$  ympärysympyrän halkaisija.

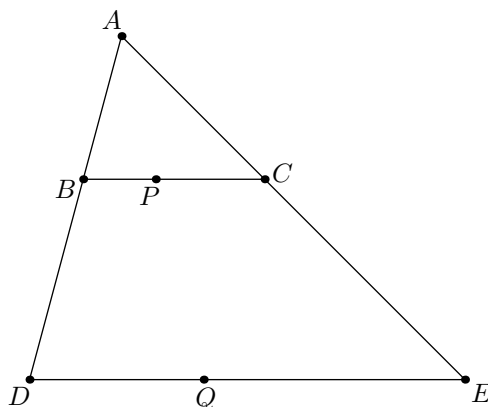
## 4.3 Homotetia

Olkoon  $ABC$  jokin kolmio, ja olkoot  $D$  ja  $E$  sellaisia pisteitä janojen  $AB$  ja  $AC$  jatkeilla, että janat  $BC$  ja  $DE$  ovat yhdensuuntaisia. Olkoon  $P$  sellainen piste janalla  $BC$ , että  $\frac{BP}{PC} = \frac{2}{3}$ , ja olkoon  $Q$  vastaavasti sellainen piste janalla  $DE$ , että  $\frac{DQ}{QE} = \frac{2}{3}$ .

<sup>11</sup>Suunnitelma voi tietysti muuttua matkan varrella.

<sup>12</sup>Mitä hyötyä on vaikean ongelman palauttamisesta helppoon ongelmaan, jos tätä helppoa ongelmaa ei saa ratkaistua?





Intuitio sanoo, että pisteet  $A$ ,  $P$  ja  $Q$  ovat samalla suoralla: kolmio  $ADE$  on vain suurennettu versio kolmiosta  $ABC$ , ja pisteiden  $P$  ja  $Q$  suhteelliset sijainnit ovat samat. Väitteen voi todistaa yhdenmuotoisilla kolmioilla. Yksityiskohdat sivuutetaan tässä.

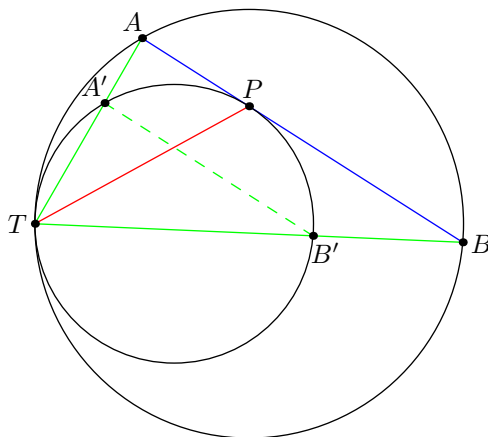
Homotetia mahdollistaa tämänkaltaisen ajatuksen formalisoinnin ja käyttämisen yleisessä tilanteessa. Homotetia on tason kuvaus, eli homotetiassa tason pisteet kuvautuvat toisille tason pisteille. Kuvauksen määrää kaksi muuttujaa: piste ja kerroin. Edellisessä esimerkissä voitaisiin tutkia  $A$ -keskistä homotetiaa, jonka kerroin on  $\frac{AD}{AB}$ . Tämä homotetia ”venyttää” tasoa, jolloin pisteet  $B$  ja  $C$  kuvautuvat pisteiksi  $D$  ja  $E$ . Vastaavasti piste  $P$  kuvautuu pisteeksi  $Q$ .

Homotetian kerroin  $k$  voi myös olla negatiivinen: tällöin pisteen  $P$  kuvaamiseksi ensin peilataan  $P$  homotetian keskuksen  $A$  yli ja sitten kerrotaan etäisyys  $AP$  luvulla  $|k|$ .

Konsepti ei siis ole kovin ihmeellinen. Kyse onkin siitä, miten eri konfiguraatioita kannattaa käsitellä. Tähän liittyen esitetään vuoden 2019 syksyllä valmennustehtävänä olleen ongelman ratkaisu.

### Tehtävä

Kaksi ympyrää sivuaa toisiaan sisäpuolisesti pisteessä  $T$ . Ulomman ympyrän jänne  $AB$  on sisemmän ympyrän tangentti pisteessä  $P$ . Osoita, että suora  $TP$  puolittaa kulman  $\angle ATB$ .



Ajatuksena on, että isompi ympyrä saadaan venyttämällä pienempää ympyrää pisteestä  $T$  nähdessä, eli toisin sanoen on olemassa  $T$ -keskinen homotetia, joka kuvaa pienemmän ympyrän isommaksi ympyräksi. Alla on esitetty väitteelle todistus.

Olkoon  $O_1$  isomman ympyrän keskipiste, ja olkoon  $O_2$  pienemmän ympyrän keskipiste. Valitaan homotetian kertoimeksi  $k = \frac{TO_1}{TO_2}$ . Tulee osoittaa, että jos  $X$  on piste pienemmän ympyrän kehällä, niin se piste  $X'$ , joka on samalla suoralla<sup>13</sup> kuin  $T$  ja  $X$  ja jolla  $TX' = k \cdot TX$ , on isommalla ympyrällä.

Tämä väite voidaan todistaa yhdenmuotoisilla kolmioilla. Tiedämme, että  $\frac{TX}{TO_2} = \frac{TX'}{TO_1}$  ja että  $\angle XTO_2 = \angle X'TO_1$ . Täten kolmiot  $TXO_2$  ja  $TX'O_1$  ovat yhdenmuotoisia. Koska kolmio  $TXO_2$  on tasakylkinen, on kolmio  $TX'O_1$  myös tasakylkinen, joten  $TO_1 = X'O_1$ . Tämä on mitä haluttiinkin.

Tehtävän voi täten ajatella seuraavasti: Valitsemme pieneltä ympyrältä pisteet  $A'$  ja  $B'$ . Piirrämme pienelle ympyrälle tangentin (kuvassa jana  $AB$ ), joka on yhdensuuntainen<sup>14</sup> janan  $A'B'$  kanssa. Olkoon  $P$  tämä tangenttipiste. Haluamme osoittaa, että jana  $TP$  puolittaa janan  $\angle A'TB'$ , eli toisin sanoen että  $P$  on kaaren  $\widehat{A'B'}$  keskipiste.

Tätä ongelmaa voi vielä halutessaan ajatella hieman eri näkökulmasta: valitaan ensiksi piste  $P$  ja piirretään sen kautta kulkeva tangentti, ja valitaan vasta sitten tangentin kanssa yhdensuuntainen ympyrän jänne  $A'B'$ . Pisteen  $P$  tulisi aina olla kaaren  $A'B'$  keskipiste riippumatta siitä, mikä on tangentin ja janteen  $A'B'$  välinen etäisyys.

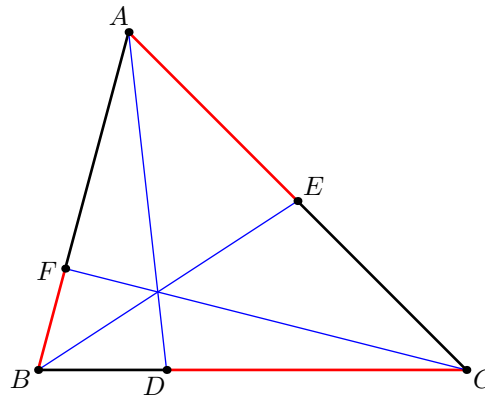
Edelliset huomiot antavat ideoita siihen, miten väitettä kannattaa lähteä todistamaan. Todistus ei ole vaikea: Jos pisteet  $A, B, A'$  ja  $B'$  ovat kuten kuvassa, niin kehäkulmalauseen tangenttiversiolla nojalla  $\angle A'B'P = \angle A'PA$ . Toisaalta koska suorat  $A'B'$  ja  $AB$  ovat yhdensuuntaisia, niin  $\angle PA'B' = \angle A'PA$ . Täten  $\angle A'B'P = \angle PA'B'$ , ja väite seuraa.

## 4.4 Cevan lause ja kolmion merkilliset pisteet

Luvun viimeisessä osiossa esitetään Cevan lause, jonka avulla voidaan todistaa kolmion merkillisten pisteiden olemassaolot.

<sup>13</sup>Ja samalla puolella pistettä  $T$  kuin  $X$ .

<sup>14</sup>Homotetiassahan suora kuvautuu aina suoraksi, joka on yhdensuuntainen alkuperäisen suoran kanssa.



Cevan lause ratkaisee seuraavan ongelman: Kolmion  $ABC$  sivuilla on pisteet  $D$ ,  $E$  ja  $F$ , kukin yhdellä sivulla. Milloin janat  $AD$ ,  $BE$  ja  $CF$  leikkaavat samassa pisteessä?

#### Lause (Cevan lause)

Olkoot  $D$ ,  $E$  ja  $F$  pisteitä kolmion  $ABC$  sivuilla  $BC$ ,  $AC$  ja  $AB$  (tässä järjestyksessä). Janat  $AD$ ,  $BE$  ja  $CF$  leikkaavat samassa pisteessä jos ja vain jos

$$\frac{AF}{FB} \cdot \frac{BD}{DC} \cdot \frac{CE}{EA} = 1.$$

Pisteet  $D$ ,  $E$  ja  $F$  jakavat sivut  $AB$ ,  $BC$  ja  $CA$  yhteensä kuuteen osaan. Cevan lauseen vasemman puolen osoittajissa on joka toinen näistä kuudesta osasta (kuvassa mustalla) ja nimittäjissä loput osat (kuvassa punaisella).

Cevan lauseen voi todistaa ovelasti käyttämällä pinta-aloja. Merkitään kolmion  $XYZ$  pinta-alaa  $[XYZ]$ . Oletetaan ensin, että janat leikkaavat samassa pisteessä  $P$ . Kolmioilla  $BDP$  ja  $CDP$  on sama pisteestä  $P$  lähtevä korkeusjana, joten niiden pinta-alojen suhde on sama kuin kantojen pituuksien suhde:

$$\frac{[PBD]}{[PDC]} = \frac{BD}{DC}.$$

Vastaavalla logiikalla kolmioilla  $ABD$  ja  $ADC$  saadaan

$$\frac{[ABD]}{[ADC]} = \frac{BD}{DC}.$$

Tästä seuraa,<sup>15</sup> että

$$\frac{[ABD] - [PBD]}{[ADC] - [PDC]} = \frac{BD}{DC},$$

eli

$$\frac{[ABP]}{[ACP]} = \frac{BD}{DC}.$$

Samalla tavalla saadaan muille sivuille

$$\frac{[BCP]}{[ABP]} = \frac{EC}{AE}$$

<sup>15</sup>Jos  $\frac{a}{b} = \frac{c}{d}$ , niin  $\frac{a-c}{b-d} = \frac{a}{b}$ . Tämä on helppo tarkistaa auki kertomalla.

ja

$$\frac{[ACP]}{[BCP]} = \frac{FA}{BF}.$$

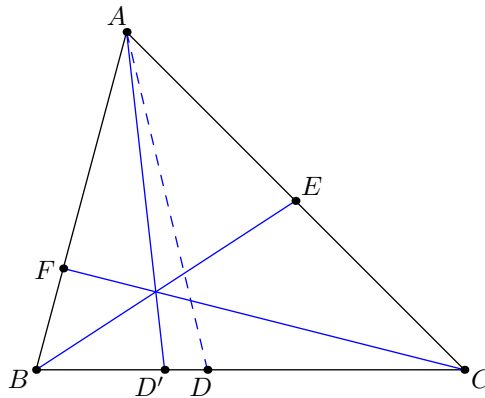
Väite seuraa kertomalla nämä kolme yhtälöä keskenään, koska pinta-alat supistuvat pois.

Olemme nyt todistaneet toisen osan Cevan lauseesta. Esimerkiksi painopisteen olemassaoloa varten mielenkiintoisempi osuus on kuitenkin ”jos sivujen pituudet toteuttavat yhtälön, niin janat  $AD$ ,  $BE$  ja  $CF$  leikkaavat samassa pisteessä”. Tämä saadaan edellisestä osasta yksikäsitteisyysargumentilla.

Oletetaan, että pisteet  $D$ ,  $E$  ja  $F$  on valittu niin, että

$$\frac{AF}{FB} \cdot \frac{BD}{DC} \cdot \frac{CE}{EA} = 1.$$

Jos janat  $AD$ ,  $BE$  ja  $CF$  leikkaavat samassa pisteessä, niin olemme valmiit. Muussa tapauksessa: olkoon  $P$  janojen  $BE$  ja  $CF$  leikkauspiste, ja olkoon  $D'$  janan  $AP$  jatkeen leikkauspiste sivun  $BC$  kanssa.



Cevan lauseen aiemmin todistetun osan nojalla pätee

$$\frac{AF}{FB} \cdot \frac{BD'}{D'C} \cdot \frac{CE}{EA} = 1,$$

joten yhdistämällä tämä pisteen  $D$  tietoihin saadaan

$$\frac{BD}{DC} = \frac{BD'}{D'C}.$$

Tästä seuraa, että  $D = D'$ . Miksi? Suhde  $\frac{BX}{XC}$  kasvaa koko ajan, kun pistettä  $X$  liikutetaan pisteestä  $B$  päin pistettä  $C$  kohti. Täten suhteet  $\frac{BD}{DC}$  ja  $\frac{BD'}{D'C}$  eivät voi olla samat millään kahdella eri pisteellä  $D$  ja  $D'$ , jotka ovat janalla  $BC$ . Tämä todistaa Cevan lauseen toisen puolen.

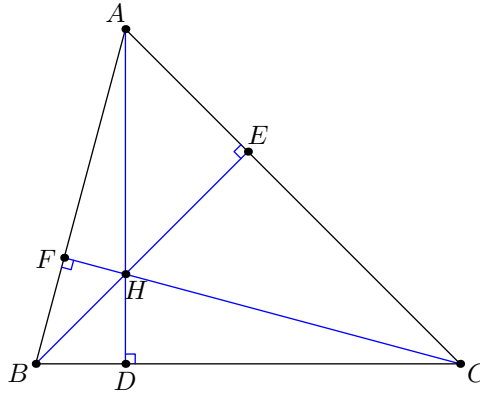
---

Osoitetaan sitten, että kolmion merkilliset pisteet ovat olemassa.

### Painopiste

Painopisteen olemassaolo on varsin triviaali: Cevan lauseen pisteet  $D, E$  ja  $F$  ovat tällöin sivujen keskipisteet, eli pätee  $\frac{AF}{FB} = \frac{BD}{DC} = \frac{CE}{EA} = 1$ , eli näiden suhteiden tulo on myös 1.

### Ortokeskus



Kuten on jo mainittu, tiedämme ortokeskukseen liittyen kaikki kulmat. Täten trigonometrialla tai yhdenmuotoisilla kolmioilla saadaan sivujen pituuksien suhteita. Kolmiot  $BAD$  ja  $BCF$  ovat yhdenmuotoiset, joten

$$\frac{BA}{BD} = \frac{BC}{BF},$$

eli

$$\frac{BF}{BD} = \frac{BC}{AB}.$$

Kirjoittamalla vastaavat lausekkeet kärjille  $A$  ja  $C$  ja kertomalla yhtälöt keskenään nähdään, että Cevan lauseen ehto pätee, mistä väite seuraa.

Edellinen todistus vaatii sen, että kolmio  $ABC$  on teräväkulmainen. Suorakulmaisella kolmiolla ortokeskus sijaitsee suoran kulman kärjessä, ja tylppäkulmaisella kolmiolla ortokeskus on kolmion ulkopuolella. Eri tapauksista on hyvä olla tietoinen, vaikkakin monesti teräväkulmaisille kolmioille toimiva todistus toimii myös suora- ja tylppäkulmaisille kolmioille.<sup>16</sup>

Ortokeskuksen olemassaolon saisi myös tutkimalla kolmion  $DEF$  sisäympyrän keskipistettä (jonka olemassaolon olemme todistaneet jo aiemmin). Kolmion  $DEF$  kulmanpuolittajat leikkaavat kolmion  $ABC$  ortokeskuksessa (mikä seuraa helpolla kulmanjahtauksella). Tämä ei ole yllättävää: aiemmin käsittelimme sivu ympyröiden keskipisteiden muodostamaa kolmiota  $I_AI_BI_C$  ja sen ominaisuuksia, ja huomasimme pisteiden  $A, B$  ja  $C$  olevan kolmion  $I_AI_BI_C$  korkeusjanojen kantapisteet.

### Sisäympyrän ja ympärysympyrän keskipisteet

<sup>16</sup>Tähän liittyy hauska fakta: jos  $H$  on kolmion  $ABC$  ortokeskus, niin  $A$  on kolmion  $HBC$  ortokeskus.

Sisäympyrän olemassaolo todistettiin jo aiemmin, mutta tämän voi todistaa myös Cevan lauseella. Muistellaan lukiosta ns. kulmanpuolittajalauseetta: Olkoon piste  $D$  kolmion  $ABC$  kulman  $\angle A$  puolittajan ja sivun  $BC$  leikkauspiste. Nyt

$$\frac{BD}{DC} = \frac{AB}{AC}.$$

Kulmanpuolittajalause on helpohko seuraus sinilauseesta. Sisäympyrän keskipisteen olemassaolo seuraa kertomalla tätä muotoa olevat yhtälöt keskenään.

Ympärysympyrän keskipisteen olemassaolon voi todistaa teräväkulmaisille kolmioille sinilauseetta käyttämällä. Todistus ei kuitenkaan suoraan yleisty tylppäkulmaisille kolmioille. Helpoin todistus ympärysympyrän keskipisteen olemassaololle onkin aiemmin esitetty keskinormaaleihin perustuva argumentti.

## 5 Projektiivinen geometria (Geometria)

Tässä luvussa esitetään projektiivisen geometrian keskeisimmät työkalut kilpailutehtäviä ajatellen. Luvun tehtävät ovat Evan Chenin kirjan *Euclidean Geometry in Mathematical Olympiads* projektiivista geometriaa käsittelevästä osiosta, ja myös teoriaosioon on otettu vaikutteita Chenin kirjasta.

### 5.1 Perustulokset

Kehäkulmalauseen avulla pystytään jahtaamaan kulmia. Monesti vastaan tulee kuitenkin ongelmia, joita ei saa ratkaistua pelkästään laskemalla kaikkia kulmia. Usein esteenä on, että joillekin kulmille ei ole olemassa mitään yksinkertaista esitystä tunnettujen kulmien avulla. Projektiivinen geometria tarjoaa työkaluja, joilla voidaan ratkaista ongelmia, joihin pelkkä kehäkulmalause ei riitä. (Tällaisia menetelmiä esiteltiin myös edellisessä luvussa.) Karkeasti voisi sanoa, että kehäkulmalauseella voidaan jahdata kulmia ja ns. perspektiivin ottamisella voidaan jahdata pituuksia.

Ensimmäisenä mainitaan pisteet äärettömydessä. Aiemmin kolmen ympyrän radikaaliakseleista puhuttaessa mainittiin, että radikaaliakselit joko leikkaavat kaikki samassa pisteessä tai ovat kaikki yhdensuuntaisia. Tapauskäsittelyn välttämiseksi määritellään piste äärettömydessä. Jos  $\ell$  on suora, niin suoralla  $\ell$  määritellään olemaan sellainen piste  $P_\infty$ , joka on ”äärettömän kaukana” kaikista tason ”normaaleista” pisteistä. Jos kaksi suoraa ovat yhdensuuntaiset, niitä vastaa sama piste äärettömydessä, ja muussa tapauksessa nämä pisteet ovat eri pisteet. Radikaaliakseleita koskevan väitteen voi nyt muotoilla niin, että radikaaliakselit leikkaavat kaikki samassa pisteessä, joka voi olla piste äärettömydessä.

Mennään sitten itse asiaan. Teoria käsittelee paljolti seuraavaksi määriteltävää harmonista suhdetta.

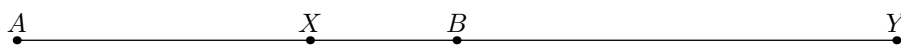
#### Määritelmä

Olkoot  $A, B, X$  ja  $Y$  tason (eri) pisteitä. Niiden harmoniseksi suhteeksi määritellään

$$\frac{\frac{AX}{AY}}{\frac{BX}{BY}}.$$

Tätä merkitään  $(A, B; X, Y)$ .

Määritelmässä pituudet ovat suunnattuja, eli ne voivat olla myös negatiivisia. Jos  $A, B, X$  ja  $Y$  ovat samalla suoralla, niin suhde on negatiivinen täsmälleen silloin, kun tasan yksi pisteistä  $X$  ja  $Y$  on pisteiden  $A$  ja  $B$  välissä. Tästä on esimerkki seuraavassa kuvassa.



Hyvin usein tarkastellaan tilannetta, jossa harmoninen suhde on  $-1$ . Tällöin rajoitutaan yleensä tilanteeseen, jossa  $A, X, B$  ja  $Y$  ovat samalla suoralla tai  $AXBY$

on jänne- nelikulmio. Huomaa, että suora voidaan ajatella ympyränä, jonka keskipiste on sopiva piste äärettömyydessä.

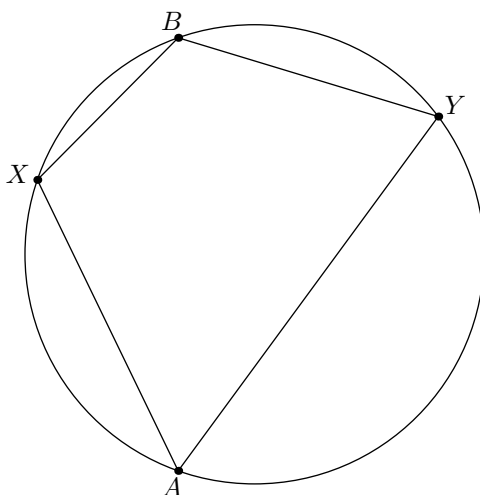
### Määritelmä

Olkoot  $A, B, X$  ja  $Y$  tason (eri) pisteitä, jotka ovat samalla ympyrällä. Sanotaan, että  $A, B, X$  ja  $Y$  muodostavat harmonisen nelikon, jos

$$(A, B; X, Y) = -1.$$

Jos  $A, B, X$  ja  $Y$  ovat samalla ympyrällä, jonka säde on äärellinen, voidaan puhua myös harmonisesta (jänne)nelikulmiosta.

Edellä esitetyssä kuvassa  $A, X, B$  ja  $Y$  muodostavat harmonisen nelikon. Alla on esimerkki harmonisesta nelikulmiosta. Huomaa, että pisteiden  $A, X, B$  ja  $Y$  tulee jälleen olla oikeassa järjestyksessä ympyrän kehällä, eli pisteiden  $X$  ja  $Y$  tulee olla eri puolilla pisteitä  $A$  ja  $B$ . Negatiivisuus käsitellään siis vastaavasti kuin suoran tapauksessa.



Seuraavaksi esitetään harmonisen suhteen ja harmonisten nelikoiden ominaisuuksia. Ensimmäisenä on kehäkulmalauseetta vastaava tulos.

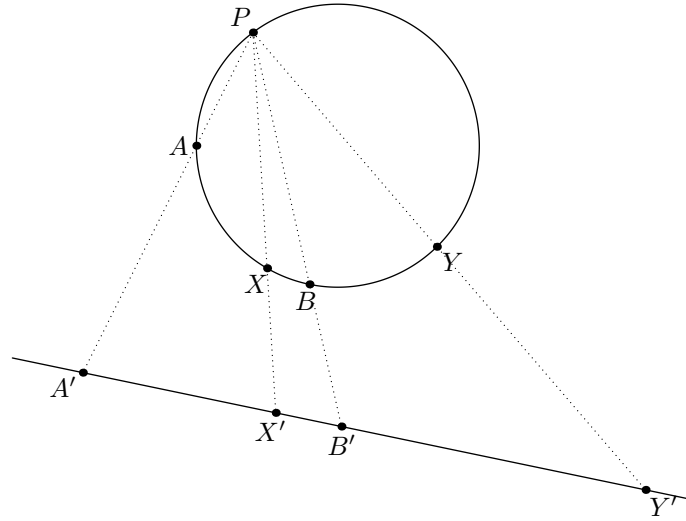
### Lemma

Olkoon  $AXBY$  jänne- nelikulmio, ja olkoon  $P$  piste tällä ympyrällä. Olkoon  $\ell$  jokin tason suora. Olkoon  $A'$  suorien  $AP$  ja  $\ell$  leikkauspiste, ja määritellään  $B', X'$  ja  $Y'$  vastaavasti. Tällöin

$$(A, B; X, Y) \stackrel{P}{=} (A', B'; X', Y').$$

Sanotaan, että ”otamme perspektiivin pisteestä  $P$ ”. Lemmassa merkintä  $\stackrel{P}{=}$  tarkoittaa normaalia yhtäsuuruutta, mutta jossa samalla annetaan tieto siitä, että otamme perspektiivin juurikin pisteen  $P$  kautta.





Väitteen voi todistaa sinilauseella seuraavasti. Kolmiosta  $A'X'P$  saadaan sinilauseella

$$\frac{A'X'}{PA'} = \frac{\sin(\angle A'PX')}{\sin(\angle A'X'P)}.$$

Vastaavasti kolmiosta  $A'Y'P$  saadaan

$$\frac{A'Y'}{PA'} = \frac{\sin(\angle A'PY')}{\sin(\angle A'Y'P)}.$$

Nyt jakamalla ylempi yhtälö alemmalla saadaan

$$\frac{A'X'}{A'Y'} = \frac{\sin(\angle A'PX')}{\sin(\angle A'PY')} \cdot \frac{\sin(\angle A'Y'P)}{\sin(\angle A'X'P)}.$$

Toistamalla edellinen todistus pisteen  $A'$  sijasta pisteelle  $B'$  saadaan

$$\frac{B'X'}{B'Y'} = \frac{\sin(\angle B'PX')}{\sin(\angle B'PY')} \cdot \frac{\sin(\angle B'Y'P)}{\sin(\angle B'X'P)}.$$

Seuraavaksi jaetaan pistettä  $A'$  koskeva yhtälö pistettä  $B'$  koskevalla yhtälöllä. Tällöin osa termeistä supistuu (huomaa, että  $\sin(x) = \sin(180^\circ - x)$ ), ja saadaan

$$\frac{\frac{A'X'}{A'Y'}}{\frac{B'X'}{B'Y'}} = \frac{\frac{\sin(\angle A'PX')}{\sin(\angle A'PY')}}{\frac{\sin(\angle B'PX')}{\sin(\angle B'PY')}}.$$

Tässä vasen puoli on harmoninen suhde  $(A', B'; X', Y')$ .

Olemme siis saaneet laskettua suhteen  $(A', B'; X', Y')$  pisteestä  $P$  lähtevien kulmien avulla. Voimme tehdä vastaavat laskut pisteille  $A, B, X$  ja  $Y$  (käyttäen sievennyksissä apuna kehäkulmalausetta). Saamme täsmälleen saman lausekkeen harmoniselle suhteelle  $(A, B; X, Y)$ . Koska laskut ovat samanlaiset kuin yllä, ne jätetään lukijalle. Täten  $(A, B; X, Y) = (A', B'; X', Y')$ , mikä on haluttu väite.

Kommentti: Sinilause on luotu muuttamaan kulmaehtoja pituusehdoiksi (ja toisin päin), ja sitä tullaan soveltamaan myös myöhempien tulosten todistuksissa. Todistus onkin hyvin luonnollinen. Ensin lasketaan sopiva pituuksien  $A'X'$ ,  $A'Y'$ ,  $B'X'$  ja  $B'Y'$  suhde ”tunnettujen kulmien” eli  $P$ :stä lähtevien kulmien avulla. Tämän jälkeen vastaava suhde lasketaan pisteille  $A, B, X$  ja  $Y$ .

Aivan vastaavaan tapaan kuin edellä voidaan todistaa seuraava väite, joka myös koskee perspektiivin ottamista.

### Lemma

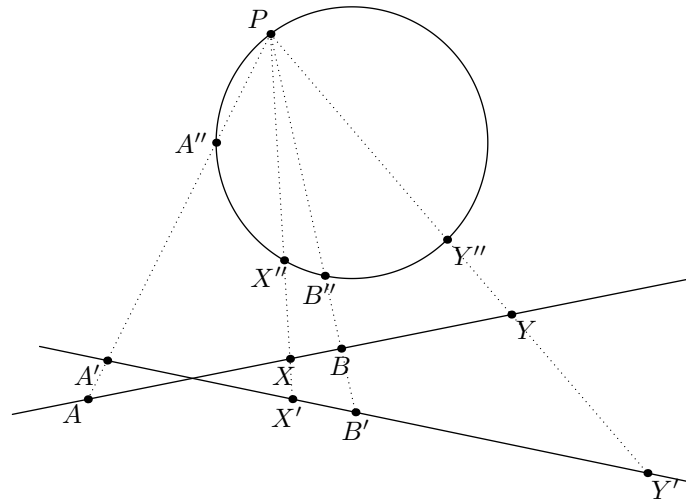
Olko  $A, B, X$  ja  $Y$  pisteitä, jotka ovat samalla suoralla  $\ell$ . Olkoon  $P$  jokin piste suoran  $\ell$  ulkopuolella. Olkoon  $\ell'$  jokin suora, ja olkoon  $A'$  suorien  $AP$  ja  $\ell'$  leikkauspiste. Määritellään pisteet  $B', X'$  ja  $Y'$  vastaavasti. Tällöin pätee

$$(A, B; X, Y) \stackrel{P}{=} (A', B'; X', Y').$$

Tämä tulos oikeastaan seuraa edellä mainitusta lemmasta. Yksi<sup>17</sup> ratkaisu on piirtää ympyrä, jonka kehällä on piste  $P$ , ja määritellä  $A''$  olemaan suoran  $AP$  leikkauspiste tämän ympyrän kanssa. Määritellään pisteet  $B'', X''$  ja  $Y''$  vastaavasti, jolloin käyttämällä ensimmäistä lemmaa saadaan

$$(A, B; X, Y) \stackrel{P}{=} (A'', B''; X'', Y'') \stackrel{P}{=} (A', B'; X', Y'),$$

ja väite seuraa.



Mainitaan vielä, että perspektiivin voi ottaa myös seuraavasti: Tutkitaan ympyrää, jolla on jänneet  $AA', BB', XX'$  ja  $YY'$ , jotka leikkaavat pisteessä  $P$ . Tällöin  $(A, B; X, Y) \stackrel{P}{=} (A', B'; X', Y')$ .<sup>18</sup>

<sup>17</sup>Tuntuu hieman hassulta, että perspektiivin ottaminen pitää perustella eri tavoilla suorien ja ympyröiden tapauksissa. (Totesimmehan aiemmin, että suorat ovat vain äärettömän suuria ympyröitä.) Ehkäpä parempi selitys ilmiölle voidaan antaa Möbius-kuvausten avulla. Möbius-kuvaukset ovat kompleksitason kuvaukset muotoa  $z \rightarrow \frac{az+b}{cz+d}$ , missä  $a, b, c$  ja  $d$  ovat vakioita. Suorat ja ympyrät kuvautuvat Möbius-kuvauksissa joko suoriksi tai ympyröiksi, ja lisäksi kuvaus säilyttää harmonisen suhteen.

<sup>18</sup>Myös tämän voi perustella Möbius-kuvauksilla.

## 5.2 Keskeiset tulokset

Seuraavaksi esitetään, mistä harmonisia nelikkoja löytää käytännössä.

Ensimmäinen tulos yhdistää janojen keskipisteet ja yhdensuuntaiset suorat. Tässä yhdensuuntaisia suoria edustaa niiden leikkauspiste äärettömyydessä. Tämän tuloksen hyödyllisyys tulee paremmin esiin myöhemmin esimerkkitehtävien yhteydessä.

### Lemma

Olkoot  $A$  ja  $B$  (eri) pisteitä. Olkoon  $M$  janan  $AB$  keskipiste, ja olkoon  $P_\infty$  suoraa  $AB$  vastaava piste äärettömyydessä. Tällöin

$$(A, B; M, P_\infty) = -1.$$

Väite seuraa suoraan määritelmästä: saadaan

$$(A, B; M, P_\infty) = \frac{\frac{AM}{AP_\infty}}{\frac{BM}{BP_\infty}}.$$

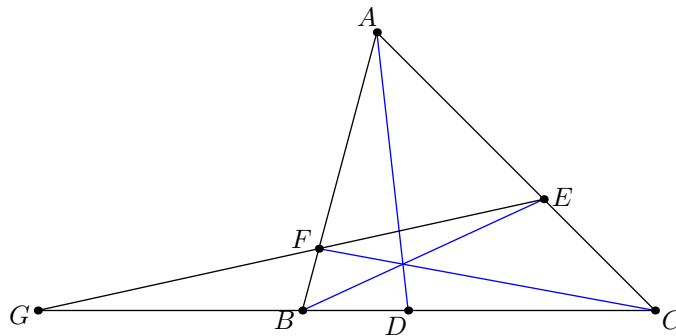
Pätee  $AM = BM$ , ja lisäksi  $AP_\infty = BP_\infty = \infty$ .<sup>19</sup> Koska  $M$  on pisteiden  $A$  ja  $B$  välissä ja  $P_\infty$  ei ole, niin etumerkiksi tulee miinus.

Seuraavat tulokset ovat epätriviaalimpia.

### Lemma

Olkoon  $ABC$  kolmio, ja olkoot  $D, E$  ja  $F$  sellaisia pisteitä janoilla  $BC, AC$  ja  $AB$ , että  $AD, BE$  ja  $CF$  leikkaavat samassa pisteessä. Olkoon  $G$  suorien  $EF$  ja  $BC$  leikkauspiste. Tällöin

$$(B, C; G, D) = -1.$$



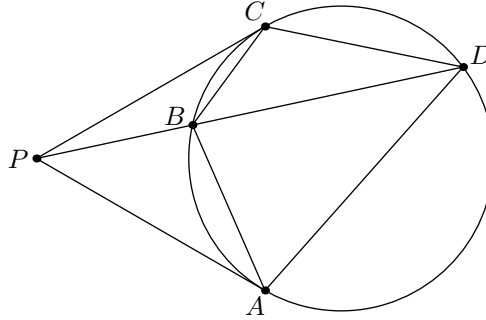
Todistuksen ideana on käyttää Cevan lausetta pisteille  $D, E$  ja  $F$ , ja Menelaoksen lausetta<sup>20</sup> pisteille  $G, F$  ja  $E$ . Väite seuraa vertaamalla näistä saatuja yhtälöitä.

<sup>19</sup>Voi olla vakuuttavampaa ajatella raja-arvoa  $\lim_{P \rightarrow P_\infty} \frac{AP}{BP}$ , missä  $P$  kulkee suoraa  $AB$  pitkin kohti pistettä  $P_\infty$ . Tämä raja-arvo on muotoa  $\lim_{x \rightarrow \infty} \frac{x}{x+c}$ , joka on 1.

<sup>20</sup>Menelaoksen lause sanoo seuraavaa: Olkoon  $ABC$  kolmio. Olkoon  $G$  piste suoralla  $BC$ ,  $E$  piste

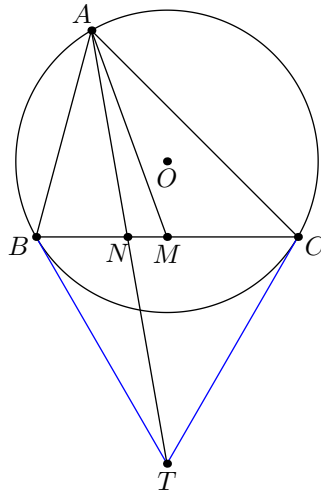
**Lemma**

Olkoon  $ABCD$  jännelikulmio.  $ABCD$  on harmoninen jos ja vain jos pisteisiin  $A$  ja  $C$  piirretyt tangentit leikkaavat suoralla  $BD$ .



Huomaa, että ehdossa voitaisiin symmetrian vuoksi tutkia myös pisteisiin  $B$  ja  $D$  piirrettyjä tangentteja.

Lemman todistamista varten tutkitaan yleisempää ns. symmediaaneja koskevaa tilannetta.

**Lemma**

Olkoon  $T$  kolmion  $ABC$  ympärysympyrän pisteisiin  $B$  ja  $C$  piirrettyjen tangenttien leikkauspiste. Olkoon  $M$  se janan  $BC$  piste, jolla  $\angle BAT = \angle MAC$ . Tällöin  $M$  on janan  $BC$  keskipiste.

suoralla  $AC$  ja  $F$  piste suoralla  $AB$ . Nyt pisteet  $G, E$  ja  $F$  ovat samalla suoralla jos ja vain jos

$$\frac{AF}{FB} \cdot \frac{BG}{GC} \cdot \frac{CE}{EA} = -1,$$

missä pituudet ovat jälleen kerran suunnattuja (mikä tarkoittaa sitä, että parillisen määrän pisteistä  $G, F$  ja  $E$  tulee olla kolmion sivuilla eikä niiden jatkeilla).

Suoraa  $AT$  kutsutaan kolmion  $ABC$  (kärjestä  $A$  lähteväksi) symmediaaniksi.

Symmediaanilemmän todistuksen ideana on käyttää sinilauseetta ja muuttaa kulmaehtoja pituusehdoiksi (kuten perspektiiviä otettaessa). Kirjoitetaan  $\alpha = \angle BAN$  ja  $\beta = \angle NAM$ , missä  $N$  on, kuten kuvaan on piirretty, janojen  $AT$  ja  $BC$  leikkauspiste.

Kolmiosta  $ABM$  saadaan

$$\frac{AM}{BM} = \frac{\sin(\angle B)}{\sin(\alpha + \beta)},$$

ja kolmiosta  $ACM$  saadaan vastaavasti

$$\frac{AM}{CM} = \frac{\sin(\angle C)}{\sin(\alpha)}.$$

Jakamalla ylempi yhtälö alemmalla saadaan

$$\frac{CM}{BM} = \frac{\sin(\angle B)}{\sin(\angle C)} \cdot \frac{\sin(\alpha)}{\sin(\alpha + \beta)}.$$

Haluamme, että tämä tulo on 1.

Kulmiin  $\alpha$  ja  $\alpha + \beta$  päästään käsiksi kolmioista  $ABT$  ja  $CBT$ . Kolmiosta  $ABT$  saadaan nimittäin

$$\frac{AT}{BT} = \frac{\sin(\angle TBA)}{\sin(\alpha)} = \frac{\sin(\angle C)}{\sin(\alpha)}.$$

Tässä jälkimmäisen yhtäsuuruuden saamiseksi on käytetty kehäkulmalauseen tangenttiversiosta saatavaa tulosta  $\angle TBC = \angle A$  sekä tietoa  $\sin(\angle A + \angle B) = \sin(\angle C)$ . Vastaavasti saadaan

$$\frac{AT}{CT} = \frac{\sin(\angle C + \angle A)}{\sin(\alpha + \beta)}.$$

Symmediaanilemmän väite seuraa huomaamalla, että  $BT = CT$  ja  $\sin(\angle C + \angle A) = \sin(\angle B)$ .

Harmonisen jännekelikulmion tangentteja koskevan lemmän todistamista varten tarvitsemme vielä toisen tiedon symmediaaneista. Osoitetaan, että pätee

$$\frac{BN}{NC} = \left( \frac{AB}{AC} \right)^2.$$

(Vrt. kulmanpuolittajalause.) Käytetään samaa notaatiota kuin yllä.

Kolmioista  $ABN$  ja  $ANC$  saadaan sinilauseella

$$\frac{BN}{AN} = \frac{\sin(\alpha)}{\sin(\angle B)}$$

ja

$$\frac{NC}{AN} = \frac{\sin(\alpha + \beta)}{\sin(\angle C)}.$$

Täten

$$\frac{BN}{NC} = \frac{\sin(\alpha)}{\sin(\alpha + \beta)} \cdot \frac{\sin(\angle C)}{\sin(\angle B)}.$$

Toisaalta kolmioista  $ABM$  ja  $AMC$  saadaan niin ikään sinilauseella

$$\frac{BM}{AM} = \frac{\sin(\alpha + \beta)}{\sin(\angle B)}$$

ja

$$\frac{MC}{AM} = \frac{\sin(\alpha)}{\sin(\angle C)}.$$

Koska  $BM = MC$ , kahdesta edellisestä yhtälöstä saadaan

$$\frac{\sin(\alpha + \beta)}{\sin(\alpha)} = \frac{\sin(\angle B)}{\sin(\angle C)}.$$

Siis  $BN/NC = (AB/AC)^2$  seuraa nyt sinilauseella kolmiosta  $ABC$ .

Todistetaan sitten alkuperäinen lemma. Oletetaan, että  $ABCD$  on harmoninen jännelikulmio, ja osoitetaan, että suora  $BD$  kulkee pisteisiin  $A$  ja  $C$  piirrettyjen tangenttien leikkauspisteen kautta. Tehdään tämä osoittamalla, että kolmioiden  $ABC$  ja  $ADC$  kärjistä  $B$  ja  $D$  piirretyt symmediaanit leikkaavat janan  $AC$  samassa kohdassa. Jos  $N_B$  ja  $N_D$  kuvaavat näiden symmediaanien ja janan  $AC$  leikkauspisteitä, niin käyttäen edellistä tulosta ja harmonisuutta saadaan

$$\frac{AN_B}{N_BC} = \left(\frac{BA}{BC}\right)^2 = \left(\frac{DA}{DC}\right)^2 = \frac{AN_D}{N_DC},$$

mistä seuraa  $N_B = N_C$  (kuten Cevan lauseen todistuksessa). Tämä todistaa toisen puolen lemmasta.

Toinen puoli lemmasta sanoo, että jos pisteisiin  $A$  ja  $C$  piirretyt tangentit leikkaavat suoralla  $BD$ , niin jännelikulmio  $ABCD$  on harmoninen. Tämä seuraa helposti yksikäsitteisyysargumentilla (kuten mm. kehäkulmalauseen ja Cevan lauseen vain jos -puolet), jonka yksityiskohdat jätetään lukijalle.

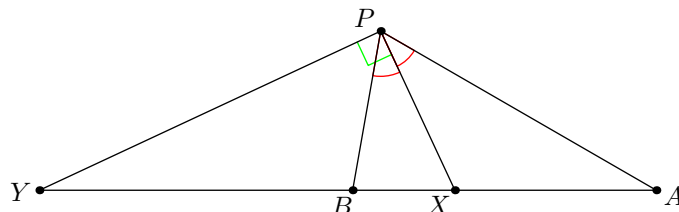
Viimeisenä mainittava tulos on myös varsin hyödyllinen.

### Lemma

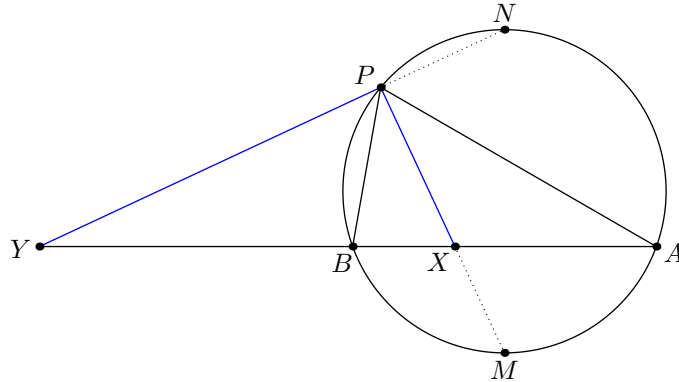
Olkoot pisteet  $A, X, B$  ja  $Y$  suoralla tässä järjestyksessä, ja olkoon  $P$  piste tämän suoran ulkopuolella. Jos mitkä tahansa kaksi seuraavista väitteistä pätevät, niin myös kolmaskin pätee.

1.  $(A, B; X, Y) = -1$ .
2.  $PX$  puolittaa kulman  $\angle APB$ .
3.  $\angle XPY = 90^\circ$ .

Lemman tilanne on esitetty seuraavassa kuvassa.



Tuloksen voi todistaa käyttäen sinilausetta. Esitetään kuitenkin hieman projektiivista geometriaa käyttävä ratkaisu. Todistuksen ideana on täydentää kuvaan kolmion  $ABP$  ympärysympyrä ja suorien  $PX$  ja  $PY$  leikkauspisteet tämän ympyrän kanssa.<sup>21</sup> Ongelma palautuu kohtalaisen tutun kuvion käsittelemiseen.



Oletetaan ensiksi, että  $\angle XPY = 90^\circ$ . Tutkitaan nyt kahta tapausta lemmän mukaisesti. Molemmissa tapauksissa on ideana ottaa ensiksi perspektiivi suoralta  $AY$  ympyrälle pisteestä  $P$ , jolloin

$$(A, B; X, Y) \stackrel{P}{=} (A, B; M, N).$$

Tämän jälkeen todistukset jakautuvat eri suuntiin.

1. Oletetaan, että pätee  $\angle BPX = \angle XPA$ . Tällöin  $M$  on pienemmän kaaren  $\widehat{AB}$  keskipiste ja  $N$  on suuremman kaaren  $\widehat{AB}$  keskipiste. Nyt  $\frac{AM}{BM} = 1$  ja  $\frac{AN}{BN} = 1$ , joten harmonisen suhteen määritelmästä saadaan  $(A, B; M, N) = -1$ , eli edellisen nojalla  $(A, B; X, Y) = -1$ .
2. Oletetaan, että pätee  $(A, B; X, Y) = -1$  eli  $(A, B; M, N) = -1$ . Oletuksen  $\angle XPY = 90^\circ$  nojalla  $MN$  on aina ympyrän halkaisija. Ei ole vaikeaa nähdä, että jos tätä halkaisijaa  $NM$  kääntää kuvassa esitetystä tilanteesta, niin jompikumpi suhteista  $\frac{AM}{AN}$  ja  $\frac{BM}{BN}$  on suurempi kuin toinen. (Vaihtoehtoisesti voitaisiin käyttää edellistä lemmaa, josta saadaan suoraan, että halkaisijalle on vain yksi vaihtoehto.) Pisteet  $M$  ja  $N$  ovat täten lyhyemmän ja pidemmän kaaren  $\widehat{AB}$  keskipisteet, mistä väite seuraa.

Enää tulee osoittaa, että jos  $\angle BPX = \angle XPA$  ja  $(A, B; X, Y) = -1$ , niin pätee  $\angle XPY = 90^\circ$ . Tämä seuraa kuten edellä: Nyt  $M$  on pienemmän kaaren  $\widehat{AB}$  keskipiste, joten ehdosta  $(A, B; X, Y) = -1$  seuraa, että  $N$  on suuremman kaaren  $\widehat{AB}$  keskipiste. Täten  $\angle MPN = 90^\circ$ , eli  $\angle XPY = 90^\circ$ .

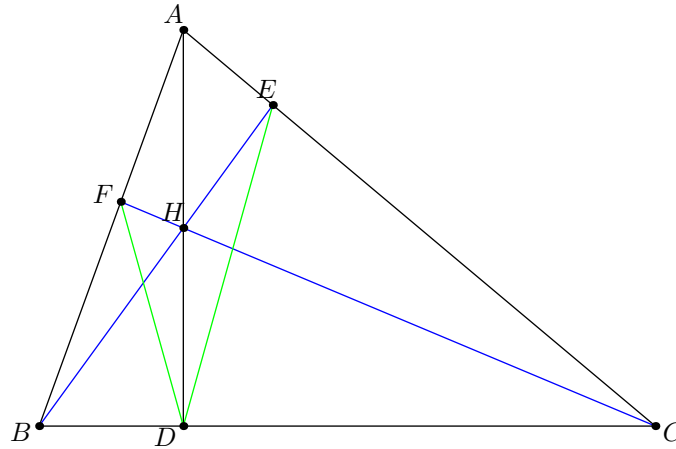
<sup>21</sup>Tätä ei ole kovin helppoa keksiä itse. Keksin tämän lähestymistavan ratkoessani projektiiviseen geometriaan liittyvää tehtävää, jossa vastaavanlainen konfiguraatio oli jo annettuna. Väitettä ei tämän huomion jälkeen ole enää kovin vaikeaa todistaa, koska jokainen yksittäinen lemmän tapaus on kohtuu suoraviivainen.

### 5.3 Esimerkkitehtäviä

Ensimmäinen tehtävä demonstroi tulosten soveltamista käytännössä. Tehtävä on Kanadan kansallisesta kilpailusta vuodelta 1994.

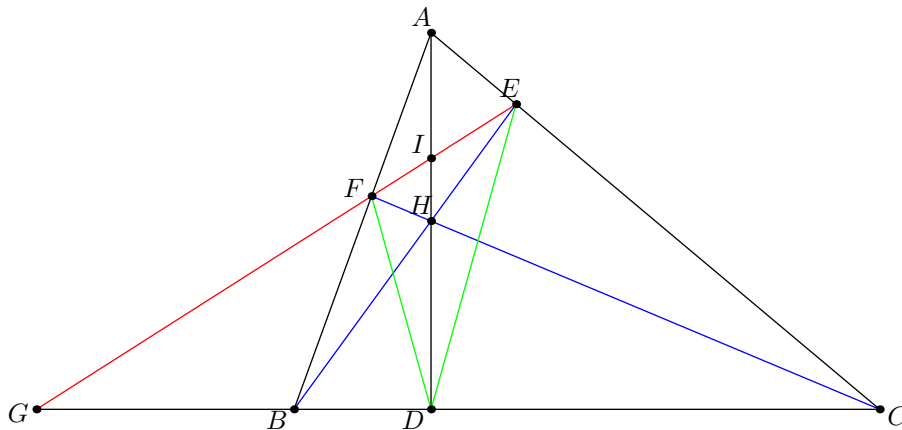
#### Tehtävä

Olkoon  $ABC$  teräväkulmainen kolmio. Olkoon  $AD$  pisteestä  $A$  piirretty korkeusjana, ja olkoon  $H$  mielivaltainen piste janalla  $AD$ . Olkoot  $E$  ja  $F$  suorien  $BH$  ja  $CH$  leikkauspisteet kolmion  $ABC$  sivujen kanssa. Osoita, että  $\angle EDH = \angle FDH$ .



Naiivi lähestymistapa olisi yrittää jahdata kuviosta kulmia. Jos  $H$  olisi ortokeskus, niin tämä onnistuisi hyvinkin helposti jännelikulmioita käyttämällä, mutta tehtävän tilanteessa yksinkertainen kulmanjahtaus ei toimi.

Mikä avuksi? Tehtävässä oleellista on (ilmeisesti) se, että  $D$  on nimenomaan korkeusjanan kantapiste, eikä vaikkapa janan  $BC$  keskipiste. Yritetään siis hyödyntää tietoa siitä, että  $\angle BDH = 90^\circ$ . Huomataan, että viimeisen lemmän nojalla ehto  $\angle FDH = \angle HDE$  voidaan muotoilla uudelleen harmonisten nelikoiden avulla. Tutkitaan siis suoraa  $FE$  tarkemmin.





Olkoon siis  $I$  janan  $FE$  leikkauspiste janan  $AH$  kanssa ja  $G$  suorien  $FE$  ja  $BC$  leikkauspiste. Haluamme osoittaa, että  $(F, E; I, G) = -1$ . Alamme siis metsästämään kuvasta harmonisia nelikoita. Muistetaan, että olemme nähneet vastaavanlaisen kuvion aiemmin: yksi lemmostahan on, että  $(B, C; D, G) = -1$ . Tästä ei enää ole vaikeaa huomata, että

$$(B, C; D, G) \stackrel{A}{=} (F, E; I, G),$$

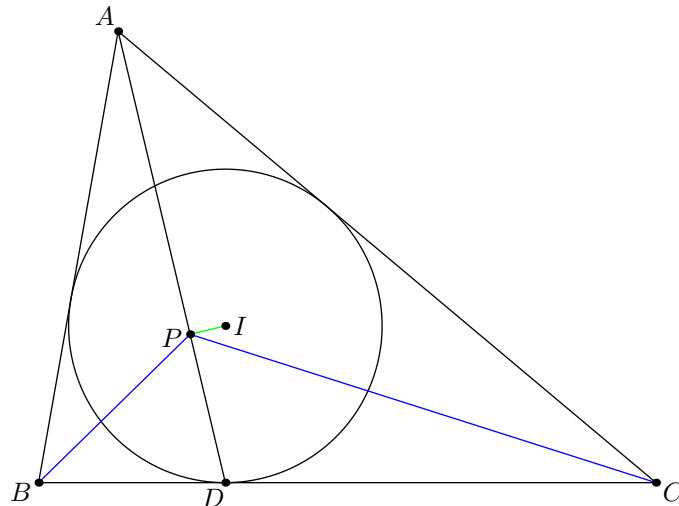
mikä ratkaisee tehtävän.

Kommentti: Harmonisten nelikoiden soveltamista ajatellen on usein hyvä, jos tehtävässä on paljon leikkauspisteitä. Usein kuviossa ei ole valmiiksi kaikkia tarvittavia pisteitä, vaan osa pitää tajuta lisätä kuvaan itse.

Toinen esimerkkitehtävä on ELMO-lyhytlistalta vuodelta 2012.

### Tehtävä

Olkoon  $ABC$  kolmio ja  $I$  sen sisäympyrän keskipiste. Olkoon  $D$  kolmion  $ABC$  sisäympyrän sivuamispiste sivun  $BC$  kanssa, ja olkoon  $P$  pisteestä  $I$  janalle  $AD$  piirretyn korkeusjanan kantapiste. Osoita, että  $\angle BPD = \angle DPC$ .



Kuten edellisessä tehtävässä myös tässä on hyvin vaikeaa päästä suoraan käsiksi kulmiin. Tämän vuoksi määritellään  $K$  olemaan suoran  $IP$  leikkauspiste suoran  $BC$  kanssa, jolloin tavoitteena on osoittaa, että  $(B, C; D, K) = -1$ .

Tämä tilannehan muistuttaa hieman edellisen tehtävän konfiguraatiota. Ehto  $(B, C; D, K) = -1$  pätee täsmälleen yhdellä pisteen  $K$  valinnalla, joka saadaan konstruotua valitsemalla janoilta  $AC$  ja  $AB$  pisteet  $E$  ja  $F$  niin, että  $AD, BE$  ja  $CF$  leikkaavat samassa pisteessä, ja ottamalla suorien  $EF$  ja  $BC$  leikkauspiste. Yritetään nyt valita sellaiset ehdon täyttävät pisteet  $E$  ja  $F$ , joiden käsittely on mahdollisimman helppoa.

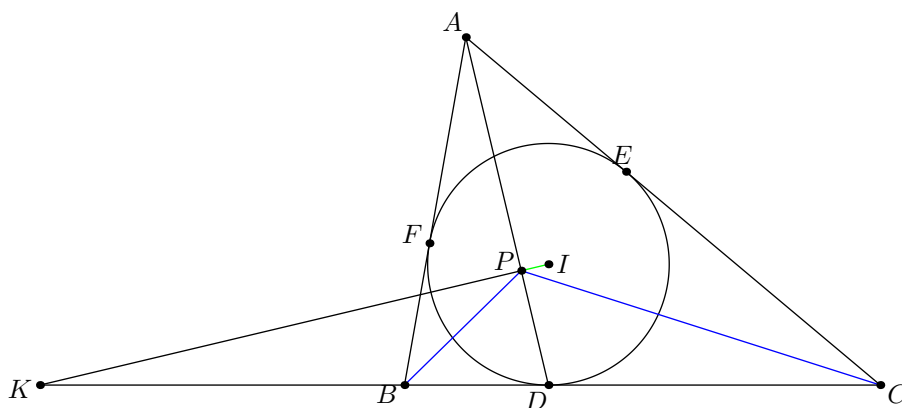
Mikä olisi luonnollinen tapa valita  $E$  ja  $F$ ? Intuitiivisesti paras olisi sellainen, jolla  $AD, BE$  ja  $CF$  vastaisivat ”samaa asiaa” (kuten vaikkapa korkeusjanat). Tällä perusteella kannattaisi pisteet  $E$  ja  $F$  valita olemaan sisäympyrän sivuamispisteet

kolmion sivujen kanssa. Leikkaavatko  $AD$ ,  $BE$  ja  $CF$  tällöin samassa pisteessä? Muistetaan, että vastaava korkeusjanoja koskeva ongelma ratkesi Cevan lauseella, ja huomataan, että sama toimii myös tässä: Jos  $E$  ja  $F$  ovat sivuamispisteet, niin tällöin mm.  $AE = AF$ , koska  $AE$  ja  $AF$  ovat sisäympyrälle pisteestä  $A$  piirretyt tangentit. Tämän avulla saadaan Cevan lauseen ehto

$$\frac{AF}{FB} \cdot \frac{BD}{DC} \cdot \frac{CE}{EA} = 1,$$

joten janat  $AD$ ,  $BE$  ja  $CF$  leikkaavat samassa pisteessä.

Tutkitaan siis seuraavaa kuvaa. Tavoitteena on osoittaa, että pisteet  $E$ ,  $F$  ja  $K$  ovat samalla suoralla.



Mikä piste  $K$  oikeastaan on? Määritelmän mukaan se on pisteeseen  $D$  piirretyä sisäympyrän tangentin ja suoran  $PI$  leikkauspiste. Mutta piste  $I$  on sisäympyrän keskipiste ja  $PI$  ja  $AD$  ovat kohtisuorassa, joten pisteen  $K$  toinen tangentti sisäympyrälle on janalla  $AD$ . Olkoon tämä tangenttipiste  $G$ .

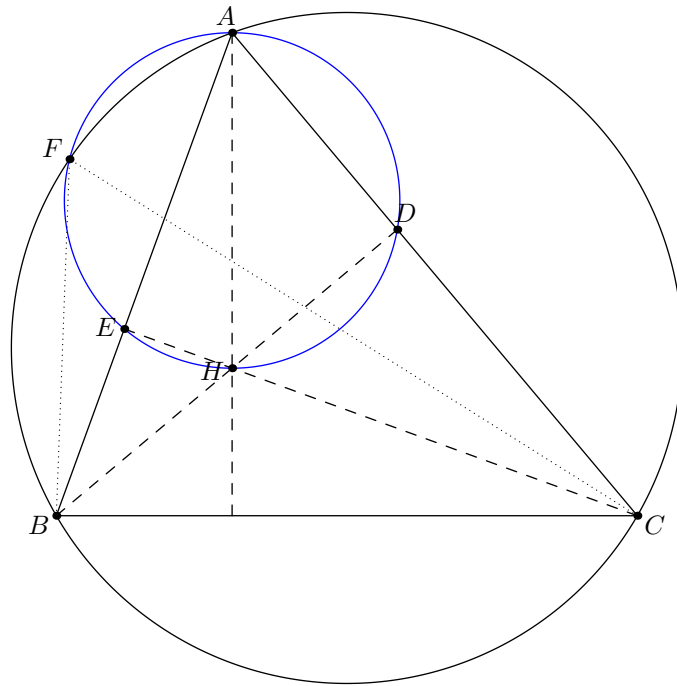
Todistettava väite on siis, että jännelikulmion  $DFGE$  pisteisiin  $D$  ja  $G$  piirretyt tangentit leikkaavat suoralla  $FE$ . Toisin sanoen nelikulmion  $DFGE$  tulisi olla harmoninen. Tämä on kuitenkin selvää, koska pisteisiin  $F$  ja  $E$  piirretyt tangentit leikkaavat suoralla  $DG$ , nimittäin pisteessä  $A$ .

Kommentti: Tässä ratkaisussa korostui asioiden katsominen oikeasta näkökulmasta. Ensimmäinen kohta oli pisteen  $K$  tulkitseminen suorien  $EF$  ja  $BC$  leikkauspisteinä. Toisessa kohdassa  $K$  taas tulkittiin tangenttien avulla. Koska harmonisia nelikoita koskevat lemmat ovat hyvin monimuotoisia, kannattaa myös tehtävien konfiguraatioita katsoa monesta eri näkökulmasta.

Viimeinen tehtävä on vuoden 2011 Brasilian kansallisesta kilpailusta.

### Tehtävä

Olkoon  $ABC$  teräväkulmainen kolmio. Olkoot  $BD$  ja  $CE$  kolmion korkeusjanoja, ja olkoon  $H$  sen ortokeskus. Kolmion  $ADE$  ympärysympyrä leikkaa kolmion  $ABC$  ympärysympyrää pisteessä  $F \neq A$ . Osoita, että kulmien  $\angle BFC$  ja  $\angle BHC$  kulmanpuolittajat leikkaavat suoralla  $BC$ .



Huomataan, että pisteillä  $D$  ja  $E$  ei ole paljoakaan väliä: kolmion  $ADE$  ympärysympyrä on vain se ympyrä, jonka halkaisija on  $AH$ .

Kulman  $\angle BFC$  puolittaja on ehkä helpointa tulkita janana  $FM$ , jossa  $M$  on (pienemmän) kaaren  $\widehat{BC}$  keskipiste. Kulman  $\angle BHC$  puolittajalle ei saa uutta muotoilua aivan yhtä helposti. Pienellä luovuudella saadaan kuitenkin seuraava idea: Peilataan  $H$  janan  $BC$  yli pisteeseen  $H'$ . Tiedetään, että tämä peilaus on kolmion  $ABC$  ympärysympyrällä. Olkoon  $N$  suuremman kaaren  $\widehat{BC}$  keskipiste. Nyt  $H'N$  on kulman  $\angle BH'C$  kulmanpuolittaja, ja se leikkaa suoraa  $BC$  symmetrian nojalla samassa kohdassa kuin kulman  $\angle BHC$  puolittaja. Ongelma on tässä muodossa ehkä hieman alkuperäistä muotoilua helpompi, koska  $H'$  on ainakin samalla ympyrällä kuin monet muutkin tehtävän pisteistä.

Haluamme siis, että nelikulmion  $BFCH'$  kulmien  $\angle BFC$  ja  $\angle BH'C$  puolittajat leikkaavat lävistäjällä  $BC$ . Voisiko tämä ehto olla sama, kuin että  $BFCH'$  on harmoninen nelikulmio? Kyllä vain. Tämän voi todistaa vaikkapa kulmanpuolittajalauseella: Jos  $X$  on kulman  $\angle BFC$  puolittajan leikkauspiste janan  $BC$  kanssa, niin

$$\frac{BX}{XC} = \frac{BF}{FC}.$$

Nyt jos  $(B, C; F, H') = -1$ , niin

$$\frac{BF}{FC} = \frac{BH'}{H'C},$$

eli pätee  $\frac{BX}{XC} = \frac{BH'}{H'C}$ , ja täten  $X$  on myös kulman  $\angle BH'C$  puolittajalla. (Toinenkin suunta pätee, eli jos kulmanpuolittajat leikkaavat lävistäjällä, niin nelikulmio on harmoninen. Todistus on sama kuin edellä.)

Voidaan keksiä parikin ideaa nelikulmion  $BFCH'$  harmonisuuden todistamiseksi. Yksi idea on ottaa perspektiivi pisteestä  $A$ , jolloin tulisi todistaa nelikulmion

*FEHD* harmonisuus. Toinen idea perustuu myös perspektiivin ottamiseen pisteestä  $A$ , mutta projektio otetaan suoralle  $BC$ . Esitämme molempiin lähestymistapoihin perustuvat ratkaisut.

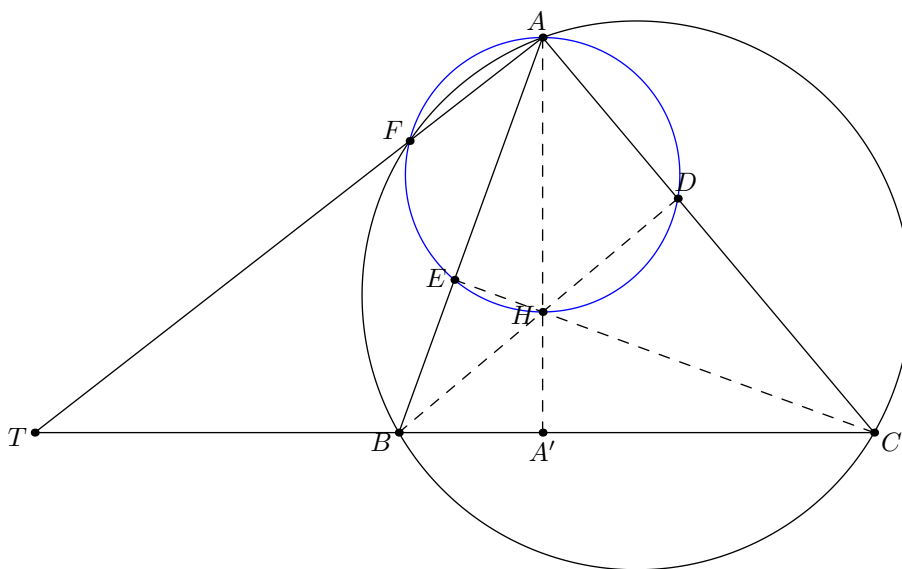
Ensimmäistä ideaa varten haluamme siis, että  $FEDH$  on harmoninen. Otetaan perspektiivi pisteestä  $H$  suoralle  $BC$ . Tällöin  $E$  kuvautuu pisteelle  $C$  ja  $D$  pisteelle  $B$ . Väite:  $F$  kuvautuu janan  $BC$  keskipisteelle. Todistus: Olkoon  $A'$  suoran  $FH$  leikkauspiste kolmion  $ABC$  ympärysympyrän kanssa. Tällöin  $\angle AFA' = \angle AFH = 90^\circ$ , eli  $AA'$  on ympyrän halkaisija. Mutta edellisessä luvussa todettiin, että pisteen  $H$  peilaus  $P$  janan  $BC$  keskipisteen yli antaa halkaisija  $AP$ , eli  $FH$  todella kulkee janan  $BC$  keskipisteen läpi. Merkitään tätä keskipistettä kirjaimella  $M$ .

Minne piste  $H$  kuvautuu? Olkoon  $\ell$  suora, joka on tangentti kolmion  $ADE$  ympärisympyrälle pisteessä  $H$ . Piste  $H$  kuvautuu perspektiiviä ottaessa suorien  $\ell$  ja  $BC$  leikkauspisteelle: tämä vastaa sitä, että valittaisiin ympyrän kehältä piste  $Q$  hyvin läheltä pistettä  $H$  ja kuvattaisiin se (vrt. kehäkulmalauseen tangenttiversio). Tangentti  $\ell$  on kohtisuorassa halkaisijaa  $AH$  kohti, joka puolestaan on kohtisuorassa suoraa  $BC$  kohti. Täten suorat  $\ell$  ja  $BC$  ovat yhdensuuntaiset, eli leikkaavat pisteessä äärettömyydessä. Siispä

$$(F, H; D, E) \stackrel{H}{=} (M, P_\infty; B, C),$$

joka on  $-1$ , kuten lemmejen yhteydessä todettiin. Tämä on mitä haluttiinkin.

Tutkitaan sitten toisen idean mukaista lähestymistapaa. Otamme siis perspektiivin nelikulmiosta  $FBH'C$  pisteen  $A$  kautta suoralle  $BC$ .



Tavoitteena on todistaa, että  $(T, B; A', C) = -1$ . Tiedämme, missä pisteen  $T$  tulisi sijaita: sen pitäisi olla suorien  $ED$  ja  $BC$  leikkauspiste. Toisin sanoen haluamme osoittaa, että suorat  $AF, ED$  ja  $BC$  leikkaavat samassa pisteessä. Avainsana tähän on radikaaliakselit: Nelikulmio  $BCDE$  on jännenelikulmio, ja nyt suorat  $AF, DE$  ja  $BC$  ovat kolmioiden  $ADE, ABC$  ja  $BCD$  ympärysympyröiden radikaaliakselit. Täten ne leikkaavat samassa pisteessä.

## 6 Lisätehtäviä (Geometria)

Tässä luvussa esitetään geometrian lisätehtäviä.

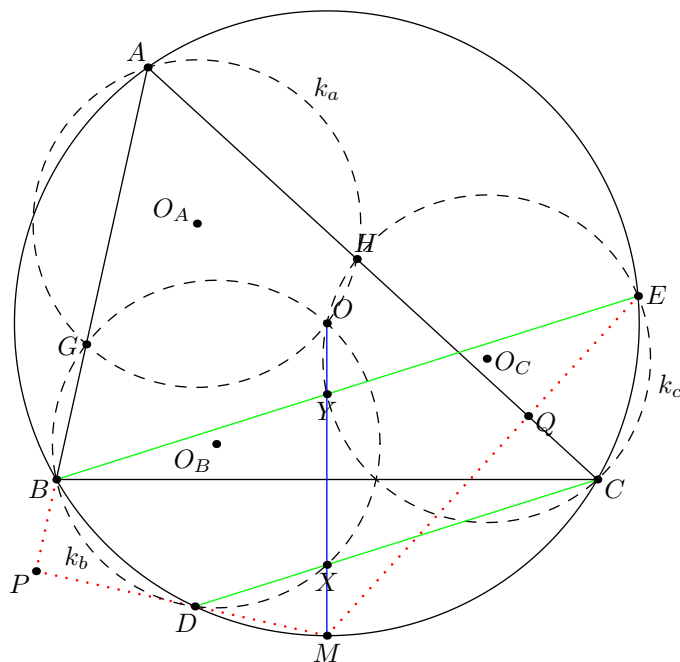
Ensimmäinen tehtävä on vuoden 2018 European Mathematical Cup -kilpailusta.

### Tehtävä

Olkoon  $ABC$  kolmio, jossa  $|AB| < |AC|$ . Olkoon  $k$  kolmion  $ABC$  ympärysympyrä, ja olkoon  $O$  ympyrän  $k$  keskipiste. Piste  $M$  on sen ympyrän  $k$  kaaren  $BC$  keskipiste, joka ei sisällä pistettä  $A$ . Olkoon  $D \neq M$  ympyrän  $k$  ja pisteestä  $M$  suoralle  $AB$  piirretyn korkeusjanan leikkauspiste. Olkoon  $E \neq M$  ympyrän  $k$  ja pisteestä  $M$  suoralle  $AC$  piirretyn korkeusjanan leikkauspiste.

Pisteet  $X$  ja  $Y$  ovat suorien  $CD$  ja  $BE$  leikkauspisteet suoran  $OM$  kanssa, vastaavasti. Olkoot  $k_b$  ja  $k_c$  kolmioiden  $BDX$  ja  $CEY$  ympärysympyrät, vastaavasti. Olkoot  $G$  ja  $H$  ympyröiden  $k_b$  ja  $k_c$  toiset leikkauspisteet suorien  $AB$  ja  $AC$  kanssa, vastaavasti. Olkoon  $k_a$  kolmion  $AGH$  ympärysympyrä.

Todista, että  $O$  on kolmion  $O_aO_bO_c$  ympärysympyrän keskipiste, missä  $O_a, O_b$  ja  $O_c$  ovat ympyröiden  $k_a, k_b$  ja  $k_c$  keskipisteet.



Tehtävässä on melkoisesti pisteitä (ja kuvaan on vielä lisätty pisteen  $M$  suorille  $AB$  ja  $AC$  piirrettyjen korkeusjanojen kantapisteet  $P$  ja  $Q$ ). Tietokoneella piirretty täydellinen kuva onkin merkittävä etu käsin piirrettyyn epätarkkaan piirroksen verrattuna. Kilpailussa kannattaa piirtää hyvä kuva tehtävästä, koska se johdattaa usein oikeiden havaintojen jäljille. Tässä tehtävässä onkin valtava määrä erilaisia huomioita.

Kuvan perusteella näyttäisi siltä, että piste  $O$  on jokaisella ympyröistä  $k_a, k_b$  ja  $k_c$ . (Tällaiset havainnot ovat syy sille, miksi piirretään hyvä kuva.) Jos näin on, niin jotta tehtävänannon väite pitäisi, tulisi jokaisella ympyröistä  $k_a, k_b$  ja  $k_c$  olla sama säde. Tämä on lohduttava huomio: jos tehtävän konfiguraatiossa on paljon erilaisia väitteitä, jotka pätevät, niin todennäköisesti ainakin jonkin niistä saa todistettua, jolloin voi päästä ratkaisuun pikku hiljaa.

Aloitetaan ratkaiseminen. Kannattaa aloittaa niistä pisteistä, jotka määritellään tehtävänannossa ensimmäisinä, koska nämä ovat luultavasti helpoimmat pisteet. Yritetään todistaa, että  $O$  on ympyrällä  $k_b$  eli että  $BDOX$  on jännenelikulmio. On monta eri kulmaehto, jotka johtaisivat tähän väitteeseen, kuten esimerkiksi  $\angle OBX = \angle ODX$  ja  $\angle BOX + \angle BDX = 180^\circ$ . Näistä ensin mainittu tapa on hyvin haastava: ei näytä helpolta laskea kulmaa  $\angle OBX$ . Jälkimmäistä ehtoa on kuitenkin helppoa soveltaa väitteen todistamiseksi.

Koska  $M$  on kaaren  $\widehat{BC}$  keskipiste, pätee

$$\angle BOX = \angle BOM = \frac{\angle BOC}{2},$$

joka on kehäkulmalauseen keskuskulmaversion nojalla yhtä suuri kuin  $\angle A$ . Koska  $\angle BDX = \angle BDC = 180^\circ - \angle A$ , väite seuraa.

Aivan vastaavasti todetaan, että  $O$  on ympyrällä  $k_c$ . Seuraavaksi voisi yrittää todistaa, että  $O$  on ympyrällä  $k_a$ . Tämä vaatisi, että  $\angle GOH = 180^\circ - \angle A$ . Yksi idea tämän todistamiseksi on kirjoittaa  $\angle GOH = 360^\circ - \angle GOM - \angle MOH$  ja käyttää tietoa siitä, että  $O$  on ympyröillä  $k_b$  ja  $k_c$ . Tämä ei kuitenkaan johda helposti ratkaisuun. Pitää keksiä jotain muuta.

On kaksikin tapaa, joilla voi edetä. Jossain kohtaa tulee todistaa, että ympyröiden  $k_b$  ja  $k_c$  (ja  $k_a$ ) säteet ovat samat. Toisaalta voisimme tehdä lisää huomioita kuvasta. Yksi tällainen huomio on, että  $k_b$  ja  $k_c$  näyttäisivät leikkaavan janalla  $BC$ .

Tutkitaan ensiksi ympyröiden  $k_b$  ja  $k_c$  säteitä. Sinilause on hyvä työkalu tähän. Helpoimmalta vaikuttava tapa soveltaa sinilauseita ympyrän  $k_b$  säteen määrittämiseksi on käyttää sitä janan  $BD$  suhteen:

$$\frac{BD}{\sin(\angle BOD)} = 2r_b,$$

missä  $r_b$  on ympyrän  $k_b$  säde. Kulma  $\angle BOD$  on helppo käsitellä: kehäkulmalauseen keskuskulmaversion nojalla  $\angle BOD = 2\angle BAD$ . Olemme saaneet siirrettyä kulman ympyrältä  $k_b$  kolmion  $ABC$  ympärysympyrälle. Pätee siis

$$2r_b = \frac{BD}{\sin(2\angle BAD)}.$$

Yksi idea on laskea pidemmälle, mitä  $\angle BAD$  on. On kuitenkin hyvä pitää mielessä, mikä lopullinen tavoite on. Haluamme saada todistettua, että  $r_b = r_c$ , missä  $r_c$  on ympyrän  $k_c$  säde. Tätä varten kannattaa kirjoittaa  $\frac{BD}{\sin(2\angle BAD)}$  mahdollisimman ”symmetriseen” muotoon. Tämän vuoksi käytetään sinilauseita kolmion  $ABC$

ympärysympyrällä, jotta saadaan eliminotua pituus  $BD$ :

$$\frac{BD}{\sin(\angle BAD)} = 2r,$$

missä  $r$  on kolmion  $ABC$  ympärysympyrän säde. Nyt

$$r_b = r \frac{\sin(\angle BAD)}{\sin(2\angle BAD)}.$$

Vastaavasti saamme

$$r_c = r \frac{\sin(\angle CAE)}{\sin(2\angle CAE)}.$$

Jotta siis  $r_b = r_c$  pätsi, tulee yhtälön muotoa

$$\frac{\sin(x)}{\sin(2x)} = \frac{\sin(y)}{\sin(2y)}$$

päteä. Intuitio sanoo, että tämä yhtälö ei toteudu kovin usein. Tarkempi perustelu etenee näin: Kirjoitetaan  $\sin(2x) = 2\sin(x)\cos(x)$  ja vastaavasti muuttujalle  $y$ , jolloin saadaan  $\cos(x) = \cos(y)$ . Koska ongelmassamme  $x$  ja  $y$  ovat väliltä  $(0^\circ, 180^\circ)$ , tulee päteä  $x = y$ . Yritetään siis todistaa, että  $\angle BAD = \angle CAE$ .<sup>22</sup>

Kulman  $\angle BAD$  laskemiseksi lähdetään siitä, miten  $D$  on määritelty. Tämä motivoi kirjoittamaan kulman  $\angle BAD$  muotoon  $\angle BMD$ . Saadaan

$$\angle BMD = \angle BMP = 90^\circ - \angle PBM = \angle ABM - 90^\circ.$$

Lasketaan  $\angle CAE$  vastaavasti:<sup>23</sup>

$$\angle CAE = \angle CME = 90^\circ - \angle MCA.$$

Enää tulee siis osoittaa, että  $\angle ABM + \angle MCA = 180^\circ$ , mutta tämä on selvää. Siis  $r_b = r_c$ .

Seuraavaksi listallamme oli todistaa, että  $k_b$  ja  $k_c$  leikkaavat janalla  $BC$ . Olkoon  $T$  ympyröiden  $k_b$  ja  $k_c$  leikkauspiste (toinen kuin  $O$ ). Tutkitaan kulmia  $\angle BTO$  ja  $\angle CTO$ . Päte

$$\angle BTO = \angle BDO.$$

Siirretään kulma kolmion  $ABC$  ympärysympyrälle kuten edellisessäkin todistuksessa.

$$\angle BDO = \frac{180^\circ - \angle BOD}{2} = \frac{180^\circ - 2\angle BAD}{2} = 90^\circ - \angle BAD.$$

Vastaavasti saadaan

$$\angle CTO = 180^\circ - \angle OEC = 180^\circ - \frac{180^\circ - \angle COE}{2} = 90^\circ + \frac{\angle COE}{2} = 90^\circ + \angle CAE.$$

<sup>22</sup>Yhtälöä  $\frac{\sin(x)}{\sin(2x)} = \frac{\sin(y)}{\sin(2y)}$  ei edes tarvitse ratkaista, jotta voi arvata, että tehtävässä pätee  $\angle BAD = \angle CAE$ .

<sup>23</sup>Tehtävänannossa on sanottu, että  $AB < AC$ . Täten  $E$  on eri puolella janaa  $AC$  kuin  $M$ , mutta  $D$  on pisteen  $M$  kanssa samalla puolella janaa  $AB$ . Tämän vuoksi lausekkeet ovat hieman eri näköisiä. Jos kulmat esittäisi suunnattuina kulmina, ei tätä omituisuutta esiintyisi.

Haluamme todistaa, että  $\angle BTO + \angle CTO = 180^\circ$ , mikä edellisen nojalla sievenee muotoon  $\angle BAD = \angle CAE$ . Tämä todistettiin jo edellä, joten  $T$  on suoralla  $BC$ .

Yritetään nyt todistaa, että  $O$  on ympyrällä  $k_a$ . Yksi idea, jota käsiteltiin jo aiemmin, on kirjoittaa

$$\angle GOH = 360^\circ - \angle GOM - \angle MOH.$$

Tässä on kuitenkin se ongelma, ettei kulmia  $\angle GOM$  ja  $\angle MOH$  voida laskea kovin helposti. Edellinen todistus kuitenkin motivoi seuraavan idean: tehdäänkin jako pisteen  $M$  sijasta pisteen  $T$  kohdalta, ja kirjoitetaan

$$\angle GOH = 360^\circ - \angle GOT - \angle TOH.$$

Kulmat  $\angle GOT$  ja  $\angle TOH$  osataan laskea:

$$\angle GOT = 180^\circ - \angle GBT = 180^\circ - \angle GBC = 180^\circ - \angle B,$$

ja vastaavasti

$$\angle TOH = 180^\circ - \angle C.$$

Nyt  $\angle GOH = 180^\circ - \angle A$ , mistä seuraa, että  $O$  on ympyrällä  $k_b$ .

Vielä pitää todistaa, että ympyrän  $k_a$  säde  $r_a$  on sama kuin ympyröiden  $k_b$  ja  $k_c$  säteet  $r_b$  ja  $r_c$ . Tämä ei ole erityisen vaikeaa. Käytetään jälleen sinilauseetta, jolloin

$$2r_a = \frac{GO}{\sin(\angle GAO)}.$$

Tässä  $GO$  voidaan esittää ympyrän  $k_b$  säteen  $r_b$  avulla:

$$2r_b = \frac{GO}{\sin(\angle GBO)}.$$

Haluamme siis osoittaa, että  $\sin(\angle GAO) = \sin(\angle GBO)$ . Tämä on kuitenkin selvää, onhan  $AOB$  tasakylkinen kolmio. Olemme valmiit.

Kommentti: Tehtävässä kriittistä oli erilaisten huomioiden tekeminen. Konfiguraatiossa on valtava määrä pisteitä, joten on luonnollista, että ratkaisu koostuu pienempien osien yhdistämisestä. Huolellisesti piirretty mallikuva mahdollistaa näiden pienempien osien huomaamisen kuviosta.

Ratkaisu onkin loppujen lopuksi melko helppo (vaikkakin kieltämättä työläs), kun kuvasta on tehty oikeat huomiot. Ensimmäinen väite: ”Piste  $O$  on ympyrällä  $k_b$ .” Todistus on suora kulmanjahtaus. Toinen väite: ”Pätee  $r_b = r_c$ .” Sinilause antaa luontevan tavan käsitellä ympärysympyröiden säteitä (eikä kovin montaa muuta tapaa tule mieleen). Tämän jälkeen ongelma ratkeaa jahtaamalla kulmia. Kolmas väite: ”Ympyröiden  $k_b$  ja  $k_c$  toinen leikkauspiste  $P$  on janalla  $BC$ .” Todistus on jälleen suoraviivainen kulmanjahtaus. Neljäs väite: ” $O$  on ympyrällä  $k_a$ .” Myös tämä seuraa kulmanjahtauksella, vaikkakin se on hieman vaikeampaa kuin aiempien väitteiden kohdalla. Viides väite: ”Pätee  $r_a = r_b$ .” Todistus on samankaltainen kuin toisen väitteen, mutta helpompi.



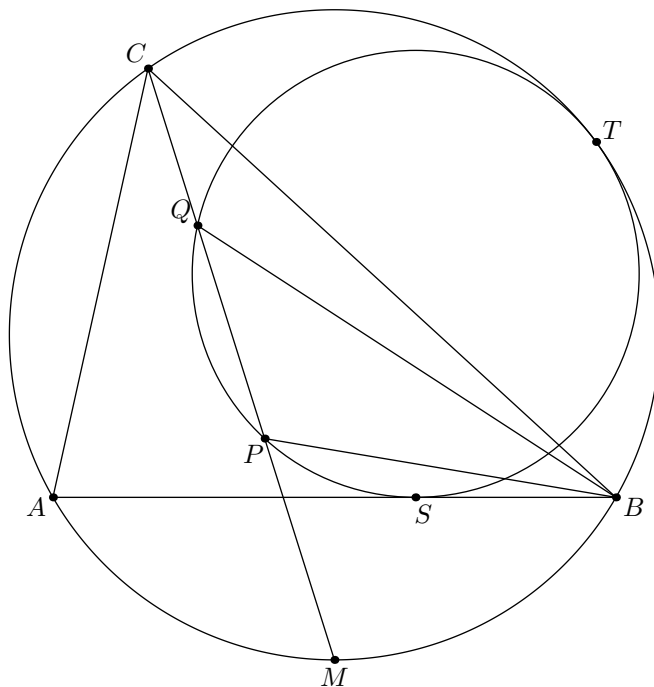
Ongelman vaikeus ei ole summa sen osaongelmien vaikeudesta. Parempi mittari vaikeudelle on vaikeimman osaongelman vaikeus ja se, kuinka vaikeaa osaongelmia on löytää tehtävän konfiguraatiosta. Tässä ratkaisussa tehdyt huomiot eivät olleet erityisen vaikeita: kuvaan oli jo valmiiksi piirretty kaikki tarvittava. Tämän vuoksi tehtävä on helpompi kuin mitä pisteitä täynnä olevasta kuvasta voisi aluksi arvata. Monesti vaikeissa geometrian tehtävissä täytyy itse keksiä kriittisiä pisteitä, joita tehtävänannossa ei suoraan mainita, ennen kuin sopivia huomioita pääsee tekemään.

Huomaa, että kolmas ja neljäs väite käytännössä todistivat seuraavan tuloksen. Olkoon  $ABC$  kolmio, ja olkoot  $D, E$  ja  $F$  jotkin pisteet sivuilla  $AB, BC$  ja  $CA$ . Tällöin kolmioiden  $AEF, BDF$  ja  $CDE$  ympärysympyrät leikkaavat samassa pisteessä. (Todistus on helppo: Määritellään  $X$  olemaan kolmioiden  $AEF$  ja  $BDF$  se leikkauspiste, joka ei ole  $F$ . Helppo ratkaisussa esiintyneen tapainen kulmanjahtaus antaa, että  $CDEX$  on jänneelikulmio.) Tulosta kutsutaan Miquelin lauseeksi, ja se tulee aina joskus vastaan geometrian tehtävissä.

Seuraava tehtävä on vuoden 2018 EGMOsta.

### Tehtävä

Olkoon  $\Gamma$  kolmion  $ABC$  ympärysympyrä. Ympyrä  $\Omega$  sivuaa janaa  $AB$  ja lisäksi se sivuaa ympyrää  $\Gamma$  pisteessä, joka on janan  $AB$  samalla puolella kuin piste  $C$ . Kulman  $\angle BCA$  puolittaja leikkaa ympyrän  $\Omega$  kahdessa eri pisteessä  $P$  ja  $Q$ . Osoita, että  $\angle ABP = \angle QBC$ .



Kuvaan on lisätty muutama luonnollinen piste, jotka enemmän tai vähemmän mainitaan tehtävänannossa. Piste  $M$  on kulman  $\angle C$  puolittajan leikkauspiste kolmion  $ABC$  ympärysympyrän kanssa ja on täten kaaren  $\widehat{AB}$  keskipiste. Pisteet  $S$  ja  $T$  ovat pienemmän ympyrän tangeeraus pisteet janan  $AB$  ja kolmion  $ABC$  ympärysympyrän

kanssa, vastaavasti. Tehtävää on vaikeaa lähteä ratkaisemaan, ellei kuviossa ole sopivia pisteitä merkittynä, joten kuvaa piirtäessä kannattaakin ajatella, mitkä ovat tehtävän kannalta oleellisia pisteitä.

Luonnollinen idea olisi yrittää naiivisti jahdata kuviosta löytyviä kulmia. Tämä ei kuitenkaan toimi – konfiguraatio ei ole otollisin kulmanjahtaukselle. (Kulmat  $\angle ABP$  ja  $\angle QBC$  ovat siitä vaikeita, että niiden pisteitä on molemmilla kuvan ympyröistä.) Täytyy keksiä jotain hienostuneempaa.

Tutkimalla kuvaa löydetään ainakin yksi asia, johon tarttua: pisteet  $M, S$  ja  $T$  näyttäisivät olevan samalla suoralla. Tämä on väite, joka ei riipu pisteistä  $C, Q$  ja  $P$ : valitsemme ainoastaan ympyrän  $\Gamma$  jängteen  $AB$ , kaaren  $\widehat{AB}$  keskipisteen  $M$  ja ympyrän  $\Omega$ , joka on tangentti ympyrälle  $\Gamma$  ja jängteelle  $AB$ . Nyt muistetaan, että tehtävää on jo käsitelty Geometrian lisämenetelmiä -luvussa homotetian yhteydessä. Sivuumme siis todistuksen yksityiskohdat tässä. (Todistus on kuitenkin vain käytännössä se, että otetaan homotetia.)

Saimme siis hieman lisää tietoa kuviosta. Yritetään nyt muodostaa sellainen suunnitelma tehtävän ratkaisemiseksi, joka on samanhenkinen kuin edellisen väitteen todistus. Samanhenkisellä tarkoitetaan tässä sitä, ettemme esimerkiksi jahtaa kulmia, vaan käytämme vaikkapa homotetiaa ja siihen liittyen yhdenmuotoisia kolmioita.

Suunnitelman muodostamiseksi mietitään, miltä kuvio näyttää, jos tehtävänannon väite  $\angle ABP = \angle QBC$  pätee. Hetken miettimisen ja kulmien laskemisen jälkeen huomataan, että tehtävänannon väitteestä seuraa

$$\angle PBM = \angle PBA + \angle ABM = \angle QBC + \angle MCB = 180^\circ - \angle CQB,$$

eli  $\angle PBM = \angle MQB$ . Tämän päättelyn voi tietysti suorittaa myös toiseen suuntaan. Ehto  $\angle PBM = \angle MQB$  tuntuu paremmalta kuin alkuperäinen väite, koska nämä kulmat ovat tavallaan ”lähempänä” toisiaan eli ne tuntuvat liittyvän toisiinsa vahvemmin.

Mietitään vielä edellistä kohtaa vähän tarkemmin. Väite käsittelee pisteitä  $M, B, P$  ja  $Q$ , ja ehdon voi tulkita kertovan, että kolmioissa  $MPB$  ja  $MBQ$  on yhtä suuret kulmat  $\angle MBQ$  ja  $\angle MQB$ . Näissä kolmioissa on kuitenkin jo samat kulmat kärjessä  $M$ :  $\angle PMB = \angle BMQ$ . Tehtävänanto pyytää siis todistamaan, että  $MPB$  ja  $MBQ$  ovat yhdenmuotoiset.

Nyt meillä on jo parempi käsitys ongelmasta: olemme todistaneet homotetialla (eli käytännössä yhdenmuotoisilla kolmioilla) pisteisiin  $M, S$  ja  $T$  liittyvän aputuloksen, ja tehtävänannon väite koskee yhdenmuotoisia kolmioita. Metsästetään siis lisää yhdenmuotoisia kolmioita.

Unohdetaan vielä hetkeksi pisteet  $C, Q$  ja  $P$  ja tutkitaan, mitä jäljelle jääneestä konfiguraatiosta saa irti. Olemme saaneet, että  $M, S$  ja  $T$  ovat samalla suoralla. Yritetään hyödyntää tätä yhdenmuotoisten kolmioiden saamiseksi. Kovin montaa mahdollisuutta tälle ei kuviosta löydy, ja pienen mietinnän jälkeen nähdään, että  $MSB$  ja  $MBT$  ovat yhdenmuotoiset. Niillä on nimittäin yhteinen kulma kärjessä  $M$  (koska  $M, S$  ja  $T$  ovat samalla suoralla), ja lisäksi

$$\angle MTB = \angle MAB = \angle MBA,$$

koska  $M$  on kaaren  $\widehat{AB}$  keskipiste.

Tutkitaan taas myös pisteitä  $C, Q$  ja  $P$ . Tiedämme nyt, että  $MSB$  ja  $MBT$  ovat yhdenmuotoiset. Lisäksi  $SPQT$  on jännenelikulmio, mistä saadaan lisää yhdenmuotoisia kolmioita, kuten  $MSP$  ja  $MQT$ . Meillä on siis tietoa siitä, miten pisteistä  $M, B, S$  ja  $T$  voidaan muodostaa yhdenmuotoisia kolmioita, ja siitä, miten pisteistä  $M, S, T, P$  ja  $Q$  voidaan muodostaa yhdenmuotoisia kolmioita. Haluaisimme jotenkin yhdistää näitä tietoja niin, että pisteistä  $M, B, P$  ja  $Q$  saataisiin yhdenmuotoisia kolmioita. Intuitio sanoo, että tämän pitäisi onnistua. Tämä idea on toteutettu alla.<sup>24</sup>

Koska  $MSB$  ja  $MBT$  ovat yhdenmuotoisia, pätee

$$\frac{MS}{MB} = \frac{MB}{MT},$$

eli  $MS \cdot MT = MB^2$ . Pisteiden potenssilla (eli yhdenmuotoisilla kolmioilla) saadaan  $MS \cdot MT = MP \cdot MQ$ . Täten  $MP \cdot MQ = MB^2$ , eli

$$\frac{MP}{MB} = \frac{MB}{MQ}.$$

Täten kolmiot  $MPB$  ja  $MBQ$  ovat yhdenmuotoiset, mistä, kuten aiemmin todettiin, väite seuraa.

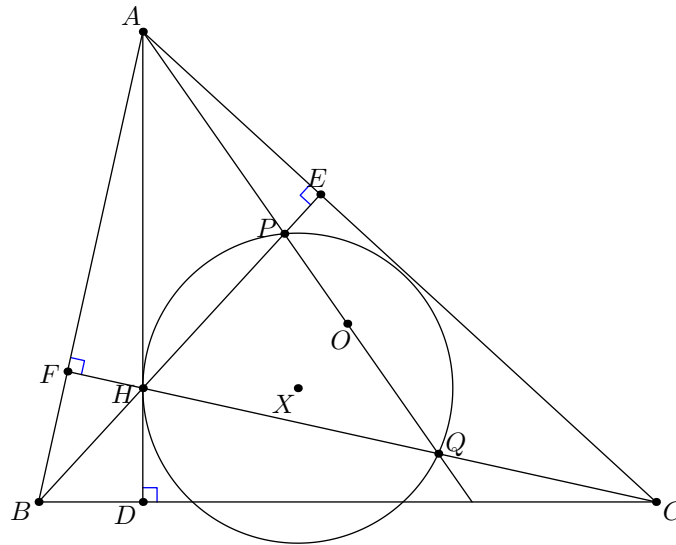
Kommentti: Vaikka ratkaisu on suhteellisen lyhyt, on tehtävä melko vaikea. Tärkeä osa ratkaisua oli saada sopiva tuntuma tehtävästä. Tätä kautta saadaan käsitys siitä, millä menetelmillä ongelman voisi ratkaista. Ratkaisun loppuosa onkin psykologisesti varsin helppo: Kun on tehnyt muutaman hyvältä vaikuttavan huomion hankalassa tehtävässä, voi päätellä, että käsittelee ongelmaa oikealla tavalla. Tämä tuo itseluottamusta tehtävän ratkaisemiseen.

Seuraava tehtävä on vuoden 2017 IMO-lyhytlistalta.

#### Tehtävä

Olkoon  $O$  teräväkulmaisen kolmion  $ABC$  ympärysympyrän keskipiste. Olkoot  $E$  ja  $F$  kärjistä  $B$  ja  $C$  piirrettyjen korkeusjanojen kantapisteet. Suora  $OA$  leikkaa janoja  $BE$  ja  $CF$  pisteissä  $P$  ja  $Q$ . Olkoon  $H$  janojen  $BE$  ja  $CF$  leikkauspiste. Osoita, että kolmion  $PQH$  ympärysympyrän keskipiste on jollain kolmion  $ABC$  mediaaneista.

<sup>24</sup>Yksi tapa löytää idealle toteutus on kirjoittaa haluttu väite näkyviin mahdollisimman monessa eri muodossa (kulmaehdoilla ja sivujen suhteita koskevin ehdoina), ja kirjoittaa kaikki jo todistetut tulokset mahdollisimman monessa eri muodossa. Sivujen pituuksia käsittelevistä ehdoista löytyy ratkaisu.



Kuvaan on piirretty myös kärjestä  $A$  lähtevä korkeusjana  $AD$  (mikä on tietysti hyvin luonnollista). Kolmion  $PHQ$  ympärysympyrän keskipisteen  $X$  lisäksi on piirretty myös itse ympyrä.

Tehtävässä pyydetään osoittamaan, että  $X$  on jollain kolmion  $ABC$  mediaaneista. Hyvä lähtökohta on selvittää, millä näistä mediaaneista  $X$  on. Kuvan perusteella näyttäisi siltä, että tämä mediaani on  $A$ -mediaani. Tämän voi oikeastaan perustella hyvinkin vakuuttavasti (mutta vedenpitävä todistus tämä ei ole): Jos  $X$  olisi kolmion  $B$ -mediaanilla, niin symmetrian vuoksi voisi ajatella, että se on myös kolmion  $C$ -mediaanilla. Tällöin  $X$  olisi kolmion  $ABC$  painopiste, eli se olisi myös  $A$ -mediaanilla.

Yritetään sitten tehdä havaintoja kuvioista. Kuvassa näyttäisi siltä, että  $AD$  on tangentti kolmion  $PHQ$  ympärysympyrälle pisteessä  $H$ . Miten tämän voisi todistaa? Kehäkulmalauseen tangenttiversio sanoo, että mikäli  $AD$  on tangentti ympyrälle, niin  $\angle PQH = \angle AHP$ . Tangenttiversio vain jos -puoli taas kertoo, että tästä kulmaehdosta seuraisi se, että  $AD$  todella on tangentti ympyrälle. Pyritään siis todistamaan, että  $\angle PQH = \angle AHP$ .

Kulman  $\angle AHP$  laskeminen on varsin helppoa. Ehkäpä lyhin todistus on tämä: koska  $CDHE$  on jännelikulmio, niin

$$\angle AHP = \angle AHE = 180^\circ - \angle DHE = \angle DCE = \angle C.$$

Kulman  $\angle HQP$  laskeminen ei ole aivan näin helppoa. Yksi idea on laskea ensiksi kolmion  $PQH$  muut kulmat  $\angle QHP$  ja  $\angle HPQ$ , jolloin saadaan tietoon myös  $\angle HQP$ . Kulman  $\angle HPQ$  laskeminen on kuitenkin (symmetrian vuoksi) aivan yhtä vaikeaa kuin kulman  $\angle HQP$ , joten tämä ei johda mihinkään.

Tässä on toinen lähestymistapa: pätee  $\angle HQP = \angle FQA = 90^\circ - \angle FAQ = 90^\circ - \angle BAO$ .<sup>25</sup> Kulman  $\angle BAO$  osaamme laskea: sen suuruus on  $90^\circ - \angle C$ . Tästä seuraa, että  $\angle HQP = \angle C$ , mikä on mitä halusimmekin.

<sup>25</sup>Motivaatio: "Mitä tiedämme pisteestä  $Q$ ?" Vastaus on, että se on korkeusjanalla  $CF$  ja suoralla  $AO$ . On siis luonnollista tutkia kolmiota  $AFQ$  ja unohtaa pisteet  $H$  ja  $P$ .

Mitä seuraavaksi? Olkoon  $M$  janan  $BC$  keskipiste. Haluamme todistaa, että pisteet  $A$ ,  $X$  ja  $M$  ovat samalla suoralla. Tiedämme, että  $HX$  ja  $DM$  ovat yhdensuuntaiset. Enää tulee todistaa, että  $X$  on oikealla etäisyydellä janasta  $AD$ , eli että

$$\frac{AH}{HX} = \frac{AD}{DM}.$$

Jos tämä yhtälö pätee, niin  $AHX$  ja  $ADM$  ovat yhdenmuotoisia suorakulmioita. Tällöin  $\angle HAX = \angle DAM$ , mistä väite seuraa.

Pystymmekö laskemaan pituudet  $AH$ ,  $HX$ ,  $AD$  ja  $DM$ ? Pituudet  $AD$  ja  $DM$  tuntuvat helpoilta:  $D$  ja  $M$  ovat helppoja pisteitä, joten nämä pituudet osataan kyllä laskea. Myös pituuden  $AH$  laskemisen luulisi onnistuvan. Ainoa epäilyttävä asia on pituuden  $HX$  eli kolmion  $HPQ$  ympärysympyrän säteen laskeminen. Ympärysympyrän säteen laskemiseen apuna toimii sinilause: tiedämme kulman  $\angle HQP$  (sen laskettiin edellä olevan  $\angle C$ ), joten sinilauseen nojalla säteen laskemiseksi riittää laskea  $HP$ . Pituus  $HP$  taas voidaan laskea sinilauseella kolmiosta  $AHP$ , koska pystymme laskemaan tämän kolmion kulmat. Voimme tätä kautta esittää pituuden  $HP$  pituuden  $AH$  avulla, ja tällöin todistettava yhtälö  $\frac{AH}{HX} = \frac{AD}{DM}$  sievenee ainakin jonkin verran.

Ryhdytään töihin. Kolmiosta  $PQH$  saadaan sinilauseella

$$\frac{PH}{\sin(\angle HQP)} = 2R,$$

missä  $R = HX$ . Koska  $\angle HQP = \angle C$ , saadaan tästä siis

$$HX = \frac{PH}{2 \sin(\angle C)}.$$

Lasketaan sitten  $PH$  sinilauseella kolmiosta  $AHP$ :

$$\frac{AH}{PH} = \frac{\sin(\angle HPA)}{\sin(\angle HAP)}.$$

Kulma  $\angle HAP = \angle A - \angle BAD - \angle CAO$  osataan laskea. Pätee<sup>26</sup>  $\angle BAD = \angle CAO = 90^\circ - \angle B$ , joten

$$\angle HAP = \angle A - (180^\circ - 2\angle B) = \angle A + 2\angle B - 180^\circ.$$

Tämän voi vielä halutessaan sieventää muotoon  $\angle B - \angle C$  käyttämällä tietoa  $180^\circ = \angle A + \angle B + \angle C$ .

Lasketaan sitten toinen kulma eli kulma  $\angle HPA$ . Tämä on myös helppoa:

$$\angle HPA = 180^\circ - \angle EPA = 180^\circ - (90^\circ - \angle OAC) = 180^\circ - \angle B.$$

<sup>26</sup>Välillä on hyödyllistä tietää, että  $\angle BAH = \angle CAO$ , eli että suorat  $AH$  ja  $AO$  ovat symmetrisiä kulman  $A$  puolittajan suhteen. (Tämä on tietysti helppo todistaa ja vastaava pätee muillekin kulmille). Sanotaan, että  $H$  ja  $O$  ovat isogonaalisesti konjugaatit (engl. isogonal conjugates). Jos isogonaalisesti konjugaatin pisteparin  $(X, Y)$  pisteestä  $X$  tiedetään jotain, saadaan usein tietoa myös pisteestä  $Y$ .

Sijoitetaan saadut tiedot paikalleen. Saamme, että

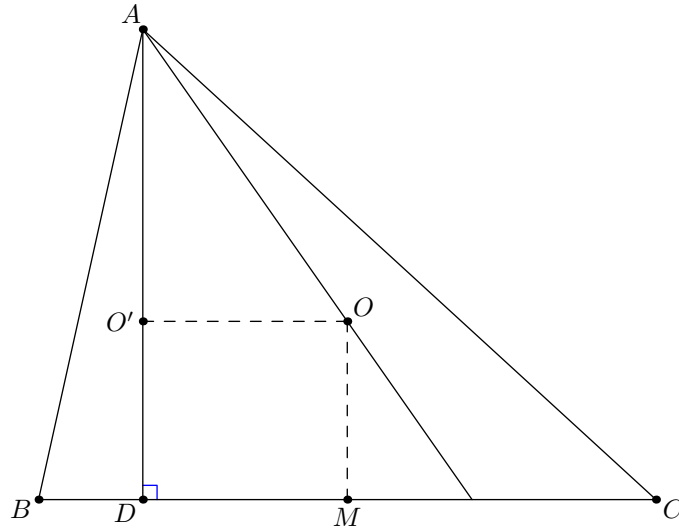
$$\frac{AH}{PH} = \frac{\sin(\angle HPA)}{\sin(\angle HAP)} = \frac{\sin(180^\circ - \angle B)}{\sin(\angle B - \angle C)} = \frac{\sin(\angle B)}{\sin(\angle B - \angle C)}.$$

Nyt

$$\frac{AH}{HX} = \frac{AH}{\frac{PH}{2\sin(\angle C)}} = \frac{AH}{PH} \cdot 2\sin(\angle C) = \frac{2\sin(\angle B)\sin(\angle C)}{\sin(\angle B - \angle C)}.$$

Tämä on hyvä, kompakti esitys suhteelle  $\frac{AH}{HX}$ . Enää tulee laskea  $\frac{AD}{DM}$ .

Pituus  $AD$  on hyvinkin helppo esittää trigonometrian avulla vaikkapa muodossa  $AD = AB \cdot \sin(\angle B)$ . Ongelmia muodostaakin pituus  $DM$ : sen voisi toki esittää muodossa  $BM - BD$ , ja voisimme laskea molemmat näistä pituuksista erikseen. Tässä on kuitenkin se huono puoli, että lausekkeisiin syntyy yhteen- ja vähennyslaskua pelkän kerto- ja jakolaskun lisäksi, jolloin haluttua yhtälöä on vaikeampi todistaa. Tämän vuoksi teemmekin pienen tempun.<sup>27</sup>



Olkoon  $O'$  pisteen  $O$  projektio suoralle  $AD$  kuten kuvassa. Nyt  $MDO'O$  on suorakulmio, ja pätee muun muassa  $DM = OO'$ . Lisäksi suorakulmaisesta kolmiosta  $AO'O$  saadaan

$$\frac{OO'}{AO} = \sin(\angle O'AO).$$

(Haluamme mieluummin käyttää sivua  $AO$  kuin sivua  $AO'$ , koska  $AO$  on kolmion  $ABC$  ympärysympyrän säde ja siten helposti käsiteltävä.) Kulma  $\angle O'AO$  laskettiin jo aiemmin: se on  $\angle B - \angle C$ . Huomaa, että termi  $\sin(\angle B - \angle C)$  esiintyi jo aiemmin suhteen  $\frac{AH}{HX}$  esityksessä – tempun hyödyllisyys perustuukin siihen, että tämä vaikea termi saadaan supistumaan. (Tämä myös motivoi tempun: kulmaa  $\angle B - \angle C$  ei voi tulkita kovin monella tavalla luonnollisesti. Se on tiettyssä mielessä ”harvinainen”.)

<sup>27</sup>Tämä tempu ei kylläkään ole aivan välttämätön. Laskemisen voi tehdä loppuun inhimillisellä vaivalla myös yhtälön  $DM = BM - BD$  kautta.

Voisi siis ajatella, että mikäli tämä kulma esiintyy suhteen  $\frac{AH}{HX}$  esityksessä, niin sitä voisi myös käyttää suhteen  $\frac{AD}{DM}$  esityksessä.) Nyt siis

$$\frac{AD}{DM} = \frac{AD}{OO'} = \frac{AD}{AO \cdot \sin(\angle O'AO)}.$$

Todistettava yhtälö  $\frac{AH}{HX} = \frac{AD}{DM}$  voidaan nyt kirjoittaa muotoon

$$2 \sin(\angle B) \sin(\angle C) = \frac{AD}{AO}.$$

Tämä on hyvin helpon oloinen yhtälö: pisteet  $D$  ja  $O$  ovat helppoja käsitellä, ja vasemmalla puolella esiintyy vain helppojen kulmien sinejä. Todistuksen loppu onkin suoraviivainen: Sinilauseen nojalla

$$AO = \frac{AB}{2 \sin(\angle C)},$$

ja pituuden  $AD$  tiedetään olevan

$$AD = \sin(\angle B) \cdot AB,$$

joten

$$\frac{AD}{AO} = \frac{\sin(\angle B) \cdot AB}{\frac{AB}{2 \sin(\angle C)}} = 2 \sin(\angle B) \sin(\angle C).$$

Tämä todistaa väitteen.

Kommentti: Tehtävä sattui ratkeamaan toistuvalla sinilauseen soveltamisella (ns. sinilausebashilla). Aina tämä lähestymistapa ei kuitenkaan toimi. Miksi se toimi nyt? Oleellista on, että tehtävän konfiguraatiosta pystyttiin laskemaan kaikki tarvittavat kulmat. Lisäksi ortokeskus ja sen kautta syntyvät suorakulmaiset kolmiot antavat hyvän lähtökohdan trigonometrian soveltamiselle (vaikkakaan tämä ei ole välttämättömän ehto sinilauseratkaisun toimimiselle). Ympärysympyröiden säteisiin päästiin niin ikään käsiksi sinilauseella. Ei sovi myöskään unohtaa ratkaisun alussa tehtyä synteettistä havaintoa, jonka avulla tehtävä saatiin muutettua muotoon, joka mahdollisti laskennallisen ratkaisun.

Edellä mainittiin, että kuviosta pystyttiin laskemaan kaikki tarvittavat kulmat. Tämä on tietysti positiivinen asia, oli ratkaisumenetelmä mikä hyvänsä.

Tässä on tehtävään toinen lähestymistapa. Ideana on, että tiedämme suuren määrän kulmia, ja kulmatiedot saadaan luontevasti tulkittua erinäisten ympyröiden kautta. (Usein kulmatiedoilla saadaan jännelikulmioita, mutta tällä kertaa saammekin tangentteja eräiden kolmioiden ympärysympyröille.)

Kulma  $\angle HPX$  osataan laskea: tiedämme kolmion  $HPQ$  kaikki kulmat (ne ovat oikeastaan  $\angle A, \angle B$  ja  $\angle C$ ), ja  $X$  on kolmion ympärysympyrän keskipiste. Saadaan  $\angle BPX = \angle HPX = 90^\circ - \angle C$ . Vastaavasti  $\angle BAP = \angle BAO = 90^\circ - \angle C$ . Siis  $\angle BPX = \angle BAP$ . Tämä tarkoittaa (tämä on kriittinen huomio), että  $PX$  on tangentti kolmion  $APB$  ympärysympyrälle. Vastaavasti saadaan, että  $QX$  on tangentti

kolmion  $AQC$  ympyräsympyrälle. Koska  $PX = QX$ , on pisteen  $X$  potenssi näiden ympyröiden suhteen sama, eli  $X$  sijaitsee niiden radikaaliakselilla. Piste  $A$  sijaitsee triviaalisti näiden ympyröiden radikaaliakselilla. Enää tulee todistaa, että myös piste  $M$  on tällä radikaaliakselilla. Tämä seuraa toteamalla, että  $MB = MC$  ja että  $BM$  ja  $CM$  ovat tangentteja kolmioiden  $APB$  ja  $AQC$  ympärysympyröille. (Käyttämällä tietoa  $\angle BAD = \angle CAO$  saadaan

$$\angle MBP = \angle CBE = \angle DAC = \angle BAO = \angle BAP,$$

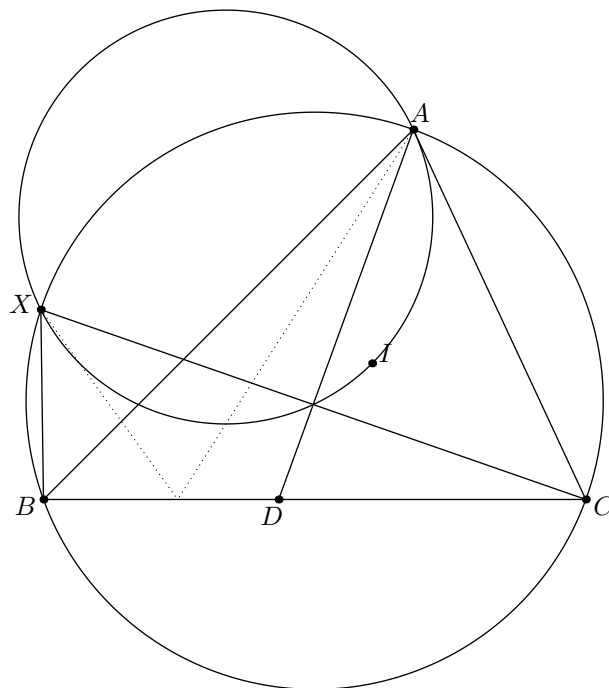
mistä väite seuraa.)

Viimeinen tehtävä on vuoden 2019 EGMOsta.

### Tehtävä

Olkoon  $ABC$  kolmio, jossa  $\angle CAB > \angle ABC$ , ja olkoon  $I$  sen sisäänpiirretyn ympyrän keskipiste. Olkoon  $D$  sellainen piste janalla  $BC$ , että  $\angle CAD = \angle ABC$ . Olkoon  $\omega$  se ympyrä, joka sivuaa suoraa  $AC$  pisteessä  $A$  ja kulkee pisteen  $I$  kautta. Olkoon  $X$  ympyrän  $\omega$  ja kolmion  $ABC$  ympärysympyrän toinen leikkauspiste. Osoita, että kulmien  $\angle DAB$  ja  $\angle CXB$  puolittajat leikkaavat pisteessä, joka on suoralla  $BC$ .

Tässä on kuva tehtävänannon tilanteesta.



Pannaan heti merille, että janat  $CX$  ja  $AD$  näyttävät leikkaavan kolmion  $AXI$  ympärysympyrällä.

Ensimmäinen askel on miettiä, miten tehtävänannon pisteitä ja janoja tulee ajatella. Esimerkiksi kulman  $\angle BXC$  puolittaja kannattaa ajatella janana  $XM$ , jossa  $M$  on kaaren  $\widehat{BC}$  keskipiste. Tutkitaan sitten pistettä  $D$ . Luonnollinen tapa hyödyntää



ehtoa  $\angle CAD = \angle ABC$  on tutkia ehtoa kolmion  $ABC$  ympärysympyrän kaarien kautta: jos  $F$  on suoran  $AD$  leikkauspiste kolmion  $ABC$  ympärysympyrän kanssa, niin pätee

$$\angle FAC = \angle DAC = \angle ABC = \angle AFC.$$

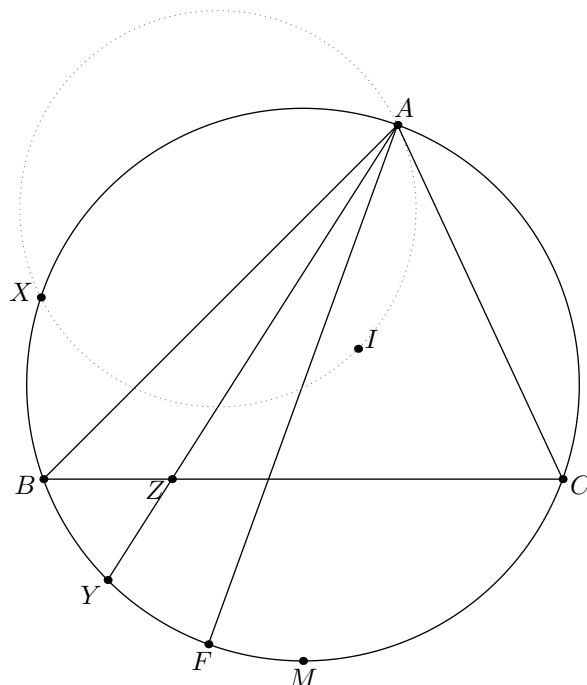
Täten  $CA = CF$ . Nyt olemme korvanneet pisteen  $D$  huomattavasti helpommalla pisteellä  $F$ , ja voimme käytännössä unohtaa pisteen  $D$ .

Edellinen tulkinta pisteelle  $F$  on siitä hyvä, että se antaa luonnollisen tavan tulkita myös kulman  $\angle BAD$  eli  $\angle BAF$  puolittajaa: se on jana  $AY$ , missä  $Y$  on kaaren  $\widehat{BF}$  keskipiste.

Ongelman vaikein rakenne vaikuttaisi olevan kolmion  $AXI$  ympärysympyrä. Pisteestä  $X$  on vaikea sanoa tässä vaiheessa paljoa muuta kuin kehäkulmalauseen tangenttiversiosta saatavan tiedon  $\angle IXA = \angle IAC = \frac{\angle A}{2}$ .

Mietitään sitten, miten voisimme todistaa tehtävänannon väitteen. Haluamme todistaa, että janojen  $AY$  ja  $XM$  leikkauspisteet janan  $BC$  kanssa ovat sama piste. Tätä ongelmaa voi lähestyä tutkimalla ensiksi näitä leikkauspisteitä yksitellen ja katsomalla, mitä ominaisuuksia niillä on. Näin saamme ainakin jotain lisätietoa tehtävästä.

Tähän mennessä saamiemme tietojen perusteella jana  $AY$  vaikuttaa paljon helpommalta kuin jana  $XM$ , joten tutkitaan ensiksi janan  $AY$  leikkauspistettä janan  $BC$  kanssa. Alla on piirretty kuva, johon tämä leikkauspiste  $Z$  on piirretty. Kolmion  $AXI$  ympärysympyrä on jätetty kuvassa taka-alalle.



Ehdon  $CF = CA$  vuoksi on luonnollista piirtää kuvaan  $C$ -keskinen ympyrä, jonka säde on  $CA$  – näin pääsemme todella käsiksi siihen, mikä piste  $F$  on. Ympyrän piirtämisen jälkeen huomataan, että myös piste  $Z$  näyttäisi olevan tällä ympyrällä.

Tämän väitteen huomaaminen on vaikeampaa kuin väitteen todistus. Saamme nimitäin laskettua kolmion  $ZAC$  kaikki kulmat, ja saamme tätä kautta todistettua sen tasakylkiseksi. Pisteiden  $F, Y$  ja  $Z$  määritelmien nojalla pätee

$$\begin{aligned}\angle ZAC &= \angle YAC = \angle YAF + \angle FAC = \\ \frac{\angle BAF}{2} + \angle B &= \frac{\angle A - \angle B}{2} + \angle B = \frac{\angle A + \angle B}{2}.\end{aligned}$$

Nyt

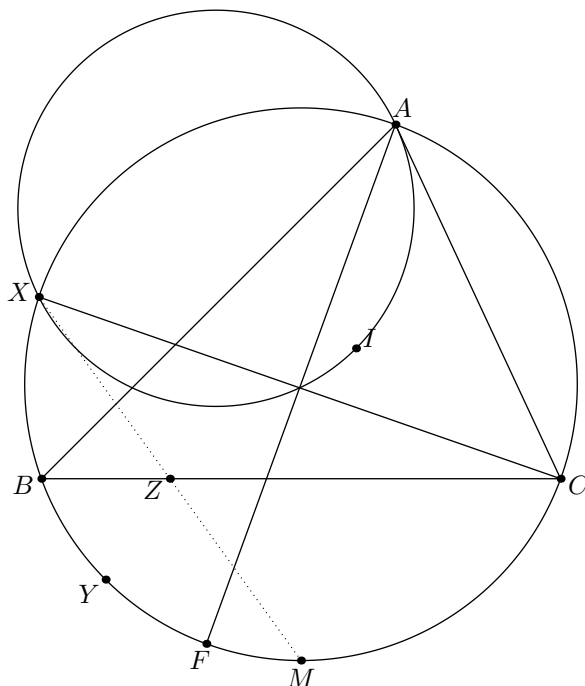
$$\angle AZC = 180^\circ - \angle ZAC - \angle C = 180^\circ - \frac{\angle A + \angle B}{2} - \angle C = \frac{\angle A + \angle B}{2} = \angle ZAC,$$

ja väite seuraa.

Edellinen tulos antaa hyvin yksinkertaisen esityksen pisteelle  $Z$ : se on se piste janalla  $BC$ , jolla  $CZ = CA$ . Voisimmekin tyytyä tähän. Huomataan kuitenkin, että  $Z$  on myös sillä ympyrällä, jonka keskipiste on  $Y$  ja säde  $YB$ . (Tätä ympyrää on luonnollista tarkastella, koska  $Y$  on kaaren  $\widehat{BF}$  keskipiste samoin kuin  $C$  on kaaren  $\widehat{AF}$  keskipiste.) Todistus on hyvinkin yksinkertainen: Edellisen huomion nojalla pätee  $\angle BZY = \angle CZA = \angle ZAC$ , ja kehäkulmalauseen nojalla  $\angle ZAC = \angle YAC = \angle YBC$ . Täten  $BZY$  on tasakylkinen kolmio, mistä väite seuraa.

Ehto siitä, että  $CZ = CA$ , on kuitenkin primitiivisempi kuin ehto  $YB = YZ$ . Pidetään siis päällimmäisenä mielessä, että  $C$  on kolmion  $AZF$  ympärysympyrän keskipiste, ja pidetään jälkimmäinen tieto taka-alalla.

Lisätään kolmion  $AXI$  ympärysympyrä takaisin kuvaan. Edellisten tulosten valossa olisi luonnollista piirtää myös  $C$ -keskinen  $CA$ -säteinen ympyrä, jonka avulla tulos  $CA = CZ$  havaittiin. Tätä ympyrää ei kuitenkaan tarvita loppuratkaisussa, joten kuvien selkeyden vuoksi ympyrä jätetään piirtämättä. Muistetaan vielä heti ratkaisun alussa tehty huomio siitä, että  $AF$  ja  $CX$  näyttäisivät leikkaavan kolmion  $AXI$  ympärysympyrällä, ja piirretään tästä syystä kuvaan janat  $CX$  ja  $AF$ . Hyvän oloinen tapa muotoilla haluttu väite on, että pisteet  $X, Z$  ja  $M$  ovat samalla suoralla. Saamme siis seuraavan kuvan:

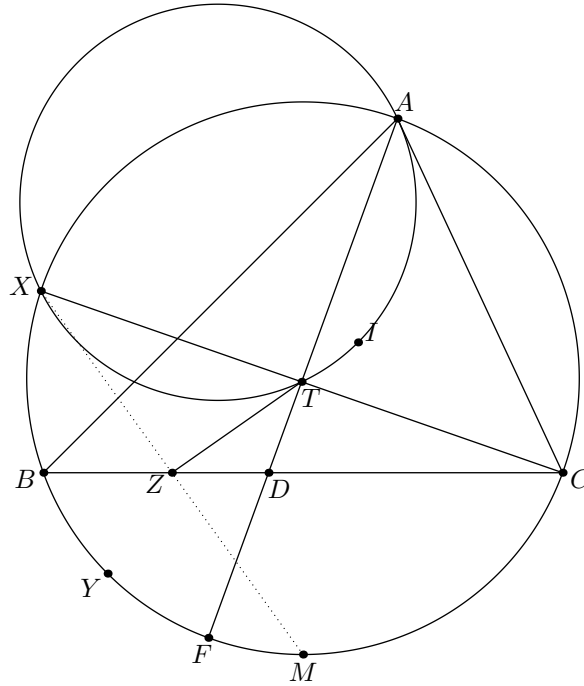


Yritetään nyt todistaa, että  $AF$  ja  $CX$  leikkaavat kolmion  $AXI$  ympärysympyrällä. Olkoon  $T$  tämä leikkauspiste. Haluamme todistaa, että  $XTIA$  on jännenelikulmio. Yksi, hyvältä tuntuva tapa todistaa tämä on yrittää todistaa väite  $\angle XTA = \angle XIA$ , koska nämä ovat suhteellisen helposti lähestyttäviä kulmia. Tämän väitteen saakin todistettua suoraan kulmanjahtauksella: kulma  $\angle XIA$  voidaan esittää kolmion  $AXI$  muiden kulmien avulla, ja kulman  $\angle XTA$  voi laskea kolmion  $ATC$  kautta. Yksityiskohdat tästä lähestymistavasta sivuutetaan. Alla on esitetty toinen tapa todistaa väite. Tämä tapa on elegantimpi, mutta se on hieman vaikeampi keksiä.

Pätee  $\angle AXT = \angle AXC = \angle B$  ja  $\angle TAC = \angle FAC = \angle B$ . Täten  $\angle AXT = \angle TAC$ . Nyt kehäkulmalauseen tangenttiversion vain jos -puolen nojalla kolmion  $AXT$  ympärysympyrä on tangentti suoralle  $AC$  pisteessä  $A$ . Tämä tarkoittaa, että kolmioiden  $AXT$  ja  $AXI$  ympärysympyrät ovat samat, joten  $AXTI$  on jänneneli-kulmio.

Piste  $T$  vaikuttaa tärkeältä: toisaalta se liittyy pisteeseen  $F$ , joka on yksi puoli tehtävää, ja toisaalta se liittyy pisteeseen  $X$  ja kolmion  $AXI$  ympärysympyrään, jotka muodostavat toisen puolen tehtävästä. Nyt, jos kuviota katsoo erityisesti pitäen pistettä  $T$  silmällä, huomaa, että pisteet  $T, I$  ja  $Z$  näyttäisivät olevan samalla suoralla.

Lähdetään todistamaan väitettä kulmanjahtauksella. Miten kannattaisi edetä? Ehkäpä helpoin muotoilu väitteelle on tällöin  $\angle ITA = \angle ZTF$ . Tässä  $\angle ITA$  tiedetään: kehäkulmalauseen tangenttiversiolla saadaan  $\angle ITA = \frac{\angle A}{2}$ . Tulee siis todistaa, että  $\angle ZTF = \frac{\angle A}{2}$ , eli yritetään jahdata kulma  $\angle ZTF$ . Yksi idea on ottaa kuvioon takaisin piste  $D$  ja tutkia kolmiota  $DTZ$ . Motivaationa toimii se, että  $\angle ZDT$  osataan laskea.



Lasketaan kulma  $\angle ZDT$ :

$$\angle ZDT = 180^\circ - \angle ADC = \angle DAC + \angle DCA = \angle B + \angle C.$$

Täten  $\angle ZTD = \frac{\angle A}{2}$  jos ja vain jos  $\angle DZT = \frac{\angle A}{2}$ . Kolmion  $ZDT$  tulisi siis olla tasakylkinen.

Ei ole selvää, miten kulmanjahtausta voisi jatkaa tästä. Kuviosta voi kuitenkin tehdä vielä lisää havaintoja pisteisiin  $I, T$  ja  $Z$  liittyen. Jos nimittäin  $I, T$  ja  $Z$  ovat samalla suoralla, niin edellisen nojalla pätsi  $\angle IZD = \frac{\angle A}{2} = \angle BAI$ . Pointtina on siis, että  $BZIA$  vaikuttaisi olevan jännelikulmio. (Kolmion  $AIB$  ympärysympyrän keskipistehän tiedetään: se on kaaren  $\widehat{AB}$  keskipiste.) Tämä on jälleen väite, jonka huomaaminen on vaikeampaa kuin sen todistaminen. Alla on helppo todistus.

Kulma  $\angle AIB$  osataan tietysti laskea (se on  $90^\circ + \frac{\angle C}{2}$ ), ja kulma  $\angle AZB$  osataan myös laskea:

$$\angle AZB = 180^\circ - \angle AZC = \angle ZAC + \angle ZCA = \frac{\angle A + \angle B}{2} + \angle C = 90^\circ + \frac{\angle C}{2}.$$

Siis  $ABZI$  on jännelikulmio. Tämä ei, ikävä kyllä, vielä näytä riittävän todistamaan, että  $I, T$  ja  $Z$  ovat samalla suoralla.

Tarkastelemalla kuviota ja laskemalla vielä lisää kulmia huomataan,<sup>28</sup> että  $TI$  ja  $MC$  ovat yhdensuuntaiset: pätee

$$\angle TIM = 180^\circ - \angle TIA = \angle AXT = \angle B = \angle IMC,$$

<sup>28</sup>Lukijasta voi tuntua, että näitä väitteitä vedetään hatusta. Motivaatio on kuitenkin yksinkertaisesti se, että yritettäessä todistaa, että  $I, T$  ja  $Z$  ovat samalla suoralla, tulee samalla todettua kaikenlaista kuvion kulmista. Kulmanjahtausta tehdessä kannattaakin pitää silmät auki, jolloin voi saada muitakin tuloksia kuin sen, mitä lähti alun perin hakemaan.

mistä väite seuraa.

Tästä motivoituneena luonnollinen idea on yrittää todistaa, että jompikumpi janoista  $ZI$  ja  $ZT$  on yhdensuuntainen janan  $MC$  kanssa. Jana  $ZI$  on tähän tarkoitukseen parempi, koska tiedämme kulman  $\angle IZC$  (koska  $BZIA$  on jännelikulmio). Viimeistely onkin helppoa:

$$\angle IZC = \frac{\angle A}{2} = \angle BCM,$$

joten  $ZI$  ja  $MC$  ovat yhdensuuntaisia. Täten  $Z, T$  ja  $I$  ovat samalla suoralla. Nyt tiedämme lisäksi, että  $DT = DZ$ .

Olemme todistaneet jo vaikka mitä, mutta itse alkuperäinen väite vielä puuttuu. Nyt voisi olla hyvä aika keskittyä siihen.<sup>29</sup> Haluamme siis todistaa, että  $X, Z$  ja  $M$  ovat samalla suoralla. Käymällä läpi eri tapoja muotoilla tämä väite nähdään seuraava muotoilu: haluamme todistaa, että  $\angle ZXC = \frac{\angle A}{2}$ . Tämä muotoilu on hyvä seuraavasta syystä: koska  $\angle TZC = \frac{\angle A}{2}$ , kehäkulmalauseen tangenttiversion nojalla  $\angle ZXT = \frac{\angle A}{2}$  pätee jos ja vain jos kolmion  $XZT$  ympärysympyrä on tangentti janalle  $BC$ .

Miltä kuvio näyttäisi, jos kolmion  $XZT$  ympärysympyrä olisi tangentti janalle  $BC$ ? Tutkimalla tangenttia  $BC$  huomataan, että pisteen potenssilla saataisiin  $CZ^2 = CT \cdot CX$ . Toisaalta pisteen potenssilla saadaan  $CT \cdot CX = CA^2$ . Saamme siis  $CZ = CA$ , mutta tämän tiesimme jo. Oleellista on, että tämä päättely voidaan tehdä toiseen suuntaan.

Pisteen potenssin nojalla  $CZ^2 = CA^2 = CT \cdot CX$ , joten

$$\frac{CT}{CZ} = \frac{CX}{CA},$$

joten kolmiot  $CZT$  ja  $CXZ$  ovat yhdenmuotoiset. Nyt  $\angle CXZ = \angle CZT = \frac{\angle A}{2}$ , mistä väite seuraa.

Kommentti: Kuvioon kannattaa rohkeasti lisätä uusia pisteitä. Heti ratkaisun alussa kuvioon lisättiin pisteet  $M$  ja  $F$ . Jälkiviisaana on ilmiselvää, että näin tehdään, mutta tämän vaiheen tärkeyttä on vaikea liioitella. Miten voi tehdä tehtävän kannalta tärkeitä pisteitä koskevia havaintoja, jos näitä pisteitä ei ole edes merkitty kuvaan? Ratkaisun aikana kuvioon lisättiin vielä piste  $T$ . Tämäkään ei vaadi kovin ihmeellistä intuitiota:<sup>30</sup> alkuperäisestä kuvasta pistää silmään, että  $CX$  ja  $AF$  näyttäisivät

<sup>29</sup>Tämä ei oikeastaan ole aivan se, miten ratkoin tehtävää. Ajatusprosessini oli enemmänkin seuraava: "Yritetään todistaa, että  $X, Z$  ja  $M$  ovat samalla suoralla. En kyllä näe mitään järkevää strategiaa tämän todistamiseksi. Tehdään siis tässä kohtaa vielä jotain muuta. Ahaa, seuraavanlainen väite näyttäisi pätevän. Todistetaan se." Seuraavaksi todistin väitteen, ja palasin ajatusprosessin alkuun. Toistin prosessia useammankin kerran ratkaisun aikana ja käytin joka kerralla jonkin verran aikaa itse pääväitteen todistamiseen. Tämä omalta osaltaan selittää, miksi tehtävien ratkaisemiseen kuluu paljon aikaa: uusia tuloksia saadessa pitää miettiä, mitä havainnoista seuraa.

<sup>30</sup>Ollessani kokemattomampi kilpailija olin hämmentynyt siitä, miten geometrian tehtävissä kuuluu keksiä, mitkä uudet pisteet kuvaan kuuluu lisätä. Lisättävät pisteet ovat usein hyvin luonnollisia, kuten tässä ratkaisussa. Yleisesti ongelmia ratkoessa ei juurikaan koskaan (ainakaan minulla) tule keksittyä mitään aivan ihmeellistä tyhjistä. Ideoilla on luonnolliset motivaatiot, ja vaikealta näyttävät askeleet koostuvatkin pienemmistä huomioista.

leikkaavan kolmion  $AXI$  ympärysympyrällä, joten tätä leikkauspistettä kannattaa tietysti tarkastella.

Minulta kului hieman turhankin kauan keksiä, miten tehtävä viimeistellään, kun pisteiden  $I, T$  ja  $Z$  on todistettu olevan samalla suoralla. Olin liian keskittynyt jahtailemaan kuviosta kulmia ja etsimään jänne-likulmioita, jotta pisteen potenssi olisi tullut heti mieleeni. Palaset loksahivat paikalleen nähdessäni pisteestä  $T$  lähtevät puolisuoran  $CX$ , joka lävistää kolmion  $AXI$  ympärysympyrää, ja ympyrän tangentit  $CZ$  ja  $CA$ . Tämä kuva muistutti riittävästi pisteen potenssin tilannetta, joten tajusin käyttää sitä.

## 7 Aritmetiikan peruslause (Lukuteoria)

Tässä luvussa käydään läpi lukuteorian perusteita. Tärkein tulos on aritmetiikan peruslause.

Aritmetiikan peruslause on syystäkin nimetty peruslauseeksi: se on hyvin perustavanlaatuisen tulos, ja ilman sitä on hyvin vaikea tehdä oikein mitään lukuteoriassa.<sup>31</sup>

Kerrataan alkuluvun määritelmä.

### Määritelmä

Kokonaislukua  $p > 1$  kutsutaan alkuluvuksi, jos se ei ole jaollinen muilla positiivisilla kokonaisluvuilla kuin 1 ja  $p$ .

Päätulos on seuraava.

### Lause (Aritmetiikan peruslause)

Olkoon  $n$  positiivinen kokonaisluku. Luku  $n$  voidaan esittää yksikäsitteisellä tavalla alkulukujen tulona.

Esimerkiksi 12 on yksikäsitteisesti  $2 \cdot 2 \cdot 3$ . Huomaa, että tulontekijöiden järjestyksellä ei ole väliä, eli vaikkapa  $2 \cdot 3 \cdot 2$  on sama tapa esittää luku 12 alkulukujen tulona kuin  $2 \cdot 2 \cdot 3$ . Usein samat alkutekijät ”kerätään” yhteen, ja luvun  $n$  alkutekijähajotelmaksi kirjoitetaan

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k},$$

missä  $p_1, \dots, p_k$  ovat eri alkulukuja ja  $a_i$  ovat positiivisia kokonaislukuja.

Tulos on uskottava, mutta sen todistaminen ei ole aivan suoraviivaista. Ennen todistusta esitetäänkin pari aputulosta, jotka ovat itsessäänkin hyödyllisiä.

### 7.1 Bezout’n lemma

Ensimmäinen tulos on Bezout’n lemma. Bezout’n lemma on näennäisesti kaukana aritmetiikan peruslauseesta, mutta sitä tullaan tarvitsemaan myöhemmin.

#### Lemma

Olkoot  $a$  ja  $b$  kokonaislukuja. Oletetaan, että ei ole olemassa ykköstä suurempaa kokonaislukua  $c$ , joka jakaa molemmat luvuista  $a$  ja  $b$ . Tällöin on olemassa sellaiset kokonaisluvut  $x$  ja  $y$ , että

$$ax + by = 1.$$

Lemman ehdon täyttäviä  $a$  ja  $b$  sanotaan yhteistekijättömiksi tai suhteelliseksi alkuluvuiksi, ja sanotaan, että lukujen  $a$  ja  $b$  suurin yhteinen tekijä on 1. Selvästikin

<sup>31</sup>Harjoitustehtävä: Todista (ilman aritmetiikan peruslauseetta), että  $2^n$  ei ole jaollinen kolmella millään positiivisella kokonaisluvulla  $n$ .

ehto on välttämätön ehto sille, että  $ax + by = 1$  jollain  $x$  ja  $y$ : muuten lemmän  $c$  jakaisi yhtälön vasemman puolen, muttei oikeaa. Esimerkiksi yhtälön  $15x + 6y = 1$  vasen puoli on aina jaollinen kolmella, kun taas oikea puoli ei ole koskaan jaollinen kolmella.

Tässä on lemmalle todistus.<sup>32</sup> Olkoon  $d$  pienin positiivinen kokonaisluku, joka voidaan esittää muodossa  $ax + by$ . Haluamme osoittaa, että  $d = 1$ . Tehdään vastaoletus, eli oletetaan, että  $d > 1$ . Kirjoitetaan  $ax_d + by_d = d$ , missä  $x_d$  ja  $y_d$  ovat kokonaislukuja.

Koska  $d > 1$  ja lukujen  $a$  ja  $b$  suurin yhteinen tekijä on 1, niin  $d$  ei voi jakaa molempia luvuista  $a$  ja  $b$ . Oletetaan, että  $d$  ei jaa lukua  $b$  (tapaus, jossa  $d$  ei jaa lukua  $a$ , on samanlainen). Kirjoitetaan jakoyhtälön avulla  $b = kd + r$ , missä  $r$  ( $0 \leq r < d$ ) on jakojäännös ja  $k$  on kokonaisosa, kun  $b$  jaetaan luvulla  $d$ . Koska  $d$  ei jaa lukua  $b$ , niin  $r$  ei ole 0, ja täten  $0 < r < d$ . Nyt

$$r = b - kd = b - k(ax_d + by_d) = a \cdot (-kx_d) + b(1 - ky_d).$$

Olemme siis saaneet esitettyä lukua  $d$  pienemmän positiivisen kokonaisluvun  $r$  muodossa  $ax + by$ . Tämä on ristiriita, eli vastaoletus on väärä, ja tuleekin päteä  $d = 1$ . Olemme valmiit.

Kommentti: Todistuksessa on siis ideana, että jos löydämme vaikkapa sellaiset luvut  $x$  ja  $y$ , että  $ax + by = 3$ , niin tätä esitystä voidaan vielä ”parantaa”, ja lopulta saadaan  $ax + by = 1$ . Todistus myös antaa tavan, jolla voidaan käytännössä löytää nämä halutut  $x$  ja  $y$ . Menetelmä ei kuitenkaan ole paras mahdollinen lukujen löytämiseen. Niin sanottu Eukleideen algoritmi on parempi tähän tarkoitukseen, mutta se on mielestäni vaikeampi kuin edellinen todistus. Tämän vuoksi edellä on esitetty toisenlainen algoritmi.

## 7.2 Eukleideen lemma

Bezout’n lemmaa sovelletaan ns. Eukleideen lemmän todistamiseen. Eukleideen lemma on hyvin luonnollinen.

### Lemma

Jos alkuluku  $p$  jakaa kahden kokonaisluvun  $a$  ja  $b$  tulon  $ab$ , niin  $p$  jakaa vähintään toisen luvuista  $a$  ja  $b$ .

Lemman tulos ei tietenkään päde muilla kuin alkuluvuilla: esimerkiksi  $6 \mid 2 \cdot 3$ , mutta 6 ei jaa kumpaakaan luvuista 2 ja 3.

Todistetaan Eukleideen lemma. Jos  $p$  jakaa luvun  $a$ , niin olemme valmiit. Oletetaan, että näin ei ole. Koska  $p$  on alkuluku, ei ole olemassa sellaista kokonaislukua  $c$  ( $c > 1$ ), joka jakaa molemmat luvuista  $a$  ja  $p$ . Siispä Bezout’n lemmän nojalla on olemassa sellaiset kokonaisluvut  $x$  ja  $y$ , että

$$ax + py = 1.$$

<sup>32</sup>Kiitokset Juho Aralalle tämän todistuksen keksimisestä.



Kerrotaan yhtälö puolittain luvulla  $b$ :

$$(ab)x + p(by) = b.$$

Oletettiin, että  $p$  jakaa tulon  $ab$ , joten  $p$  jakaa molemmat yhtälön vasemman puolen termeistä. Täten  $p$  jakaa niiden summan ja siten oikean puolen luvun  $b$ . Tämä todistaa väitteen.

Eukleideen lemma yleistyy useammalle luvulle suoraan induktiolla: jos  $p$  on alkuluku, joka jakaa lukujen  $a_1, a_2, \dots, a_n$  tulon, niin  $p$ :n tulee jakaa vähintään yksi näistä luvuista.

### 7.3 Aritmetiikan peruslauseen todistus

Ensimmäiseksi todistetaan, että jokainen ykköstä suurempi positiivinen kokonaisluku  $n$  voidaan esittää jollain tavalla alkulukujen tulona (missä alkulukujen määrä saa olla 1). Tehdään vastaoletus, ja tutkitaan pienintä lukua  $n$ , jota ei voida esittää alkulukujen tulona.

Jos  $n$  on alkuluku, on se alkulukujen tulo, mikä johtaa ristiriitaan. Jos taas  $n$  ei ole alkuluku, niin  $n$  voidaan määritelmän mukaan kirjoittaa muodossa  $ab$ , missä  $1 < a, b < n$ . Koska  $a$  ja  $b$  ovat pienempiä kuin  $n$  ja  $n$  on pienin luku, jota ei voida esittää alkulukujen tulona,  $a$  ja  $b$  voidaan esittää alkulukujen tulona. Mutta nyt myös tulo  $ab$  on alkulukujen tulo ja  $ab = n$ , ristiriita.

Siis vastaoletus oli väärä, eli jokainen ykköstä suurempi positiivinen kokonaisluku on alkulukujen tulo.

(Tapauksessa  $n = 1$  voisi ajatella, että tulossa ei ole yhtäkään alkulukua, vaan kyseessä on ns. tyhjä tulo.)

Keskitytään sitten vaikeampaan osuuteen, eli tulon yksikäsitteisyyteen. Oletetaan, että luku  $n$  voidaan esittää kahdella tavalla alkulukujen tulona: olkoon

$$n = p_1 p_2 p_3 \cdots p_k = q_1 q_2 q_3 \cdots q_m,$$

missä  $p_1, p_2, \dots, p_k$  ja  $q_1, q_2, \dots, q_m$  ovat alkulukuja. Halutaan osoittaa, että nämä esitykset ovat samat, kuten tapauksessa  $12 = 2 \cdot 2 \cdot 3 = 2 \cdot 3 \cdot 2$ .

Tutkitaan alkulukua  $p_1$ . Se jakaa vasemman puolen  $p_1 p_2 \cdots p_k$  ja täten myös oikean puolen  $q_1 q_2 \cdots q_m$ . Luvun  $p_1$  tulee jakaa Eukleideen lemmän (monen luvun version) vuoksi jokin luvuista  $q_i$ . Koska lukujen järjestyksellä ei ole väliä, voidaan olettaa, että  $i = 1$  eli että  $p_1$  jakaa luvun  $q_1$ .

Luku  $q_1$  on alkuluku, joka on jaollinen luvulla  $p_1$ . Tulee olla  $p_1 = q_1$ , ja yhtälö  $p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_m$  yksinkertaistuu muotoon

$$p_2 p_3 \cdots p_k = q_2 q_3 \cdots q_m.$$

Ongelma on palautettu helpompaan versioon, ja näin voidaan jatkaa: Lukua  $p_2$  vastaa jokin alkuluku oikealla puolella yhtälöä, vaikkapa luku  $q_2$ . Supistetaan luvut  $p_2$  ja  $q_2$  pois ja jatketaan.

Prosessi loppuu siihen, kun toisella puolella ei ole enää alkulukuja eli kun toinen puoli on 1. Tällöin myös toisen puolen tulee olla 1, eli molemmat puolet olivat alun perin samat. Tämä todistaa alkutekijähajotelman yksikäsitteisyyden.

## 7.4 Aritmetiikan peruslauseen seurauksia

Aritmetiikan peruslause on ennen kaikkea fakta, joka auttaa ajattelemaan kokonaislukuja ”oikealla” tavalla. Esimerkiksi jaollisuus määräytyy täysin alkutekijähajotelman kautta: luku  $a$  jakaa luvun  $b$  täsmälleen silloin, kun jokaisen alkutekijän eksponentti luvussa  $a$  on enintään vastaava eksponentti luvussa  $b$ . (Todistuksen idea: toinen suunta on selvä, ja toista suuntaa varten tehdään vastaoletus, jonka jälkeen sovelletaan Eukleideen lemmaa.) Ennen kuin mainitaan lisää ominaisuuksia, esitetään kätevä notaatio.

### Määritelmä

Olkoon  $n \neq 0$  kokonaisluku, ja olkoon  $p$  alkuluku. Merkitään notaatiolla  $v_p(n)$  luvun  $p$  eksponenttia luvun  $n$  alkutekijähajotelmassa.

### Esimerkki

Pätee  $v_2(12) = 2$ ,  $v_3(12) = 1$  ja  $v_5(12) = 0$ .

Jokainen positiivinen kokonaisluku  $n$  voidaan ajatella äärettömänä lukujonona  $v_2(n), v_3(n), v_5(n), v_7(n), \dots$ . Tässä muutama huomio:

1. Positiiviset kokonaisluvut  $a$  ja  $b$  ovat samat täsmälleen silloin, kun kaikilla alkuluvuilla  $p$  pätee  $v_p(a) = v_p(b)$ .
2. Luku  $a$  jakaa luvun  $b$  täsmälleen silloin, kun  $v_p(a) \leq v_p(b)$  kaikilla alkuluvuilla  $p$ .
3. Nollasta eroavien kokonaislukujen  $a$  ja  $b$  suurin yhteinen tekijä  $\text{sy}(a, b)$  (eli suurin kokonaisluku, joka jakaa molemmat luvuista  $a$  ja  $b$ ) on

$$2^{\min(v_2(a), v_2(b))} 3^{\min(v_3(a), v_3(b))} 5^{\min(v_5(a), v_5(b))} \dots$$

Huomaa, että tulossa on vain äärellisen monta ykkösestä poikkeavaa termiä.

4. Nollasta eroavien kokonaislukujen  $a$  ja  $b$  pienin yhteinen jaettava  $\text{py}(a, b)$  (eli pienin positiivinen kokonaisluku, joka on jaollinen molemmilla luvuista  $a$  ja  $b$ ) on

$$2^{\max(v_2(a), v_2(b))} 3^{\max(v_3(a), v_3(b))} 5^{\max(v_5(a), v_5(b))} \dots$$

Tässäkin tulossa on vain äärellisen monta ykkösestä poikkeavaa termiä.

Huomioista 3 ja 4 saadaan, että kaikilla alkuluvuilla  $p$  pätee

$$\begin{aligned} v_p(ab) &= v_p(a) + v_p(b) = \min(v_p(a), v_p(b)) + \max(v_p(a), v_p(b)) \\ &= v_p(\text{sy}(a, b)) + v_p(\text{py}(a, b)) = v_p(\text{sy}(a, b)\text{py}(a, b)), \end{aligned}$$

ja ensimmäisen huomion nojalla nyt pätee  $ab = \text{sy}(a, b)\text{py}(a, b)$ .

Tässä on pari samantyylistä huomiota. Ensimmäinen koskee tekijöiden määrää.

### Lemma

Positiivisen kokonaisluvun  $n$  tekijöiden määrä on  $(v_2(n) + 1) \cdot (v_3(n) + 1) \cdot (v_5(n) + 1) \cdot \dots$

Ykköstä suurempia tulontekijöitä on jälleen vain äärellinen määrä.

Lemman todistus on luonnollinen. Luvun  $n$  tekijän  $m$  tulee olla sellainen, että  $v_p(m) \leq v_p(n)$  kaikilla alkuluvuilla  $p$ . Toisaalta jos  $v_p(m) \leq v_p(n)$  kaikilla  $p$ , niin  $m$  myös on luvun  $n$  tekijä. Kysymys siis on: kuinka monta sellaista lukujonoa  $v_2(m), v_3(m), v_5(m), \dots$  on olemassa, jolla  $v_p(m) \leq v_p(n)$  kaikilla  $p$ ?

Luvulle  $v_2(m)$  vaihtoehdot ovat  $0, 1, 2, \dots, v_2(n)$ , eli vaihtoehtoja on  $v_2(n) + 1$  kappaletta. Vastaavasti luvulle  $v_p(m)$  on  $v_p(n) + 1$  vaihtoehtoa kaikilla  $p$ . Tämä johtaa vastaukseen.

### Esimerkki

Lasketaan luvun 1080 tekijöiden määrä. Luvun 1080 alkutekijähajotelma on  $2^3 \cdot 3^3 \cdot 5$ . Valittaessa luvun 1080 tekijöitä luvun 2 eksponentille on 4 vaihtoehtoa  $0, 1, 2, 3$ , luvun 3 eksponentille on 4 vaihtoehtoa ja luvun 5 eksponentille on 2 vaihtoehtoa. Muiden alkulukujen eksponenteille on 1 vaihtoehto: eksponentti 0.

Siispä tekijöitä on  $4 \cdot 4 \cdot 2 = 32$  kappaletta.

### Tekijöiden summa

Vastaavalla logiikalla kuin aiemmin saadaan luvun  $n$  tekijöiden summa. Tulos itsessään ei ole erityisen tärkeä, mutta todistuksen idea on näppärä.

### Lemma

Luvun  $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$  tekijöiden summa on

$$\frac{p_1^{a_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{a_2+1} - 1}{p_2 - 1} \dots \frac{p_k^{a_k+1} - 1}{p_k - 1}.$$

Kuten aiemmin, voimme ”rakentaa” luvulle  $n$  tekijän  $m$  valitsemalla ensiksi eksponentin  $v_{p_1}(m) \leq a_1$  alkuluvulle  $p_1$ , sitten eksponentin  $v_{p_2}(m) \leq a_2$  luvulle  $p_2$  ja niin edelleen. Tämän voi muotoilla niin, että valitaan tulon

$$\begin{aligned} & \left(1 + p_1 + p_1^2 + \dots + p_1^{a_1}\right) \\ & \cdot \left(1 + p_2 + p_2^2 + \dots + p_2^{a_2}\right) \\ & \quad \dots \\ & \cdot \left(1 + p_k + p_k^2 + \dots + p_k^{a_k}\right) \end{aligned}$$

jokaisesta tulontekijästä yksi termi: ensimmäisestä  $p_1^{v_{p_1}(m)}$ , toisesta  $p_2^{v_{p_2}(m)}$  ja niin edelleen. Koska käymme läpi kaikki tavat rakentaa tekijät ja summaamme tulokset, on haluttu tekijöiden summa sama kuin koko tulo. Geometrisen summan avulla saadaan

$$1 + p_i + p_i^2 + \dots + p_i^{a_i} = \frac{p_i^{a_i+1} - 1}{p_i - 1},$$

mikä viimeistelee todistuksen.

Lukija voi harjoituksena miettiä, miten lasketaan luvun  $n$  tekijöiden tulo.

Käytännössä kaikissa edellä esitetyissä tuloksissa yksittäisten alkulukujen muodostamia ehtoja pystyi yhdistelemään ja saamaan kokonaiskuvan. Esimerkkinä suurin yhteinen tekijä luvuille  $a$  ja  $b$ : valitaan jokin alkuluku  $p$  ja sen suurin potenssi, joka jakaa molemmat luvuista  $a$  ja  $b$ , ja kerrotaan nämä potenssit yhteen.

**Monissa tilanteissa yksittäisten alkulukujen muodostamat ehdot voidaan yhdistää kokonaiskuvaksi.**

Tämä on yleinen teema. Yleisemmin puhutaan, että ”lokaalit” ehdot tai väitteet yhdistetään ”globaaliksi” tulokseksi. Tämä teema toistuu useaan kertaan lukuteorian materiaalissa. Käymme seuraavaksi läpi pari aiheeseen liittyvää esimerkkitehtävää.

## 7.5 Esimerkkitehtäviä

### Tehtävä

Olkoot  $a$  ja  $b$  sellaisia positiivisia kokonaislukuja, joilla  $a^2b|a^3+b^3$ . Osoita, että  $a = b$ .

Väitteen  $a = b$  todistamiseksi riittää todistaa, että  $v_p(a) = v_p(b)$  kaikilla alkuluvuilla  $p$ . Jaollisuusehto antaa, että  $v_p(a^2b) \leq v_p(a^3 + b^3)$  kaikilla  $p$ . Selvästi  $v_p(a^2b) = v_p(a^2) + v_p(b) = 2v_p(a) + v_p(b)$ , mutta oikean puolen laskeminen on vaikeampaa. Tässä auttaa seuraava lemma.

### Lemma

Olkoot  $x$  ja  $y$  positiivisia kokonaislukuja. Päte

$$v_p(x + y) \geq \min(v_p(x), v_p(y)).$$

Lisäksi jos  $v_p(x) \neq v_p(y)$ , niin  $v_p(x + y) = \min(v_p(x), v_p(y))$ .

Huomautus: jos  $v_p(x) = v_p(y)$ , voi päteä  $v_p(x + y) > \min(v_p(x), v_p(y))$ : näin käy esimerkiksi tapauksessa  $x = 1$  ja  $y = p - 1$ . Lisäksi väite pätee  $+$ -merkin sijasta myös miinusmerkillä, kuten todistuksesta nähdään.

Lemman todistus on suoraviivainen: selvästi jos  $p^k|x$  ja  $p^k|y$ , niin  $p^k|x + y$ . Vali-

taan  $k = \min(v_p(x), v_p(y))$ , mikä todistaa epäyhtälön. Yhtäsuuruustapausta varten huomataan, että mikäli  $v_p(x) \neq v_p(y)$ , niin

$$p^{\min(v_p(x), v_p(y))+1}$$

jakaa täsmälleen yhden luvuista  $x$  ja  $y$ , joten se ei voi jakaa summaa  $x + y$ .

Palataan tehtävän ratkaisuun. Haluaisimme, että  $v_p(a) = v_p(b)$ , joten oletetaan, että  $v_p(a) \neq v_p(b)$ , ja yritetään saada ristiriita.

Tutkitaan ensiksi tapaus  $v_p(a) > v_p(b)$ . Tällöin  $v_p(a^3) \neq v_p(b^3)$ , ja lemmän toisen osan avulla

$$v_p(a^3 + b^3) = \min(v_p(a^3), v_p(b^3)) = v_p(b^3) = 3v_p(b).$$

Siispä  $v_p(a^2b) = 2v_p(a) + v_p(b) \leq 3v_p(b)$ , eli  $v_p(a) \leq v_p(b)$ . Tämä on ristiriita oletuksen  $v_p(a) > v_p(b)$  kanssa.

Tutkitaan sitten tapaus  $v_p(b) > v_p(a)$ . Vastaavasti kuin edellä saadaan  $v_p(a^3 + b^3) = 3v_p(a)$ , joten  $2v_p(a) + v_p(b) \leq 3v_p(a)$ , mikä johtaa ristiriitaan kuten edellä.

Täten tulee päteä  $v_p(a) = v_p(b)$  kaikilla  $p$ , eli  $a = b$ .

Seuraavana on samantyylinen esimerkki, joka on esiintynyt vuoden 2007 Baltian tie -kilpailussa.

### Tehtävä

Olkoot  $a$  ja  $b$  positiivisia kokonaislukuja, joilla  $b < a$  ja luku  $a^3 + b^3 + ab$  on jaollinen luvulla  $ab(a - b)$ . Osoita, että  $ab$  on kokonaisluvun kuutio.

Haluamme osoittaa, että  $ab$  on kokonaisluvun kuutio. Toisin sanoen halutaan, että  $v_p(ab) = v_p(a) + v_p(b)$  on jaollinen kolmella kaikilla alkuluvuilla  $p$ . Tutkitaan jälleen lukuja  $v_p(a)$  ja  $v_p(b)$  sekä jaollisuusehtoa.

Tiedämme siis, että  $v_p(ab(a - b)) \leq v_p(a^3 + b^3 + ab)$ . Kuten edellisessä ratkaisussa on nytkin hyödyllistä jakautua tapauksiin, jotta  $v_p$ -lausekkeiden arvot saadaan laskettua.

Tutkitaan ensin tapausta  $v_p(a) > v_p(b)$ . Tällöin edellisen tehtävän lemmän yhtäsuuruusosion avulla

$$v_p(ab(a - b)) = v_p(a) + 2v_p(b).$$

Yritetään sitten laskea  $v_p(a^3 + b^3 + ab)$ . Tämä ei onnistu suoraan, koska emme tiedä, mikä luvuista  $v_p(a^3)$ ,  $v_p(b^3)$  ja  $v_p(ab)$  on pienin. Tiedämme ainoastaan, että  $v_p(a^3) > v_p(b^3)$ , eli pienin luku on joko  $v_p(b^3)$  tai  $v_p(ab)$ . Jakaudutaan osatapauksiin.

*Tapaus 1:*  $v_p(b^3) < v_p(ab)$ . Tällöin  $v_p(a^3 + b^3 + ab) = v_p(b^3) = 3v_p(b)$ . Tätä  $v_p(ab(a - b)) = v_p(a) + 2v_p(b) > 3v_p(b)$ , mikä on ristiriita.

*Tapaus 2:*  $v_p(ab) < v_p(b^3)$ . Tällöin  $v_p(a^3 + b^3 + ab) = v_p(ab) = v_p(a) + v_p(b)$ . Jotta pätee  $v_p(a) + 2v_p(b) \leq v_p(a) + v_p(b)$ , tulee päteä  $v_p(b) = 0$ , mutta tällöin ehto  $v_p(ab) < v_p(b^3)$  ei toteudu. Ristiriita.

*Tapaus 3:*  $v_p(ab) = v_p(b^3)$ . Tällöin  $v_p(ab) = 3v_p(b)$  on jaollinen kolmella, ja saimme mitä halusimme.

Tapaus  $v_p(a) < v_p(b)$  etenee vastaavalla tavalla (lausekkeet ovat käytännössä symmetrisiä lukujen  $a$  ja  $b$  suhteen).

Tutkitaan vielä tapaus  $v_p(a) = v_p(b) = t$ . Saamme  $v_p(ab(a-b)) \geq 3t$ , ja jos  $t > 0$ , niin  $v_p(a^3 + b^3 + ab) = 2t$ . Tämä ei käy, eli tulee olla  $t = 0$ . Tällöin  $v_p(ab) = 0$  on jaollinen kolmella, kuten halusimmekin.

Siis kaikissa mahdollisissa tapauksissa pätee, että  $v_p(ab)$  on jaollinen kolmella. Olemme valmiit.

Kommentti: Ratkaisussa oli jonkin verran tapauskäsittelyä, mutta se ei vaatinut nerokkaita oivalluksia. Joka kohdassa jakauduttiin sopiviin tapauksiin, jotta termit  $v_p(ab(a-b))$  ja  $v_p(a^3 + b^3 + ab)$  saatiin laskettua. Tämän jälkeen saatiin joko ristiriita tai haluttu väite.

Viimeisenä esitettävä tehtävä on selvästi aiempia vaikeampi.

### Tehtävä

Etsi kaikki positiiviset kokonaisluvut  $a$  ja  $b$ , joilla  $a^b = b^a$ .

Potenssiin korottaminen ei tunnetusti ole vaihdannainen operaatio, eli esimerkiksi  $2^3 \neq 3^2$ . Tästä huolimatta pätee  $2^4 = 4^2$ . Yhtälöllä on lisäksi triviaaliratkaisu  $a = b$ . Onko tässä kaikki ratkaisut yhtälölle?

Nähdään, että jos  $a$  ja  $b$  antavat ratkaisun, niin niillä tulee olla samat alkutekijät. Luonnollinen seuraava askel on tutkia näiden alkutekijöiden eksponentteja. Olkoon  $v_p(a) = x$  ja  $v_p(b) = y$ , ja oletetaan, että  $x, y > 0$ . Vertaamalla alkuluvun  $p$  eksponenttia yhtälön vasemmalla ja oikealla puolella saadaan

$$bx = ay$$

eli

$$\frac{x}{y} = \frac{a}{b}.$$

Tämä tarkoittaa, että suhde  $\frac{x}{y}$  ei riipu valitusta alkuluvusta  $p$ : lopputulos on aina  $\frac{a}{b}$ . Jos  $\frac{x}{y} = \frac{a}{b}$  on supistetussa muodossa  $\frac{X}{Y}$ , niin kaikilla  $p$  pätee  $X|v_p(a)$  ja  $Y|v_p(b)$ . Tällöin on olemassa jokin kokonaisluku  $m$  (joka voi riippua luvusta  $p$ ), jolla  $v_p(a) = mX$  ja  $v_p(b) = mY$ . Kirjoitetaan  $f(p) = m$ .

Tästä motivoituneena määritellään kokonaisluku

$$c = 2^{f(2)} 3^{f(3)} 5^{f(5)} \dots,$$

jotta saadaan  $c^X = a$  ja  $c^Y = b$ . Jos  $c = 1$ , niin  $a = b = 1$ . Muussa tapauksessa sijoitus alkuperäiseen yhtälöön antaa

$$c^{Xb} = c^{Ya},$$

eli  $Xb = Ya$ , eli

$$Xc^Y = Yc^X.$$

Yhtälöllä on triviaaliratkaisu  $X = Y$  (eli  $a = b$ ). Etsitään muita ratkaisuja. Symmetrian nojalla voidaan olettaa, että  $X > Y$ . Tällöin

$$c^{X-Y} = \frac{X}{Y}.$$

Vasen puoli on kokonaisluku, joten myös oikean puolen tulee olla, eli  $Y|X$ . Kirjoitetaan  $X = Yt$ , missä  $t \geq 2$  on kokonaisluku. Saadaan

$$c^{(t-1)Y} = t.$$

Idea on, että vasen puoli on suurempi kuin oikea puoli, ellei  $t$  ole pieni. Jos nimittäin  $t > 2$ , niin

$$c^{(t-1)Y} \geq 2^{t-1} > t.$$

Siispä  $t = 2$ , eli  $c^Y = 2$ , mistä seuraa  $Y = 1, c = 2$  ja siten  $X = 2$ . Tästä saadaan ratkaisu  $a = c^X = 4$  ja  $b = c^Y = 2$ . Lisäksi on symmetrinen ratkaisu  $a = 2$  ja  $b = 4$ , sekä aiemmin todettu triviaaliratkaisu  $a = b$ . Yhtälöllä ei ole muita ratkaisuja.

Kommentti: Ratkaisu koostuu kahdesta osasta. Ensimmäisessä osassa todistetaan, että on olemassa kokonaisluku  $c$  niin, että  $c^X = a$  ja  $c^Y = b$  positiivisilla kokonaisluvulla  $X$  ja  $Y$ . Sijoitetaan nämä yhtälöön  $a^b = b^a$ . Toisessa osassa ratkaisua todistetaan, että syntyneellä yhtälöllä  $c^{X-Y} = \frac{X}{Y}$  ei ole muita ratkaisuja kuin  $X = Y$  ja  $X = 2, Y = 1$  (sekä  $Y = 2, X = 1$ ).

Ensimmäisen osan voi tehdä useammalla tavalla. Esitetty  $v_p$ -menetelmä on yksi tapa, joka lähestyy ongelmaa konkreettisesti alkutekijähajotelman kautta. Toinen tapa on ottaa  $a$ -kantainen logaritmi puolittain ja saada yhtälö  $\frac{b}{a} = \log_a(b)$ . Tämä tarkoittaa, että  $\log_a(b)$  on rationaaliluku  $\frac{b}{a} = \frac{X}{Y}$ , mistä saadaan halutut yhtälöt  $c^X = a$  ja  $c^Y = b$ .

Toisen osan arvion  $c^{(t-1)Y} \geq 2^{t-1} > t$  tyyliiset arviot ovat usein hyödyllisiä: monesti tehtävissä voi saada ylimääräistä tietoa muuttujista tekemällä sopivia epäyhtälöitä. Joskus arviot ovat suhteellisen helppoja (kuten tässä), joskus taas ratkaisu voi perustua hyviin arvioihin. Luvussa Arviointi ja epäyhtälöt keskitytään tarkemmin tähän aiheeseen.

Lukuteorian lisätehtäviä -luvussa on esitetty vielä yksi tehtävä, joka perustuu alkutekijähajotelmien eksponenttien tutkimiseen mutta joka on huomattavasti tähän mennessä esitettyjä vaikeampi.

Tehtävään on myös aivan muunlainen ratkaisu: annettu yhtälö antaa  $a^{1/a} = b^{1/b}$ . Tutkimalla derivaattaa funktion  $f(x) = x^{1/x}$  nähdään olevan aidosti vähenevä, kun  $x > e$ . Siis jos  $a \neq b$ , sekä  $a$  että  $b$  eivät voi olla suurempia kuin  $e \approx 2.7$ . Tästä saadaan, että epätriviaaleilla ratkaisuilla tulee päteä  $a = 2$  tai  $b = 2$ , mistä saadaan edellä löydetty ratkaisut.

## 8 Kongruenssit (Lukuteoria)

Tässä luvussa käydään läpi kongruenssien perusteet.

### 8.1 Motivaatio

Istut vankilan sellissä. Eteesi tuodaan kaksi paperilappua, joissa kummassakin on yksi positiivinen kokonaisluku, toisessa  $a$  ja toisessa  $b$ . Sinut vapautetaan, jos osaat kertoa, mikä on luvun  $a + b$  viimeinen numero. Sellissä on kuitenkin hyvin pimeää, etkä siksi tarkalleen näe, mitkä luvut paperilappuihin on kirjoitettu. Kykenet erottamaan vain, että luvun  $a$  viimeinen numero on 2 ja että luvun  $b$  viimeinen numero on 3. Pystytkö ratkaisemaan ongelman?

Vastaus on myönteinen: luvun  $a + b$  viimeinen numero on  $2 + 3 = 5$ . Tämä on intuitiivisesti melko selvää. Väitettä voisi perustella kuvittelemalla mitä tapahtuu, kun luvut  $a$  ja  $b$  lasketaan allekkain yhteen. Ensiksi lasketaan ykkösten paikalle tuleva numero (tässä tapauksessa  $2 + 3 = 5$ ), tämän jälkeen siirrytään kymmenten paikalle, sitten satojen ja niin edelleen. Yhteenlaskun lopputuloksessa ykkösten paikalle tulevaan numeroon vaikuttaa vain alkuperäisten lukujen ykkösten paikalla olevat numerot.

Entä jos luvun  $a + b$  sijasta olisikin haluttu tietää, mikä on tulon  $ab$  viimeinen numero? Tässäkin tapauksessa ongelman ratkaiseminen onnistuu: luvun  $ab$  viimeinen numero on  $2 \cdot 3 = 6$ . Tämä ei välttämättä ole aivan yhtä intuitiivista kuin yhteenlaskun tapauksessa. Perustelun voi hoitaa tutkimalla allekkain kertolaskua vastaavaan tapaan kuin yhteenlaskun tapauksessa. Kertolaskun lopputuloksessa ykkösten paikalle tulevaan numeroon vaikuttavat vain alkuperäisten lukujen ykkösten paikalla olevat numerot.

Jos lukujen  $a$  ja  $b$  viimeiset numerot olisivat olleet vaikkapa 7 ja 8, niin nyt luvun  $a + b$  viimeinen numero ei tietenkään ole  $7 + 8 = 15$ , vaan tästä tulee vähentää 10, jolloin viimeinen numero on siis 5. Vastaavasti tulon  $ab$  viimeinen numero ei ole  $7 \cdot 8 = 56$ , vaan viimeinen numero saadaan ottamalla viimeisten numeroiden tulon viimeinen numero.

Tämä on kongruenssien perusidea. Kehittelemme ideaa hieman eteenpäin.

Luvun  $a$  viimeisen numeron voi ajatella olevan jakojäännös, kun luku  $a$  jaetaan luvulla 10 (vaikkakaan tämä ei välttämättä aluksi tunnu luonnollisimmalta tavalta ajatella asiaa). Edellä esitetty esimerkki siis kertoo, että jakojäännöksiä voidaan laskea yhteen ja kertoa keskenään: jos luvun  $a$  jakojäännös kymmenellä jaettaessa on 2 ja luvun  $b$  jakojäännös on 3, niin luvun  $a + b$  jakojäännös on  $2 + 3$  ja luvun  $ab$  jakojäännös on  $2 \cdot 3$ .

Luku 10 ei tietenkään ole mitenkään erityinen: olemme vain tottuneet esittämään lukuja kymmenjärjestelmässä, jossa on 10 numeroa (0, 1, 2, 3, 4, 5, 6, 7, 8, 9). Samat ominaisuudet pätevät, vaikka tutkisimme jakojäännöksiä vaikkapa seitsemällä jaettaessa. Esimerkiksi jos luvun  $a$  jakojäännös seitsemällä jaettaessa on 2 ja luvulla  $b$  tämä jakojäännös on 4, niin saamme lukujen  $a + b$  ja  $ab$  jakojäännökset summaamalla



tai kertomalla jakojäännökset 2 ja 4 (kertolaskun kohdalla luvusta  $2 \cdot 4 = 8$  tulee vielä vähentää 7, jotta saadaan jakojäännös, joka on pienempi kuin jakaja).

Kongruenssit antavat kätevän tavan puhua jakojäännöksistä.

### Määritelmä

Olkoot  $a, b$  ja  $m$  ( $m > 0$ ) kokonaislukuja. Jos luvuilla  $a$  ja  $b$  on sama jakojäännös jaettaessa luvulla  $m$  (eli toisin sanoen  $m \mid a - b$ ), niin merkitään

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

Sanotaan, että  $a$  ja  $b$  ovat kongruentteja modulo  $m$ . Lukua  $m$  kutsutaan moduloksi. Puhekielessä sanotaan usein lyhyesti ” $a$  on  $b$  modulo  $m$ ”.

Esimerkiksi  $a \equiv b \pmod{10}$  tarkoittaa, että luvuilla  $a$  ja  $b$  on sama jakojäännös kymmenellä jaettaessa (eli niiden viimeiset numerot ovat samat).

### Esimerkki

Seuraavat kongruenssiyhtälöt pätevät:

- $13 \equiv 3 \pmod{10}$
- $25 \equiv 15 \pmod{10}$
- $10 \equiv 3 \pmod{7}$
- $-4 \equiv 3 \pmod{7}$

## 8.2 Perusominaisuuksia

Totesimme edellä, että jos luvun  $a$  viimeinen numero on 2 (eli  $a \equiv 2 \pmod{10}$ ) ja luvun  $b$  viimeinen numero on 3 (eli  $a \equiv 3 \pmod{10}$ ), niin

$$a + b \equiv 2 + 3 \pmod{10}$$

ja

$$ab \equiv 2 \cdot 3 \pmod{10}.$$

Toisin sanoen voimme laskea kongruenssiyhtälöitä yhteen ja voimme myös kertoa niitä keskenään (kunhan modulo on yhtälöissä sama).

Kongruenssin merkintää ” $\equiv$ ” ei olekaan sattumalta valittu niin, että se näyttää samalta kuin yhtäsuuruusmerkki ” $=$ ”. Mainitaan ensiksi pari selvää huomiota kongruensseista.

- Jos  $a \equiv b \pmod{m}$ , niin  $b \equiv a \pmod{m}$ .
- Kaikilla  $a$  pätee  $a \equiv a \pmod{m}$ .

- Jos  $a \equiv b \pmod{m}$  ja  $b \equiv c \pmod{m}$ , niin  $a \equiv c \pmod{m}$ .

Jos väitteet haluaa perustella formaalisti, kannattaa käyttää jaollisuuteen perustuvaa määritelmää kongruensseille (eli  $a \equiv b \pmod{m}$  jos  $m \mid a - b$ ). Esimerkiksi viimeisessä kohdassa väite seuraa siitä, että  $m \mid a - b$  ja  $m \mid b - c$  johtaa ehtoon  $m \mid (a - b) + (b - c) = a - c$ .<sup>33</sup>

Kuten edellä totesimme, kongruenssiyhtälöitä voi siis laskea yhteen ja kertoa keskenään:

### Lemma

Olkoot  $a, b, c, d$  ja  $m$  ( $m > 0$ ) kokonaislukuja. Oletetaan, että  $a \equiv b \pmod{m}$  ja  $c \equiv d \pmod{m}$ . Tällöin

1.  $a + c \equiv b + d \pmod{m}$
2.  $a - c \equiv b - d \pmod{m}$
3.  $ac \equiv bd \pmod{m}$ .

Pointti on siis:

**Kongruenssiyhtälöitä voi käsitellä kuten tavallisia yhtälöitä.**

Aivan kaikki ehdot eivät säily, kuten myöhemmin nähdään eksponenttifunktioita käsiteltäessä, mutta perusominaisuudet toimivat kuten voi odottaa.

Perustelimmekin lemmän väitteitä viimeisiä numeroita tarkasteltaessa, mutta esitetään niille kuitenkin hieman formaalimmat perustelut.

Aloitetaan ensimmäisestä. Tiedämme, että  $m \mid a - b$  ja  $m \mid c - d$ . Täten  $m \mid (a - b) + (c - d) = (a + c) - (b + d)$ , mikä on haluttu väite.

Toinen väite seuraa vastaavasti: Oletamme, että  $m \mid a - b$  ja  $m \mid c - d$ , joten  $m \mid (a - b) - (c - d) = (a - c) - (b - d)$ .

Kolmas väite on hieman vaikeampi. Koska  $m \mid a - b$ , voidaan kirjoittaa  $a - b = mk$  jollain kokonaisluvulla  $k$ . Siispä  $a = b + mk$ . Vastaavasti  $c = d + mn$  jollain kokonaisluvulla  $n$ . Nyt

$$ac = (b + mk)(d + mn) = bd + mnb + mkd + m^2kn \equiv bd + 0 + 0 + 0 = bd \pmod{m}.$$

(Tässä yhtäsuuruusmerkkien  $=$  tilalla voisi käyttää kongruenssimerkkejä  $\equiv$ , koska jos  $x = y$ , niin  $x \equiv y \pmod{m}$ ). On kuitenkin selkeämpää, kun yhtäsuuruusmerkkiä käytetään silloin, kun sen tiedetään pätevän.)

Asettamalla lemmaan  $c = a$  ja  $d = b$  saadaan, että mikäli  $a \equiv b \pmod{m}$ , niin  $a \cdot a \equiv b \cdot b \pmod{m}$ , eli  $a^2 \equiv b^2 \pmod{m}$ . Kongruenssiyhtälöitä voi siis neliöidä. Potenssiinkorottaminen onnistuu myös yleisesti, mikä seuraa helpolla induktiolla:

<sup>33</sup>Merkintä muotoa  $x \mid y = z$  tarkoittaa, että  $x \mid y$  ja  $y = z$ .

jos  $a \equiv b \pmod{m}$  ja  $a^{k-1} \equiv b^{k-1} \pmod{m}$ , niin kertomalla yhtälöt yhteen saadaan  $a^k \equiv b^k \pmod{m}$ .

Tätä voi vielä yleistää:

#### Lause (Polynomit kongruensseissa)

Olkoon  $P$  polynomi, jonka kertoimet ovat kokonaislukuja. Olkoot  $a, b$  ja  $m$  sellaisia kokonaislukuja, että  $a \equiv b \pmod{m}$ . Tällöin

$$P(a) \equiv P(b) \pmod{m}.$$

Väite on käytännössä katsoen jo todistettu: Jos  $a \equiv b \pmod{m}$ , niin tiedämme, että

- $a^k \equiv b^k \pmod{m}$  kaikilla kokonaisluvuilla  $k \geq 0$
- kongruenssiyhtälön saa kertoa puolittain kokonaisluvulla
- kongruenssiyhtälöitä saa laskea yhteen

Voimme siis ”rakentaa” polynomin  $P$ . Jos vaikkapa  $P(x) = 123x^{456} + 789x^3 + 100x^2$ , niin voimme summata yhtälöt

$$123a^{456} \equiv 123b^{456} \pmod{m},$$

$$789a^3 \equiv 789b^3 \pmod{m}$$

ja

$$100a^2 \equiv 100b^2 \pmod{m}.$$

Väite seuraa tästä.

### 8.3 Esimerkkitehtävä

Esitetään viimeisiä numeroita käsittelevä tehtävä, jota on luontevaa lähestyä moduloilla. Esimerkiksi ylioppilaskokeessa (pitkä matematiikka, kevät 2011, tehtävä 12) ja MAOLin alkukilpailussa (avoin sarja, 2017, tehtävä 1) on esiintynyt vastaavia tehtäviä.

#### Tehtävä

Mikä on luvun  $123^{34} + 123^{456}$  viimeinen numero?

Toisin sanoen haluamme laskea luvun  $123^{34} + 123^{456}$  modulo kymmenen. Tätä varten hajotetaan ongelma kahteen osaan: lasketaan, mitä on  $123^{34}$  modulo kymmenen ja mitä on  $123^{456}$  modulo kymmenen. Kongruenssien perusominaisuuksien vuoksi tiedämme, että vastaus saadaan summaamalla näistä saatavat jakojäännökset yhteen.

Tuumasta toimeen. Lasketaan ensiksi, mitä on  $12^{34} \pmod{10}$ . Aluksi voidaan todeta, että kantaluku 12 voidaan korvata luvulla 2. Niinpä niin: tiedämme, että

$$12 \equiv 2 \pmod{10}$$

ja että kongruenssiyhtälöitä saa korottaa johonkin potenssiin. Korottamalla potenssiin 34 saadaan

$$12^{34} \equiv 2^{34} \pmod{10}.$$

Voimme siis tutkia luvun  $12^{34}$  sijasta lukua  $2^{34}$ .

Ei ole ilmeistä, miten lasketaan luvun  $2^{34}$  viimeinen numero. Tämä onnistuu kuitenkin listaamalla muutaman ensimmäisen kakkosen potenssin viimeiset numerot. Ensimmäiset 10 kakkosen potenssia ovat

$$2, 4, 8, 16, 32, 64, 128, 256, 512, 1024,$$

ja näiden viimeiset numerot ovat

$$2, 4, 8, 6, 2, 4, 8, 6, 2, 4.$$

Nähdään säännönmukaisuus: viimeiset numerot toistuvat neljän pituisissa jaksoissa. Tämän väitteen perustelu onnistuu jälleen kerran kongruenssien perusominaisuuksilla: Tiedämme, että jos jonkin luvun viimeinen numero on 2, niin kertomalla luku kahdella saadaan viimeiseksi numeroksi 4. Kertomalla uudestaan saadaan viimeiseksi numeroksi 8. Seuraavaksi saadaan viimeiseksi numeroksi 6 (koska tulon  $8 \cdot 2 = 16$  viimeinen numero on 6). Kertomalla vielä kerran kahdella saadaan viimeiseksi numeroksi 2. Pääsimme siihen, mistä lähdimmekin.

Nyt huomataan, että  $34 = 2 + 8 \cdot 4$ , jossa 4 on jakson pituus, eli luvun  $2^{34}$  viimeinen numero on sama kuin luvun  $2^2$ . Siis

$$12^{34} \equiv 4 \pmod{10}.$$

Prosessi on aivan vastaava luvun  $123^{456}$  kohdalla. Ensiksi todetaan, että

$$123^{456} \equiv 3^{456} \pmod{10},$$

ja listaamalla kolmosen potensseja nähdään viimeisten numeroiden toistuvan seuraavasti:

$$3, 9, 7, 1, 3, 9, 7, 1, \dots$$

Luku 456 on jaollinen neljällä, joten osumme jakson neljänteen lukuun eli ykköseen. Siis

$$3^{456} \equiv 1 \pmod{10}.$$

Yhdistämällä edelliset huomiot saadaan, että

$$12^{34} + 123^{456} \equiv 4 + 1 \equiv 5 \pmod{10}.$$

Siis viimeinen numero on 5.

Kommentti: Huomasimme, että eksponenttilausekkeissa kuten  $12^{34}$  voidaan kantalukua redusoida modulo 10, eli

$$12^{34} \equiv 2^{34} \pmod{10}.$$

Eksponenttia ei kuitenkaan saa käsitellä vastaavalla tavalla. Totesimme edellä, että luvun  $2^n$  viimeinen numero on aina jokin numeroista 2, 4, 8, 6 ja että jokainen numero esiintyy neljän välein. Siis eksponenttia tulee tutkia modulo 4, ei modulo 10.

Ei ole sattumaa, että viimeiset numerot käyttäytyvät jaksollisesti. Tähän teemaan keskitytään tarkemmin seuraavassa luvussa.

## 8.4 Kiinalainen jäännöslause

Kilpailutehtävissä käytetyistä kongruensseihin liittyvistä tuloksista kiinalainen jäännöslause on (kongruenssien perusominaisuuksien jälkeen) selvästi yksi yleisimmistä ja tärkeimmistä. Johdatteluna toimii seuraava tehtävä.

### Tehtävä

Olkoon  $x$  kokonaisluku. Tiedetään, että  $x \equiv 1 \pmod{3}$ . Mitä voidaan sanoa luvun  $x$  jakojäännöksestä jaettaessa luvulla 4?

Vastaus: ei yhtikäs mitään. Jos nimittäin  $x = 1$ , ehto  $x \equiv 1 \pmod{3}$  pätee, ja  $x \equiv 1 \pmod{4}$ . Jos  $x = 4$ , saadaan  $x \equiv 0 \pmod{4}$ . Jos  $x = 7$ , niin  $x \equiv 3 \pmod{4}$ , ja jos  $x = 10$ , niin  $x \equiv 2 \pmod{4}$ .

Tässä on toinen samankaltainen tehtävä.

### Tehtävä

Olkoon  $x$  kokonaisluku. Tiedetään, että  $x$  on pariton. Mitä voidaan sanoa luvun  $x$  jakojäännöksestä jaettaessa luvulla 4?

Tällä kertaa voidaan sanoa jotain: ei voi päteä  $x \equiv 0 \pmod{4}$ , koska tällöin  $x$  olisi jaollinen neljällä, joten se olisi parillinen. Vastaavasti ei voi päteä  $x \equiv 2 \pmod{4}$ . Vaihtoehdot  $x \equiv 1 \pmod{4}$  ja  $x \equiv 3 \pmod{4}$  ovat kuitenkin mahdollisia, kuten nähdään arvoilla  $x = 1$  ja  $x = 3$ .

Kiinalainen jäännöslause kertoo juuri tästä ilmiöstä. Kun tutkittavat modulot ovat yhteistekijättömiä,<sup>34</sup> mitään tietoa ei välity eri kongruenssiehtojen välillä. Tämä voidaan muotoilla seuraavasti.

<sup>34</sup>Entä se tapaus, jossa moduloilla on yhteisiä tekijöitä? Yleistetty kiinalainen jäännöslause vastaa tähän kysymykseen: yhtälöryhmällä  $x \equiv a_i \pmod{m_i}$ ,  $1 \leq i \leq n$  on ratkaisu jos ja vain jos  $\text{sy}(m_i, m_j) \mid a_i - a_j$  kaikilla  $i \neq j$ . (En ole tarvinnut tulosta kovinkaan montaa kilpailutehtävää ratkoessani, mutta tulos on mielestäni luonnollinen ja kiinnostava.) Todistuksen idea: Kiinalaisen jäännöslauseen nojalla ehto  $x \equiv a_i \pmod{m_i}$  voidaan muotoilla ehtoina  $x \equiv a_i \pmod{p^{v_p(m_i)}}$ . Eri luvut  $m_i$  antavat nyt tietoa siitä, mitä  $x$  on modulo  $p$ :n potenssit. Enää tulee tutkia, ovatko ehdot yhteensopivia sen tiedon kanssa, joka saadaan isoimmasta  $p$ :n potenssista.

**Lause (Kiinalainen jäännöslause)**

Olkoon  $n$  positiivinen kokonaisluku. Olkoot  $m_1, m_2, \dots, m_n$  positiivisia kokonaislukuja, jotka ovat pareittain yhteistekijättömiä. Olkoot  $a_1, a_2, \dots, a_n$  mielivaltaisia kokonaislukuja. Tällöin on olemassa kokonaisluku  $x$ , jolla

$$x \equiv a_i \pmod{m_i}$$

kaikilla  $1 \leq i \leq n$ . Lisäksi tämä  $x$  on yksikäsitteinen modulo  $m_1 m_2 \cdots m_n$ .

**Esimerkki**

Valitaan lauseeseen  $n = 2$ ,  $m_1 = 3$ ,  $m_2 = 4$  ja  $a_1 = 1$ . Lause sanoo, että kaikilla luvun  $a_2$  valinnoilla on olemassa  $x$ , jolla  $x \equiv 1 \pmod{3}$  ja  $x \equiv a_2 \pmod{4}$ . Tämä vastaa juurikin ensimmäisen tehtävän tilannetta.

On monta tapaa, jolla lauseen voi visualisoida. Yksi tapa on kuvitella  $n$  kappaletta hedelmäpyöriä, joista ensimmäisessä on  $m_1$  eri hedelmän kuvaa, toisessa  $m_2$  kuvaa, ja näin jatkuu, kunnes viimeisessä on  $m_n$  kuvaa. Yhden askeleen aikana jokaista hedelmäpyörää pyöräytetään yksi askel eteenpäin. Lause sanoo, että kaikki mahdolliset hedelmäyhdistelmät tullaan käymään läpi, kunhan  $\text{syt}(m_i, m_j) = 1$  kaikilla  $i \neq j$ . Lisäksi ehto ”tämä  $x$  on yksikäsitteinen modulo  $m_1 m_2 \cdots m_n$ ” tarkoittaa, että samat hedelmien yhdistelmät toistuvat aina täsmälleen  $m_1 m_2 \cdots m_n$  askeleen välein.

Tämä ajattelutapa melkein jo todistaa väitteen. Numeroidaan pyörän  $i$  hedelmät luvuin  $0, 1, \dots, m_i - 1$ . Aloitetaan lauseen yksikäsitteisyysosan todistamisesta. Oletetaan, että on olemassa kaksi ajanhetkeä  $t_1$  ja  $t_2$ , joina näkyvissä ovat samat hedelmät. Osoitetaan, että  $t_1 \equiv t_2 \pmod{m_1 m_2 \cdots m_n}$ .

Pyörässä 1 näkyy samat hedelmät, joten tulee olla  $t_1 \equiv t_2 \pmod{m_1}$ , koska ensimmäisen pyörän hedelmät toistuvat  $m_1$  askeleen välein. Siispä  $m_1 | t_1 - t_2$ . Vastaavasti pyörille  $2, 3, \dots, n$  saadaan  $m_2 | t_1 - t_2, \dots, m_n | t_1 - t_2$ .

Koska luvut  $m_1, m_2, \dots, m_n$  ovat yhteistekijättömiä, pätee  $m_1 m_2 \cdots m_n | t_1 - t_2$ . Siispä samat kuviot voivat toistua vain  $m_1 m_2 \cdots m_n$  ajanhetken välein, mikä todistaa yksikäsitteisyyden.

Miten todistetaan, että jokainen hedelmäyhdistelmä esiintyy prosessin aikana? Tutkitaan ajanhetkiä  $0, 1, 2, \dots, m_1 m_2 \cdots m_n - 1$ . Edellisen päättelyn nojalla näillä ajanhetkillä näkyvillä ovat eri hedelmäyhdistelmät. Mutta koska mahdollisia hedelmäyhdistelmiä on  $m_1 m_2 \cdots m_n$  kappaletta, tulee jokaisen yhdistelmän esiintyä. Tämä todistaa lauseen.

Esitetään pari esimerkkiä kiinalaisen jäännöslauseen käytöstä.

**Tehtävä**

Ratkaise yhtälöryhmä

$$\begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5}. \end{cases}$$

Kiinalainen jäännöslause kertoo, että yhtälöryhmällä on ratkaisu ja että tämä ratkaisu on yksikäsitteinen modulo  $2 \cdot 3 \cdot 5 = 30$ . Lause ei kuitenkaan kerro, miten ratkaisu löydetään. Yksi tapa on valita aina kaksi yhtälöä ja yhdistää ne.

Tutkitaan ensiksi yhtälöitä  $x \equiv 1 \pmod{2}$  ja  $x \equiv 2 \pmod{3}$ . Tällä yhtälöparilla on yksikäsitteinen ratkaisu modulo 6, ja tämä saadaan kokeilemalla kaikki kuusi vaihtoehtoa. Saadaan  $x \equiv 5 \pmod{6}$ .

Enää tulee ratkoa yhtälöpari  $x \equiv 5 \pmod{6}$ ,  $x \equiv 3 \pmod{5}$ . Koska tällä yhtälöparilla on ratkaisu modulo  $6 \cdot 5 = 30$ , voidaan käydä läpi kaikki 30 eri vaihtoehtoa  $0, 1, 2, \dots, 29$ . Tämä on hieman hidasta, ja kokeilemista voidaankin nopeuttaa käymällä läpi vain ne vaihtoehdot, joilla  $x \equiv 5 \pmod{6}$ . Nämä ovat 5, 11, 17, 23 ja 29. Tästä nähdään, että ratkaisu on  $x \equiv 23 \pmod{30}$ .

**Tehtävä**

Olkoon  $n$  positiivinen kokonaisluku. Osoita, että on olemassa jotkin  $n$  peräkkäistä positiivista kokonaislukua, jotka ovat jaollisia jonkin alkuluvun neliöllä.

Haluamme siis löytää positiivisen kokonaisluvun  $x$ , jolla luvut  $x, x+1, x+2, \dots, x+n-1$  ovat kaikki jaollisia jonkin alkuluvun neliöllä. Yritetään valita ne alkuluvut, joiden neliöillä nämä luvut ovat jaollisia: valitaan luvulle  $x$  alkuluku  $p_0$ , luvulle  $x+1$  alkuluku  $p_1$  ja jatketaan näin, kunnes viimeiseksi luvulle  $x+n-1$  valitaan alkuluku  $p_{n-1}$ . Haluamme siis, että  $x+i \equiv 0 \pmod{p_i^2}$  kaikilla  $i$ . Tällä yhtälöryhmällä on ratkaisu, kunhan alkuluvut  $p_i$  ovat eri alkulukuja. Osa kelpaavista kokonaisluvuihin  $x$  ovat tietysti positiivisia.

Kiinalainen jäännöslause on hyvä pitää mielessä: se on jälleen esimerkki monen lokaalin ehdon yhdistämisestä yhdeksi globaaliksi ehdoksi.

## 8.5 Jakolasku kongruensseissa

Voiko kongruensseissa tehdä jakolaskuja? Voi, mutta tämä vaatii varovaisuutta. Esimerkiksi  $6 \equiv 12 \pmod{2}$ , mutta tätä yhtälöä ei saa jakaa puolittain kahdella. Kolmella jakaminen kuitenkin onnistuu. Miksi toinen onnistuu ja toinen ei?

Tutkitaan yhtälöä muotoa  $ac \equiv bc \pmod{m}$ , jonka haluamme jakaa puolittain luvulla  $c$ . Tiedämme siis, että  $m|ac - bc = c(a - b)$ , ja haluaisimme saada ehdon  $m|a - b$ . Edellä totesimme, että aina tämä ei onnistu, joten yritetään saada jotain muuta.

Aritmetiikan peruslauseen yhteydessä todettiin, että jaollisuutta voi tutkia yksi

alkuluku kerrallaan. Valitaan siis jokin alkuluku  $p$ . Olkoon  $M$  luvun  $p$  eksponentti luvun  $m$  alkutekijähajotelmassa, ja määritellään  $C$  vastaavasti. Olkoon vielä  $D$  luvun  $p$  eksponentti erotuksen  $a - b$  alkutekijähajotelmassa. Koska  $m|c(a - b)$ , pätee  $M \leq C + D$ , eli  $M - C \leq D$ . Tämä kertoo, että  $p^{M-C}$  jakaa luvun  $a - b$ .

Väitteessä ” $p^{M-C}$  jakaa luvun  $a - b$ ” ei ole järkeä, jos  $C > M$ . Tällöin alkuluvun  $p$  eksponentista luvussa  $a - b$  ei voida sanoa mitään. Muussa tapauksessa päättely toimii. Tapaukset voidaan yhdistää sanomalla, että  $p^{M-\min(M,C)}|a - b$ .

Olemme saaneet kirjoitettua jokaista alkulukua koskevat ehdot. Nämä lokaalit ehdot voidaan yhdistää globaaliksi ehdoksi. Minimi eksponenteista  $M$  ja  $C$  voidaan muotoilla näppärästi suurimman yhteisen tekijän avulla seuraavan lemmän mukaisesti.

### Lemma

Olkoot  $a, b, c$  ja  $m$  ( $m > 0$ ) kokonaislukuja. Oletetaan, että  $ac \equiv bc \pmod{m}$ . Tällöin

$$a \equiv b \left( \text{mod } \frac{m}{\text{sy}(m, c)} \right).$$

Tärkein tapaus lemmasta on  $\text{sy}(m, c) = 1$ , jolloin modulo ei muutu.

Kysymyksen ”voiko kongruensseissa tehdä jakolaskuja?” voi tulkita myös toisella tavalla: jos valitaan kaksi kokonaislukua  $a$  ja  $b$ , tarkoittaako  $\frac{a}{b} \pmod{m}$  mitään järkevää?

Jos merkitään  $\frac{a}{b} \equiv x \pmod{m}$ , tulisi luvun  $x$  toteuttaa ehto  $a \equiv bx \pmod{m}$ . Tämä ei onnistu, jos esimerkiksi  $b = 0$  ja  $a = 1$ . Tämä ei yllätä: nollalla ei muutenkaan saa jakaa. Yhtälöllä  $a \equiv bx \pmod{m}$  on kuitenkin aina ratkaisu, jos  $\text{sy}(m, b) = 1$ : Haluamme, että  $m|a - bx$  eli että  $a - bx = my$  jollain kokonaisluvulla  $y$ . Mutta Bezout’n lemmän nojalla yhtälöllä  $bx + my = 1$  on ratkaisu, ja kertomalla yhtälöin puolittain luvulla  $a$  saadaan  $bX + mY = a$  sopivilla kokonaisluvuilla  $X$  ja  $Y$ .

### Esimerkki

Luvun, joka on  $\frac{1}{2} \pmod{3}$ , tulisi olla sellainen luku  $x$ , joka kerrottuna kahdella antaa ykkösen. Siis  $2x \equiv 1 \pmod{3}$ . Tällä yhtälöllä on uniikki ratkaisu  $x \equiv 2 \pmod{3}$ .

Yleisestikin vastaavalla lineaarisella yhtälöllä  $bx \equiv a \pmod{m}$  on uniikki ratkaisu, kunhan  $\text{sy}(m, b) = 1$ : Jos  $x_1$  ja  $x_2$  ovat ratkaisuja, niin  $bx_1 \equiv a \equiv bx_2 \pmod{m}$ , eli  $m|b(x_1 - x_2)$ . Koska  $\text{sy}(m, b) = 1$ , tästä seuraa  $m|x_1 - x_2$ , eli  $x_1 \equiv x_2 \pmod{m}$ .

Saadut tulokset ovat erityisen hyviä, kun modulo  $m$  on alkuluku  $p$ . Tällöin  $\frac{a}{b} \pmod{p}$  voidaan ajatella kokonaislukuna modulo  $p$ , kunhan  $b$  ei ole  $0 \pmod{p}$ . Erityisesti todetaan, että  $\frac{1}{b} \pmod{p}$  on järkevä merkintä. Tätä lukua kutsutaan luvun  $b$  käänteisluvuksi modulo  $p$ .



## 9 Eksponenttifunktiot ja neliönjäännökset (Lukuteoria)

Tässä luvussa käydään syvemmin läpi kongruenssien ominaisuuksia.

### 9.1 Fermat'n pieni lause

Kongruenssiyhtälöitä voidaan laskea yhteen ja kertoa keskenään, ja jakolasku toimii jotenkuten. Lisäksi jos  $a \equiv b \pmod{m}$ , niin  $P(a) \equiv P(b) \pmod{m}$  kaikilla kokonaislukukertoimisilla polynomeilla  $P$ . Vaikuttaa siltä, että kaikki toimii kuten pitääkin. Varmaan myös eksponenttifunktiot käyttäytyvät samanlaisella logiikalla? Ei aivan.

#### Esimerkki

Pätee  $0 \equiv 3 \pmod{3}$ , mutta  $2^0 \equiv 1 \not\equiv 2 \equiv 2^3 \pmod{3}$ .

#### Esimerkki

Pätee  $2^0 \equiv 1 \pmod{2}$ , ja kaikilla positiivisilla kokonaisluvuilla  $x$  pätee  $2^x \equiv 0 \pmod{2}$ .

Eksponenttifunktiot eivät siis käyttäydy samalla tavalla kuin polynomit, mutta ne käyttäytyvät tästä huolimatta melko säännöllisesti. Tärkeä tulos tähän liittyen on Fermat'n pieni lause.

#### Lause (Fermat'n pieni lause)

Olkoon  $p$  alkuluku, ja olkoon  $a$  kokonaisluku, joka ei ole jaollinen luvulla  $p$ . Tällöin

$$a^{p-1} \equiv 1 \pmod{p}.$$

Esitetään tulokselle perustelu ennen varsinaista todistusta. Tutkitaan lukuja  $a^0, a^1, a^2, \dots \pmod{p}$ . Koska kokonaisluvut antavat vain  $p$  erisuurta jakojäännöstä luvulla  $p$  jaettaessa, tulee jossain kohtaa lukujen  $a^n$  olla jaksollisia, eli ne alkavat toistaa samoja lukuja, jotka ovat jo esiintyneet.

Tässä toistettavien lukujen listassa tulee olla luku  $a^0 = 1$ . Oletetaan nimittäin, että lukujono alkaa toistaa itseään kohdasta  $i$  lähtien ja että toistuvia lukuja on  $T$  kappaletta. Tällöin  $a^i \equiv a^{i+T} \pmod{p}$ . Jos  $i = 0$ , olemme valmiit. Muuten, koska  $\text{syt}(a, p) = 1$ , voidaan yhtälö jakaa puolittain luvulla  $a$ , ja saadaan  $a^{i-1} \equiv a^{i-1+T} \pmod{p}$ . Tämä on ristiriidassa sen kanssa, että lukujono toistaa itseään vasta kohdasta  $i$  lähtien. Täten  $a^T \equiv 1 \pmod{p}$  jollain  $T > 0$ .

**Esimerkki**

Luvun 2 potenssit  $2^0, 2^1, 2^2, \dots$  ovat  $1, 2, 4, 3, 1, 2, 4, 3, \dots$  modulo 5. Tässä toistuvia lukuja on  $T = 4$  kappaletta.

Miksi juuri  $T = p - 1$  kelpaa? Syy tälle on se, että luvun  $a$  potensseille  $a^0, a^1, a^2, \dots \pmod{p}$  on  $p - 1$  eri mahdollisuutta, nimittäin luvut  $1, 2, \dots, p - 1 \pmod{p}$  (tämä selitys ei ole kovin syvällinen – todistus antaa paremman käsityksen).

Fermat’n pieni lause siis osoittaa, että eksponenttifunktio on jaksollinen jaksolla  $p - 1$ . Tilanne on erilainen kuin esimerkiksi polynomeilla, joiden todettiin olevan jaksollisia jaksolla  $p$ .

Esitetään sitten lauseelle todistus. Olkoon  $S = \{1, 2, 3, \dots, p - 1\}$ , ja olkoon  $T = \{a, 2a, 3a, \dots, (p - 1)a\}$ . Osoitetaan, että ” $S$  ja  $T$  ovat samat modulo  $p$ ”. Tarkemmin sanoen osoitetaan seuraavat väitteet.

- Jokaista joukon  $T$  alkioita  $t$  vastaa uniikki joukon  $S$  alkio  $s$ , jolla  $t \equiv s \pmod{p}$
- Mitään kahta alkioita  $t_1, t_2 \in T$  ei vastaa sama alkio  $s \in S$ .

Jokainen joukon  $T$  alkio on muotoa  $ka$ , missä  $1 \leq k \leq p - 1$  on kokonaisluku. Ensimmäinen väite seuraa tästä: Haluamme, että  $p \nmid ka$ . Mutta jos  $p \mid ka$ , niin joko  $p \mid k$  tai  $p \mid a$ , mutta kumpikaan vaihtoehto ei ole mahdollinen.

Toinen väite on myös selvä: Jos  $t_1 \equiv t_2 \pmod{p}$ , niin  $k_1a \equiv k_2a \pmod{p}$  jollain kokonaisluvuilla  $1 \leq k_1 \neq k_2 \leq p - 1$ . Koska  $\text{syte}(a, p) = 1$ , voidaan jakaa puolittain luvulla  $a$ , jolloin saadaan  $k_1 \equiv k_2 \pmod{p}$ . Erotus  $k_1 - k_2$  on täten jaollinen luvulla  $p$ , ja koska  $1 \leq k_1, k_2 \leq p - 1$ , niin  $|k_1 - k_2| < p$ . Tulee siis olla  $k_1 - k_2 = 0$ , eli  $k_1 = k_2$ , mikä on ristiriita.

Väitteistä seuraa, että joukkojen  $S$  ja  $T$  alkioden tulot ovat samat modulo  $p$ , eli

$$1 \cdot 2 \cdot 3 \cdots (p - 1) \equiv a \cdot 2a \cdot 3a \cdots (p - 1)a \pmod{p}.$$

Koska  $\text{syte}((p - 1)!, p) = 1$ , voidaan jakaa puolittain luvulla  $(p - 1)!$ , jolloin saadaan

$$1 \equiv a \cdot a \cdot a \cdots a = a^{p-1} \pmod{p}.$$

Tämä todistaa väitteen.

## 9.2 Eulerin lause

Fermat’n pieni lause on hyvä tulos, mutta onko olemassa vastaavaa väitettä muille kuin alkulukumoduloille? On, mutta muotoilu on aavistuksen verran teknisempi. Ensin määritellään  $\phi$ -funktio.<sup>35</sup>

<sup>35</sup> $\phi$  lausutaan ”fi”.

**Määritelmä**

Olkoon  $n$  positiivinen kokonaisluku. Määritellään  $\phi(n)$  olemaan niiden kokonaislukujen  $m$  määrä, joilla  $1 \leq m \leq n$  ja  $\text{sy}(m, n) = 1$ .

**Esimerkki**

Pätee  $\phi(6) = 2$ , koska mahdollisista kandidaateista 1, 2, 3, 4, 5 ja 6 ainoastaan kaksi ovat yhteistekijättömiä luvun 6 kanssa, nimittäin luvut 1 ja 5.

**Esimerkki**

Kaikilla alkuluvuilla  $p$  pätee  $\phi(p) = p - 1$ , koska kandidaateista  $1, 2, \dots, p - 1, p$  ainoastaan luku  $p$  ei kelpaa.

**Esimerkki**

Olkoon  $p$  alkuluku ja  $k \geq 1$  kokonaisluku. Tällöin  $\phi(p^k) = p^k - p^{k-1}$ , koska kandidaateista  $1, 2, \dots, p^k$  kelpaavat kaikki paitsi ne, jotka ovat jaollisia luvulla  $p$ . Epäkelpavia lukuja on  $p^{k-1}$ , joten kelpavia on  $p^k - p^{k-1}$ .

Seuraava tulos yleistää Fermat'n pientä lausetta.

**Lause (Eulerin lause)**

Olkoon  $n$  positiivinen kokonaisluku, ja olkoon  $a$  sellainen kokonaisluku, että  $\text{sy}(a, n) = 1$ . Tällöin

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

Eulerin lauseen todistus on käytännössä katsoen sama kuin edellä esitetty Fermat'n pienen lauseen todistus. Tällä kertaa joukoksi  $S$  valitaan niiden lukujen  $s$  joukko, joilla  $1 \leq s \leq n$  ja  $\text{sy}(s, n) = 1$ , ja joukoksi  $T$  luvut muotoa  $as$ , missä  $s \in S$ . Yksityiskohtainen tarkastelu jätetään lukijalle.

Käytännön tarkoituksia varten  $\phi$ -funktion arvoja olisi kiva osata laskea. Seuraava tulos antaa suoran kaavan funktion arvoille.

**Lemma**

Olkoon  $n$  positiivinen kokonaisluku, jonka alkutekijähajotelma on

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}.$$

Tällöin

$$\phi(n) = \prod_{1 \leq i \leq k} p_i^{a_i-1} (p_i - 1).$$

Kaavan voi myös kirjoittaa sievemmin muotoon

$$\phi(n) = n \prod_{1 \leq i \leq k} \left(1 - \frac{1}{p_i}\right).$$

Väitteen todistus perustuu siihen faktaan, että  $\phi(p^a) = p^{a-1}(p-1)$  kaikilla alkuluvuilla  $p$  ja kokonaisluvuilla  $a \geq 1$ . Tämä todistettiin jo edellä esitetyissä esimerkeissä. Enää tulee yhdistää nämä tiedot.<sup>36</sup>

Ideana on käyttää kiinalaista jäännöslausetta. Tutkitaan kandidaatteja  $1, 2, \dots, n$ . Valitaan jokin kandidaatti  $x$ . Tämä  $x$  määräytyy yksikäsitteisesti, kun tiedetään, mitä  $x$  on modulo  $p_i^{a_i}$  kaikilla  $i$ : tällöin kiinalaisen jäännöslauseen avulla tiedetään, mitä  $x$  on modulo  $n$ . Lisäksi kandidaatti  $x$  on kelpaava jos ja vain jos  $x$  on yhteistekijätön kaikkien lukujen  $p_i^{a_i}$  kanssa.

Voimme siis luoda kaikki kelpaavat luvut  $x$  seuraavalla tavalla: Valitaan kokonaisluvut  $b_1, b_2, \dots, b_k$ , joilla  $b_i$  ja  $p_i^{a_i}$  ovat yhteistekijättömiä kaikilla  $i$ , ja valitaan  $x$  olemaan (kiinalaisen jäännöslauseen) yhtälöryhmän  $x \equiv b_i \pmod{p_i^{a_i}}$  ratkaisu väliltä  $[1, n]$ . Käymällä läpi kaikki vaihtoehdot luvuille  $b_1, b_2, \dots, b_k$  saadaan kelpaavat luvut täsmälleen kerran, kun vaaditaan vielä, että  $0 \leq b_i < p_i^{a_i}$  kaikilla  $i$ .

Kuinka monta vaihtoehtoa luvuille  $b_1, b_2, \dots, b_n$  on? Yksittäiselle  $b_i$  on  $\phi(p_i^{a_i})$  vaihtoehtoa, ja kertomalla yksittäisten lukujen  $b_i$  vaihtoehtojen määrä saadaan kelpaavien lukujen määrä. Tämä todistaa halutun väitteen.

Seuraavana esitetään ratkaisu Johdantotehtäviä-luvussa esitettyyn tehtävään. Ratkaisussa kantavana teemana on eksponenttifunktioiden jaksollisuus kongruensseissa.

### Tehtävä

Etsi kaikki positiiviset kokonaisluvut  $x$  ja  $y$ , joilla  $|3^x - 2^y| = 1$ .

Käytännössä ratkaistavana on kaksi eri yhtälöä. Ensimmäinen on  $3^x - 2^y = 1$  ja toinen  $3^x - 2^y = -1$ . Ensimmäisellä näistä on ainakin kaksi ratkaisua  $(x, y) = (1, 1), (2, 3)$ , ja toisella on ainakin yksi ratkaisu  $(x, y) = (1, 2)$ . Voisi veikata, että se yhtälö, jolla on enemmän ratkaisuja, on vaikeampi. Aloitetaan siis yhtälöstä  $3^x - 2^y = -1$ .

Yksi idea yhtälön ratkaisemiseksi on tutkia sitä modulo  $m$  jollain positiivisella kokonaisluvulla  $m$ . Jos nimittäin pätee  $3^x - 2^y = -1$ , niin pätee  $3^x - 2^y \equiv -1 \pmod{m}$  kaikilla  $m$ . Tätä kautta voisimme saada tietoa luvuista  $x$  ja  $y$ .

Millainen olisi hyvä  $m$ ? Ainakin jos  $m$  on kakkosen tai kolmosen potenssi, niin jompikumpi termeistä  $3^x$  ja  $2^y$  on 0 modulo  $m$  (kun muuttujien  $x$  ja  $y$  arvot ovat suuria). Valitaan ensiksi  $m = 3$ . Nyt pätee  $-2^y \equiv -1 \pmod{3}$ , eli  $2^y \equiv 1 \pmod{3}$ . Tämä selvästikin vaatii, että  $y$  on parillinen. Saimme siis tietoa luvusta  $y$ , mikä on tietysti edistystä, mutta tehtävä ei ole vielä ratkennut. Kokeillaan muita luvun  $m$  valintoja.

Valitaan  $m = 4$ . Koska  $y$  on parillinen, niin  $y \geq 2$ , ja tällöin  $-1 \equiv 3^x - 2^y \equiv 3^x \pmod{4}$ . Tästä saadaan ehto  $x \equiv 1 \pmod{2}$ . Yritetään vielä seuraavaa sellaista

<sup>36</sup>Jälleen lokaalit tiedot yhdistetään globaaliksi tulokseksi.

luvun  $m$  arvoa, joka on kakkosen tai kolmosen potenssi, eli lukua  $m = 8$ . Jos  $y \geq 3$ , niin  $-1 \equiv 3^x - 2^y \equiv 3^x \pmod{8}$ . Tällä yhtälöllä ei kuitenkaan ole ratkaisuja, koska luvun 3 potenssit ovat aina 1 tai 3 modulo 8. Siis ainoa mahdollisuus on  $y = 2$ , ja tästä saadaan ratkaisu  $x = 1$  ja  $y = 2$ .

Tutkitaan sitten yhtälöä  $3^x - 2^y = 1$ . Kuten edellä voimme tutkia yhtälöä modulo kakkosen ja kolmosen potenssit. Esimerkiksi modulo 16 saadaan (olettaen, että  $y \geq 4$ ) ehto  $x \equiv 0 \pmod{4}$ . Modulo 9 saadaan (olettaen, että  $x \geq 2$ ) ehto  $y \equiv 3 \pmod{6}$ .

Yhtälöä voisi tutkia vielä esimerkiksi modulo 64 ja modulo 81. Huomataan kuitenkin, että vaikka yhtälöistä saadaan lisää tietoa luvuista  $x$  ja  $y$ , niin emme kuitenkaan saa rajoitettua yhtälön ratkaisuja. Täytyy siis keksiä jotain muuta.

Voisimmeko jotenkin hyödyntää saatuja tietoja  $x \equiv 0 \pmod{4}$  ja  $y \equiv 3 \pmod{6}$ ? Ainakin tietoa  $x \equiv 0 \pmod{4}$  voisi hyödyntää valitsemalla moduloksi  $m$  sellaisen luvun, että kolmosen potenssien jakso modulo  $m$  on jaollinen neljällä. Helpoin tapa toteuttaa tämä idea on valita  $m = 5$ , jolloin Fermat'n pienen lauseen nojalla kolmosen potenssit toistuvat modulo 5 neljän jaksoissa. (Tämän voi tietysti myös tarkistaa tässä tapauksessa käsin). Koska tiedämme, että  $x \equiv 0 \pmod{4}$ , niin pätee  $3^x \equiv 3^0 \equiv 1 \pmod{5}$ . Täten

$$1 = 3^x - 2^y \equiv 1 - 2^y \pmod{5},$$

joten  $2^y$  on jaollinen viidellä. Tämä on selvästi mahdotonta.

Muistetaan, että aiemmin teimme oletukset  $y \geq 4$  ja  $x \geq 2$ . Käytimme lopulta vain oletuksella  $y \geq 4$  saatavaa tietoa, joten tulee enää käsitellä ne tapaukset, joissa  $y < 4$ . Näiden tapausten läpikäynti on helppoa, ja saamme ratkaisut  $(x, y) = (1, 1), (2, 3)$ .

Kaiken kaikkiaan johdantokappaleessa löydetty ratkaisut  $(x, y) = (1, 1), (1, 2), (2, 3)$  ovat yhtälön  $|3^x - 2^y| = 1$  ainoat ratkaisut.

Kommentti: Jos tutkisimme polynomiyhtälöitä eli vaikkapa yhtälöä  $x^2 - 3y^2 = 17$  (joka esiintyy myöhemmin esimerkkit tehtävänä), niin emme voisi mitenkään yhdistellä eri (yhteistekijättömällä) moduloilla saatavia tietoja. Tämä johtuu siitä, että vaikkapa modulo 2 yhtälöstä saadaan ehtoja siitä, mitä  $x$  ja  $y$  ovat modulo 2, ja tutkiminen modulo 5 antaa tietoa siitä, mitä  $x$  ja  $y$  ovat modulo 5. Kiinalaisen jäännöslauseen perusteella nämä ehdot eivät kommunikoi mitenkään keskenään.

Tässä tehtävässä tilanne on kuitenkin toinen. Tutkimalla modulo 16 saimme tiedon  $x \equiv 0 \pmod{4}$ . Tämä kertoo, mitä  $3^x$  on modulo 5. Syy tähän eroon polynomien ja eksponenttifunktioiden välillä on arvojen jaksollisuus: polynomien arvot ovat jaksollisia modulo  $m$  jaksolla  $m$ , mutta eksponenttifunktioiden jaksot ovat jotain aivan muuta. Esimerkiksi kolmosen potenssit ovat jaksollisia jaksolla neljä sekä modulo 16 että modulo 5. Yhteistekijättömät modulot 16 ja 5 siis kommunikoivat keskenään, toisin kuin polynomien tapauksessa.

Näillä ideoilla saamme myös käsitystä siitä, miten tehtävässä kannattaa valita eri moduloita  $m$ : Valitaan niitä niin, että saamme mahdollisimman paljon toisistaan riippuvia kongruenssiehtoja luvuille  $x$  ja  $y$ . Tämä saavutetaan valitsemalla moduloksi  $m$  sellaisia lukuja, että lukujen 2 ja 3 potenssien jaksojen pituudet modulo  $m$  sisältävät paljon yhteisiä tekijöitä. Ratkaisussa tämä saavutettiin kolmosen po-

tensseille arvoilla  $m = 16$  ja  $m = 5$ , joilla nämä jaksojen pituudet olivat samat.<sup>37</sup> Eksponenttifunktioiden jaksollisuuden tutkimista jatketaan seuraavassa luvussa.

### 9.3 Neliönjäännökset

Tutkitaan kokonaislukuja modulo 3. Huomataan, että  $0^2 \equiv 0 \pmod{3}$ ,  $1^2 \equiv 1 \pmod{3}$  ja  $2^2 \equiv 1 \pmod{3}$ . Mikään näistä neliöistä ei ole  $2 \pmod{3}$ . Tästä oikeastaan seuraa, että yhtälöllä  $x^2 \equiv 2 \pmod{3}$  ei ole ratkaisua:

Valitaan mielivaltainen kokonaisluku  $x$ . Tiedetään, että  $x$  on joko 0, 1 tai 2 modulo 3. Jos  $x \equiv 0 \pmod{3}$ , niin neliöimällä yhtälö saadaan  $x^2 \equiv 0^2 \equiv 0 \pmod{3}$ . Vastaavasti muissa tapauksissa saadaan  $x^2 \equiv 1^2 \equiv 1 \pmod{3}$  ja  $x^2 \equiv 2^2 \equiv 1 \pmod{3}$ .

Mitä tapahtuu, jos 3 korvataan jollain muulla alkuluvulla?<sup>38</sup>

#### Määritelmä

Olkoon  $p$  alkuluku. Sanotaan, että kokonaisluku  $a$  on neliönjäännös modulo  $p$ , jos on olemassa kokonaisluku  $x$ , jolla  $x^2 \equiv a \pmod{p}$  ja  $p \nmid a$ . Vastaavasti sanotaan, että  $a$  on neliönepäjäännös modulo  $p$ , jos  $x^2 \not\equiv a \pmod{p}$  kaikilla  $x$  ja  $p \nmid a$ . Luvut  $a \equiv 0 \pmod{p}$  eivät ole neliönjäännöksiä eivätkä neliönepäjäännöksiä.

#### Esimerkki

Luku 1 on neliönjäännös modulo 3, ja luku 2 on neliönepäjäännös modulo 3.

Kuinka monta neliönjäännöstä tai neliönepäjäännöstä on modulo  $p$ ? Tehdään pieni lista:

- Jos  $p = 2$ , on 1 neliönjäännös: 1. Neliönepäjäännöksiä on 0 kappaletta.
- Jos  $p = 3$ , on 1 neliönjäännös: 1. Neliönepäjäännöksiä on 1 kappale.
- Jos  $p = 5$ , on 2 neliönjäännöstä: 1 ja 4. Neliönepäjäännöksiä on 2 kappaletta.
- Jos  $p = 7$ , on 3 neliönjäännöstä: 1, 2 ja 4. Neliönepäjäännöksiä on 3 kappaletta.
- Jos  $p = 11$ , on 5 neliönjäännöstä: 1, 3, 4, 5 ja 9. Neliönepäjäännöksiä on 5 kappaletta.

<sup>37</sup>Muistan joskus nähneeni tehtävän, jossa tutkittiin ainakin viittä eri moduloa, joista viimeinen oli 37. Silloin ajattelin, että ratkaisu oli aivan mahdoton, mutta ratkaisulle on selvä motivaatio: Luku 37 on alkuluku, joten Fermat'n pienen lauseen nojalla eksponenttifunktiot ovat jaksollisia modulo 37 jaksolla 36. Luvulla 36 on vain pieniä alkutekijöitä, joten se kommunikoi hyvin muiden kongruenssiehtojen kanssa.

<sup>38</sup>Mielivaltainen kokonaislukumodulo voidaan palauttaa kiinalaisella jäännöslauseella alkuluvun potensseihin, ja tämä ei ole paljoa vaikeampi tapaus kuin jos modulo olisi alkuluku (katso Lukuteorian lisätehtävät -luvun toisen tehtävän kommentti).

Vaikuttaisi siltä, että neliönjäännöksiä ja -epäjäännöksiä on aina sama määrä, eli  $\frac{p-1}{2}$  (paitsi kun  $p = 2$ ).

### Lemma

Olkoon  $p$  pariton alkuluku. Luvuista  $1, 2, \dots, p-1$  täsmälleen  $\frac{p-1}{2}$  ovat neliönjäännöksiä modulo  $p$ .

Neliönjäännökset saadaan listaamalla  $1^2, 2^2, 3^2, \dots, (p-1)^2$ . Näissä tulisi olla  $\frac{p-1}{2}$  eri lukua.

Valitaan  $p = 13$ . Tällöin luvut  $1^2, 2^2, \dots, 12^2$  ovat

$$1, 4, 9, 3, 12, 10, 10, 12, 3, 9, 4, 1 \pmod{13}.$$

Säännönmukaisuus on selvä: ensimmäiset  $\frac{p-1}{2}$  lukua ovat eri lukuja, ja sitten samat luvut toistuvat käänteisessä järjestyksessä. Loppuosan toistuminen johtuu yksinkertaisesti yhtälöstä  $x^2 \equiv (p-x)^2 \pmod{p}$ , mikä seuraa suoralla laskulla:

$$(p-x)^2 = p^2 - 2px + x^2 \equiv x^2 \pmod{p}.$$

Entä alkuosan käyttäytyminen?

Haluamme osoittaa, että  $a^2 \not\equiv b^2 \pmod{p}$ , kun  $1 \leq a, b \leq \frac{p-1}{2}$  ja  $a$  ja  $b$  ovat erisuuria. Oletetaan, että olisikin  $a^2 \equiv b^2 \pmod{p}$ . Tällöin  $p \mid a^2 - b^2 = (a-b)(a+b)$ . Eukleideen lemmän nojalla joko  $p \mid a-b$  tai  $p \mid a+b$ . Kumpikaan näistä ei ole mahdollinen vaihtoehto, koska  $1 \leq a, b \leq \frac{p-1}{2}$  ja  $a \neq b$ . Olemme valmiit.

Tässä on pari yksinkertaista esimerkkiä neliönjäännösten sovelluksesta yhtälöiden kokonaislukuratkaisujen etsimiseen. Ensimmäinen on vanha valmennustehtävä.

### Tehtävä

Määritä yhtälön  $x^2 - 3y^2 = 17$  kaikki kokonaislukuratkaisut.

Kokeilemalla pieniä lukujen  $x$  ja  $y$  arvoja ei löydetä ratkaisuja. Syy tälle on seuraava: Jos  $(x, y)$  on ratkaisu, niin  $x^2 - 3y^2 = 17$ , ja täten  $x^2 - 3y^2 \equiv 17 \pmod{3}$ . Tästä seuraa  $x^2 \equiv 2 \pmod{3}$ , mikä on mahdotonta. Ratkaisuja ei siis ole.

Todistus perustuu siihen, että halutulla yhtälöllä ei ole ratkaisuja modulo 3. Vastaavaa ideaa voi hyödyntää yleisemminkin korvaamalla luvun 3 jollain muulla kokonaisluvulla. Tässä on toinen samantyylinen esimerkki.

### Tehtävä

Määritä yhtälön  $x^2 + y^2 + z^2 = 3996$  kaikki kokonaislukuratkaisut.

Koska  $a^2 \geq 0$  kaikilla  $a$ , tulee kaikkien luvuista  $x, y$  ja  $z$  olla enintään  $\sqrt{3996}$ , koska muuten vasen puoli olisi suurempi kuin oikea. Siispä mahdollisia kandidaatteja luvuille  $x, y$  ja  $z$  on vain äärellisen monta, eli ne voisi periaatteessa käydä läpi. Vaihtoehtoja on kuitenkin liikaa käsin kokeiltavaksi, joten mietitään jotain muuta.

Voidaan kokeilla moduloita. Yhtälön tarkkaileminen modulo 2 tai modulo 3 ei tunnu antavan mitään hyödyllistä, mutta modulo 4 saadaan jotain: koska luvut  $0^2, 1^2, 2^2$  ja  $3^2$  ovat  $0, 1, 0, 1$  modulo 4, pätee  $a^2 \equiv 0 \pmod{4}$  tai  $a^2 \equiv 1 \pmod{4}$  kaikilla kokonaisluvuilla  $a$ . On neljä mahdollista tapausta:

1. Kaikki kolme lukua  $x, y$  ja  $z$  ovat sellaisia, joiden neliö on  $0 \pmod{4}$ . Tällöin  $x^2 + y^2 + z^2 \equiv 0 \pmod{4}$ .
2. Kaksi lukua luvuista  $x, y$  ja  $z$  ovat sellaisia, joiden neliö on  $0 \pmod{4}$ , ja kolmannen neliö on  $1 \pmod{4}$ . Tällöin  $x^2 + y^2 + z^2 \equiv 1 \pmod{4}$ .
3. Yksi neliö on  $0 \pmod{4}$ , ja kaksi muuta ovat  $1 \pmod{4}$ . Tällöin  $x^2 + y^2 + z^2 \equiv 2 \pmod{4}$ .
4. Kaikki neliöt ovat  $1 \pmod{4}$ , jolloin  $x^2 + y^2 + z^2 \equiv 3 \pmod{4}$ .

Koska  $3996 \equiv 0 \pmod{4}$ , vain ensimmäinen vaihtoehto kelpaa. Siis  $x^2 \equiv y^2 \equiv z^2 \equiv 0 \pmod{4}$ , mikä tarkoittaa, että luvut  $x, y$  ja  $z$  ovat parillisia. Voidaan siis kirjoittaa  $x = 2a$ ,  $y = 2b$  ja  $z = 2c$ , missä  $a, b, c$  ovat kokonaislukuja. Nyt

$$x^2 + y^2 + z^2 = 4a^2 + 4b^2 + 4c^2 = 3996,$$

eli  $a^2 + b^2 + c^2 = 999$ . Yhtälö on samantyylinen kuin aiemminkin, mutta yhtälön oikea puoli on pienentynyt. Tämä on edistystä.

Modulo 4 ei juurikaan auta enää: saamme, että  $a, b$  ja  $c$  ovat parittomia, mutta se siitä. Voidaan kokeilla muita moduloita. Modulo 8 sattuu toimimaan: voidaan tarkistaa, että  $x^2 \equiv 0, 1$  tai  $4 \pmod{8}$ . Ei ole mahdollista valita kolmea lukua joukosta  $\{0, 1, 4\}$  niin, että niiden summa olisi  $999 \equiv 7 \pmod{8}$ . Tämän takia ratkaisuja ei ole.

Onko mitään nopeaa tapaa määrittää, onko jokin tietty kokonaisluku neliönjäännös modulo  $p$ ? Yksi tapa on listata neliöt  $1^2, 2^2, \dots, \left(\frac{p-1}{2}\right)^2$ , mutta on myös nopeampi menetelmä. Esitetään teoriaa, jonka sovelluksena saadaan tämä nopeampi menetelmä sekä muita tuloksia.

### Määritelmä

Olkoon  $a$  kokonaisluku, ja olkoon  $p$  alkuluku. Määritellään Legendren symboli  $\left(\frac{a}{p}\right)$  seuraavasti: jos  $a$  on neliönjäännös modulo  $p$ , niin  $\left(\frac{a}{p}\right) = 1$ , jos  $a$  on neliönepäjäännös modulo  $p$ , niin  $\left(\frac{a}{p}\right) = -1$ , ja muuten  $\left(\frac{a}{p}\right) = 0$ .

Merkintä muistuttaa ikävästi jakolaskua, mutta kontekstista voi päätellä, mitä tarkoitetaan.

Huomioita:

1. Jos  $a \equiv b \pmod{p}$ , niin  $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ .



2. Kahden neliönjäännöksen tulo on neliönjäännös: jos  $x^2 \equiv a \pmod{p}$  ja  $y^2 \equiv b \pmod{p}$ , niin  $(xy)^2 \equiv ab \pmod{p}$ .

Seuraava lemma yleistää jälkimmäistä huomiota.

### Lemma

Olkoon  $p$  alkuluku. Kaikilla kokonaisluvuilla  $a$  ja  $b$  pätee

$$\left(\frac{a}{p}\right) \left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right).$$

Tulosta voi tavallaan ajatella tulon merkkisääntönä. Reaaliluvuissa luku on neliö jos ja vain jos se on epänegatiivinen. Kahden neliön tulo on neliö, neliö kerrottuna epäneliöllä on epäneliö, ja kahden epäneliön luvun tulo on neliö. Lemman tulos todistaa saman kokonaisluvuille modulo  $p$ .

Lemma selvästi pätee, jos  $a \equiv 0 \pmod{p}$  tai  $b \equiv 0 \pmod{p}$ , koska tällöin saadaan  $0 = 0$ . Oletetaan, että  $a, b \not\equiv 0 \pmod{p}$ . Edellä todistettiin tapaus  $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) = 1$  eli merkkivaihtoehto  $(+, +)$ .

Tutkitaan seuraavana tapaus  $(-, +)$ . Oletetaan siis, että  $a$  on neliönepäjäännös ja  $b$  on neliönjäännös, ja yritetään todistaa, että  $ab$  on neliönepäjäännös. Tehdään vastaoletus: luku  $ab$  on neliönjäännös modulo  $p$ . Kirjoitetaan  $x^2 \equiv b \pmod{p}$  ja  $y^2 \equiv ab \pmod{p}$ . Koska  $b \not\equiv 0 \pmod{p}$ , on luvuilla  $b$  ja  $x$  käänteisluvut  $b^{-1}$  ja  $x^{-1}$  modulo  $p$ . Nyt

$$a \equiv ab \cdot b^{-1} \equiv y^2 \cdot (x^{-1})^2 \equiv (yx^{-1})^2 \pmod{p},$$

eli  $a$  onkin neliönjäännös modulo  $p$ , mikä on ristiriita.

Merkkivaihtoehto  $(+, -)$  seuraa symmetrian nojalla.

Jäljellä on vaikein tapaus  $(-, -)$ , eli se, että kahden neliönepäjäännöksen tulo on neliönjäännös. Idea todistuksessa on valita jokin neliönepäjäännös ja todistaa, ettei sitä voi esittää kahden neliönepäjäännöksen tulona. Tämä tehdään laskemalla tietynlaisten parien lukumääriä.

Valitaan jokin neliönepäjäännös  $c$ . Kuinka monta paria sellaista paria  $(a, b)$  on, joilla  $ab \equiv c \pmod{p}$ ? Koska  $c \not\equiv 0 \pmod{p}$ , niin  $a, b \not\equiv 0 \pmod{p}$ . Jokaista luvun  $a$  vaihtoehtoa  $1, 2, \dots, p-1$  vastaa yksikäsitteinen  $b$ , nimittäin  $a^{-1}c$ . Siis yhtälöllä  $ab \equiv c \pmod{p}$  on täsmälleen  $p-1$  ratkaisua.

Mitä näistä ratkaisuista voidaan sanoa? Jos  $a$  on neliönjäännös (tällaisia ratkaisuja on  $\frac{p-1}{2}$  kappaletta), niin  $b$ :n tulee olla neliönepäjäännös. Jos taas  $b$  on neliönjäännös (tällaisia ratkaisuja on myös  $\frac{p-1}{2}$  kappaletta), niin  $a$  on neliönepäjäännös. Nämä tapaukset käsittelevät kaikki  $p-1$  ratkaisua. Jokaisessa näistä ratkaisuista tasan yksi luvuista  $a$  ja  $b$  on neliönjäännös, mikä todistaa väitteen: lukua  $c$  ei voi esittää kahden neliönepäjäännöksen tulona.

Seuraavaksi esitetään ilman todistuksia pari neliönjäännöksiin liittyvää tulosta. Todistuksista kiinnostuneelle lukijalle suositellaan valmennuksen sivuilta löytyvää Esa Vesalaisen materiaalia Lyhyt johdatus alkeelliseen lukuteoriaan. Materiaalissa esitetään myös erilainen todistus edelliselle lemmalle.<sup>39</sup>

### Lemma

Olkoon  $p$  pariton alkuluku. Tällöin  $-1$  on neliönjäännös modulo  $p$  täsmälleen silloin, kun  $p \equiv 1 \pmod{4}$ .

### Lemma

Olkoon  $p$  pariton alkuluku. Tällöin  $2$  on neliönjäännös modulo  $p$  täsmälleen silloin, kun  $p \equiv 1 \pmod{8}$  tai  $p \equiv 7 \pmod{8}$ .

Edelliset kaksi lemmaa toimivat täydennyksinä seuraavalle tulokselle. Todistusta ei esitetä tässä, mutta myös tämän väitteen todistus on esitetty Vesalaisen materiaalissa.

### Lause (Neliönjäännösten resiprookkilaki)

Olkoot  $p$  ja  $q$  parittomia alkulukuja. Jos vähintään toinen luvuista  $p$  ja  $q$  on  $1 \pmod{4}$ , niin  $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ , ja muuten (kun  $p \equiv q \equiv 3 \pmod{4}$ ) pätee  $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$ .

Esitetään nyt aiemmin luvattu menetelmä, jonka avulla pystyy laskemaan arvon  $\left(\frac{a}{p}\right)$  nopeasti. Tehdään tämä esimerkin kautta.

### Esimerkki

Lasketaan  $\left(\frac{1010}{2017}\right)$  (ei ole ilmeistä, että 2017 on alkuluku, mutta näin on).

Hajotetaan 1010 alkutekijöihin:  $1010 = 2 \cdot 5 \cdot 101$ . Käyttämällä ”tulon merkkisääntöä” saadaan

$$\left(\frac{1010}{2017}\right) = \left(\frac{2}{2017}\right) \left(\frac{5}{2017}\right) \left(\frac{101}{2017}\right).$$

Lasketaan jokainen termi yksitellen. Ensimmäiseen termiin ei voida käyttää resiprookkilakia (koska 2 ei ole pariton alkuluku), mutta voidaan käyttää toista täydentävää tulosta: pätee  $2017 \equiv 1 \pmod{8}$ , joten 2 on neliönjäännös modulo 2017. Ensimmäinen termi on siis  $+1$ .

<sup>39</sup>Pidän Vesalaisen esittämää todistusta Legendren symbolin tulon merkkisäännölle parempana, koska se on luonnollinen osa neliönjäännösten teoriaa ja koska vastaavilla menetelmillä saadaan osoitettua muun muassa se, että  $-1$  on neliönjäännös modulo  $p$  jos ja vain jos  $p \equiv 1 \pmod{4}$ . Esittämäni todistus parien lukumääriä laskemalla on kuitenkin mielestäni helpompi keksiä itse, minkä vuoksi esitin tämän ratkaisun.

Toiseen termiin voidaan soveltaa resiprookkilakia, eli saadaan

$$\left(\frac{5}{2017}\right) = \left(\frac{2017}{5}\right) = \left(\frac{2}{5}\right),$$

joten tämä termi on  $-1$ .

Viimeiseen termiin voidaan vastaavasti soveltaa resiprookkilakia:

$$\left(\frac{101}{2017}\right) = \left(\frac{2017}{101}\right).$$

Nähdään, että  $2017 = 2020 - 3 \equiv -3 \pmod{101}$ . Enää tulee laskea

$$\left(\frac{-3}{101}\right) = \left(\frac{-1}{101}\right) \left(\frac{3}{101}\right).$$

Ensimmäinen termi on  $+1$  ensimmäisen täydentävän lemmän nojalla, ja toinen termi on  $-1$  resiprookkilain avulla.

Keräämällä tulokset yhteen saadaan, että  $\left(\frac{1010}{2017}\right) = 1$ .

Huomaa, että neliönjäännösten resiprookkilaki ja sen täydennystulokset antavat tavan laskea symbolin  $\left(\frac{a}{p}\right)$  arvon millä tahansa alkuluvulla  $p$  ja kokonaisluvulla  $a$ . Tämän luvun viimeinen tehtävä demonstroi tätä ideaa.

### Tehtävä

Olko  $a$  kokonaisluku. Oletetaan, että  $a$  ei ole neliöluku. Osoita, että on olemassa äärettömän monta alkulukua  $p$ , joilla  $a$  on neliönepäjäännös modulo  $p$ .

Ehto siitä, ettei  $a$  ole neliöluku, on selvästi välttämätön väitteen pätevyydelle.

Mistä aloitetaan? Tutkitaan jotain yksinkertaista tapausta, vaikkapa  $a = -1$ . Tällöin halutaan, että äärettömän monella alkuluvulla  $p$  pätee  $p \equiv 3 \pmod{4}$ . Tämä väite pätee ja on erikoistapaus erittäin tunnetusta Dirichlet'n lauseesta. Lauseen tulos on hyvin uskottavan kuuloinen, ja tulos on hyvä pitää mielessä.

### Lause (Dirichlet'n lause)

Olko  $a$  ja  $b$  yhteistekijättömiä positiivisia kokonaislukuja. On olemassa äärettömän monta alkulukua  $p$ , joilla  $p \equiv a \pmod{b}$ .

Tämä ratkaisee tapauksen  $a = -1$ . Myös tapaus  $a = 2$  ratkeaa tämän lauseen ja täydennystuloksen avulla.

Edetään hieman vaikeampaan tapaukseen: olko  $a = q$  jollain alkuluvulla  $q$ . Voidaan olettaa, että  $q > 2$ . Halutaan

$$\left(\frac{q}{p}\right) = -1.$$

Käytetään neliönjäännösten resiprookkilakia. Yritetään valita  $p \equiv 1 \pmod{4}$ , jolloin resiprookkilakia käytettäessä ei synny etumerkkiä  $-$ . Näillä  $p$  halutaan

$$\left(\frac{p}{q}\right) = -1.$$

Tämä onnistuu: Koska  $q > 2$ , on olemassa neliönepäjäännös  $a \pmod{q}$ . Valitaan  $p$  niin, että  $p \equiv a \pmod{q}$  ja  $p \equiv 1 \pmod{4}$ . Nämä ehdot voidaan kirjoittaa kiinalaisen jäännöslauseen avulla muodossa  $p \equiv b \pmod{4q}$  sopivalla  $b$ . Päte  $\text{synt}(b, 4q) = 1$  (miksi?), joten Dirichlet'n lause todistaa väitteen.

Yritetään sitten ratkaista yleinen tapaus. Oletetaan yksinkertaisuuden vuoksi ensiksi, että  $a > 0$  ja että  $a$  on pariton. Kirjoitetaan  $a = q_1^{e_1} q_2^{e_2} \cdots q_n^{e_n}$ , missä  $q_i$  ovat erisuuria parittomia alkulukuja. Saadaan

$$\left(\frac{a}{p}\right) = \left(\frac{q_1^{e_1}}{p}\right) \left(\frac{q_2^{e_2}}{p}\right) \cdots \left(\frac{q_n^{e_n}}{p}\right).$$

Jos  $e_i$  on parillinen, niin  $\left(\frac{q_i^{e_i}}{p}\right) = 1$  (paitsi jos  $p = q_i$ , mutta tämä poissulkee vain äärellisen monta  $p$ ). Nämä termit voidaan unohtaa. Jos  $e_i$  on pariton, niin  $\left(\frac{q_i^{e_i}}{p}\right) = \left(\frac{q_i}{p}\right)$ .

Olkoot  $r_1, r_2, \dots, r_k$  ne alkuluvut  $q_i$ , joiden eksponentti luvussa  $a$  on pariton. Saamme siis

$$\left(\frac{a}{p}\right) = \left(\frac{r_1}{p}\right) \left(\frac{r_2}{p}\right) \cdots \left(\frac{r_k}{p}\right).$$

Nyt vaikuttaa hyvältä tilaisuudelta käyttää resiprookkilakia. Kuten alkulukutapauksessa oletetaan nytkin, että  $p \equiv 1 \pmod{4}$ . Saadaan

$$\left(\frac{r_1}{p}\right) \cdots \left(\frac{r_k}{p}\right) = \left(\frac{p}{r_1}\right) \cdots \left(\frac{p}{r_k}\right).$$

Haluamme siis valita luvun  $p$  niin, että tämä tulo on  $-1$ . Naiivi tapa on yrittää valita  $p$  niin, että ensimmäinen termi on  $-1$  ja loput termit ovat  $+1$ . Tämä myös onnistuu. Alkuluvut  $r_i$  ovat oletuksen nojalla parittomia, joten on olemassa neliönepäjäännös  $t \pmod{r_1}$ . Valitaan  $p$  seuraavasti:

- $p \equiv t \pmod{r_1}$ . Näin saadaan ensimmäisestä termistä  $-1$ .
- $p \equiv 1 \pmod{r_i}$  kaikilla  $i \geq 2$ . Näin saadaan muista termeistä  $+1$ .
- $p \equiv 1 \pmod{4}$ . Tätä ehtoa käytettiin resiprookkilakia sovellettaessa.

Ehdot voidaan yhdistää kiinalaisella jäännöslauseella, eli saadaan  $p \equiv s \pmod{m}$ . Jälleen pätee  $\text{synt}(s, m) = 1$  (miksi?), joten Dirichlet'n lause todistaa väitteen. (Missä kohtaa käytettiin tietoa siitä, että  $a$  ei ole neliöluku?)

Oletimme, että  $a > 0$  ja että  $a$  on pariton. Muut tapaukset voidaan kuitenkin käsitellä vastaavalla tavalla (tarkastelu on hieman vaivalloinen, muttei mitenkään vaikea, joten se sivuutetaan).

Huomaa, että vastaavalla tavalla saadaan luotua äärettömän monta alkulukua  $p$ , joilla  $a$  on neliönjäännös modulo  $p$ . Tämä ongelma on yksityiskohtien puolesta helpompi kuin edellä esitetty.<sup>40</sup>

---

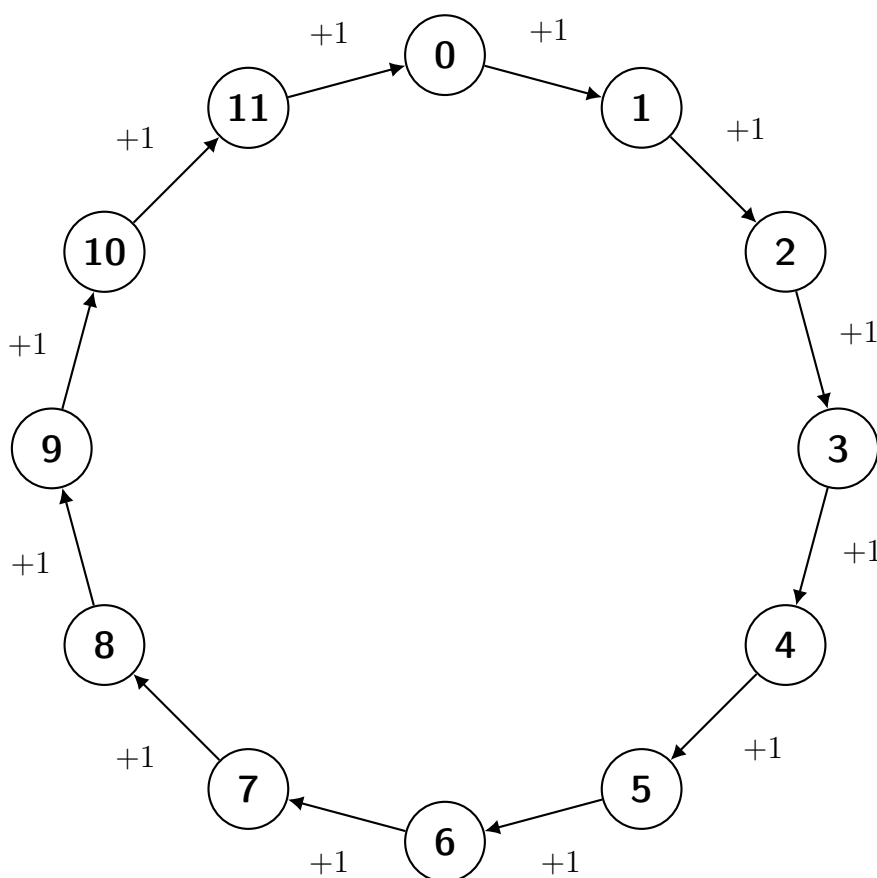
<sup>40</sup>Tämän ongelman voi ratkaista myös toisella tavalla tutkimalla niitä  $p$ , jotka jakavat jonkin polynomin  $P(x) = x^2 - a$  arvoista kokonaislukupisteessä (katso Lukuteorian lisätehtävät -luvun toisen tehtävän kommentti, erityisesti Schurin lause).

## 10 Primitiivijuuret (Lukuteoria)

Tässä luvussa käsitellään primitiivijuuria modulo alkuluvut.

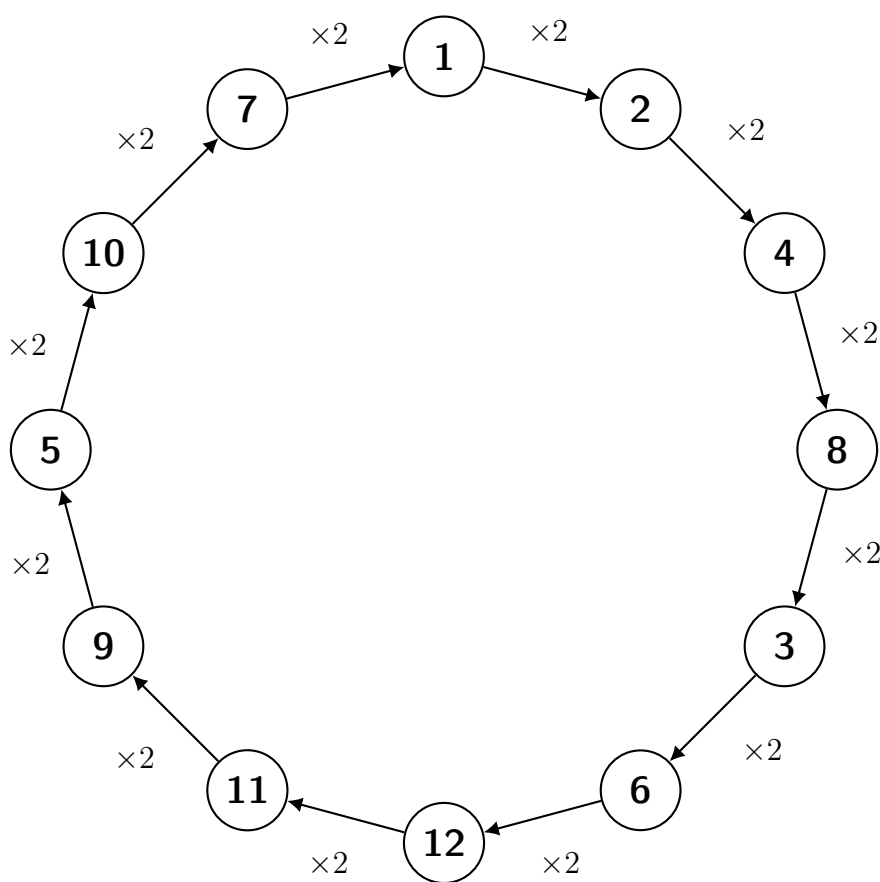
### 10.1 Primitiivijuurien idea

Yhteenlasku moduloissa on yksinkertaista: Esimerkiksi luvut modulo 12 voidaan ajatella kellotauluna, jossa neljän lisääminen vastaa neljän verran eteenpäin liikkumista. Alla on kuvio, joka kuvastaa yhteenlaskua modulo 12.



Luvut modulo 12 aseteltuna sykliin.

Entä kertolasku? Kertolasku voi aluksi tuntua vaikeammalta kuin yhteenlasku. Tästä huolimatta esimerkiksi modulo 13 kertolasku onnistuu tavallaan samaan tapaan kuin yhteenlasku modulo 12. Tutkitaan seuraavaa kuviota.



Kakkosen potenssit modulo 13 aseteltuna sykliin.

Ympyröissä olevat luvut kuvaavat lukuja modulo 13. Huomataan, että jokainen jakojäännöksistä  $1, 2, \dots, 12$  esiintyy ympyröissä täsmälleen kerran. (Jakojäännös  $0 \pmod{13}$  ei ole missään ympyrässä, koska nolla on kertolaskua ajatellen erikoisasemassa.) Syklissä seuraava luku on aina edellinen kerrottuna kahdella, kun kertolasku tehdään (tietenkin) modulo 13.

Sanotaan, että kaksi on primitiivijuuri modulo 13, koska sen potenssit antavat kaikki muut luvut  $\pmod{13}$  (paitsi luvun 0). (Osoittautuu, että jokaisella alkuluvulla on olemassa vähintään yksi primitiivijuuri, tosin 2 ei ole aina primitiivijuuri.)

Ideana on, että kertolaskun *rakenne* modulo 13 on hyvin yksinkertainen – yhtä yksinkertainen kuin yhteenlasku modulo 12. Operaatio “kerro kahdella (modulo 13)” on hyvin samankaltainen kuin “lisää yksi (modulo 12)”.

Kuvitellaan esimerkiksi, että haluamme vaikkapa laskea, mitä on  $3 \cdot 11$  modulo 13. Tämän voi tietysti suoraan laskea olevan  $7 \pmod{13}$  (ja tämä onkin käytännössä yksinkertaisin tapa). Tässä on mielenkiintoisempi lähestymistapa, joka perustuu edellisen kuvion tarkastelemiseen:

Edellisessä kuviossa luku 3 saadaan aloittamalla luvusta 1 ja siirtymällä 4 askelta eteenpäin. Tämä vastaa sitä, että  $2^4 \equiv 3 \pmod{13}$ . Vastaavasti luku 11 saadaan aloittamalla luvusta 1 ja siirtymällä 7 askelta eteenpäin. Tämä vastaa sitä, että  $2^7 \equiv 11 \pmod{13}$ . Nyt lukujen 3 ja 11 tulo saadaan aloittamalla luvusta 1 ja

siirtymällä  $4 + 7 = 11$  askelta eteenpäin, jolloin päädytään lukuun 7.

(Tämä toimii potenssin laskusääntöjen takia:  $3 \cdot 11 \equiv 2^4 \cdot 2^7 \equiv 2^{11} \pmod{13}$ , ja kohdassa 11 on luku  $7 \pmod{13}$ .)

Mutta mitä hyötyä tästä kaikesta on?

Mietitään hetki aiempien lukuteorian lukujen sisältöjä. Yksi ensimmäisistä tuloksista oli Fermat'n pieni lause. Modulo 13 tämä kertoo, että  $a^{12} \equiv 1 \pmod{13}$ , kunhan  $a$  ei ole jaollinen kolmellatoista. Tämän pätevyyden näkee suoraan tutkimalla edellistä kuviota: Valitaan jokin luku, vaikkapa  $a = 6$ . Otetaan syklin luku 6: lähdettäessä liikkeelle ykkösestä se löytyy 5 askeleen päästä. Tästä nähdään, että luku  $6^{12} \pmod{13}$  saadaan laskettua lähtemällä ykkösestä ja kulkemalla  $5 \cdot 12$  askelta eteenpäin. Mutta  $5 \cdot 12$  vastaa viittä täyttä kierrosta, eli tämän seurauksena päädytään takaisin ykköseen.

Yleisesti jos valitaan syklistä kohdasta  $x$  jokin luku (joka on tällöin siis  $2^x \pmod{13}$ ), tämän luvun  $12$ :s potenssi löytyy syklistä kohdasta  $12x$ . Koska  $12x$  on jaollinen kahdellatoista, on tämä luku 1.

Huomataan siis, että Fermat'n pieni lause modulo 13 vastaa käytännössä sitä, että modulo 12 pätee  $12a \equiv 0 \pmod{12}$  millä tahansa kokonaisluvulla  $a$ . Tämä on selvää.

Tutkitaan sitten neliönjäännöksiä. Tapauksessa  $p = 13$  neliönjäännökset modulo  $p$  saadaan helposti listattua: ne ovat

$$1, 3, 4, 9, 10, 12.$$

Huomataan, että nämä ovat täsmälleen ne luvut, jotka saadaan, kun aloitetaan luvusta 1 ja siirrytään parillinen määrä askelia eteenpäin: 1 saadaan siirtymällä eteenpäin nolla askelta, 3 saadaan neljällä askeleella, 4 kahdella askeleella, 9 kahdeksalla, 10 kymmenellä ja 12 kuudella. Näin käy myös yleisesti. Vastaavasti neliönepäjäännöksiä ovat parittoman askeleen päässä olevat luvut.

Huomataan siis, että esimerkiksi väite “neliönjäännöksiä modulo 13 on 6 kappaletta” vastaa sitä, että “parillisia lukuja modulo 12 on 6 kappaletta”. Neliönjäännösten tapauksessa tutkitaan siis funktion  $x^2$  saamia arvoja modulo  $p$ , ja tämä on kuin tutkisi funktion  $2x$  saamia arvoja modulo  $p - 1$ .

Lisäksi edellisessä luvussa käsitelty Legendren symbolin multiplikatiivisuus saadaan myös todistettua. Tutkitaan esimerkiksi väitettä “kahden neliönepäjäännöksen tulo on neliönjäännös”. Jos valitaan mitkä tahansa kaksi neliönepäjäännöstä, sijaitsevat ne syklissä parittoman määrän askelia päässä ykkösestä, joten niiden tulo sijaitsee parillisen määrän askelia päässä. Siten tulo on neliönjäännös.

Huomataan siis, että Legendren symbolin multiplikatiivisuus vastaa sitä, että parillisten lukujen summa on parillinen, parillisen ja parittoman luvun summa on pariton ja kahden parittoman luvun summa on parillinen.

Kaiken kaikkiaan ideana on, että kertolaskua koskeville tuloksille (kuten Fermat'n pienelle lauseelle ja Legendren symbolin multiplikatiivisuudelle) on vastineet yhteenlaskun puolella ( $12x \equiv 0 \pmod{12}$ , kahden luvun summan parillisuussäännöt) ja että nämä yhteenlaskun vastineet ovat usein varsin yksinkertaisia.



Lukiessa alla olevaa tekstiä kannattaa pitää mielessä yllä esitetty kuvio kakkosen potensseista modulo 13.

## 10.2 Asteet ja niiden perusominaisuudet

Fermat'n pieni lause sanoo, että kaikilla alkuluvuilla  $p$  ja kokonaisluvuilla  $a$ , joilla  $\text{sy}(a, p) = 1$ , pätee  $a^{p-1} \equiv 1 \pmod{p}$ . Luku  $p - 1$  ei kuitenkaan aina ole pienin eksponentti  $n$ , jolla  $a^n \equiv 1 \pmod{p}$ .

### Esimerkki

Fermat'n pieni lause sanoo, että  $3^{12} \equiv 1 \pmod{13}$ , mutta oikeastaan pätee myös  $3^3 \equiv 1 \pmod{13}$ .

Tästä motivoituneena määritellään luvun aste. Laajennamme käsittelyä myös muillekin kuin alkulukumoduloille. (Todistukset eivät ole yhtään sen vaikeampia kuin vain alkulukumoduloita käytettäessä.<sup>41</sup> Ideoiden hahmottamista varten kannattaa miettiä tapausta  $p = 13$ .)

### Määritelmä

Olkoon  $m$  positiivinen kokonaisluku, ja olkoon  $a$  kokonaisluku, jolla  $\text{sy}(a, m) = 1$ . Määritellään  $\text{ord}_m(a)$  olemaan pienin positiivinen kokonaisluku  $n$ , jolla  $a^n \equiv 1 \pmod{m}$ .

### Esimerkki

Pätee  $\text{ord}_{13}(3) = 3$ , koska  $3^1$  ja  $3^2$  eivät ole  $1 \pmod{13}$ , mutta  $3^3$  on. Vastaavasti  $\text{ord}_{13}(2) = 12$  (kuten aiemmasta kuviosta nähtiin).

Aloitetaan tärkeällä lemmalla.

### Lemma

Olkoon  $m$  positiivinen kokonaisluku, ja olkoon  $a$  kokonaisluku, jolla  $\text{sy}(a, m) = 1$ . Jos jollain kokonaisluvulla  $n$  pätee  $a^n \equiv 1 \pmod{m}$ , niin  $\text{ord}_m(a) \mid n$ .

Väite on hyvinkin luonnollinen. Mietitään esimerkiksi tapausta  $m = 13, a = 3$ , jolloin  $\text{ord}_p(a) = 3$ . Tällöin tulos sanoo, että jos  $3^n \equiv 1 \pmod{13}$ , niin  $n$ :n tulee olla jaollinen kolmella. Tämä ei yllätä: Asteen määritelmän nojalla kolmosen potenssit modulo 13 kulkevat kolmen jaksoissa. Täten nähdään, että jos  $n$  olisi  $1 \pmod{3}$ , niin olisi  $3^n \equiv 3 \pmod{13}$ , ja jos  $n$  olisi  $2 \pmod{3}$ , niin olisi  $3^n \equiv 9 \pmod{13}$ . (Tässä on hyvä miettiä aiempaa aiemmin esitettyä kuviota.)

<sup>41</sup>Varoituksen sana: Jos  $m$  on positiivinen kokonaisluku, niin lukuja  $a$ , joilla  $\text{sy}(a, m) = 1$ , ei voi välttämättä asettaa sykliin samaan tapaan kuin tapauksessa  $m = 13$ . (Näin käy esimerkiksi tapauksessa  $m = 8$ : jokaisen luvuista  $1, 3, 5, 7$  neliö on  $1 \pmod{8}$ .) Toisin sanoen jokaisella positiivisella kokonaisluvulla  $m$  ei ole olemassa primitiivijuuria. Kuten on mainittu, kaikilla alkuluvuilla kuitenkin on primitiivijuuria.

Tässä on tarkka perustelu yleiselle tapaukselle. Tehdään vastaoletus: Oletetaan, että  $\text{ord}_m(a) \nmid n$ . Kirjoitetaan  $n \equiv r \pmod{\text{ord}_m(a)}$ , missä  $0 < r < \text{ord}_m(a)$ . Koska  $n \equiv r \pmod{\text{ord}_m(a)}$ , niin

$$a^n \equiv a^r \pmod{m}.$$

Oletuksen nojalla  $a^n \equiv 1 \pmod{m}$ , joten  $a^r \equiv 1 \pmod{m}$ . Siis  $r$  on positiivinen kokonaisluku, joka on pienempi kuin  $\text{ord}_m(a)$  ja jolla pätee  $a^r \equiv 1 \pmod{m}$ . Tämä on ristiriidassa luvun  $\text{ord}_m(a)$  määritelmän kanssa, joten  $\text{ord}_m(a) \mid n$ .

Ennen kuin jatketaan eteenpäin, tehdään pari huomautusta. Ensinnäkin lemmän tulos ja Eulerin lause antavat suoraan  $\text{ord}_m(a) \mid \phi(m)$  kaikille  $m$  ja  $a$ . Toiseksi lemmän todistuksen idea yleistyy seuraavaan väitteeseen. Henkilökohtaisesti tykkään tuloksesta todella paljon ja pidän sitä myös tärkeänä. Käytän siitä nimitystä syt-kikka.

### Lause (Syt-kikka)

Olkoon  $m$  positiivinen kokonaisluku, ja olkoon  $a$  kokonaisluku, jolla  $\text{syt}(a, m) = 1$ . Jos joillain nollasta eroavilla kokonaisluvuilla  $n$  ja  $k$  pätee  $a^n \equiv 1 \pmod{m}$  ja  $a^k \equiv 1 \pmod{m}$ , niin tällöin myös

$$a^{\text{syt}(n,k)} \equiv 1 \pmod{m}.$$

Aiemmin puhuttiin, että kertolaskua koskeville tuloksille on vastineita yhteenlaskussa. Tämän tuloksen vastine on seuraava: jos  $na \equiv 0 \pmod{m}$  ja  $ka \equiv 0 \pmod{m}$ , niin  $\text{syt}(n, k)a \equiv 0 \pmod{m}$ . Tämä on kenties helpompi hahmottaa kuin kertolaskuversio. (Todistus yhteenlaskuversiolla on käytännössä sama kuin syt-kikalle.)

Todistus: Tiedämme, että  $\text{ord}_p(a) \mid n$  ja  $\text{ord}_p(a) \mid k$ . Tästä seuraa, että  $\text{ord}_p(a)$  jakaa lukujen  $n$  ja  $k$  suurimman yhteisen tekijän, mistä puolestaan seuraa  $a^{\text{syt}(n,k)} \equiv 1 \pmod{m}$ .

Tässä on vielä toinen todistus: Olkoon  $d = \text{syt}(n, k)$ . Tällöin

$$\text{syt}\left(\frac{n}{d}, \frac{k}{d}\right) = 1.$$

Bezout'n lemmän nojalla on olemassa kokonaisluvut  $x$  ja  $y$ , joilla

$$\frac{n}{d}x + \frac{k}{d}y = 1$$

eli  $nx + ky = d$ . Korotetaan yhtälö  $a^n \equiv 1 \pmod{m}$  potenssiin  $x$  (joka voi olla negatiivinen, mutta tämä ei haittaa, koska luvun  $a$  käänteisalkio modulo  $m$  on olemassa ehdon  $\text{syt}(a, m) = 1$  nojalla), jolloin saadaan  $a^{nx} \equiv 1 \pmod{m}$ . Vastaavasti  $a^{ky} \equiv 1 \pmod{m}$ , joten kertomalla nämä saadaan

$$a^{nx+ky} = a^d \equiv 1 \pmod{m},$$

mikä on haluttu väite.

Huomautus: käytännössä samalla todistuksella voi todistaa, että mikäli  $a^n \equiv b^n \pmod{m}$  ja  $a^k \equiv b^k \pmod{m}$ , missä  $\text{syt}(a, m) = \text{syt}(b, m) = 1$ , niin  $a^{\text{syt}(n,k)} \equiv b^{\text{syt}(n,k)} \pmod{m}$ .

$(\text{mod } m)$ . Tämä versio oikeastaan seuraa myös edellä todistetusta lauseen versiosta luvulle  $\frac{a}{b}$ . Käytän myös tästä tuloksesta nimitystä syt-kikka.

Mainitaan vielä toinen seuraus lemmasta ”jos  $a^n \equiv 1 \pmod{m}$ , niin  $\text{ord}_m(a) \mid n$ ”.

#### Lemma

Olkoon  $m$  positiivinen kokonaisluku ja  $a$  kokonaisluku, jolla  $\text{syt}(a, m) = 1$ . Jos joillain kokonaisluvuilla  $n$  ja  $k$  pätee  $a^n \equiv a^k \pmod{m}$ , niin  $n \equiv k \pmod{\text{ord}_m(a)}$ .

Todistus on suoraviivainen: ehto antaa  $a^{n-k} \equiv 1 \pmod{m}$ , joten  $\text{ord}_m(a) \mid n - k$ , mikä on haluttu väite.

### 10.3 Primitiivijuuren olemassaolo

Todistetaan sitten itse päätulos:

#### Lause (Primitiivijuuren olemassaolo)

Olkoon  $p$  alkuluku. On olemassa primitiivijuuri modulo  $p$ .

Todistus ei ole helpoimmasta päästä. Tarvitsemme muutaman aputuloksen. Ensimmäisenä aputuloksena esitetään Lagrangen lause.

#### Lause (Lagrangen lause)

Olkoon  $p$  alkuluku, ja olkoon  $P$  kokonaislukukertoiminen polynomi, jonka korkeimman asteen termin kerroin ei ole  $0 \pmod{p}$ . Tällöin yhtälöllä

$$P(x) \equiv 0 \pmod{p}$$

on enintään  $\deg(P)$  ratkaisua, kun vaaditaan, että  $0 \leq x < p$ .

Tuloksen ei pitäisi tulla täytenä yllätyksenä ottaen huomioon, että normaalistikin polynomeilla on enintään asteensa verran nollakohtia. Itse asiassa todistus Lagrangen lauseelle on täsmälleen sama kuin Polynomit-luvussa esitetty todistus tavallisille yhtälöille, koska polynomien jakoyhtälö toimii myös modulo  $p$ . Todistusta ei siksi kopioida tähän, mutta lukija voi halutessaan varmentaa tämän itse.

(Yleisemmin voi kysyä: miksei kaikkia samoja asioita, joita tehdään normaalisti rationaaliluvuilla, voisi tehdä modulo  $p$ ? Modulo  $p$  voidaan kuitenkin tehdä täysin samoja laskutoimituksia kuin muutenkin: yhteen-, vähennys-, kerto- ja jakolaskut toimivat kuten pitääkin. Lisäksi rationaalilukuja voi ajatella kokonaislukuina modulo  $p$ , kunhan ei jaeta nollalla.<sup>42</sup>)

<sup>42</sup>Yleisesti lukujoukkoja, joilla on hyvin määritellyt yhteen- ja kertolasku, kutsutaan kunniksi (englanniksi field). Siis esimerkiksi rationaaliluvut tai kokonaisluvut modulo alkuluku muodostavat kunnan. Kaikilla kunnilla toimii esimerkiksi polynomien jakoyhtälö, ja todistus on käytännössä sama kuin rationaaliluvuilla (koska rationaaliluvut ovat kunta). Tämä selittää, miksi rationaaliluvuilla ja

Palataan takaisin primitiivijuuriin. Esitetään pari luonnollista kysymystä asteista.

1. Totesimme, että  $\text{ord}_p(a) \mid \phi(p) = p - 1$  kaikilla  $a$  ja  $p$ . Löytyykö kaikille luvun  $p - 1$  tekijöille  $d$  sellainen  $a$ , että  $\text{ord}_p(a) = d$ ?
2. Jos vastaus edelliseen kysymykseen on myönteinen, niin montako tällaista  $a$  on?

Kysymys 1 on varmaankin vaikea: tapauksessa  $d = p - 1$  kyse on juurikin primitiivijuuren olemassaolosta, mitä olemme todistamassa. Kysymys 2 sattuu olemaan helpompi. Ratkaistaan se.

Olkoon  $a$  siis kokonaisluku, jonka aste modulo  $p$  on  $d$ . Yritetään generoida lukuja, joiden aste modulo  $p$  on myös  $d$ . Tutkitaan lukuja muotoa  $a^n$ , missä  $n$  on positiivinen kokonaisluku. Mitkä ovat niiden asteet? Tähän vastaa seuraava lemma.

### Lemma

Jos luvun  $a$  aste modulo  $p$  on  $d$ , niin luvun  $a^n$  aste modulo  $p$  on

$$\frac{d}{\text{syt}(n, d)}.$$

Tässä on intuitiivinen tapa tulkita lemmän tulosta: Jotta luvusta  $a$  saa potenssiin korottamalla luvun  $1 \pmod{p}$ , niin eksponentin tulee olla jaollinen luvulla  $d$ . Tutkittaessa lukua  $a^n$  olemme jo valmiiksi korottaneet lukua  $a$  potenssiin  $n$ . Tämä ”auttaa” saamaan luvun  $a$  joksikin potenssiksi ykkösen. Eksponentti  $n$  auttaa lemmassa esitetyn luvun  $\text{syt}(n, d)$  verran.

(Tämän näkee kenties helpommin yhteenlaskun vastineesta: jos  $d$  on pienin luku, jolla  $ad \equiv 0 \pmod{m}$ , niin pienin luku  $d'$ , jolla  $(an)d' \equiv 0 \pmod{m}$ , on  $d/\text{syt}(n, d)$ .)

Lemman todistamiseksi tutkitaan luonnollisesti yhtälöä  $(a^n)^x \equiv 1 \pmod{m}$  eli  $a^{nx} \equiv 1 \pmod{m}$ . Tämä on ekvivalenttia sen kanssa, että  $d = \text{ord}_m(a) \mid nx$ , eli

$$\frac{d}{\text{syt}(n, d)} \mid x.$$

Tämä todistaa väitteen.

Lemman avulla saamme tasan  $d$  kappaletta lukuja, joiden aste on jokin luvun  $d$  tekijä, nimittäin luvut  $a^0, a^1, a^2, \dots, a^{d-1}$ . Huomaamme, että luvun  $b$  aste on luvun  $d$  tekijä jos ja vain jos  $b$  on polynomin  $P(x) = x^d - 1$  nollakohta (modulo  $p$ ). Lagrangen lauseen nojalla tällä polynomilla on enintään  $d$  nollakohtaa. Siis luvut muotoa  $a^n$ ,  $0 \leq n < d$ , ovat kaikki luvut, joiden asteet jakavat luvun  $d$ . Erityisesti todetaan, että tästä joukosta löytyvät kaikki luvut, joiden asteet ovat tasan luku  $d$ .

Lemmasta ja tästä havainnosta saadaan, että on olemassa täsmälleen  $\phi(d)$  lukua, joiden aste on  $d$ : jotta luvun  $a^n$  asteeksi saadaan  $d$ , tulee valita  $\text{syt}(n, d) = 1$ , ja  $\phi$ -funktio määritelmän nojalla laskee näiden  $n$  määrän.

kokonaisluvuilla modulo  $p$  on paljon yhteisiä ominaisuuksia: kaikilla kunnilla on nämä ominaisuudet.

Ratkaistaan sitten kysymys 1 käyttäen kysymyksen 2 vastausta. Tiedämme siis, että jokaisella  $d|p-1$  on olemassa joko 0 tai  $\phi(d)$  kappaletta lukuja, joiden aste on  $d$ . Osoitetaan, että millään luvulla  $d$  tämä määrä ei ole nolla. Tällöin erikoistapauksena saadaan arvolla  $d = p-1$  todistettua primitiivijuurien olemassaolo.

Olkoon  $f(d)$  niiden lukujen määrä, joiden aste on  $d$ . Pointtina on, että

$$\sum_{d|p-1} f(d) = p-1,$$

koska jokaisen luvuista  $1, 2, \dots, p-1$  aste on jokin luvun  $p-1$  tekijä, joten jokainen luku "kasvattaa" summaa  $\sum f(d)$  yhdellä. Olemme siis valmiit, jos osoitamme, että

$$\sum_{d|p-1} \phi(d) = p-1,$$

koska tällöin epäyhtälöissä muotoa  $f(d) \leq \phi(d)$  tulee aina päteä yhtäsuuruus. Tämä tulos pätee muillekin luvuille kuin luvuille muotoa  $p-1$ :

### Lemma

Olkoon  $n$  positiivinen kokonaisluku. Tällöin

$$\sum_{d|n} \phi(d) = n.$$

Lemman voi todistaa parillakin tavalla. Esitetään todistus, joka muistuttaa aiemmin nähtyjä todistuksia luvun  $n$  tekijöiden määrälle ja summalle.

Kirjoitetaan  $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ . Tällöin kaikki luvun  $n$  tekijät  $d$  ovat muotoa  $p_1^{b_1} p_2^{b_2} \dots p_k^{b_k}$ , missä  $b_i \leq a_i$  kaikilla  $i$ . Tekijöiden summaa laskiessa ideana on kerätä kaikki tekijät  $d$  tulosta

$$\begin{aligned} & \left(1 + p_1 + p_1^2 + \dots + p_1^{a_1}\right) \\ & \cdot \left(1 + p_2 + p_2^2 + \dots + p_2^{a_2}\right) \\ & \quad \dots \\ & \cdot \left(1 + p_k + p_k^2 + \dots + p_k^{a_k}\right). \end{aligned}$$

Idea on nytkin sama: keräämme tekijät tulosta

$$\begin{aligned} & \left(\phi(1) + \phi(p_1) + \phi(p_1^2) + \dots + \phi(p_1^{a_1})\right) \\ & \cdot \left(\phi(1) + \phi(p_2) + \phi(p_2^2) + \dots + \phi(p_2^{a_2})\right) \\ & \quad \dots \\ & \cdot \left(\phi(1) + \phi(p_k) + \phi(p_k^2) + \dots + \phi(p_k^{a_k})\right). \end{aligned}$$

Eli siis luvun  $d = p_1^{b_1} \cdots p_k^{b_k}$  muodostamiseksi valitaan tulontekijästä  $i$  termi  $\phi(p_i^{b_i})$ . Huomaa, että  $\phi$ -funktion multiplikatiivisuus<sup>43</sup> antaa

$$\phi(p_1^{b_1})\phi(p_2^{b_2}) \cdots \phi(p_k^{b_k}) = \phi(p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}) = \phi(d),$$

eli saamme todella haluamamme termin  $\phi(d)$ .

Summa termeistä  $\phi(d)$  on siis edellä esitetty tulo. Tulo sievenee nätisti, koska  $i$ :s tulontekijä on

$$\begin{aligned} & \phi(1) + \phi(p_i) + \phi(p_i^2) + \cdots + \phi(p_i^{a_i}) \\ &= 1 + (p_i - 1) + (p_i^2 - p_i) + \cdots + (p_i^{a_i} - p_i^{a_i-1}) \\ &= p_i^{a_i}. \end{aligned}$$

Tulo on täten  $p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} = n$ , joten olemme valmiit lemmän kanssa, ja primitiivijuuren olemassaolo on täten todistettu.

Kommentti: Primitiivijuuren olemassaolon todistus koostui kahdesta osasta; kysymyksestä 1 ja kysymyksestä 2. Kysymyksen 2 todistus oli lokaali: riitti tutkia lukua, jonka aste on  $d$ , ja tästä saatiin käytännössä kaikki haluttu tieto.

Kysymyksen 1 todistus oli globaali: nopeasti vilkaisemalla ei ole mitään ongelmaa, jos jollakin yksittäisellä  $d$  ei olisi olemassa lukua  $a$ , jolla  $\text{ord}_p(a) = d$ . Tällöin iso kuva kuitenkin hajoaa: pätee  $p - 1 = \sum f(d) \leq \sum \phi(d) = p - 1$ , joten todellisuudessa kaikilla  $d$  tulee päteä  $f(d) = \phi(d)$ .

Todistus osoittaa samalla, että primitiivijuuria modulo  $p$  on  $\phi(p - 1)$  kappaletta.

Vielä voi kysyä: ”Millä  $m$  on olemassa primitiivijuuri modulo  $m$ ?” Eli millä luvuilla  $m$  on olemassa sellainen luku  $a$ , jonka aste modulo  $m$  on  $\phi(m)$ ? Vastaus tähän kysymykseen on seuraava:

#### Lause (Primitiivijuuren olemassaolo)

Olkoon  $m$  positiivinen kokonaisluku. Modulo  $m$  on olemassa primitiivijuuri jos ja vain jos  $m$  on  $1, 2, 4, p^k$  tai  $2p^k$ , missä  $p$  on pariton alkuluku ja  $k$  on positiivinen kokonaisluku.

Lausetta ei todisteta tässä, mutta aiemmin mainitun Esa Vesalaisen monisteen Lyhyt johdatus alkeelliseen lukuteoriaan luvussa 6 todistetaan, että on olemassa primitiivijuuri modulo  $p^k$  parittomilla alkuluvuilla  $p$ . Harjoitustehtävissä 43 ja 46 käsitellään loput tapaukset.

## 10.4 Esimerkkitehtäviä

Esitetään pari esimerkkitehtävää, joissa voi käyttää apuna todistettuja tuloksia. Ensimmäisenä esitettävä tehtävä on hyvin tunnettu.

<sup>43</sup>Multiplikatiivisuus tarkoittaa siis sitä, että  $\phi(mn) = \phi(m)\phi(n)$  kaikilla positiivisilla kokonaisluvuilla  $m$  ja  $n$ , joilla  $\text{syt}(m, n) = 1$ .

**Tehtävä**

Osoita, että ei ole olemassa kokonaislukua  $n$  ( $n > 1$ ), jolla  $n \mid 2^n - 1$ .

Teemme tietysti vastaoletuksen. Ehdon voi muokata muotoon  $2^n \equiv 1 \pmod{n}$ , jolloin tilanne muistuttaa enemmän aiemmin käsiteltyjä tuloksia. Saamme siis  $\text{ord}_n(2) \mid n$ . Lisäksi  $\text{ord}_n(2) \mid \phi(n)$ , joten syt-kikan avulla saamme (koska  $n$  on varmasti pariton)

$$2^{\text{syt}(n, \phi(n))} \equiv 1 \pmod{n}.$$

Suurin yhteinen tekijä on kuitenkin vaikea laskea. Jos  $n$  olisi alkuluku, niin tämä olisi helppoa: saisimme  $\text{syt}(n, n-1)$ , joka on 1.

Voimme kuitenkin tuoda tehtävään alkulukuja: ehdosta  $2^n \equiv 1 \pmod{n}$  seuraa, että  $2^n \equiv 1 \pmod{p}$  kaikilla luvun  $n$  alkutekijöillä  $p$ . Siis  $\text{ord}_p(2) \mid n$  ja  $\text{ord}_p(2) \mid p-1$ , joten syt-kikan nojalla

$$2^{\text{syt}(n, p-1)} \equiv 1 \pmod{p}.$$

Suurin yhteinen tekijä on vieläkin vaikea laskea: luvulla  $n$  voi olla lukua  $p$  pienempiä alkutekijöitä, jotka jakavat luvun  $p-1$ . Tämä voidaan kuitenkin estää valitsemalla  $p$  pienimmäksi luvun  $n$  alkutekijöistä. Tällöin  $\text{syt}(n, p-1) = 1$  ja  $2^1 \equiv 1 \pmod{p}$ , mikä on ristiriita.

Edellä esitetyssä todistuksessa valitaan luvun  $n$  pienin alkutekijä  $p$ . Tämä ei onnistu, jos  $n = 1$ . Väite tuli kuitenkin osoittaa vain arvoille  $n > 1$ .

Seuraavassa tehtävässä ei varsinaisesti tarvita todistettuja tuloksia. Ratkaisun opetuksena onkin se, että tieto tunnetuista tuloksista antaa intuitiota, joka johtaa ratkaisuun.

**Tehtävä**

Osoita, että yhtälöllä  $x^3 + y^4 = 7$  ei ole kokonaislukuratkaisuja.

Idea väitteen todistamiseksi on käyttää kongruenssiehtoja: jos yhtälöllä ei ole ratkaisua modulo  $m$  jollain  $m$ , ei sillä voi olla kokonaislukuratkaisuja. Kiinalaisen jäännöslauseen takia riittää käsitellä moduloita, jotka ovat alkuluvun potensseja. Tutkitaan ensiksi vain alkulukumoduloita.

Millainen  $p$  olisi hyvä modulo ristiriidan saamiseksi? Olisi hyvä, jos kuutioiden ja neljänsien potenssien määrä modulo  $p$  olisi pieni. Voidaanko tämä määrä laskea? Voidaan:

**Lemma**

Olkoon  $p$  alkuluku, ja olkoon  $d > 0$  kokonaisluku. On olemassa

$$\frac{p-1}{\text{syt}(p-1, d)} + 1$$

lukua muotoa  $x^d \pmod{p}$ , missä  $x$  on kokonaisluku.

(On jälleen valaisevaa miettiä, mitä tulos kertoo tapauksessa  $p = 13$ . Yhteenlaskun vastine: kuinka monta lukua muotoa  $dx \pmod{m}$  on olemassa? Ei ole kovin vaikeaa nähdä, että vastaus on  $m/\text{syt}(m, d)$ .)

Tässä termi  $+1$  syntyy siitä, että luku 0 on aina  $d$ :s potenssi. Huomaa, että määrä riippuu ainoastaan luvusta  $p$  ja lukujen  $p-1$  ja  $d$  suurimmasta yhteisestä tekijästä eikä suoraan luvusta  $d$ . Tämä muistuttaa hieman aiemmin todistettua tulosta luvun  $a^n$  asteesta.

Olko  $g$  primitiivijuuri modulo  $p$ . Jos  $x$  ( $x \not\equiv 0 \pmod{p}$ ) on täydellinen  $d$ :s potenssi, niin  $x \equiv y^d \pmod{p}$  jollain  $y$ . Tälle  $y$  voidaan kirjoittaa  $y \equiv g^Y \pmod{p}$  jollain kokonaisluvulla  $Y$ , joten nyt  $x \equiv g^{Yd}$ . Tästä nähdään, että  $d$ :nnet (nollasta eroavat) potenssit modulo  $p$  ovat täsmälleen kaikki luvut muotoa  $g^{dn}$ , missä  $n$  on kokonaisluku (ja lisäksi luku 0 on  $d$ :s potenssi).

Kuinka monta eri lukua muotoa  $g^{dn}$  on olemassa? Oletetaan, että  $g^{dn} \equiv g^{dm} \pmod{p}$ . Tällöin  $g^{d(n-m)} \equiv 1 \pmod{p}$ , eli  $d(n-m) \equiv 0 \pmod{p-1}$  luvun  $g$  primitiivijuuriominaisuuden vuoksi. Tämä on ekvivalenttia ehdon

$$n - m \equiv 0 \left( \text{mod } \frac{p-1}{\text{syt}(d, p-1)} \right)$$

kanssa. Tästä siis nähdään, että arvoilla  $n = 0, 1, \dots, \frac{p-1}{\text{syt}(d, p-1)} - 1$  saadaan kaikki funktion  $g^{dn}$  eri arvot, ja lemmän tulos seuraa.

Siirrytään takaisin tehtävän pariin. Lemman nojalla kannattavaa olisi valita  $p$  niin, että  $1 + \frac{p-1}{\text{syt}(p-1, d)}$  on pieni. Toisin sanoen halutaan, että  $p$  on pieni ja  $\text{syt}(p-1, d)$  on suuri, kun  $d = 3$  ja  $d = 4$ . Kannattaa siis valita  $p \equiv 1 \pmod{3}$  ja  $p \equiv 1 \pmod{4}$  eli  $p \equiv 1 \pmod{12}$ . Pienin tämän ehdon toteuttava alkuluku on  $p = 13$ . Tämä toimii: Listaamalla kuutiot modulo 13 saadaan, että kuutiot ovat kongruentteja jonkin luvusta 0, 1, 5, 8 ja 12 kanssa modulo 13. Vastaavasti neljännet potenssit ovat kongruentteja jonkin luvusta 0, 1, 3 ja 9 kanssa modulo 13. Nyt on helppoa tarkistaa, että kolmannen ja neljännen potenssin summa modulo 13 ei voi olla 7.

Kommentti: Tehtävän ratkaisun pystyy tiivistämään yhdellä lauseella: ”Yhtälöllä ei ole ratkaisua modulo 13.” Kilpailutilanteessa kannattaa toki kirjoittaa ratkaisuun vain moduloa 13 koskevat päättelyt, mutta mikäli ratkaisuprosessia haluaa selittää jollekulle, on hyvä perustella, mistä keksitään tutkia juurikin moduloa 13.

Ratkaisun lemmän todistus perustui primitiivijuurien käyttämiseen. Yleisesti primitiivijuurien tutkiminen on hyvä idea esimerkiksi  $d$ :nsiä potensseja käsitellessä, koska primitiivijuurilla voidaan kuvata hyvin kokonaislukujen modulo  $p$  kertolaskun rakennetta. Lukuteorian lisätehtävät -luvun viimeinen tehtävä on tästä erinomainen esimerkki.

Seuraava tehtävä on vuoden 2016 Baltian tie -kilpailusta.



**Tehtävä**

Olkoon  $p > 3$  alkuluku, jolla  $p \equiv 3 \pmod{4}$ . Positiivista kokonaislukua  $a_0$  kohden määritetään kokonaislukujen jono  $a_0, a_1, \dots$ , jossa  $a_n = a_{n-1}^{2^n}$  kaikilla  $n = 1, 2, \dots$ . Todista, että on mahdollista valita sellainen  $a_0$ , että osajono  $a_N, a_{N+1}, a_{N+2}, \dots$  ei ole vakio modulo  $p$  millään positiivisella kokonaisluvulla  $N$ .

Lukujonon rekursioyhtälö on niin yksinkertainen, että luvuille  $a_n$  voisi olla suora kaava lukujen  $n$  ja  $a_0$  avulla ilmaistuna. Yritetään etsiä se listaamalla pari ensimmäistä lukujonon termiä. Saadaan  $a_1 = a_0^2$ ,  $a_2 = a_1^2 = a_0^{2^2}$  ja  $a_3 = a_2^2 = a_0^{2^3}$ . Listaamalla vielä pari termiä  $a_4 = a_0^{2^{10}}$  ja  $a_5 = a_0^{2^{15}}$  kuvio alkaa löytymään: luvun 2 eksponentit ovat 1, 3, 6, 10, 15, ... eli kolmioluvut<sup>44</sup>  $\frac{n(n+1)}{2}$ . Siis

$$a_n = a_0^{2^{\frac{n(n+1)}{2}}}$$

kaikilla  $n \geq 0$ , mikä on helppo todistaa induktiolla.

Mitä haluamme? Haluamme, että  $a_n \not\equiv a_{n-1} \pmod{p}$  äärettömän monella  $n$ . Siis

$$a_0^{2^{\frac{n(n+1)}{2}}} \not\equiv a_0^{2^{\frac{n(n-1)}{2}}} \pmod{p},$$

eli jos  $a_0 \not\equiv 0 \pmod{p}$  (ja tämä valinta on pakko tehdä), niin

$$a_0^{2^{\frac{n(n+1)}{2}} - 2^{\frac{n(n-1)}{2}}} \not\equiv 1 \pmod{p}.$$

Asteiden avulla tulkittuna tämä tarkoittaa, että

$$2^{\frac{n(n+1)}{2}} - 2^{\frac{n(n-1)}{2}} \not\equiv 0 \pmod{\text{ord}_p(a_0)}.$$

Jotta tämä ehto toteutuisi, on paras luvun  $a_0$  valinta sellainen, jolla  $\text{ord}_p(a_0) = p - 1$ . Tämä siksi, että millä tahansa luvun  $a_0$  valinnalla pätee  $\text{ord}_p(a_0) \mid p - 1$ , joten kaikkein rajoittavin ehto saadaan silloin, kun aste on  $p - 1$ .

Valitaan siis  $a_0$  primitiivijuureksi. Nyt haluamme, että

$$2^{\frac{n(n+1)}{2}} - 2^{\frac{n(n-1)}{2}} \not\equiv 0 \pmod{p-1}.$$

Tämä on jaollisuusehto: tutkitaan sitä alkuluvun potenssi kerrallaan. Kakkosen potenssien puolesta vasen puoli on aina 0 tarpeeksi suurilla  $n$ . Tutkitaan siis jotain muuta alkulukua  $q$ , joka jakaa luvun  $p - 1$ . Tällainen on olemassa, koska  $p - 1$  ei ole jaollinen neljällä ehdon  $p \equiv 3 \pmod{4}$  vuoksi ja koska  $p - 1 > 2$ .

Haluamme siis, että

$$2^{\frac{n(n+1)}{2}} \not\equiv 2^{\frac{n(n-1)}{2}} \pmod{q},$$

<sup>44</sup>Kolmioluvut ovat siis 1,  $1 + 2 = 3$ ,  $1 + 2 + 3 = 6$ ,  $1 + 2 + 3 + 4 = 10$  ja niin edelleen. Nimitys tulee siitä, että esimerkiksi 10 palloa voidaan asetella tasasivuisiksi kolmioksi, jonka sivun pituus on 4 ja jonka sisus on täytetty.

eli jakamalla luvun  $q$  kanssa yhteistekijättömällä termillä  $2^{\frac{n(n-1)}{2}}$  saamme

$$2^n \not\equiv 1 \pmod{q}.$$

Tämä ehto toteutuu varmasti äärettömän monella  $n$ . Olemme siis valmiit.

Kommentti: Tehtävänannossa on pari erikoista ehtoa. Ensinnäkin vaaditaan  $p \equiv 3 \pmod{4}$ , ja toiseksi  $p = 3$  on jostakin syystä erikoistapaus. Näistä ehdoista ei kuitenkaan tarvitse aluksi välittää, vaan voidaan rohkeasti lähteä tutkimaan haluttua väitettä. Ehtojen  $p > 3$  ja  $p \equiv 3 \pmod{4}$  käyttäminen tulee ratkaisussa melkein kuin itsestään: jotta saamme todistettua väitteen, tarvitsemme luvun  $p-1$  parittoman alkutekijän, ja tämän olemassaolon ehdot takaavat. Muutenkin ratkaisu etenee lähinnä niin, että aina tehdään luonnollisin asia: nerokkaita oivalluksia ei tarvita.

Viimeisenä esitettävä tehtävä on vuoden 2008 Baltian tie -kilpailusta.

### Tehtävä

Positiiviset kokonaisluvut  $a$  ja  $b$  toteuttavat yhtälön

$$a^b - b^a = 1008.$$

Osoita, että  $a$  ja  $b$  ovat kongruenteja modulo 1008.

Hajotetaan ongelma heti osatehtäviin: koska  $1008 = 2^4 \cdot 3^2 \cdot 7$ , on (kiinalaisen jäännöslauseen nojalla) ekvivalenttia todistaa, että  $a \equiv b \pmod{2^4}$ ,  $a \equiv b \pmod{3^2}$  ja  $a \equiv b \pmod{7}$ .

Mistä aloitetaan? Tapauskäsittelyä olisi turhan paljon, jos lähtisi suoraan todistamaan vaikkapa väitettä  $a \equiv b \pmod{2^4}$ . Aloitetaan helpommista väitteistä: osoitetaan ensin, että  $a \equiv b \pmod{2}$ . Tämä seuraakin suoraan yhtälön parillisuudesta.

Osoitetaan sitten, että  $a \equiv b \pmod{4}$ . Tapauksessa  $a \equiv b \equiv 1 \pmod{2}$  Eulerin lauseella saadaan  $a^b \equiv a^1 \pmod{4}$  ja vastaavasti  $b^a \equiv b^1 \pmod{4}$ , joten

$$0 \equiv 1008 = a^b - b^a \equiv a^1 - b^1 \equiv a - b \pmod{4}.$$

Täten  $a \equiv b \pmod{4}$ , jos  $a$  ja  $b$  ovat parittomia. Jos taas  $a$  ja  $b$  olisivat molemmat parillisia ja molemmat vähintään 5, niin yhtälön  $a^b - b^a = 1008$  vasen puoli olisi jaollinen luvulla  $2^5$  ja oikea puoli ei olisi. Tulee siis tutkia vain neljä tapausta:  $a = 2, b = 2, a = 4$  ja  $b = 4$ . Ei ole vaikeaa todistaa, että nämä eivät anna yhtälölle ratkaisuja.<sup>45</sup>

Tiedämme siis, että  $a \equiv b \pmod{4}$  ja että sekä  $a$  että  $b$  ovat parittomia. Käytetään nyt Eulerin lausetta modulolle 8: Saadaan  $x^4 \equiv 1 \pmod{8}$  kaikilla parittomilla  $x$ , joten koska  $a \equiv b \pmod{4}$ , niin  $x^a \equiv x^b \pmod{8}$ . Täten

$$0 \equiv 1008 = a^b - b^a \equiv a^a - b^a \pmod{8},$$

<sup>45</sup>Yhtälöllä on kyllä vähintään yksi ratkaisu:  $a = 1009$  ja  $b = 1$ . Tämä ratkaisu toteuttaa ehdon  $a \equiv b \pmod{1008}$ .

eli  $a^a \equiv b^a \pmod{8}$ . Toisaalta Eulerin lauseen nojalla  $a^4 \equiv 1 \equiv b^4 \pmod{8}$ , joten syt-kikalla saadaan

$$a^{\text{syt}(a,4)} \equiv b^{\text{syt}(a,4)} \pmod{8},$$

eli  $a \equiv b \pmod{8}$ .

Nyt ei enää tarvita suurta luovuutta tutkia moduloa 16. Pätee  $a \equiv b \pmod{8}$ , joten Eulerin lauseen nojalla  $x^a \equiv x^b \pmod{16}$  kaikilla parittomilla  $x$ , eli kuten edellä saadaan

$$0 \equiv 1008 = a^b - b^a \equiv a^a - b^a \pmod{16}.$$

Eulerin lauseella  $a^8 \equiv 1 \equiv b^8 \pmod{16}$ , joten saamme syt-kikalla  $a \equiv b \pmod{16}$ .

Siirrytään sitten moduloiden  $3^2$  ja 7 pariin. Aloitetaan pienimmästä modulosta eli luvusta 3. Todetaan, että jos  $3|a$  tai  $3|b$ , niin sekä  $a$  että  $b$  ovat jaollisia kolmella. Mutta jos  $a$  ja  $b$  olisivat jaollisia kolmella, niin  $a^b - b^a$  olisi jaollinen luvulla 27, toisin kuin luku 1008.

Oletetaan siis, että  $a, b \not\equiv 0 \pmod{3}$ . Nyt käyttämällä Eulerin lausetta ja tietoa  $a \equiv b \equiv 1 \pmod{2}$  saadaan

$$0 \equiv 1008 \equiv a^b - b^a \equiv a^1 - b^1 \pmod{3},$$

eli  $a \equiv b \pmod{3}$ . Tutkitaan sitten moduloa 9. Tiedämme, että  $a \equiv b \pmod{6}$ , joten saamme jälleen Eulerin lauseella

$$0 \equiv 1008 \equiv a^b - b^a \equiv a^a - b^a \pmod{9}.$$

Täten  $a^a \equiv b^a \pmod{9}$ , joten taas syt-kikalla  $a \equiv b \pmod{9}$ .

Vielä käsitellään modulo 7. Käytetään tietoa  $a \equiv b \pmod{6}$ , jolloin

$$0 \equiv a^b - b^a \equiv a^a - b^a \pmod{7},$$

joten vielä kerran syt-kikalla (koska  $a$  ja  $b$  eivät voi molemmat olla jaollisia seitsemällä) saadaan  $a^{\text{syt}(a,6)} \equiv b^{\text{syt}(a,6)} \pmod{7}$ , eli  $a \equiv b \pmod{7}$ . Olemme valmiit.

Kommentti: Ratkaisu vaati jonkin verran tekemistä, kuten tehtävien ratkaiseminen joskus vaatii. Lisävaivaa aiheuttivat erikoistapaukset, joissa joko 2 tai 3 jakaa jommankumman luvuista  $a$  tai  $b$ , koska tällöin Eulerin lausetta ei voi soveltaa.

Ratkaisun idea on kuitenkin suoraviivainen: Kerätään helppo tieto  $a \equiv b \pmod{2}$ , ”korotetaan” tämä tiedoksi  $a \equiv b \pmod{4}$ , ja korottamalla vielä kahdesti saadaan  $a \equiv b \pmod{16}$ . Toistamalla vastaava moduloille 3, 9 ja 7 saadaan haluttu väite. Ja vaikka erikoistapaukset, joissa  $\text{syt}(6, ab) > 1$ , ovat ikäviä, ei niiden käsitteleminen ole vaikeaa, vaan ainoastaan työlästä.

On myös mahdollista todistaa, että yhtälön ainoa ratkaisu on  $a = 1009, b = 1$ , mutta todistus on enemmän algebraa kuin lukuteoriaa.

## 11 Lisätehtäviä (Lukuteoria)

Tässä luvussa esitetään haastavia esimerkkitehtäviä lukuteoriasta.

Ensimmäinen tehtävä on IMO-lyhytlistalta vuodelta 2011.

### Tehtävä

Olkoot  $d_1, d_2, \dots, d_9$  erisuuria positiivisia kokonaislukuja, ja olkoon  $P(x) = (x + d_1) \cdots (x + d_9)$ . Osoita, että on olemassa sellainen positiivinen kokonaisluku  $N$ , että kaikilla kokonaisluvuilla  $x \geq N$  luku  $P(x)$  on jaollinen jollain lukua 20 isommalla alkuluvulla.

Tehtävänannon väite kuulostaa erittäin uskottavalta – totta kai näin on. Väite on myös sen näköinen, että kannattaa tehdä vastaoletus. Nyt  $P(x)$  on äärettömän monella  $x$  muotoa

$$P(x) = p_1^{a_1} p_2^{a_2} \cdots p_M^{a_M},$$

missä luvut  $p_1, \dots, p_M$  ovat lukua 20 pienemmät alkuluvut. Alkuluvut  $p_i$  ovat

$$2, 3, 5, 7, 11, 13, 17, 19,$$

eli niitä on  $M = 8$  kappaletta. Tämä on yhden pienempi kuin kokonaislukujen  $d_i$  määrä. Ei ole vielä selvää, miten tämä auttaa, mutta asia on hyvä pistää muistiin.

Koska  $P(x)$  on tulo termeistä  $(x + d_i)$ , tulee jokaisen näistä tulontekijöistä olla myös lukua 20 pienempien alkulukujen tulo. Jokainen näistä luvuista  $x + d_i$  voidaan siis, aritmetiikan peruslauseen nojalla, ajatella kahdeksan pituisena lukujonona

$$V_i = (v_2(x + d_i), v_3(x + d_i), \dots, v_{19}(x + d_i)).$$

Huomaa, että  $V_i$  riippuu luvusta  $x$ .

Mitä näistä lukujonoista voidaan sanoa? Jos  $x$  on hyvin suuri, niin jokainen luvuista  $x + d_i$  on hyvin suuri, ja tällöin joidenkin alkutekijöiden eksponentit tulevat olemaan hyvin suuria. Kukin lukujonoista  $V_1, \dots, V_9$  sisältää siis vähintään yhden hyvin suuren luvun. Luonnollinen seuraava askel on käyttää laatikkoperiaatetta ja huomata, että joillain kahdella lukujonolla  $V_i$  ja  $V_j$  on samassa kohdassa jokin hyvin suuri luku. (Koska lukujonoja on yksi enemmän kuin lukujonoissa on jäseniä.)

Saadaanko tästä ristiriita? Kyllä vain. Jos esimerkiksi  $V_1$  ja  $V_2$  sisältävät hyvin suuren luvun ensimmäisessä kohdassaan, niin määritelmien nojalla luvuilla  $x + d_1$  ja  $x + d_2$  on hyvin suuri kakkosen eksponentti alkutekijähajotelmassaan. Siis näiden lukujen erotus  $d_1 - d_2$  on myös jaollinen jollain suurella kakkosen potenssilla. Tämä ei kuitenkaan onnistu. Muut tapaukset ratkeavat vastaavasti.

Kommentti: Esitetty ratkaisu sivuuttaa yksityiskohtia, jotka liittyvät suurien lukujen koskeviin epäyhtälöihin, ja kilpailussa nämä kohdat olisi hyvä perustella hieman tarkemmin. Formalisointi ei kuitenkaan ole kovin vaikeaa: jos todella voimme valita mielivaltaisen suuria lukuja  $x$ , joilla väite ei päde, niin voimme myös valita mielivaltaisen suuria eksponentteja luvuille  $x + d_i$ , ja niin edelleen.

Toinen luonnollinen idea tehtävän ratkaisemiseksi olisi tutkia 9 luvun  $d_i$  sijasta aluksi pienempää määrää. Esimerkiksi jos lukuja  $d_i$  olisi kaksi kappaletta, niin vastaava väite olisi, että  $(x+d_1)(x+d_2)$  on kakkosen potenssi vain äärellisellä määrällä positiivisia kokonaislukuja  $x$ . Tämän voi todistaa esitetyn ratkaisun idealla, mutta myös toteamalla, että peräkkäisten kakkosen potenssien välit kasvavat mielivaltaisen suuriksi (ja siten suuremmiksi kuin  $|d_1 - d_2|$ ). Kolmella luvulla polynomi  $P$  on  $P(x) = (x+d_1)(x+d_2)(x+d_3)$ . Tässä eri vaihtoehtoja todistukselle on jo vähemmän, ja tätä esimerkkiä tutkimalla voi keksiä ratkaisun alkuperäiseen ongelmaan.

Tehtävänannon väite on hyvin heikko ja paljon vahvempiakin tuloksia on todistettu (mutta todistukset vaativat hyvin voimakasta kalustoa kilpailumatematiikan ulkopuolelta). Muun muassa seuraava tulos pätee: Olkoot  $A$  ja  $B$  joitain (suuria) vakioita. On olemassa vain äärellisen monta positiivisten kokonaislukujen paria  $x$  ja  $y$ , joilla  $|x - y| < A$  ja joilla lukujen  $x$  ja  $y$  kaikki alkutekijät ovat pienempiä kuin  $B$ . Tästä seuraa esimerkiksi se, että on olemassa vain äärellisen monta kakkosen ja kolmosen potenssia, joiden etäisyys on alle 100, ja että edellisen IMO-lyhytlistan tehtävän tulos pätee myös polynomille  $P(x) = (x+d_1)(x+d_2)$ .

Myös seuraava, vahvempi tulos pätee. Olkoon  $C$  jokin (suuri) vakio ja olkoon  $n$  positiivinen kokonaisluku. On olemassa vain äärellisen monta (ei välttämättä positiivisista) kokonaislukuista koostuvaa jonoa  $x_1, \dots, x_n$ , jolla on seuraavat ominaisuudet:

- Lukujen  $x_1, \dots, x_n$  jokainen alkutekijä on pienempi kuin  $C$ .
- Pätee  $x_1 + \dots + x_n = 0$ .
- Ei ole olemassa epätyhjää osajoukkoa  $S \subset \{1, 2, \dots, n\}$ , jonka koko on pienempi kuin  $n$  ja jolla

$$\sum_{i \in S} x_i = 0.$$

- Pätee  $\text{syty}(x_1, \dots, x_n) = 1$ .

Tässä ensimmäiset kaksi ehtoa ovat oleellisisimmat, ja viimeiset kaksi vain poissulkevat ilmeisiä tapoja luoda keinotekoisesti lisää ratkaisuja yhtälölle  $x_1 + \dots + x_n = 0$ . Tuloksen seurauksena saadaan esimerkiksi se, että on olemassa vain äärellisen monta positiivista kokonaislukukolmikkoa  $a, b, c$ , joilla  $|2^a + 3^b - 5^c| < 100$  (valitaan  $n = 4$ ,  $C = 100$  ja tutkitaan niitä yhtälön  $x_1 + \dots + x_4 = 0$  ratkaisuja, joilla  $x_1, x_2$  ja  $x_3$  ovat muotoa  $2^a, 3^b$  ja  $5^c$  ja joilla  $|x_4| < 100$ ).

Seuraava tehtävä on Kiinan IMO-joukkueen valintakokeesta vuodelta 2015.

### Tehtävä

Osoita, että on olemassa äärettömän monta sellaista positiivista kokonaislukua  $n$ , että luku  $n^2 + 1$  ei ole jaollinen minkään alkuluvun neliöllä.

On ainakin kaksi tapaa lähestyä tehtävää: ensimmäinen on yrittää vetää hatusta sopivia luvun  $n$  arvoja, ja toinen on tutkia, millaiset luvut  $n$  toteuttavat tai ovat

toteuttamatta tehtävänannon ehdon. Ensimmäisen tavan arvailemista voisi auttaa se, että hankitaan ensin tietoa toisen lähestymistavan mukaisesti.<sup>46</sup>

Oletetaan, että  $n^2 + 1$  on jaollinen jollain alkuluvun neliöllä  $p^2$ . Huomataan, että  $p$  ei voi olla 2, koska  $n^2$  on aina joko 0 tai 1 modulo 4. Vastaavasti  $p$  ei voi olla 3, koska  $n^2 + 1$  ei koskaan ole jaollinen kolmella, saati sitten yhdeksällä.

Yleisesti, jotta voisi päteä  $p^2 | n^2 + 1$ , niin tulee päteä  $p | n^2 + 1$  eli

$$n^2 \equiv -1 \pmod{p}.$$

Täten  $-1$  on neliönjäännös modulo  $p$ , joten (käyttämällä neliönjäännöskappaleen tuloksia) saadaan, että tulee olla  $p \equiv 1 \pmod{4}$  (tai  $p = 2$ , mutta tämä tapaus käsiteltiin jo).

Jos yhtälöllä  $n^2 \equiv -1 \pmod{p}$  on ratkaisu, niin onko myös yhtälöllä  $n^2 \equiv -1 \pmod{p^2}$  ratkaisu? Totesimme, että arvolla  $p = 2$  näin ei ole, mutta helpolla laskeemisella saadaan, että arvolla  $p = 5$  yhtälöllä  $n^2 \equiv -1 \pmod{p^2}$  on ratkaisu  $n = 7$ .

Yhtälöllä  $n^2 \equiv -1 \pmod{p}$  on aina enintään kaksi ratkaisua (ks. neliönjäännöskappale), ja oikeastaan jos  $p \equiv 1 \pmod{4}$ , niin sillä on täsmälleen kaksi ratkaisua. Olkoot  $t$  ja  $-t$  jotkin ratkaisut. Jotta nyt voisi päteä  $n^2 \equiv -1 \pmod{p^2}$ , niin tulee päteä  $n^2 \equiv -1 \pmod{p}$ , eli  $n \equiv t \pmod{p}$  tai  $n \equiv -t \pmod{p}$ .

Yhtälön  $n^2 \equiv -1 \pmod{p^2}$  ratkaisut ovat siis muotoa  $n = px \pm t$ , missä  $x$  on jokin kokonaisluku. Tutkitaan  $+$ -tapausta (toinen tapaus on analoginen). Halutaan siis, että

$$(px + t)^2 \equiv -1 \pmod{p^2},$$

eli kertomalla auki saadaan

$$(px)^2 + 2(px)t + t^2 \equiv -1 \pmod{p^2}.$$

Termi  $(px)^2$  on 0 modulo  $p^2$ , eli yhtälö palautuu muotoon  $2pxt + t^2 \equiv -1 \pmod{p^2}$ . Tätä on vielä hieman vaikea käsitellä: tiedämme kyllä, että  $t^2 \equiv -1 \pmod{p}$ , mutta emme tiedä, mitä  $t^2$  on modulo  $p^2$ . Kirjoitetaan siis  $t^2 = kp - 1$ , missä  $k$  on jokin kokonaisluku. Yhtälömme muuttuu muotoon

$$2pxt + kp - 1 \equiv -1 \pmod{p^2}$$

eli

$$2pxt + kp \equiv 0 \pmod{p^2}$$

eli

$$2tx + k \equiv 0 \pmod{p}.$$

Tämä on lineaarinen yhtälö modulo  $p$  muuttujan  $x$  suhteen. Kunhan  $p$  ei jaa muuttujan  $x$  kerrointa  $2t$ , niin yhtälöllä on yksi (ja vain yksi) ratkaisu  $x$ . Koska  $t$  ei selvästi voi olla  $0 \pmod{p}$ , niin  $p \nmid 2t$  kaikilla parittomilla  $p$ .

<sup>46</sup>Emme ratkaisussa tule esittämään ensimmäisen tavan mukaista lähestymistapaa, koska toinen tapa johtaa ratkaisuun. (En tiedä tehtävään ensimmäisen lähestymistavan mukaista ratkaisua, ja olen hieman epäileväinen sellaisen ratkaisun olemassaolosta.)

Mitä siis todistimme? Todistimme, että yhtälön  $n^2 \equiv -1 \pmod{p}$  yhdestä ratkaisusta  $n = t$  voidaan luoda ratkaisu yhtälölle  $n^2 \equiv -1 \pmod{p^2}$ . Lisäksi tämä ratkaisu on yksikäsitteinen, kun vaadimme, että  $n \equiv t \pmod{p}$ . Voimme siis ”nostaa” ratkaisuja modulo  $p$  ratkaisuuksi modulo  $p^2$  ja vieläpä yksikäsitteisellä tavalla.

Tästä saadaan, että yhtälöllä  $n^2 \equiv -1 \pmod{p^2}$  on aina täsmälleen kaksi ratkaisua, kun  $p \equiv 1 \pmod{4}$ : kahdesta ratkaisusta yhtälölle  $n^2 \equiv -1 \pmod{p}$  saadaan molemmista yksi ratkaisu yhtälölle modulo  $p^2$ . Jos  $p \not\equiv 1 \pmod{4}$ , niin ratkaisuja ei ole. Ratkaisuja on siis melko harvassa. Tämä motivoi seuraavan kysymyksen:

Valitaan satunnainen positiivinen kokonaisluku  $n$ . Millä todennäköisyydellä  $n^2 + 1$  on jaollinen jollain alkuluvun neliöllä?

Todennäköisyys sille, että  $n^2 + 1$  on jaollinen alkuluvun  $p$  neliöllä  $p^2$  on 0, mikäli  $p \not\equiv 1 \pmod{4}$ , ja muuten  $\frac{2}{p^2}$ . Jos  $p = 5$ , niin  $\frac{2}{p^2}$  on kahdeksan prosenttia, ja arvolla  $p = 13$  tämä on jo hieman alle puolitoista prosenttia. Jos todennäköisyyksien summa on alle 100 prosenttia, niin tehtävä on ratkennut.

(Todennäköisyyksien summa voisi toki teoriassa olla yli 100 prosenttia, vaikka tehtävänannon väite pätisikin, koska  $n^2 + 1$  voi olla jaollinen samanaikaisesti usean eri alkuluvun neliöllä. Mutta jos todennäköisyyksien summa on alle 100 prosenttia, niin alkulukujen neliöitä on niin harvassa, että ne eivät jaa muotoa  $n^2 + 1$  olevia lukuja riittävän usein, vaikka kunkin luvun  $n^2 + 1$  jakaisi korkeintaan yksi alkuluvun neliö. Jos siis todennäköisyyksien summa on alle 100 prosenttia, niin positiivisella osuudella kaikista luvuista  $n$  pätee, että  $n^2 + 1$  on neliövapaa, eli erityisesti todetaan, että näitä  $n$  on äärettömän monta.)

Haluamme siis todistaa, että

$$\sum \frac{2}{p^2} < 1$$

eli että

$$\sum \frac{1}{p^2} < \frac{1}{2},$$

missä  $p$  käy läpi kaikki alkuluvut, jotka ovat 1 modulo 4.

Tutkimme ensiksi, mitä on summa  $\sum \frac{1}{n^2}$ , missä  $n$  käy läpi kaikki positiiviset kokonaisluvut. Tämän summan laskeminen tunnetaan Baselin ongelmana, ja ratkaisu sanoo, että summa on tasan  $\frac{\pi^2}{6} \approx 1.65$ . Tämän avulla saa melko helposti riittävän arvion vastaavalle summalle alkulukujen yli. Tässä esitetään toinen tapa, joka ei vaadi Baselin ongelman ratkaisun tietämistä.

Muutetaan summan  $\sum \frac{1}{n^2}$  termejä niin, että saadaan teleskooppisumma:

$$\begin{aligned} & \frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \cdots \\ & < \frac{1}{1} + \frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \frac{1}{3 \cdot 4} + \cdots \\ & = 1 + \left( \frac{1}{1} - \frac{1}{2} \right) + \left( \frac{1}{2} - \frac{1}{3} \right) + \left( \frac{1}{3} - \frac{1}{4} \right) + \cdots \\ & = 2. \end{aligned}$$

Siis summa  $\sum \frac{1}{n^2}$  on pienempi kuin 2. Verrataan tähän summaa alkulukujen  $p \equiv 1 \pmod{4}$  yli. Niihi tapa olisi ottaa summa  $\sum \frac{1}{n^2} < 2$  ja vähentää tästä termit  $\frac{1}{1^2}, \frac{1}{2^2}, \frac{1}{3^2}, \frac{1}{4^2}, \frac{1}{6^2}$  ja niin edelleen. Tämä ei kuitenkaan anna riittäviä arvioita ainakaan kovin helposti. Toinen, ovelampi tapa on arvioida

$$\sum_{p \equiv 1 \pmod{4}} \frac{1}{p^2} \leq \sum_{n \equiv 1 \pmod{4}, n > 1} \frac{1}{n^2},$$

eli unohdamme alkulukurajoituksen. Ideana on, että pätee esimerkiksi

$$\frac{1}{5^2} < \frac{1}{4} \left( \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \frac{1}{5^2} \right),$$

ja vastaavasti yleisesti pätee

$$\frac{1}{(4n+1)^2} < \frac{1}{4} \left( \frac{1}{(4n-2)^2} + \frac{1}{(4n-1)^2} + \frac{1}{(4n)^2} + \frac{1}{(4n+1)^2} \right).$$

Näillä arvioilla saadaan

$$\sum_{p \equiv 1 \pmod{4}} \frac{1}{p^2} < \sum_{n \equiv 1 \pmod{4}, n > 1} \frac{1}{n^2} \leq \frac{1}{4} \sum_{n \geq 2} \frac{1}{n^2} = \frac{1}{4} \left( \sum_{n \geq 1} \frac{1}{n^2} - 1 \right) < \frac{1}{4}.$$

Tämä on riittävä arvio, joten olemme valmiit.

Kommentti: Ratkaisun loppuosa ei ole aivan formaali. Emme nimittäin voi sanoa valitsevamme ”satunnaista positiivista kokonaislukua  $n$ ”, vaan meidän tulee valita  $n$  satunnaisesti joltain isolta väliltä  $[1, N]$  ja antaa  $N$ :n kasvaa suureksi. Tällöin niiden lukujen  $n$  määrä, joilla  $n^2 + 1$  on jaollinen luvulla  $p^2$ , on enintään  $\left\lceil \frac{N}{p^2} \right\rceil$ . Haluamme osoittaa, että summa tätä muotoa olevista termeistä on alle  $0.999N$ .

Kattofunktioit eivät kuitenkaan tässä tapauksessa vaikuta summaan merkittävästi: Kaikissa nolasta eroavissa termeissä tulee päteä  $p \leq N$ , eli termejä on yhtä monta kuin niitä alkulukuja  $p \equiv 1 \pmod{4}$ , jotka ovat enintään  $N$ . Koska lukua  $N$  pienempiä alkulukuja on noin  $\frac{N}{\log(N)}$  (tätä tulosta kutsutaan alkulukulauseeksi – tulos on hyvin epätriviaali), niin arvioimalla  $\left\lceil \frac{N}{p^2} \right\rceil < \frac{N}{p^2} + 1$  ja etenemällä kuten ratkaisussa saadaan haluttu argumentti läpi.

Ratkaisun ideat ovat luonnollisia: Millä luvuilla  $n$  tehtävänannon väite ei päde? Toimiiko satunnainen  $n$ ? Molempien kysymysten vastausten todistukset ovat päällisin puolin melko teknisiä. Ensimmäisen kysymyksen vastauksen todistus kuitenkin yksinkertaisesti vastaa sitä, miten ratkaisuja kannattaisi etsiä konkreettisilla esimerkeillä.

Toisen ongelman todistus taas oli hieman tekninen sen takia, että esitetty ratkaisu ei ole optimaalinen. Jos esimerkiksi tietää Baselin ongelman ratkaisun, niin saa heti paljon paremman arvion summalle  $\frac{1}{n^2}$ , ja tarvittavan arvion summalle alkulukujen yli saa vaikka seuraavasti:

$$\sum_{p \equiv 1 \pmod{4}} \frac{1}{p^2} \leq \sum_{n \geq 3} \frac{1}{n^2} = \frac{\pi^2}{6} - 1 - \frac{1}{4},$$



ja koska  $\frac{\pi^2}{6}$  on alle 1.7 (helppo lasku), niin tästä saadaan tarvittava arvio.

Toinen tapa lyhentää toisen osan todistusta on tehdä teleskooppisumman yhteydessä hieman tarkempi arvio: pätee esimerkiksi, että

$$\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} = \frac{1}{1^2} + \left( \frac{1}{1 \cdot 2} - \frac{1}{4} \right) + \left( \frac{1}{2 \cdot 3} - \frac{1}{18} \right),$$

joten saamme nyt talteen  $\frac{1}{4} + \frac{1}{18} > 0.25 + 0.05 = 0.3$  verran termejä. Siis teleskooppisummalla saa arvion  $\sum \frac{1}{n^2} < 1.7$ , ja nyt ratkaisu saadaan kuten edellä, mutta ilman tarkkaa arvoa  $\frac{\pi^2}{6}$ .

Vielä kolmas tapa olisi valita  $n$  olemaan satunnainen viidellä jaollinen kokonaisluku. Tällöin  $n^2 + 1$  ei ole koskaan jaollinen viidellä, joten voimme unohtaa termin  $\frac{1}{5^2}$ . Toimimalla vastaavasti riittävän monelle ensimmäisistä alkuluvuista relevantti summa  $\sum \frac{1}{p^2}$  saadaan niin pieneksi kuin halutaan. Tämä lähestymistapa antaa hieman epäsuoremman tavan todistaa väitteen, mutta varsinaisia laskuja ei tarvitse tehdä (kunhan on osoittanut, että summa  $\sum \frac{1}{p^2}$  suppenee).

On avoin ongelma, onko olemassa äärettömän monta lukua  $n$ , jolla  $n^2 + 1$  on alkuluku. Itse asiassa millekään vähintään toisen asteen polynomille ei ole todistettu, että se saa äärettömän monta alkulukuarvoa. Ensimmäisen asteen polynomithan käsittelee Dirichlet'n lause. On kuitenkin todistettu, että  $n^2 + 1$  on äärettömän usein enintään kahden alkuluvun tulo.

---

Ratkaisun motivoimana esitetään hieman lisätuloksia, jotka koskevat kokonaislukukukertoimisia polynomeja. Ensin esitetään neljä tähän liittyvää perustulosta. Tämän jälkeen käydään läpi esimerkkitehtävä, jossa tuloksia sovelletaan käytännössä ja jonka avulla tulosten hyödyllisyys tulee paremmin ilmi.

### Henselin lemma.

Edellisessä ratkaisussa korotettiin yhtälön  $x^2 + 1 \equiv 0 \pmod{p}$  ratkaisuja korkeammille  $p$ :n potensseille. Henselin lemma sanoo, että tämä toimii yleisestikin: jos  $P$  on kokonaislukukertoiminen polynomi ja  $a$  on sellainen kokonaisluku, että  $P(a) \equiv 0 \pmod{p}$  ja  $P'(a) \not\equiv 0 \pmod{p}$ , niin yhtälöllä  $P(x) \equiv 0 \pmod{p^k}$  on ratkaisu millä tahansa kokonaisluvulla  $k$ . Tässä  $P'$  on polynomin  $P$  derivaatta. Lisäksi pätee, että ratkaisu  $a$  modulo  $p$  korottuu yksikäsitteisesti ratkaisuksi modulo  $p^2$ , siitä modulo  $p^3$  ja niin edelleen.

Tässä on lyhyesti Henselin lemmän todistus. Suoralla laskulla voidaan osoittaa, että yhtälö

$$P(a + bp^k) \equiv P(a) + bp^k P'(a) \pmod{p^{k+1}}$$

pätee kaikilla kokonaisluvuilla  $a, b, k \geq 0$  ja alkuluvuilla  $p$ .<sup>47</sup> Oletetaan nyt, että  $P(a) \equiv 0 \pmod{p}$  ja  $P'(a) \not\equiv 0 \pmod{p}$ , ja kirjoitetaan  $P(a) = pA$ . Edellisen nojalla

---

<sup>47</sup>Todistuksen idea: Kirjoitetaan  $P(x) = a_d x^d + \dots + a_0$  ja kerrotaan termit  $a_i(a + bp^k)^i$  auki binomilauseella. Melkein kaikki termit ovat nolla modulo  $p^{k+1}$ , jolloin kokoamalla jäljelle jääneet termit saadaan yhtälön oikea puoli. Tämä myös kertoo, miten identiteettiin voi päätyä itse: yritetään vain korottaa yhtälön ratkaisuja kuten esimerkkitehtävässä, eli yritetään laskea  $P(a + bp^k)$ .

nyt  $P(a+bp) \equiv p(A+bP'(a)) \pmod{p^2}$ . Oletuksen nojalla  $P'(a) \not\equiv 0 \pmod{p}$ , joten on olemassa sellainen (yksikäsitteinen)  $b$ , jolla  $A+bP'(a) \equiv 0 \pmod{p}$ . Olemme saaneet yhtälölle  $P(x) \equiv 0 \pmod{p^2}$  ratkaisun  $x = a + bp$  (jolla  $P'(x) \equiv P'(a) \not\equiv 0 \pmod{p}$ ). Tätä prosessia voidaan selvästi jatkaa korkeammillekin  $p$ :n potensseille.

Kuinka rajoittava Henselin lemmän ehto  $P'(a) \not\equiv 0 \pmod{p}$  on? Tähän vastaa Bezout'n lemma.

### Bezout'n lemma.

Bezout'n lemma esiteltiin Aritmetiikan peruslause -luvussa kokonaisluvuille, mutta vastaava väite pätee myös polynomeille: jos  $P$  ja  $Q$  ovat yhteistekijättömiä kokonaislukukertoimisia polynomeja, niin on olemassa kokonaislukukertoimiset polynomit  $X$  ja  $Y$ , joilla  $P(x)X(x) + Q(x)Y(x) = N$ , missä  $N \neq 0$  on kokonaisluku. Tässä polynomit  $P$  ja  $Q$  ovat yhteistekijättömiä, jos ei ole olemassa epävakioita polynomia, joka jakaa ne molemmat.<sup>48</sup> Bezout'n lemmän polynomeille voi todistaa samoin kuin kokonaisluvuille käyttämällä polynomien jakoyhtälöä.

Polynomia kutsutaan jaottomaksi, jos se ei ole jaollinen millään epävakioilla polynomeilla, jonka aste on sitä pienempi. (Vertaa tätä alkuluvun määritelmään.) Jos  $P$  on jaoton, niin  $P$  ja  $P'$  ovat yhteistekijättömiä: polynomin  $P'$  aste on yhden pienempi kuin polynomin  $P$ , joten mikään epävakio polynomi ei voi jakaa molempia näistä polynomeista. Täten Bezout'n lemmän nojalla pätee  $P(x)X(x) + P'(x)Y(x) = N$  joillain kokonaislukukertoimisilla polynomeilla  $X$  ja  $Y$  ja kokonaisluvulla  $N \neq 0$ . Nyt jos  $a$  on kokonaisluku, jolla  $P(a) \equiv 0 \pmod{p}$  ja  $P'(a) \equiv 0 \pmod{p}$  niin  $p \mid P(a)X(a) + P'(a)Y(a) = N$ , eli  $p \mid N$ . Täten Henselin lemmän ehto  $P'(a) \not\equiv 0 \pmod{p}$  on toteutumatta vain äärellisen monella alkuluvulla  $p$ , kun  $P$  on jaoton.

Entä onko ehto polynomin jaottomuudesta oleellinen? Yllä verrattiin jaottomia polynomeja alkulukuihin. Päteekin, että jokainen kokonaislukukertoiminen polynomi voidaan esittää jaottomien polynomien tulona käytännössä yksikäsitteisellä tavalla (eli kun tulontekijöiden järjestystä ei huomioida ja kun polynomien  $P(x)$  ja  $kP(x)$  ajatellaan olevan käytännössä samat  $k$ :n ollessa vakio). Tähän liittyen tärkeä tulos on Gaussin lemma.

### Gaussin lemma.

Gaussin lemma sanoo, että jos kokonaislukukertoimisen polynomin  $P$  voi esittää kahden epävakion rationaalikertoimisen polynomin tulona, niin se voidaan esittää kahden epävakion kokonaislukukertoimisen polynomin tulona.<sup>49</sup> Ei siis tarvitse murheitä, ovatko tekijöihinjaon polynomit rationaalikertoimisia, vaan kaikki voidaan tehdä kokonaislukukertoimilla.

### Schurin lause.

<sup>48</sup>Polynomi  $A$  jakaa polynomin  $B$ , jos on olemassa polynomi  $C$ , jolla  $A(x) = B(x)C(x)$ .

<sup>49</sup>Todistuksen idea: Kirjoitetaan  $P = AB$ , missä  $A$  ja  $B$  ovat epävakioita polynomeja, joiden kertoimet ovat rationaalisia. Kertomalla yhtälön puolittain sopivalla kokonaisluvulla saadaan  $kP = CD$ , missä  $k \neq 0$  on kokonaisluku ja  $C$  ja  $D$  ovat epävakioita kokonaislukukertoimisia polynomeja. Valitaan pienin  $k$ , jolla tällainen esitys on olemassa. Jos  $k \neq 1$ , hyvä. Muuten tutkitaan jotakin luvun  $k$  alkutekijää  $p$ . Polynomin  $CD$  jokainen kerroin on jaollinen luvulla  $p$ . Tästä seuraa, että joko  $C$ :n tai  $D$ :n kaikki kertoimet ovat jaollisia luvulla  $p$  (tutkimalla polynomien  $C$  ja  $D$  korkeimpia termejä, jotka eivät ole  $0 \pmod{p}$ ).

Tutkitaan niitä alkulukuja  $p$ , joilla yhtälöllä  $P(x) \equiv 0 \pmod{p}$  on kokonaislukuratkaisu. Schurin lause sanoo, että mikäli  $P$  on epävakio, niin tämä yhtälö ratkeaa äärettömän monella alkuluvulla  $p$ . Todistus jätetään harjoitustehtäväksi.<sup>50</sup> Näitä alkulukuja  $p$  kutsutaan polynomin  $P$  alkutekijöiksi.<sup>51</sup> On siis perusteltua sanoa, että Henselin lemmän ehto ei ole kovinkaan rajoittava jaottomilla polynomeilla: polynomeilla on äärettömän monta alkutekijää, ja Henselin lemmän ehto on toteutumatta vain äärellisen monella.

Sitten luvattu esimerkkitehtävä. Väite voi vaikuttaa viattomalta, mutta tehtävää on vaikeaa lähestyä, elleivät kokonaislukukertoimisten polynomien ominaisuudet ole tuttuja.

### Tehtävä

Olkoon  $P$  epävakio kokonaislukukertoiminen polynomi. Oletetaan, että kaikilla kokonaisluvulla  $n$  luku  $P(n)$  on jonkin kokonaisluvun neliö. Osoita, että on olemassa sellainen polynomi  $Q$ , että  $P(x) = Q(x)^2$ .

Tutkitaan ensin tapausta, jossa  $P$  on jaoton (mutta epävakio). Valitaan jokin alkuluku  $p$ , jolla yhtälöllä  $P(x) \equiv 0 \pmod{p}$  on ratkaisu. Olkoon  $x = a$  yksi ratkaisu. Henselin lemmän nojalla tästä voidaan korottaa yksikäsitteisesti ratkaisu  $x = a + bp$  yhtälölle  $P(x) \equiv 0 \pmod{p^2}$  ainakin kaikilla paitsi äärellisen monella  $p$ . Schurin lauseen nojalla  $p$  voidaan kuitenkin valita niin isoksi kun halutaan. Nyt siis  $P(a) \equiv 0 \pmod{p}$  ja  $P(a + bp) \equiv 0 \pmod{p^2}$ .

Koska Henselin lemmän ratkaisun korotus voidaan tehdä vain yhdellä tavalla, niin mikäli  $x \equiv a \pmod{p}$  ja  $x \not\equiv a + bp \pmod{p^2}$ , niin pätee  $P(x) \not\equiv 0 \pmod{p^2}$ . Tällainen  $x$  voidaan selvästi valita (vaikkapa  $x = a + (b + 1)p$ ). Tällöin  $P(x)$  ei ole neliö: pätee  $P(x) \equiv P(a) \equiv 0 \pmod{p}$  ja  $P(x) \not\equiv 0 \pmod{p^2}$ , mutta jos neliöluku on jaollinen alkuluvulla  $p$ , niin se on jaollinen luvulla  $p^2$ .

Osaamme siis ratkaista ongelman jaottomilla polynomeilla  $P$ . Yleisessä tapauksessa  $P$  voidaan kirjoittaa jaottomien kokonaislukukertoimisten polynomien  $Q_1, \dots, Q_k$  tuloksi (Gaussin lemmän nojalla). Siis  $P(x) = Q_1(x) \cdots Q_k(x)$ . Tämä ei vielä aivan vastaa kokonaislukujen alkutekijähajotelmaa: edellinen esitys vastaa sitä, että 72 kirjoitettaisiin muodossa  $2 \cdot 2 \cdot 2 \cdot 3 \cdot 3$ , mutta haluaisimme kirjoittaa sen muodossa  $2^3 \cdot 3^2$ .<sup>52</sup> Tämän vuoksi ”yhdistämme” ne polynomit  $Q_i$ , jotka ovat samoja. Tämä on varsin suoraviivaista.

<sup>50</sup>Vinkki: imitoi Eukleideen todistusta alkulukujen äärettömyydelle. (Alkulukujen äärettömyyden todistus löytyy Esitietoja-luvun lopusta.) Alkulukujen äärettömyyshän on tapaus  $P(x) = x$ .

<sup>51</sup>Sivuhuomautus alkutekijöistä: Tapauksessa  $x^2 + 1$  tiedämme, että polynomin  $x^2 + 1$  alkutekijät ovat ne alkuluvut, jotka ovat  $1 \pmod{4}$  (ja alkuluku 2). Toisen asteen polynomien käsittely voidaan hoitaa käyttämällä neliönjäännösten teoriaa (yksityiskohdat jätetään innokkaille lukijoille). Yleisessä tapauksessa ei ole mitään nättiä tapaa karakterisoida polynomien alkutekijöitä. Tiedetään kuitenkin, että polynomin  $P$  alkutekijöiden ”osuus” kaikista alkuluvuista on jokin positiivinen luku, joka on vähintään  $\frac{1}{\deg(P)}$ . Esimerkiksi polynomin  $x^2 + 1$  alkutekijöitä on (tietystä mielessä) puolet alkuluvuista.

<sup>52</sup>Monesti on hyödyllistä verrata polynomeja käsitteleviä tuloksia niiden kokonaislukuversioihin.

Oletetaan, että polynomit  $Q_i$  ja  $Q_j$  eivät ole yhteistekijättömiä. Tällöin on olemassa jokin epävakio polynomi, joka jakaa ne molemmat. Koska  $Q_i$  ja  $Q_j$  ovat jaottomia (eli ”alkulukupolynomeja”), tämä on mahdollista vain, jos  $Q_i$  ja  $Q_j$  ovat vakiokerttoimen päässä toisistaan: on olemassa rationaaliluku  $r$ , jolla  $Q_i = rQ_j$ . Voimme nyt korvata termin  $Q_i$  polynomin  $P$  ”alkutekijähajotelmasta” polynomilla  $rQ_j$ .

Toistamalla edellä mainittua prosessia päästään lopulta tilanteeseen

$$P(x) = cR_1(x)^{e_1} R_2(x)^{e_2} \cdots R_m(x)^{e_m},$$

missä  $R_1, \dots, R_m$  ovat pareittain yhteistekijättömiä, jaottomia polynomeja,  $c$  on rationaaliluku ja luvut  $e_i$  ovat positiivisia kokonaislukuja. Merkitään  $c = \frac{a}{b}$ , missä  $a$  ja  $b$  ovat kokonaislukuja. Kerrotaan yhtälö puolittain vielä luvulla  $b^2$ , jotta päästään eroon nimittäjistä:

$$b^2 P(x) = abR_1(x)^{e_1} \cdots R_m(x)^{e_m}.$$

Kerroimme yhtälön puolittain nimenomaan luvulla  $b^2$  emmekä luvulla  $b$ , koska nyt yhtälön vasen puoli on kokonaisluvun neliö aina, kun  $x$  on kokonaisluku.

Saatetaan sitten ratkaisu maaliin. Oletetaan ensiksi, että kaikki eksponentit  $e_i$  ovat parillisia. Jotta  $b^2 P(x)$  voi olla neliö, tulee luvun  $ab$  olla kokonaisluvun neliö. Jos taas  $ab$  on neliö, niin  $b^2 P(x)$  on polynomin neliö ja täten  $P(x)$  on polynomin neliö. Tässä tapauksessa olemme valmiit.

Oletetaan sitten, että jokin eksponentti on pariton. Oletetaan vaikka, että  $e_1$  on pariton. Idea on redusoida ongelma jaottoman polynomin tapaukseen. Valitaan jokin indeksi  $i > 1$ . Bezout’n lemmän nojalla on olemassa vain äärellisen monta alkulukua  $p$  niin, että  $R_1(n) \equiv R_i(n) \equiv 0 \pmod{p}$  jollain kokonaisluvulla  $n$ . Tutkitaan vain niitä suuria alkulukuja, joilla tätä ilmiötä ei tapahdu millään  $i$ . Unohdetaan myös ne  $p$ , jotka jakavat luvun  $ab$ .

Schurin lauseen nojalla on olemassa jokin tässä mielessä suuri alkuluku  $p$ , jolla yhtälöllä  $R_1(x) \equiv 0 \pmod{p}$  on ratkaisu. Jaottomia polynomeja käsittelevän osuuden nojalla tiedämme, että nyt on olemassa sellainen kokonaisluku  $n$ , että  $R_1(n) \equiv 0 \pmod{p}$  ja  $R_1(n) \not\equiv 0 \pmod{p^2}$ . Nyt luku  $b^2 P(n)$  on oletuksen nojalla neliö, mutta  $b^2 P(n)$  voidaan esittää kahden luvun tulona: luvun  $R_1(n)^{e_1}$  (jonka alkutekijähajotelman luvun  $p$  eksponentti on  $e_1$ , joka on pariton) ja luvun

$$abR_2(n)^{e_2} \cdots R_m(n)^{e_m}$$

(joka ei ole jaollinen luvulla  $p$ ). Tämä on ristiriita. Olemme valmiit.

Kommentti: Tehtävän ratkaisu käyttää jokaista aiemmin mainituista neljästä perustuloksesta. Henselin lemmää käytetään polynomien arvojen alkutekijöiden eksponenttien tutkimiseen, Gaussin lemmalla muodostetaan alkutekijähajotelma, Bezout’n lemmalla todistetaan (muun muassa) tämän alkutekijähajotelman eri alkuluvun potenssien riippumattomuus ja Schurin lauseen nojalla voidaan unohtaa kaikki äärellisen monta ongelmallista alkulukua.

Tässä valossa ratkaisu voikin tuntua vaikealta: sehän käyttää lukuisia epätriviaaleja tuloksia. Tämä on tietysti totta. Jälkiviisaana ratkaisu on kuitenkin hyvin helppo: jaoton tapaus ratkaistaan Henselin lemmalla ja yleisesti vain tutkitaan jotain

alkutekijähajotelman alkuluvun potenssia. Suuri osa ratkaisusta oli vain intuitiivisten ajatusten formalisointia. Väitteet kuten ”voimme valita yhtälön  $P(x) \equiv 0 \pmod{p}$  ratkaisun, joka ei ole yhtälön  $P(x) \equiv 0 \pmod{p^2}$  ratkaisu”, ”voimme muodostaa polynomille alkutekijähajotelman” ja ”eri jaottomat polynomit eivät juurikaan kommunikoi keskenään” käyvät järkeen, mutta ne vaativat hieman syventymistä yksityiskohtiin. Kun nämä ideat ja niiden formalisoinnit on kerran nähnyt ja sisäistänyt, ei niitä ole enää kovin vaikeaa soveltaa itse.

Seuraava tehtävä on Kiinan IMO-joukkueen valintakokeesta vuodelta 2010.

### Tehtävä

Olkoon  $f(n)$  luvun  $n$  niiden (positiivisten) tekijöiden summa, jotka ovat pienempiä kuin  $n$ . Määritellään  $f^1(n) = f(n)$ , ja  $f^{i+1}(n) = f^i(f(n))$  kaikilla  $i \geq 1$ . Olkoon  $k$  positiivinen kokonaisluku. Osoita, että on olemassa positiivinen kokonaisluku  $n$ , jolla  $n < f(n) < f^2(n) < \dots < f^k(n)$ .

Esimerkiksi  $f^2(12) = f(f(12)) = f(1 + 2 + 3 + 4 + 6) = f(16) = 1 + 2 + 4 + 8 = 15$ . Haluaisimme siis, että luku, jonka tekijöiden summa (pois lukien luku itse) lasketaan, kasvaisi joka iteraatiolla eli joka vaiheessa. Esimerkissä ensimmäinen vaihe toimii, koska  $16 > 12$ , mutta toinen vaihe ei toimi, koska  $15 < 16$ . Täten  $n = 12$  toimii esimerkiksi tehtävään arvolla  $k = 1$ , muttei enää arvolla  $k = 2$ .

Tämän tehtävän kohdalla tehdään poikkeuksellisesti niin, että ensin esitetään puhtaaksi kirjoitettu ratkaisu. Tämän jälkeen mietitään, miten ratkaisuun olisi voinut päätyä itse.

*Ratkaisu:* Valitaan  $n = 6p_1p_2 \cdots p_k$ , missä  $p_1 \equiv -1 \pmod{6}$ ,  $p_i \equiv -1 \pmod{p_{i-1}^2}$  kaikilla  $2 \leq i \leq k$  ja  $p_1, p_2, \dots, p_k$  ovat alkulukuja. Tämä valinta on mahdollinen Dirichlet'n lauseen nojalla valitsemalla alkutekijät järjestyksessä  $p_1, p_2, \dots, p_k$ .

Ratkaisun ydin on seuraava lemma.

### Lemma

Kaikilla  $0 \leq i < k$  pätee  $f^i(n) > 6$ ,  $6 \mid f^i(n)$  ja  $v_{p_j}(f^i(n)) = 1$  kaikilla  $1 \leq j \leq k - i$ .

Todistetaan lemma induktiolla muuttujan  $i$  suhteen. Tapaus  $i = 0$  on selvä.<sup>53</sup> Suoritetaan induktioaskel.

Oletetaan, että lemmän väite pätee arvolla  $i = m$ , ja merkitään  $\sigma(n) = f(n) + n$ . Nyt pätee

$$f^{m+1}(n) = f(f^m(n)) = \sigma(f^m(n)) - f^m(n).$$

Oletuksen nojalla  $f^m(n)$  on jaollinen kuudella. Lisäksi, koska  $m \leq k - 1$ , pätee  $v_{p_1}(f^m(n)) = 1$ . Täten funktion  $\sigma$  multiplikatiivisuuden avulla saadaan

$$\sigma(f^m(n)) = \sigma(p_1)\sigma\left(\frac{f^m(n)}{p_1}\right) = (p_1 + 1)\sigma\left(\frac{f^m(n)}{p_1}\right) \equiv 0 \pmod{6}$$

<sup>53</sup>Voimme siis määritellä  $f^0(n) = n$  kaikilla  $n$ . Mikäli lukija ei ole tähän tyytyväinen, hän voi halutessaan todistaa väitteen arvolla  $i = 1$ . Todistus on käytännössä sama kuin induktioaskeleessa.

oletuksen  $p_1 \equiv -1 \pmod{6}$  nojalla. Täten  $6 \mid f^{m+1}(n)$ .

Todistetaan vastaavasti, että  $v_{p_j}(f^{m+1}(n)) = 1$  kaikilla  $j \leq k - (m + 1)$ . Induktiooletuksen nojalla  $v_{p_{j+1}}(f^m(n)) = 1$ , joten vastaavasti kuin edellä

$$\sigma(f^m(n)) = \sigma(p_{j+1})\sigma\left(\frac{f^m(n)}{p_{j+1}}\right) = (p_{j+1} + 1)\sigma\left(\frac{f^m(n)}{p_{j+1}}\right) \equiv 0 \pmod{p_j^2}$$

luvun  $p_{j+1}$  valinnan nojalla. Täten  $f^{m+1}(n) = \sigma(f^m(n)) - f^m(n)$  on kahden sellaisen luvun erotus, joista ensimmäinen on jaollinen luvulla  $p_j^2$  ja jälkimmäinen on jaollinen luvulla  $p_j$ , muttei luvulla  $p_j^2$  (induktiooletuksen nojalla). Täten  $v_{p_j}(f^{m+1}(n)) = 1$ .

Lopuksi todetaan, että lemmän osa  $f^{m+1}(n) > 6$  seuraa ehdoista  $6 \mid f^{m+1}(n)$  ja  $v_{p_1}(f^{m+1}(n)) = 1$ . Lemma on näin todistettu.

Lemman seurauksena  $f^i(n)$  on jaollinen kuudella ja isompi kuin 6 kaikilla  $0 \leq i < k$ , joten

$$f^{i+1}(n) > \frac{f^i(n)}{2} + \frac{f^i(n)}{3} + \frac{f^i(n)}{6} = f^i(n),$$

mistä tehtävänannon väite seuraa.

Ennen kuin lähdetään miettimään motivaatiota ratkaisun takana, käydään ensiksi läpi, mitä ratkaisussa oikeastaan tapahtuu. Ideana on pakottaa luku  $f^i(n)$  olemaan jaollinen kuudella arvoilla  $i = 0, 1, \dots, k - 1$ , koska tällöin saadaan ratkaisun lopussa esitetty epäyhtälö  $f^{i+1}(n) > f^i(n)$ .

Mihin tämä kuudella jaollisuus perustuu? Tämä saadaan ratkaisussa pakottamalla luvuille  $f^i(n)$  alkutekijä  $p_1$  eksponentilla 1 (eli  $v_{p_1}(f^i(n)) = 1$ ). Tällöin  $f^{i+1}(n) = \sigma(f^i(n)) - f^i(n)$  on kahden luvun erotus, joista kumpikin on jaollinen kuudella.

Ehto  $v_{p_1}(f^i(n)) = 1$  puolestaan säilytetään ehdolla  $v_{p_2}(f^i(n)) = 1$ . Ideana on siis, että alkuluku  $p_2$  ”suojelee” alkutekijää  $p_1$ , aivan kuten  $p_1$  suojelee luvun  $f^i(n)$  jaollisuutta kuudella. Vastaavasti  $p_{j+1}$  suojelee lukua  $p_j$  kaikilla  $j$ . Kuudella jaollisuus saadaan siis säilytettyä suojelijoiden ketjulla  $p_1, p_2, \dots, p_k$ . Mikään ei suojele alkutekijää  $p_k$ , jolloin se katoaa ensimmäisen funktion  $f$  iteroinnin jälkeen. Yleisesti yhdellä iteroinnilla katoaa aina seuraava suojelija jonon päästä.

Nyt siis tiedämme, mitä ratkaisussa tapahtuu, ja saimme myös jonkinlaista käsitystä siitä, miten ratkaisun voisi keksiä. Tässä on vielä hieman lisää ajatuksia ratkaisuprosessista.

Kuudella jaollisuus on varsin luonnollinen idea, koska se on yksi (ja ehkäpä yksinkertaisin) vastaus kysymykseen ”Miten voisimme pakottaa ehdon  $f(n) > n$ ?”

Ratkaisua miettiessäni tutkin seuraavaksi tehtävää arvolla  $k = 2$ , eli epäyhtälöketjua

$$n < f(n) < f(f(n)).$$

Tässä ensimmäinen epäyhtälö saadaan siis valitsemalla  $n$  suuremmaksi kuin 6 ja kuudella jaolliseksi. Vastaavasti voisi yrittää todistaa seuraavaa epäyhtälöä  $f(n) < f(f(n))$  valitsemalla luvun  $f(n)$  olemaan jaollinen kuudella (tiedämmehän, että

helpoin tapa varmistaa epäyhtälö  $k < f(k)$  on valita  $k$  olemaan jaollinen kuudella: meillä ei siis oikein ole muutakaan vaihtoehtoa<sup>54</sup>).

Miten voimme pakottaa luvun  $f(k)$  olemaan jaollinen kuudella? Tämän tapauksen käsittelyä helpottaa funktion  $\sigma$  määrittelemine asettamalla  $\sigma(n) = f(n) + n$ , jolloin  $\sigma(n)$  on luvun  $n$  kaikkien tekijöiden summa. Tekijöiden summalle tiedetään Aritmetiikan peruslause -luvussa todistettu kaava

$$\sigma(p_1^{a_1} \cdots p_t^{a_t}) = \prod_{1 \leq i \leq t} \frac{p_i^{a_i+1} - 1}{p_i - 1}.$$

Lisäksi huomataan, että mikäli  $n$  on jaollinen kuudella, niin  $\sigma(n) \equiv f(n) \pmod{6}$ , joten on aivan sama asia pakottaa luku  $\sigma(n)$  olemaan jaollinen kuudella kuin pakottaa luku  $f(n)$  olemaan jaollinen kuudella.

Ehdon  $\sigma(n) \equiv 0 \pmod{6}$  varmistamiseksi yksi idea on valita luvun  $\sigma(n)$  kaavasta jokin tulontekijä  $\frac{p_i^{a_i+1}-1}{p_i-1}$  ja asettaa se olemaan jaollinen kuudella. Tähän on luontevaa valita  $a_i = 1$  ja  $p_i \equiv -1 \pmod{6}$ . Ehto  $p \equiv -1 \pmod{6}$  pätee Dirichlet'n lauseen nojalla äärettömän monella alkuluvulla  $p$ .

Huomaamme siis, että valinnalla  $n = 6p$ , missä  $p$  ( $p \equiv -1 \pmod{6}$ ) on alkuluku, saadaan ketju  $n < f(n) < f(f(n))$ .

Ei ole enää kovin vaikeaa jatkaa tätä ideaa eteenpäin: Tiedämme nyt, miten saadaan toteutettua epäyhtälöketju  $n < f(n) < f(f(n))$ . Jotta tehtävä saadaan ratkaistua arvolla  $k = 3$ , tulee varmistaa epäyhtälöketjun

$$n < f(n) < f^2(n) < f^3(n)$$

pätevyys. Tämän ketjun voi nähdä koostuvan kahdesta osasta:  $n < f(n)$  ja  $f(n) < f^2(n) < f^3(n)$ . Ensimmäinen osa on helppo varmistaa. Toista osaa varten tulee soveltaa tapauksen  $k = 2$  ratkaisua luvulle  $f(n)$  luvun  $n$  sijasta. Yritämme siis saada luvun  $f(n)$  olemaan jaollinen kuudella ja saada ehdon  $v_p(f(n)) = 1$  pätemään jollain  $p \equiv -1 \pmod{6}$ . Tämän voi saavuttaa valitsemalla  $n = 6pq$ , missä  $q$  ( $q \equiv -1 \pmod{p^2}$ ) on alkuluku.

Valinnan  $n = 6pq$ ,  $q \equiv -1 \pmod{p^2}$  motivaationa on tutkia yhtälöä  $f(n) = \sigma(n) - n$ . Ehdon  $v_p(f(n)) = 1$  varmistamiseksi on kaksi vaihtoehtoa:<sup>55</sup>

1. Valitaan  $v_p(\sigma(n)) \geq 2$  ja  $v_p(n) = 1$ .
2. Valitaan  $v_p(\sigma(n)) = 1$  ja  $v_p(n) \geq 2$ .

Jälkimmäinen vaihtoehto on selvästi huonompi kuin ensimmäinen: lukua  $\sigma(n)$  on vaikeampi käsitellä kuin lukua  $n$ , joten vaikeampi ehto  $v_p(m) = 1$  kannattaa mieluummin varata luvulle  $n$  kuin luvulle  $\sigma(n)$ . Nyt naiivi tapa saada  $v_p(\sigma(n)) \geq 2$  on valita luvulle  $n$  alkutekijä  $q$  eksponentilla 1, missä  $q \equiv -1 \pmod{p^2}$ .

<sup>54</sup>Periaatteessa voisimme myös pakottaa ehdon  $k < f(k)$  valitsemalla luvun  $k$  olemaan jaollinen kaikilla alkuluvuilla väliltä  $[100, N]$ , missä  $N$  on riittävän suuri kokonaisluku, ja yleisesti valita luvuille  $k, f(k), f^2(k), \dots$  naiivisti valtavan määrän alkutekijöitä. (Alkulukujen käänteislukujen summa hajaantuu.) Tämän idean toteuttaminen on kuitenkin työläämpää kuin esitetyn ratkaisun.

<sup>55</sup>Periaatteessa myös valinnoilla  $v_p(n) = v_p(\sigma(n)) = 0$  tai  $v_p(n) = v_p(\sigma(n)) = 1$  voitaisiin saada  $v_p(f(n)) = 1$ , mutta tämä on huomattavasti vaikeampaa.

Näillä ideoilla ei ole enää vaikeaa yleistää ratkaisua mielivaltaiselle  $k$ .

Kommentti: Tehtävässä käytettiin Dirichlet'n lausetta osana ratkaisua. Lukuteorian tehtävissä Dirichlet'n lause on hyvä työkalu sopivien alkulukujen valitsemiseen, monesti yhdessä kiinalaisen jäännöslauseen kanssa. Tästä nähtiin esimerkki jo ne-lönjäännöksiä käsittelevässä kappaleessa.

Seuraavaksi esitetään tehtävä ELMO-lyhytlistalta vuodelta 2017. Lukuteorian lisäksi algebra on tehtävässä huomattavassa osassa.

### Tehtävä

Olkoon  $C$  positiivinen kokonaisluku. Osoita, että ei ole olemassa sellaista ääretöntä erisuurten positiivisten kokonaislukujen jonoa  $a_1, a_2, \dots$ , jolla kaikilla  $k \geq 1$  pätee

$$a_{k+1}^k \mid C^k a_1 a_2 \cdots a_k.$$

Yritetään muodostaa tehtävänannon mukainen lukujono, jotta nähdään, mikä menee pieleen. Tätä kautta voidaan saada ideoita siihen, miten väite kannattaa todistaa.

Ensimmäinen luonnollinen askel on tutkia jaollisuusehtoja yksittäisen alkuluvun potenssien kautta. Saamme

$$k \cdot v_p(a_{k+1}) \leq k \cdot v_p(C) + \sum_{i=1}^k v_p(a_i)$$

eli

$$v_p(a_{k+1}) \leq v_p(C) + \frac{v_p(a_1) + v_p(a_2) + \dots + v_p(a_k)}{k}.$$

Täten  $v_p(a_{k+1})$  on enintään lukujen  $v_p(a_i)$  keskiarvo plus jokin vakio.

Luonteva idea olisi yrittää aina valita  $v_p(a_{k+1})$  suurimmaksi mahdolliseksi luvuksi. Ei ole vaikeaa huomata, että tällöin keskiarvot  $\frac{1}{k}(v_p(a_1) + \dots + v_p(a_k))$  kasvavat mielivaltaisen suuriksi, kunhan  $v_p(C) > 0$ . Miksei tämä ole vastaesimerkki tehtävänannon väitteelle? Ongelmaksi tulee, että luvut  $v_p(a_i)$  kasvavat liian hitaasti, jolloin samat luvut toistuvat lukujonossa useampaan kertaan.

Nyt tiedämme, mistä tehtävässä on kyse: luvuille  $v_p(a_i)$  on annettu epäyhtälöt, ja tulee todistaa, että epäyhtälöt pakottavat jotkin luvut  $a_i$  olemaan yhtä suuria.

Huomaamme, että tehtävässä on vain äärellisen monta ”mielenkiintoista” alkulukua  $p$ , eli siis sellaisia alkulukuja, jotka jakavat jonkin luvuista  $a_i$ , on vain äärellisen monta. Tarkemmin pätee, että mikäli  $p|a_i$  jollain  $i$ , niin  $p|C \cdot a_1$ . Väite seuraa helpolla vastaoletuksella: Oletetaan, että  $p \nmid C \cdot a_1$  ja oletetaan, että  $p|a_i$  jollain  $i$  (jolloin  $i \geq 2$ ). Valitaan pienin tällainen  $i$ , jolloin  $v_p(a_1) = v_p(a_2) = \dots = v_p(a_{i-1}) = 0$ . Edellistä keskiarvoepäyhtälöä käyttämällä saadaan

$$v_p(a_i) \leq v_p(C) + \frac{v_p(a_1) + \dots + v_p(a_{i-1})}{i-1} = 0,$$

mikä on ristiriita oletuksen  $p|a_i$  kanssa.



Olkoot  $p_1, p_2, \dots, p_n$  ne alkuluvut, jotka jakavat vähintään toisen luvuista  $a_1$  ja  $C$ . Tiedämme nyt, että jokainen  $a_i$  voidaan määrittää, kunhan tiedetään luvut  $v_{p_1}(a_i), v_{p_2}(a_i), \dots, v_{p_n}(a_i)$ .

Tehtävää voi visualisoida seuraavasti. Jos  $n = 2$ , niin luvut  $a_i$  voidaan kuvata eksponenteilla  $v_{p_1}(a_i)$  ja  $v_{p_2}(a_i)$ . Nämä kaksi lukua voidaan tulkita  $xy$ -koordinaatiston pisteiden koordinaatteina. Emme saa valita samaa pistettä kahdesti, ja lisäksi rajoitteena on, että uuden pisteen  $x$ - ja  $y$ -koordinaatit saavat olla enintään edellisten  $x$ - tai  $y$ -koordinaattien keskiarvo plus jokin vakio.

Voidaan ajatella, että jokainen johonkin hetkeen mennessä valittu piste on aluksi jossain neliössä, jonka vasen alakulma on origo  $(0, 0)$  ja oikea ylänurkka on  $(N, N)$ . Uusi piste voi olla sellainen, jonka  $x$ - tai  $y$ -koordinaatti on yli  $N$ . Tällöin saamme laajennettua aluetta, jossa pisteet sijaitsevat. Tehtävässä pyydetään osoittamaan, ettei tämä laajentuminen voi tapahtua liian nopeasti.

Tutkitaan yksiulotteista tapausta, jossa siis  $n = 1$ . Merkitään  $b_k = v_{p_1}(a_k)$  ja  $c = v_{p_1}(C)$ . On annettuna epäyhtälö

$$b_{k+1} \leq c + \frac{b_1 + b_2 + \dots + b_k}{k},$$

ja haluamme, että mikään luku ei toistu kahdesti lukujonossa  $b_1, b_2, \dots$ . Tutkitaan vielä konkreettista tapausta, jossa  $c = 2$  ja  $b_1 = 0$ . Jos valitsemme lukujonoon aina suurimman mahdollisen luvun, niin jono näyttää tältä:

$$0, 2, 3, 3, 4, 4, 4, 4, 5, 5, 5, 5, \dots$$

Mitä pidemmälle lukujono etenee, sitä kauemmin kestää, että päästään yhtä isompaan lukuun. Näyttäisi oikeastaan siltä, että  $b_k \approx \log(k)$  eli että lukujono kasvaa todella hitaasti.

Yritetään todistaa, että edellä esitetty ilmiö tapahtuu väistämättä, vaikka luvut  $b_1$  ja  $c$  olisivat suuria ja vaikkei aina valittaisi suurinta mahdollista lukua. Tätä varten on luontevaa yrittää rajoittaa lukujen keskiarvon kasvunopeutta. Yritetään muotoilla annettu epäyhtälö uudelleen keskiarvojen avulla. Olkoon  $s_k = b_1 + b_2 + \dots + b_k$ . Päte

$$b_{k+1} = s_{k+1} - s_k \leq c + \frac{s_k}{k},$$

eli

$$s_{k+1} \leq c + \frac{s_k}{k} \cdot (k+1),$$

joten jakamalla puolittain luvulla  $k+1$  saadaan vasemmalle puolelle keskiarvo:

$$\frac{s_{k+1}}{k+1} \leq \frac{c}{k+1} + \frac{s_k}{k}.$$

Jos nyt merkitään ensimmäisen  $k$  luvun keskiarvoa  $A_k = \frac{s_k}{k}$ , niin saadaan

$$A_{k+1} \leq \frac{c}{k+1} + A_k.$$

Tästä nähdään, että lukujono todella kasvaa hyvin hitaasti; tarkemmin sanoen yhtä hitaasti kuin harmoninen sarja. Purkamalla epäyhtälöä nimittäin nähdään, että

$$\begin{aligned}
 & A_{k+1} \\
 & \leq \frac{c}{k+1} + A_k \\
 & \leq \frac{c}{k+1} + \frac{c}{k} + A_{k-1} \\
 & \vdots \\
 & \leq \frac{c}{k+1} + \frac{c}{k} + \dots + \frac{c}{2} + A_1 \\
 & = A_1 + c \left( \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{k+1} \right).
 \end{aligned}$$

Lukiosta tiedetään, että harmoninen sarja kasvaa suunnilleen yhtä nopeasti kuin  $\log(k)$ . (Nopea perustelu: voidaan arvioida

$$\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \frac{1}{7} \leq \frac{1}{1} + \frac{1}{2} + \frac{1}{2} + \frac{1}{4} + \frac{1}{4} + \frac{1}{4} + \frac{1}{4} = 3,$$

ja yleisesti termejä voidaan arvioida aina edelliseen kakkosen potenssiin. Tämä ei anna optimaalista ylärajaa,<sup>56</sup> mutta tarkoituksimme raja on hyvinkin riittävä.)

Todistuksen viimeistely on helppoa. Valitaan jokin suuri luku  $N$ . Koska luvut  $A_1, A_2, \dots$  kasvavat edellisen nojalla noin logaritmistä vauhtia, pätee  $A_k \leq T \log(N)$  jollain luvusta  $c$  riippuvalla (mahdollisesti suurella) vakiolla  $T$  kaikilla  $k \leq N$ . Tällöin  $b_i \leq c + T \log(N)$  kaikilla  $i \leq N$ . Luvuille  $b_i$  on siis vain  $T \log(N) + c$  verran ”liikkumatilaa”, ja tähän tilaan ei mahdu  $N$  eri lukua, kun  $N$  on riittävän suuri.

---

Edellä ratkaistiin yksiulotteinen tapaus  $n = 1$ . Yleinen tapaus seuraa kuitenkin suoraan edellisestä todistuksesta: Jokaiselle käsiteltävistä  $n$  alkuluvusta  $p_1, \dots, p_n$  voidaan määritellä keskiarvo

$$A_{i,k} = \frac{v_{p_i}(a_1) + v_{p_i}(a_2) + \dots + v_{p_i}(a_k)}{k}.$$

Jokaiselle  $i = 1, 2, \dots, n$  on olemassa jokin vakio  $T_i$ , jolla

$$A_{i,k} \leq T_i \log(k)$$

kaikilla  $k$ .

Valitaan jokin suuri  $N$ . Jokaisella luvulla  $a_k$  ( $k \leq N$ ) tulee päteä  $v_{p_i}(a_k) \leq c_i + T_i \log(N)$  jaollisuusehdosta seuraten. Täten liikkumatilaa eli eri mahdollisuuksia luvuille  $a_i$  on vain

$$(c_1 + T_1 \log(N))(c_2 + T_2 \log(N)) \cdots (c_n + T_n \log(N)),$$

---

<sup>56</sup>Tällä lähestymistavalla saadaan  $\sum_{i=1}^k \frac{1}{i} \leq \log_2(k)$ , mutta parempi approksimaatio on  $\sum_{i=1}^k \frac{1}{i} \approx \ln(k)$ . Tämä arvio on alle 1 päässä tarkasta arvosta.

mikä on alle  $N$ , kun  $N$  on suuri, koska logaritmit eivät kasva läheskään lineaarista vauhtia (tämän tarkempi perustelu jätetään lukijalle.)

Kommentti: Tehtävässä on annettu jaollisuusehto, jota voidaan tutkia lokaalisti yksi alkuluku kerrallaan (ja tässä tehtävässä tämä on selvästi luonnollisin tapa tulkita väitettä). Tämän lisäksi vaaditaan, että luvut  $a_i$  ovat keskenään erisuuria, mikä puolestaan on globaali ehto. Tässäkin ratkaisussa tulee hieman tasapainotella sen kanssa, tutkitaanko tilannetta lokaalisti vai globaalisti.

Viimeisenä esitettävä tehtävä on oma luomukseni. Pidän tehtävästä hyvin paljon, koska väite on hieman yllättävä ja ratkaisu koskee mielestäni tärkeää lukuteoriaan liittyvää ajattelutapaa.

### Tehtävä

Olkoon  $n$  positiivinen kokonaisluku. Osoita, että on olemassa äärellinen joukko  $S$ , jonka alkiot ovat ykköstä suurempia kokonaislukuja ja joka toteuttaa seuraavat ehdot.

1. Mitään joukon  $S$  alkioita ei voi esittää muodossa  $a^b$ , missä  $a$  ja  $b$  ( $b > 1$ ) ovat kokonaislukuja.
2. Kaikilla alkuluvuilla  $p$  on olemassa kokonaisluku  $x$  ja joukon  $S$  alkio  $s$  niin, että  $x^n - s$  on jaollinen luvulla  $p$ .

Haluamme siis muodostaa lukujoukon niin, että kaikilla alkuluvuilla  $p$  jokin sen jäsenistä on  $n$ :s potenssi modulo  $p$ .

Aloitetaan helpoimmasta (epätriviaalista) tapauksesta  $n = 2$ . Tällöin ongelma koskee neliönjäännöksiä ja voidaan muotoilla Legendren symbolin avulla: haluamme, että

$$\left(\frac{s}{p}\right) = 1$$

kaikilla  $p$ , kun  $s$  valitaan sopivasti (jokaiselle  $p$  erikseen). Jos joukossa  $S$  on vain yksi alkio  $a$ , niin tiedämme neliönjäännöksiä käsittelevän kappaleen perusteella, että mikäli  $a$  ei ole neliö, niin äärettömän monella  $p$  pätee

$$\left(\frac{a}{p}\right) = -1.$$

Luku  $a$  ei oletuksen nojalla saa olla neliö. Siis tehtävään ei tapauksessa  $n = 2$  ole ratkaisua, jossa  $|S| = 1$ .

Haluaisimme jonkin tavan pakottaa jonkin Legendren symboleista olemaan 1, ja tämä ei onnistu, jos valitsemme vain yhden luvun. Käytännössä ainoa tavat, joilla tiedämme Legendren symbolien arvojen liittyvän toisiinsa, ovat multiplikatiivisuus eli se, että

$$\left(\frac{a}{p}\right) \left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right),$$

ja neliönjäännösten resiprookkilaki. Tutkitaan ensiksi multiplikatiivisuudesta saatavia tuloksia.

Jotta saamme erilaisia riippuvuuksia joukon  $S$  alkioden Legendren symboleille, kannattaa joukkoon valita paljon erilaisia tuloja samoista luvuista. Pienin tällainen joukko on  $S = \{2, 3, 6\}$ . Huomataan, että tämä toimii: Jos nimittäin pätesi

$$\left(\frac{2}{p}\right) = \left(\frac{3}{p}\right) = \left(\frac{6}{p}\right) = -1,$$

niin multiplikatiivisuuden nojalla pätesi myös

$$\left(\frac{2 \cdot 3 \cdot 6}{p}\right) = (-1) \cdot (-1) \cdot (-1) = -1,$$

mikä on mahdotonta, koska  $2 \cdot 3 \cdot 6 = 6^2$  on neliö. Siis kaikilla  $p$  vähintään yksi luvuista 2, 3 ja 6 on neliönjäännös modulo  $p$ .

Edellä esitetty ratkaisu ei suoraan yleisty korkeammille luvun  $n$  arvoille, koska näille ei ole vastaavaa multiplikatiivista symbolia. Erilaisten tulojen tutkiminen vaikuttaa kuitenkin hyvältä idealta myös yleisessä tapauksessa: tiedämme nimittäin, että kahden  $n$ :nnen potenssin tulo on myös  $n$ :s potenssi, koska jos  $x^n \equiv a \pmod{p}$  ja  $y^n \equiv b \pmod{p}$ , niin  $(xy)^n \equiv ab \pmod{p}$ .

Ongelmana on siis se, että jos  $a$  ja  $b$  eivät ole  $n$ :nsiä potensseja, niin niiden tulo ei välttämättä ole  $n$ :s potenssi, jos  $n > 2$ . Esimerkiksi tapauksessa  $n = 3$  ja  $p = 7$  luvut 2 ja 5 eivät ole kuutioita modulo 7, ja niiden tulo  $10 \equiv 3 \pmod{7}$  ei myöskään ole kuutio. Tämän vuoksi tapauksen  $n = 2$  konstruktio  $S = \{2, 3, 6\}$  ei välttämättä toimi.

Tutkitaan tapausta  $n = 3$ . Kriittinen havainto on se, että joissain tapauksissa kahden epäkuution luvun tulo on kuutio, ja näin on oikeastaan aika usein. Esimerkiksi modulo 7 luvut 2 ja 3 eivät ole kuutioita modulo 7, mutta niiden tulo  $6 \equiv -1 \pmod{7}$  on kuutio  $(-1)^3$ .

Yksi tapa tämän idean selventämiseksi on käyttää primitiivisiä juuria.<sup>57</sup> Olkoon  $g$  primitiivijuuri modulo  $p$ . Jokainen luku  $x$ , joka ei ole  $0 \pmod{p}$ , voidaan esittää  $g$ :n potenssina:  $g^y \equiv x \pmod{p}$ . Merkitään jotain tällaista lukua  $y$  merkinnällä  $\ell(x)$ . (Tämä  $\ell(x)$  on uniikki modulo  $p-1$ .) Jos  $\ell(x)$  on jaollinen kolmella, niin  $x$  on tietysti kuutio. Muussa tapauksessa  $\ell(x)$  on joko 1 tai 2  $\pmod{3}$ .

Tutkitaan sitten luvun  $\ell(xy)$  jaollisuutta kolmella, kun tiedetään luvut  $\ell(x)$  ja  $\ell(y)$ . Ensinnäkin, koska

$$g^{\ell(x)+\ell(y)} \equiv g^{\ell(x)} g^{\ell(y)} \equiv xy \equiv g^{\ell(xy)} \pmod{p},$$

niin  $\ell(xy) \equiv \ell(x) + \ell(y)$ .<sup>58</sup> Jos nyt joko  $\ell(x)$  tai  $\ell(y)$  on jaollinen kolmella, niin kaikki on hyvin: luku  $x$  tai luku  $y$  on kuutio. Lisäksi jos  $\ell(x) \equiv 1 \pmod{3}$  ja  $\ell(y) \equiv 2 \pmod{3}$ , niin  $\ell(xy) \equiv 1 + 2 \equiv 0 \pmod{3}$ , eli  $xy$  on kuutio. Vastaavasti menetellään, jos  $\ell(x) \equiv 2 \pmod{3}$  ja  $\ell(y) \equiv 1 \pmod{3}$ .

<sup>57</sup>Primitiiviset juuret ja täydelliset potenssit liittyvät yleisesti hyvin vahvasti toisiinsa, joten primitiivisten juurten tutkiminen on luonnollinen (ja hyvä) idea.

<sup>58</sup>Oikeastaan  $\ell(xy) \equiv \ell(x) + \ell(y) \pmod{p-1}$ .

Jäljelle jäävät tapaukset  $\ell(x) \equiv \ell(y) \equiv 1 \pmod{3}$  ja  $\ell(x) \equiv \ell(y) \equiv 2 \pmod{3}$ . Näissä tapauksissa pätee  $\ell(xy) \equiv 2 \pmod{3}$  ja  $\ell(xy) \equiv 1 \pmod{3}$ , vastaavasti, joten  $S = \{x, y, xy\}$  ei vielä ole ratkaisu tehtävään. Tämä ongelma voidaan kuitenkin korjata lisäämällä joukkoon  $S$  vielä lisää lukujen tuloja: jos  $\ell(x) \equiv 1 \pmod{3}$  ja  $\ell(xy) \equiv 2 \pmod{3}$ , niin tällöin  $\ell(x^2y) \equiv 1 + 2 \equiv 0 \pmod{3}$ . Vastaavasti tapauksessa  $\ell(x) \equiv 2 \pmod{3}$ ,  $\ell(xy) \equiv 1 \pmod{3}$  saadaan, että  $x^2y$  on kuutio.

Olemme saaneet ratkaistua tehtävän tapauksessa  $n = 3$ : voimme valita joukoksi  $S = \{x, y, xy, x^2y\}$ , missä  $x$  ja  $y$  ovat sellaisia kokonaislukuja, että  $x, y, xy$  ja  $x^2y$  eivät ole täydellisiä potensseja. Tämä onnistuu esimerkiksi valinnalla  $x = 2$  ja  $y = 3$ , jolloin kelpaava joukko on  $S = \{2, 3, 6, 12\}$ .

Luonnollisesti yleiselle  $n$  yritetään menetellä vastaavasti. Kokeillaan siis valita joukoksi  $S$  joukko  $\{x, y, xy, x^2y, \dots, x^{n-1}y\}$ . Tällöin haluamme, että joko  $\ell(x) \equiv 0 \pmod{n}$  tai  $\ell(x^k y) = k\ell(x) + \ell(y) \equiv 0 \pmod{n}$  jollain  $0 \leq k < n$ . Huomataan, että jälkimmäinen ehto on lineaarinen yhtälö muuttujan  $k$  suhteen, joten sillä on ratkaisu ainakin silloin, kun  $\ell(x)$  ja  $n$  ovat yhteistekijättömiä. Jos  $n$  on alkuluku, niin tällöin joko  $\ell(x)$  ja  $n$  ovat yhteistekijättömiä tai  $\ell(x) \equiv 0 \pmod{n}$ , ja meillä on ratkaisu tehtävään. Tapauksessa  $n = 4$  voisi kuitenkin olla, että  $\ell(x) \equiv 2 \pmod{4}$  ja  $\ell(y) \equiv 1 \pmod{4}$ , jolloin konstruktio ei toimikaan.

Pitää siis keksiä jotain muuta. Edellä joukkoon  $S$  lisättiin vain kahden luvun  $x$  ja  $y$  tuloja. Meillä on kuitenkin paljon enemmän valinnanvaraa – voimme lisätä joukkoon  $S$  vaikka mitä. Yksi (muttei todellakaan ainoa) toimiva idea on muodostaa joukko  $S$  seuraavasti: Ensinnäkin joukkoon  $S$  lisätään suuri määrä alkulukuja. Esimerkiksi  $n$  ensimmäistä alkulukua  $p_1, \dots, p_n$  riittävät. Toiseksi lisätään kaikki sellaiset näistä alkuluvuista saatavat tulot, jotka ovat neliövapaita, eli joissa mikään alkuluku  $p_i$  ei esiinny useammin kuin kerran. Tällöin siis  $|S| = 2^n - 1$ .

Ongelma palautuu nyt seuraavaan muotoon: on annettu luvut  $\ell(p_1), \ell(p_2), \dots, \ell(p_n)$ , ja haluamme osoittaa, että näistä voidaan valita jokin osajoukko niin, että tämän osajoukon lukujen summa on jaollinen luvulla  $n$ . Tehtävä palautuu siis kombinatoriikan ongelmaksi. Tämä ongelma ei ole aivan helppo, mutta pienen mietinnän jälkeen voi keksiä seuraavan ratkaisun: Tutkitaan lukuja

$$\ell(p_1), \ell(p_1) + \ell(p_2), \ell(p_1) + \ell(p_2) + \ell(p_3), \dots, \ell(p_1) + \ell(p_2) + \dots + \ell(p_n).$$

Jos jokin näistä luvuista on jaollinen luvulla  $n$ , niin olemme valmiit. Muussa tapauksessa ne antavat enintään  $n - 1$  eri jakojäännöstä jaettaessa luvulla  $n$ , joten jotkin kaksi lukua antavat saman jakojäännöksen. Näiden lukujen erotus on jaollinen luvulla  $n$  ja on myös edelleen jokin summa luvuista  $\ell(p_i)$ , joten olemme valmiit.

Kommentti: Ratkaisun loppuosa ei ole helpoin mahdollinen. Helpompaa olisi valita joukkoon  $S$  ensimmäisten vaikkapa  $n^2$  alkuluvun tulot (missä jokainen luku esiintyy vain kerran), jolloin luvuista  $\ell(p_1), \dots, \ell(p_{n^2})$  jotkin  $n$  ovat samat modulo  $n$ . Näiden lukujen  $\ell(p_i)$  summa on siis jaollinen luvulla  $n$  ja näiden  $p_i$  tulo on joukossa  $S$ , mikä ratkaisee ongelman. Valitsin kuitenkin yllä esitetyn toteutuksen, koska se todistaa hieman vahvemman väitteen (ja koska keksin sen itse ensiksi). Huomaa, että  $n - 1$  alkulukua ei riitä, koska voisi olla  $\ell(p_i) \equiv 1 \pmod{n}$  kaikilla  $i$ .

Valitsin funktion  $\ell(x)$  merkinnäksi nimenomaan l-kirjaimen siitä syystä, että

funktio vastaa logaritmia:  $\ell(x)$  on kuin  $\log_g(x)$  modulo  $p$ . Kaikki normaalien logaritmien laskusäännöt toimivat myös tässä tilanteessa, esimerkkinä ratkaisussa käytetty  $\ell(xy) = \ell(x) + \ell(y)$ . (Huomaa, että  $\ell(x)$  on uniikki modulo  $p-1$ , eli oikeasti tulisi kirjoittaa  $\ell(xy) \equiv \ell(x) + \ell(y) \pmod{p-1}$ . Lisäksi  $\ell(x)$  riippuu valitusta primitiivijuuresta  $g$ .)

Legendren symbolin arvot ovat  $-1$  ja  $1$  (ja  $0$ ). Jos kuutioille määritteli vastaavasti ”kuutiollisen Legendren symbolin”, niin sen arvoissa olisi hyvä olla  $1$ , sellaisia lukuja, joiden kuutiot ovat ykkösiä (aivan kuten neliönjäännöksillä  $-1$  on sellainen luku, jonka neliö on  $1$ ), sekä luku  $0$ . Tällöin arvot olisivat siis  $1, \omega, \omega^2$  ja  $0$ , missä  $\omega$  on sellainen (kompleksi)luku, jolla  $\omega^3 = 1$  mutta  $\omega \neq 1$ . Nyt voitaisiin määritellä kuutiollisen Legendren symbolin arvon muuttujalla  $x$  olevan  $1$ , jos  $\ell(x) \equiv 0 \pmod{3}$ ,  $\omega$ , jos  $\ell(x) \equiv 1 \pmod{3}$  ja  $\omega^2$ , jos  $\ell(x) \equiv 2 \pmod{3}$  (ja  $0$ , jos  $p|x$ ). Tällä määritelmällä kuutiollinen Legendren symboli on multiplikatiivinen.<sup>59</sup>

Yleisesti arvolla  $n$  voisi määritellä  $n$ :nsien potenssien Legendren symbolin vastaavasti, jolloin sen arvot olisivat niin sanotut  $n$ :nnet yksikköjuuret eli sellaiset kompleksiluvut, joiden  $n$ :nnet potenssit ovat ykkösiä. Arvolla  $n = 2$  nämä ovat yksinkertaisesti  $1$  ja  $-1$ , ja esimerkiksi arvolla  $n = 4$  nämä ovat  $1, i, -1$  ja  $-i$ . Tämä antaa vaihtoehtoisen tavan tulkita tehtävää.

Tutkitaan taas tapausta  $n = 3$ . Jos  $p \equiv 2 \pmod{3}$ , niin tällöin kaikki luvut ovat kuutioita modulo  $p$ , kuten Asteet ja primitiivijuuret -kappaleessa nähtiin, joten nämä alkuluvut  $p$  eivät ole mielenkiintoisia. Jos  $p \equiv 1 \pmod{3}$  ja  $g$  on primitiivinen juuri modulo  $p$ , niin luku  $g^{\frac{p-1}{3}}$  on sellainen, jonka kuutio on  $1 \pmod{p}$ , mutta joka ei itsessään ole  $1 \pmod{p}$ . Tämä siis vastaa edellä määriteltyä kolmatta yksikköjuurta  $\omega$ .

Edelliset huomiot koskevat samaa teemaa, jota on käsitelty jo aiemminkin: ”normaalit luvut”, eli vaikkapa rationaaliluvut tai kompleksiluvut, eivät eroa paljoakaan kokonaisluvuista modulo  $p$ . Normaalit laskutoimitukset, mukaan lukien jakolasku, toimivat normaalisti. Normaalisti toimii myös polynomien jakoyhtälö, ja nyt todettiin vielä logaritmien ja yksikköjuurienkin toimivan vastaavasti kompleksiluvuissa ja kokonaisluvuissa modulo  $p$ . Tämä vastaavuus on todella vahva.<sup>60</sup>

Ratkaisussa todettiin, että jos  $n$  on alkuluku, niin on olemassa sellainen toimiva joukko  $S$ , jonka koko on  $n + 1$ . On mahdollista todistaa (kilpailumatematiikan ulkopuolisia menetelmiä käyttämällä), että ei ole olemassa toimivaa joukkoa  $S$ , jonka koko olisi enintään  $n$ . Tämän voi tulkita niin, että (ainakin kun  $n$  on alkuluku) esitetty lähestymistapa ongelmalle on tietystä mielessä oikea. Yleisesti joukon  $S$  minimikoko voi olla suurempi kuin  $n + 1$ . Esimerkiksi arvolla  $n = 4$  pienimmän ratkaisun koko on  $6$ .

<sup>59</sup>Huomaa, että käytännössä todistimme samalla normaalin Legendren symbolin multiplikatiivisuuden.

<sup>60</sup>Vastaavuudesta voisi kertoa enemmänkin (graduni ”Polynomial and exponential equations modulo primes” käsittelee tätä aihetta), mutta tässä ei mennä tämän syvemmälle.

## 12 Polynomit (Algebra)

Tässä luvussa käydään läpi polynomien perusominaisuuksia.

### 12.1 Algebran peruslause

Seuraava tulos on hyvin perustavanlaatuinen, ja se oletetaan monissa materiaaleissa valmiiksi tunnetuksi.

#### Lause (Algebran peruslause)

Olkoon  $P(x)$  polynomi, jonka aste on  $n$  ja joka ei ole nollapolynomi. Tällöin polynomilla  $P$  on tasan  $n$  nollakohtaa.

Huomaa, että esimerkiksi polynomin  $P(x) = (x - 1)^2$  nollakohtien määrä on 2, koska kohdassa  $x = 1$  on kaksinkertainen nollakohta, joka lasketaan kahdesti.

Nollakohdat voivat olla kompleksilukuja. Esimerkiksi polynomilla  $P(x) = x^2 + 1$  ei ole reaalisia nollakohtia (koska  $x^2 + 1 \geq 0 + 1 > 0$  kaikilla reaaliluvuilla  $x$ ), mutta kaksi kompleksista nollakohtaa  $x = i$  ja  $x = -i$  löytyy.

Algebran peruslausetta ei todisteta tässä. Monet sen todistukset käyttävät tietoja, joita ei esiinny lukiossa eikä kilpailuissa. Mainitaan kuitenkin, että riittää todistaa, että jokaisella epävakioilla polynomilla  $P$  on vähintään yksi nollakohta. Tällöin voidaan soveltaa seuraavaksi esitettävää polynomien jakoyhtälöä ja löytää loput nollakohdat.

### 12.2 Polynomien jakoyhtälö

Kokonaislukujen tapaan myös polynomeille on jakoyhtälö.

#### Lause (Polynomien jakoyhtälö)

Olkoot  $A(x)$  ja  $B(x)$  polynomeja (joiden kertoimet voivat olla rationaalilukuja, reaalilukuja tai kompleksilukuja). Oletetaan, että  $B$  ei ole vakio polynomi. Tällöin on olemassa sellaiset polynomit  $P$  ja  $Q$ , että  $\deg(Q) < \deg(B)$  ja että

$$A(x) = P(x)B(x) + Q(x).$$

Lisäksi jos polynomien  $A$  ja  $B$  kertoimet ovat rationaalilukuja, niin  $P$  ja  $Q$  voidaan valita niin, että myös niiden kertoimet ovat rationaalisia. Vastaava väite pätee reaalilukukertoimille.

Haluamme siis löytää polynomin  $Q$ , jolla  $\deg(Q) < \deg(B)$  ja jolla  $A(x) - Q(x)$  on jaollinen polynomilla  $B$ . Tilannetta voi verrata kokonaislukujen jakoyhtälöön, jossa haluamme löytää kokonaisluvulle  $a$  sellaisen kokonaisluvun  $q$ , että  $0 \leq q < b$  ja  $a \equiv q \pmod{b}$ .

Todistamme väitteen ”redusoimalla polynomia  $A$  modulo  $B$ ”. Esimerkiksi jos  $A(x) = x^3$  ja  $B(x) = x^2 + 1$ , niin  $x^3 = x \cdot x^2 \equiv x \cdot (-1) = -x \pmod{x^2 + 1}$ , ja haluttu  $Q$  on löydetty.

Yleisesti jos  $\deg(A) < \deg(B)$ , voidaan valita  $Q = A$ , ja olemme valmiit. Muussa tapauksessa tutkitaan polynomia

$$A_*(x) = A(x) - cx^{\deg(A)-\deg(B)}B(x),$$

missä  $c$  on sellainen vakio, että polynomin  $A_*(x)$  termin  $x^{\deg(A)}$  kerroin on 0. Saamme redusoitua polynomin  $A$  polynomiksi  $A_*$ , jonka aste on pienempi kuin polynomin  $A$ . Jatkamalla tätä prosessia riittävän pitkään päädytään tilanteeseen, jossa pätee  $\deg(A) < \deg(B)$ . Tällöin olemme valmiit: polynomi  $P$  saadaan summaamalla prosessin aikana käytetyt termit  $cx^{\deg(A)-\deg(B)}$ .

Tärkeä sovellus jakoyhtälölle on seuraava lemma.

### Lemma

Olkoon  $A(x)$  polynomi, jolla on nollakohta  $a$ . Tällöin on olemassa polynomi  $P$ , jolla

$$A(x) = (x - a)P(x).$$

Väitteen todistus on jakoyhtälön avulla suoraviivainen: Jaetaan polynomi  $A$  polynomilla  $x - a$ . Tällöin  $A(x) = (x - a)P(x) + Q(x)$  jollain polynomilla  $Q$ , jolla  $\deg(Q) < \deg(x - a) = 1$ . Polynomin  $Q$  tulee siis olla vakiopolynomi. Tämän vakiopolynomin tulee olla 0, koska  $0 = A(a) = (a - a)P(a) + Q(a) = Q(a)$ , joten  $A(x) = (x - a)P(x)$ .

Lemma on hyödyllinen esimerkiksi yhtälöitä ratkottaessa: jos löydetään yhtälölle  $A(x) = 0$  ratkaisu  $x = a$ , voidaan yhtälön ratkaiseminen palauttaa pienempiasteiseen yhtälöön  $P(x) = 0$ .

Lemman avulla voidaan todistaa, että astetta  $n$  olevalla polynomilla  $P$  on enintään  $n$  nollakohtaa ilman, että käytetään algebran peruslausetta. Jos nimittäin nollasta eroavalla polynomilla  $P$  olisi vähintään  $n + 1$  nollakohtaa, niin voitaisiin kirjoittaa  $P(x) = (x - \alpha_1)Q(x)$ , missä  $\alpha_1$  on ensimmäinen näistä nollakohdista ja  $Q$  on jokin polynomi. Nyt  $Q$ :n aste on  $n - 1$  ja sillä on  $n$  nollakohtaa. Voimme edetä näin. Lopulta saamme vakiopolynomin, jolla on yksi nollakohta. Tästä seuraa, että tämä vakio on nolla, mutta tällöin myös  $P$  on nollapolynomi.

## 12.3 Rationaalinen juuri

On olemassa yksinkertainen kriteeri, jolla voi määrittää, onko kokonaislukukertoimisella polynomilla rationaalisia juuria.



**Lause (Rationaaliset juuret)**

Olkoon  $P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ , missä kertoimet  $a_i$  ovat kokonaislukuja ja  $a_n \neq 0$ . Tällöin kaikki polynomin  $P$  rationaaliset juuret muotoa  $\frac{s}{t}$  (missä  $\text{syty}(s, t) = 1$ ) ovat sellaisia, joilla  $s|a_0$  ja  $t|a_n$ .

Todistetaan lause. Olkoon  $\frac{s}{t}$ , missä  $\text{syty}(s, t) = 1$ , jokin polynomin  $P$  rationaalinen juuri. Tutkitaan lauseketta  $P(\frac{s}{t})$ . Saadaan

$$0 = P\left(\frac{s}{t}\right) = a_n \frac{s^n}{t^n} + a_{n-1} \frac{s^{n-1}}{t^{n-1}} + \dots + a_1 \frac{s}{t} + a_0.$$

Koska tutkimme jaollisuutta, on luontevaa kertoa puolittain luvulla  $t^n$ , jolloin jokainen termi saadaan kokonaisluvuksi:

$$0 = a_n s^n + a_{n-1} t s^{n-1} + \dots + a_1 t^{n-1} s + a_0 t^n.$$

Ensimmäistä lukuun ottamatta kaikki termit ovat jaollisia luvulla  $t$ . Koska summa on 0, eli jaollinen  $t$ :llä, tulee olla  $t|a_n s^n$ . Koska  $\text{syty}(s, t) = 1$ , seuraa tästä  $t|a_n$ . Vastaavasti  $s|a_0 t^n$ , eli  $s|a_0$ .

**Esimerkki**

Ratkaise yhtälö  $x^3 + \frac{5}{3}x^2 + \frac{11}{3}x + 2 = 0$ .

Jotta polynomi saadaan kokonaislukukertoimiseksi, tulee yhtälö ensiksi kertoa puolittain luvulla 3. Saadaan  $3x^3 + 5x^2 + 11x + 6 = 0$ . Tiedetään, että rationaaliset juuret ovat muotoa  $\frac{p}{q}$ , missä  $p|6$  ja  $q|3$ . Vaihtoehtoja on siis maksimissaan 16: luvun  $p$  tulee olla jokin luvuista 1, 2, 3 ja 6, ja luvun  $q$  tulee olla joko 1 tai 3, ja lisäksi tulee huomioida negatiiviset ratkaisut etumerkillä  $-$ .

Ei vie kovin paljoa aikaa käydä 16 vaihtoehtoa läpi. Monesti läpikäyntiä voi kuitenkin nopeuttaa helpoilla havainnoilla. Nämä havainnot voivat olla esimerkiksi seuraavanlaisia.

Koska polynomin kertoimet  $3x^3 + 5x^2 + 11x + 6$  kaikki kertoimet ovat positiivisia, ei ratkaisu voi olla positiivinen.

Jos  $q = 1$ , olisi ratkaisu kokonaisluku. Ratkaisu ei voi olla pariton kokonaisluku, koska tällöin  $3x^3 + 5x^2 + 11x + 6$  on pariton, eikä siis 0. Laskemalla nähdään, että  $x = -2$  ja  $x = -6$  eivät ole ratkaisuja. Siis kokonaislukuratkaisuja ei ole.

Jos  $q = 3$ , luku  $p$  ei saa olla jaollinen kolmella, koska muuten  $\frac{p}{q}$  olisi kokonaisluku. Täten  $p = 1$  tai  $p = 2$  eli  $x = -\frac{1}{3}$  tai  $x = -\frac{2}{3}$ .

Kokeilemalla löydetään ratkaisu  $x = -\frac{2}{3}$ . Polynomien jakokulmalla saadaan

$$3x^3 + 5x^2 + 11x + 6 = (3x + 2)(x^2 + x + 3).$$

Muut nollakohdat saadaan ratkaisemalla toisen asteen yhtälö  $x^2 + x + 3 = 0$ .

Yhtälöillä ei tietenkään aina ole rationaalisia ratkaisuja, ja näihin tapauksiin menetelmä ei auta.

## 12.4 Vietan kaavat

Tutkitaan toisen asteen polynomeja  $ax^2 + bx + c$  ( $a \neq 0$ ). Tiedetään, että tämän polynomin nollakohdat ovat

$$\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Nollakohtien summa on siis

$$\frac{-b + \sqrt{b^2 - 4ac}}{2a} + \frac{-b - \sqrt{b^2 - 4ac}}{2a} = -\frac{b}{a}.$$

Lopputulos on yllättävän sievä. Entä nollakohtien tulo? Tulo on

$$\frac{-b + \sqrt{b^2 - 4ac}}{2a} \cdot \frac{-b - \sqrt{b^2 - 4ac}}{2a}.$$

Lauseke sievenee käyttämällä yhtälöä  $(x + y)(x - y) = x^2 - y^2$ . Saamme

$$\frac{(-b)^2 - (\sqrt{b^2 - 4ac})^2}{(2a)^2} = \frac{4ac}{4a^2} = \frac{c}{a}.$$

Jälleen saatiin yllättävän sievä lopputulos. Mistä tämä johtuu?

Syy ilmiölle on, että polynomit voidaan esittää nollakohtiensa avulla.

### Lemma

Olkoon  $P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$  polynomi. Olkoot sen  $n$  juurta  $\alpha_1, \alpha_2, \dots, \alpha_n$ . Tällöin

$$P(x) = a_n(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n).$$

Todistus: Polynomilla  $P$  on nollakohta  $\alpha_1$ , joten se voidaan kirjoittaa muodossa  $P(x) = (x - \alpha_1)Q_1(x)$ . Polynomilla  $Q_1$  on nollakohdat  $\alpha_2, \alpha_3, \dots, \alpha_n$ , joten se voidaan kirjoittaa muodossa  $Q_1(x) = (x - \alpha_2)Q_2(x)$ . Näin voidaan jatkaa: lopulta  $Q_{n-1}(x)$  voidaan kirjoittaa muodossa  $(x - \alpha_n)Q_n(x)$ . Polynomilla  $Q_n(x)$  ei ole enää juuria, joten se on vakio. Purkamalla sijoitukset saadaan

$$P(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)Q_n(x).$$

Vertaamalla termin  $x^n$  kerrointa puolittain saadaan, että vakion  $Q_n(x)$  tulee olla  $a_n$ . Tämä todistaa väitteen.

Lemmasta seuraa Vietan kaavat, jotka selittävät aiemmin havaitun ilmiön.

**Lause (Vietan kaavat)**

Olkoon  $P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$  polynomi. Olkoot sen  $n$  juurta  $\alpha_1, \alpha_2, \dots, \alpha_n$ . Tällöin

$$\prod_{i=1}^n \alpha_i = (-1)^n \cdot \frac{a_0}{a_n}$$

ja

$$\sum_{i=1}^n \alpha_i = -\frac{a_{n-1}}{a_n}.$$

Yleisemmin: Olkoon  $S_k$  summa, joka saadaan laskemalla yhteen kaikki mahdolliset  $k$  eri juuren  $\alpha_i$  tulot. (Edellä esitetyt tulo ja summa ovat  $S_n$  ja  $S_1$ .) Tällöin

$$S_k = (-1)^k \cdot \frac{a_{n-k}}{a_n}.$$

Lauseen väite seuraa yhtälöstä

$$a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 = a_n (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n).$$

Yhtälön oikea puoli on lukujen  $S_i$  määritelmän nojalla

$$a_n (x^n - S_1 x^{n-1} + S_2 x^{n-2} - S_3 x^{n-3} + \dots + (-1)^n S_n).$$

Vertailemalla termien  $x^k$  kertoimia saadaan haluttu väite.

**Esimerkki**

Tutkitaan polynomia  $x^3 + 2x^2 + 3x + 4$ . Olkoot sen nollakohdat  $a, b$  ja  $c$ . Tiedetään, että

$$x^3 + 2x^2 + 3x + 4 = (x - a)(x - b)(x - c).$$

Kerrotaan oikea puoli auki:

$$(x - a)(x - b)(x - c) = x^3 - (a + b + c)x^2 + (ab + bc + ca)x - abc.$$

Vertailemalla termin  $x^2$  kerrointa näissä esityksissä saadaan  $a + b + c = -2$ . Vastaavasti  $ab + bc + ca = 3$  ja  $abc = -4$ .

Tutkitaan sitten Johdantotehtäviä-luvun tehtävää.

**Tehtävä**

Yhtälöllä  $x^3 + 2x^2 + 3x + 4 = 0$  on kolme ratkaisua. Merkitään niitä kirjaimin  $a, b$  ja  $c$ . Laske  $a^2 + b^2 + c^2$ .

Edellinen esimerkki kertoo, mitä ovat  $a + b + c$ ,  $ab + bc + ca$  ja  $abc$ , mutta nämä eivät suoraan anna vastausta. Vastauksen voi kuitenkin esittää näiden lausekkeiden

avulla: auki kertominen nimittäin antaa, että

$$a^2 + b^2 + c^2 = (a + b + c)^2 - 2(ab + bc + ca).$$

Oikea puoli on  $(-2)^2 - 2 \cdot 3 = -2$ . Siispä  $a^2 + b^2 + c^2 = -2$ . Huomaa, että neliöiden summa voi olla negatiivinen, koska  $a, b$  ja  $c$  eivät välttämättä ole reaalityyppisiä.

Voisiko vastaavaa menetelmää soveltaa vaikkapa lausekkeen  $a + 2b + 3c$  arvon laskemiseen? Ei, koska tunnetut polynomit  $a + b + c$ ,  $ab + bc + ca$  ja  $abc$  ovat symmetrisiä muuttujien  $a, b$  ja  $c$  suhteen, joten niiden yhdistelmäkin on. Kysymyksessä ei oikeastaan olisi järkeä, jos  $a^2 + b^2 + c^2$  korvattaisiin lausekkeella  $a + 2b + 3c$ , koska vastaus riippuisi siitä, mikä juuri olisi  $a$ , mikä  $b$  ja mikä  $c$ . Tehtävän polynomin tulee siis myös olla symmetrinen.

Toisaalta kaikilla symmetrisillä polynomeilla menetelmä toimii. Tämä on seuraava aihe.

## 12.5 Symmetriset polynomit

Aloitetaan symmetristen polynomien määritelmällä.

### Määritelmä

Olkoon  $n$  positiivinen kokonaisluku, ja olkoot  $a_1, a_2, \dots, a_n$  muuttujia. Sanoetaan, että polynomi  $P(a_1, a_2, \dots, a_n)$  on symmetrinen muuttujien  $a_1, \dots, a_n$  suhteen, jos kaikilla permutaatioilla  $f : \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\}$  pätee

$$P(a_1, a_2, \dots, a_n) = P(a_{f(1)}, a_{f(2)}, \dots, a_{f(n)}).$$

Määritelmä on hieman tekninen, mutta intuitiivisesti on selvää, milloin polynomi on symmetrinen.

### Esimerkki

Polynomi  $P(a, b, c) = a^2 + b^2 + c^2$  on symmetrinen, mutta polynomi  $Q(a, b, c) = a + 2b + 3c$  ei ole.

Esitettävää päätulosta varten määritellään vielä alkeissymmetrispolynomit.

### Määritelmä

Olkoon  $n$  positiivinen kokonaisluku, ja olkoot  $a_1, a_2, \dots, a_n$  muuttujia. Kokonaisluvulle  $1 \leq k \leq n$  määritellään  $S_k$  olemaan se polynomi, joka saadaan summaamalla kaikki mahdolliset tulot  $k$  eri luvusta  $a_i$ . Polynomeja  $S_1, S_2, \dots, S_n$  kutsutaan  $n$ :siksi alkeissymmetrispolynomeiksi.

### Esimerkki

Kolmannet alkeissymmetrispolynomit ovat  $S_1 = a + b + c$ ,  $S_2 = ab + bc + ca$  ja  $S_3 = abc$ .

**Esimerkki**

Neljännet alkeissymmetrispolynomit ovat  $S_1 = a + b + c + d$ ,  $S_2 = ab + ac + ad + bc + bd + cd$ ,  $S_3 = abc + abd + acd + bcd$  ja  $S_4 = abcd$ .

Alkeissymmetrispolynomit ovat siis samat polynomit, joita käsiteltiin jo aiemmin Vietan kaavojen yhteydessä. Päättös on seuraava.

**Lause (Symmetristen polynomien peruslause)**

Olko  $n$  positiivinen kokonaisluku, ja olko  $P(a_1, a_2, \dots, a_n)$  symmetrinen polynomi. Tällöin  $P$  voidaan esittää  $n$ :nsien alkeissymmetrispolynomien avulla, eli on olemassa  $n$  muuttujan polynomi  $Q$ , jolla  $Q(S_1, S_2, \dots, S_n) = P$ .

**Esimerkki**

Polynomi  $a^2 + b^2 + c^2$  on symmetrinen, joten se voidaan esittää alkeissymmetrispolynomien  $a + b + c$ ,  $ab + bc + ca$  ja  $abc$  avulla:  $a^2 + b^2 + c^2 = (a + b + c)^2 - 2(ab + bc + ca)$ .

Lausetta ei todisteta formaalisti, mutta käydään läpi, miten esitys löydetään.

**Esimerkki**

Etsi polynomille  $P(a, b, c) = a^3 + b^3 + c^3$  esitys alkeissymmetrispolynomien avulla.

Etsitään esitys vähentämällä polynomista  $P$  polynomi  $(a + b + c)^3$ . Jäljelle jää  $P_1(a, b, c) = P(a, b, c) - (a + b + c)^3 = -3(a^2b + a^2c + b^2a + b^2c + c^2a + c^2b) - 6abc$ . Huomaa, että lopputulos on symmetrinen.

Riittää siis enää esittää  $P_1(a, b, c)$ . Yritetään eliminoida termit muotoa  $a^2b$ . Tämä saadaan tehtyä tulolla  $(a + b + c)(ab + bc + ca)$ , joka on auki kerrottuna summa termeistä muotoa  $a^2b$  plus  $3abc$ . Lisätään siis polynomiin  $P_1(a, b, c)$  polynomi  $3(a + b + c)(ab + bc + ca)$ . Saamme

$$P_2(a, b, c) = P_1(a, b, c) + 3(a + b + c)(ab + bc + ca) = 3abc.$$

Polynomien  $P_2$  voi esittää alkeissymmetrispolynomien avulla, joten myös polynomien  $P_1$  voi, ja siten myös polynomien  $P$  voi. Esitys saadaan purkamalla sijoitukset:

$$\begin{aligned} P(a, b, c) &= P_1(a, b, c) + (a + b + c)^3 \\ &= P_2(a, b, c) - 3(a + b + c)(ab + bc + ca) + (a + b + c)^3 \\ &= 3abc - 3(a + b + c)(ab + bc + ca) + (a + b + c)^3 \end{aligned}$$

Esitystavan etsimiseen on selkeä logiikka, jota seuraamalla päästään maaliin: eliminoidaan aina ”isoimmat” lausekkeet. Edellisessä esimerkissä eliminoitiin ensiksi

termit muotoa  $a^3$  (valinnanvaraa ei ollut). Tämän jälkeen oli kaksi vaihtoehtoa: eliminoidaan joko termit  $a^2b$  tai termi  $abc$ . Termi  $a^2b$  on kuitenkin isompi, joten se eliminoidiin ensimmäisenä. Lopussa on jäljellä enää ”pieni” termi  $abc$ , joka ratkeaa suoraan.

Logiikka, jolla määritellään isoin termi, on yksinkertainen. Tutkitaan termejä  $a^x b^y c^z$ , ja oletetaan, että  $x \geq y \geq z$ . Isoin termi on se, jolla on suurin luvun  $x$  arvo. Jos muuttujan  $x$  arvot ovat samat, vertaillaan luvun  $y$  arvoa ja niin edelleen. Tämän vuoksi termi  $a^3 = a^3 b^0 c^0$  on suurempi kuin  $a^2b = a^2 b^1 c^0$ . Luonnollinen tapa ajatella järjestystä on sanakirja, jossa on sanoja  $xyz$  (kuten 300 ja 210): isoin termi on se, joka on sanakirjassa viimeisenä.

Eliminointiin käytettävä polynomi on yksikäsitteinen. Ensimmäisessä askeleessa haluttiin eliminoida termit  $a^3$ . Ainoa tapa tähän on valita lauseke  $(a + b + c)^3$ , koska muualta ei saa termiä  $a^3$ . Vastaavasti termien  $a^2b$  eliminointiin ainoa mahdollisuus oli  $(a + b + c)(ab + bc + ca)$ , koska muualta ei saa termiä  $a^2b$  (paitsi polynomista  $(a + b + c)^3$ , mutta tätä ei voida enää käyttää, koska syntyisi iso termi  $a^3$ ).

Symmetristen polynomien peruslauseen todistus perustuu juuri näihin havaintoihin: redusoidaan polynomia niin, että jäljelle jää aina vain pienempiä ja pienempiä termejä.

## 12.6 Monen muuttujan polynomit

Edellä käsiteltiin symmetrisiä polynomeja. Mitä voidaan yleisesti sanoa monen muuttujan polynomeista?

Monen muuttujan polynomit käyttäytyvät paljolti samalla tavalla kuin yhden muuttujan polynomit. Yleinen ajatus onkin, että vaikkapa kahden muuttujan polynomia  $P(x, y)$  voi aluksi käsitellä polynomina muuttujan  $y$  suhteen. Tällöin muuttujaa  $x$  pidetään vakiona. Etuna tässä on se, että esimerkiksi jakoyhtälöä voidaan soveltaa tälle muuttujan  $y$  polynomille.

Esitetään esimerkkitehtävä. Vaikka tehtävä on näennäisesti epäyhtälötehtävä, perustuu ratkaisu juuri edellä esitettyyn ideaan. Tehtävä on esiintynyt helmikuun 2018 valmennustehtävissä.

### Tehtävä

Olkoot  $x, y$  ja  $z$  reaalilukuja, jotka toteuttavat ehdot  $x + y \geq 2z$  ja  $y + z \geq 2x$ . Osoita, että

$$5(x^3 + y^3 + z^3) + 12xyz \geq 3(x^2 + y^2 + z^2)(x + y + z)$$

ja että yhtäsuuruus vallitsee jos ja vain jos  $x + y = 2z$  tai  $y + z = 2x$ .

Tutkitaan polynomia  $P(x, y, z) = 5(x^3 + y^3 + z^3) + 12xyz - 3(x^2 + y^2 + z^2)(x + y + z)$ . Haluamme osoittaa, että tämä on aina vähintään 0 ja että nollakohtia ovat muun muassa  $x + y = 2z$  ja  $y + z = 2x$ . Nollakohtien tarkistaminen on helppoa ja jätetään lukijalle. Yhden muuttujan polynomeilla nollakohdista saadaan tulontekijä, joten yritetään samaa monen muuttujan tilanteessa.

Tutkitaan täten kolmen muuttujan polynomia  $P(x, y, z)$  polynomina muuttujan  $z$  suhteen, jonka kertoimet ovat polynomeja muuttujista  $x$  ja  $y$ . Jaetaan  $P$  jakokulmassa polynomilla  $2z - (x + y)$  muuttujan  $z$  suhteen. Saadaan

$$P(x, y, z) = (2z - (x + y))Q(x, y, z) + R(x, y, z).$$

Jakoyhtälön toiminnan vuoksi voidaan olettaa, että polynomin  $R$  aste muuttujan  $z$  suhteen on pienempi kuin polynomin  $2z - (x + y)$  aste (muuttujan  $z$  suhteen). Siis  $R$  on vakio muuttujan  $z$  suhteen, eli  $R$  on kahden muuttujan polynomi  $R(x, y)$ .

Sijoitetaan yllä  $z = \frac{x+y}{2}$ . Tällöin  $P(x, y, z) = 0$  ja  $2z = x + y$ . Yhtälö on siis

$$R(x, y) = 0.$$

Koska  $x$  ja  $y$  olivat mielivaltaisia, on polynomin  $R$  oltava nollapolynomi. Täten

$$P(x, y, z) = (2z - (x + y))Q(x, y, z).$$

Vastaavalla menettelyllä muille symmetrisille lausekkeille saadaan

$$P(x, y, z) = (2z - (x + y))(2y - (x + z))(2x - (y + z))A(x, y, z)$$

jollain polynomilla  $A$ . Koska polynomin  $P$  aste on 3 ja oikean puolen aste on  $\deg(A) + 3$ , tulee polynomin  $A$  olla vakiopolynomi  $c$ . On helppoa tarkistaa, että  $c = 1$  tutkimalla vaikkapa termin  $x^3$  kerrointa. Tehtävän viimeistely tästä ei ole enää vaikeaa.

## 13 Arviointi ja epäyhtälöt (Algebra)

Tässä luvussa esitetään tehtäviä, joissa erilaisten arvioiden ja epäyhtälöiden tekeminen on oleellisessa osassa. Tämän lisäksi luvun lopussa käsitellään lyhyesti klassisia epäyhtälöitä.

### 13.1 Johdanto

Aloitetaan muutamalla tuloksella, jotka johdattelevat aiheeseen. Tulokset ovat melko intuitiivisia, joten todistukset sivuutetaan, mutta lukija voi halutessaan miettiä niitä itseksensä.

#### Esimerkki

Kaikilla riittävän suurilla  $n$  pätee  $n < 2^n$ .

#### Esimerkki

Kaikilla riittävän suurilla  $n$  pätee  $n^{100} < 2^n$ .

#### Esimerkki

Kaikilla riittävän suurilla  $n$  pätee  $n^{100} < 1.01^n$ .

Edellä esitetyt tulokset käytännössä sanovat, että polynomit kasvavat hitaammin kuin eksponenttifunktiot.

Tässä ja myöhemmin käytetään usein virkettä ”Kaikilla tarpeeksi suurilla  $n$  pätee väite  $V$ ”. Tämä tarkoittaa, että ”On olemassa sellainen  $c$ , että kaikilla  $n > c$  pätee väite  $V$ .” Ensimmäinen muotoilu on lyhyempi ja välittää saman idean hieman selvemmin kuin jälkimmäinen, joten käytämme sitä.

### 13.2 Jaollisuusesimerkkejä

Seuraavat kaksi esimerkkiä perustuvat seuraavaan helppoon huomioon: jos  $a|b$ , niin pätee joko  $b = 0$  tai  $|a| \leq |b|$ .

Aloitetaan helpolla esimerkillä.

#### Tehtävä

Määritä kaikki positiiviset kokonaisluvut  $m$  ja  $n$ , joilla  $m|n+1$  ja  $n|m+1$ .

Karkeasti idea on seuraava: Koska  $m | n+1$ , niin  $m \leq n+1$ , joten  $m$  on enintään noin  $n$ . Vastaavasti  $n$  on enintään noin  $m$ , joten  $n$  ja  $m$  ovat suunnilleen yhtä suuria.

Tässä on yksityiskohdat: Ehdosta  $m|n+1$  seuraa  $m \leq n+1$ , ja vastaavasti



saadaan  $n \leq m + 1$ . Yhdistämällä nämä tiedot saadaan

$$n - 1 \leq m \leq n + 1.$$

Tulee tutkia kolme helppoa tapausta:

*Tapaus 1:*  $m = n - 1$ . Tällöin  $n|m + 1$  toteutuu varmasti ja  $m|n + 1$  tarkoittaa, että  $n - 1|n + 1$ , mistä seuraa  $n - 1|2$ . Siispä  $n - 1 = 1$  tai  $n - 1 = 2$ , joten saadaan ratkaisut  $(m, n) = (1, 2)$  ja  $(m, n) = (2, 3)$ .

*Tapaus 2:*  $m = n$ . Tällöin  $n|m + 1$  vaatii, että  $n = 1$ , ja tästä saadaan ratkaisu  $m = n = 1$ .

*Tapaus 3:*  $m = n + 1$ . Tämä on sama kuin tapaus  $m = n - 1$ , mutta luvut  $m$  ja  $n$  on vaihdettu toisin päin. Saadaan ratkaisut  $(m, n) = (2, 1)$  ja  $(m, n) = (3, 2)$ .

Kommentti: Tehtävän voi ratkoa myös toisella tavalla. Ratkaisu perustuu seuraavaan huomioon: jos  $m|n + 1$ , mutta  $m \neq n + 1$ , niin  $m$  on enintään  $\frac{n+1}{2}$ . Jos siis oletamme, että  $m \neq n + 1$ , niin yhdessä ehdon  $n|m + 1$  kanssa nyt pätee

$$n \leq m + 1 \leq \frac{n+1}{2} + 1 = \frac{n}{2} + \frac{3}{2}.$$

Tästä seuraa, että  $n \leq 3$ . Tehtävän viimeistely voidaan nyt tehdä samaan tapaan kuin yllä.

Seuraavana on toinen jaollisuustehtävä, joka on esiintynyt vuonna 2009 Japanin kansallisessa kilpailussa.

### Tehtävä

Määritä kaikki kokonaisluvut  $n$ , joilla  $2^n + n|8^n + n$ .

Jaollisuusehdosta saatava epäyhtälö  $2^n + n \leq 8^n + n$  pätee tietysti kaikilla  $n$ , joten tämä ei auta. Tulee siis tehdä jotain muuta.

Ideana on redusoida lukua  $8^n + n$  modulo  $2^n + n$ , jolloin saadaan toivottavasti pieni jakojäännös, jonka tulee olla 0 modulo  $2^n + n$ . Tällöin saadaan hyödyllinen epäyhtälö.

Tuumasta toimeen. Yksi tapa toteuttaa idea on seuraava: pätee

$$2^n \equiv -n \pmod{2^n + n},$$

joten kuutioimalla puolittain saadaan

$$8^n \equiv -n^3 \pmod{2^n + n},$$

eli

$$2^n + n|8^n + n^3.$$

Yhdistämällä tämän tietoon  $2^n + n|8^n + n$  saadaan

$$2^n + n|n^3 - n.$$

Tämä näyttää jo varsin hyvältä: suurilla luvun  $n$  arvoilla pätee  $2^n + n > n^3 - n \neq 0$ , joten enää tulee tutkia pienet tapaukset. Kysymys kuuluu: kuinka suurilla  $n$  epäyhtälö  $2^n + n > n^3 - n$  pätee?

On monta tapaa saada jokin sopiva raja. Tässä on yksi niistä: Ehto  $2^n + n > n^3 - n$  pätee ainakin silloin, kun  $2^n \geq n^3$ . Huomataan, että väite pätee arvolla  $n = 10$ , koska

$$2^{10} = 1024 \geq 1000 = 10^3.$$

Jos lukua  $n$  kasvatetaan yhdellä, niin  $2^n$  kaksinkertaistuu. Toisaalta luku  $n^3$  enintään kaksinkertaistuu, kun  $n \geq 7$ :

$$(n+1)^3 = n^3 + 3n^2 + 3n + 1 \leq n^3 + 3n^2 + 3n^2 + n^2 = n^3 + 7n^2 \leq n^3 + n \cdot n^2 = 2n^3.$$

Siispä induktiolla saadaan todistettua, että  $2^n \geq n^3$  pätee kaikilla  $n \geq 10$ . Täten kaikki tehtävän ratkaisut ovat alle 10, ja nämä voidaan vain käydä käsin läpi. Tätä helpottaa se, että ehto  $2^n + n | 8^n + n$  pätee täsmälleen silloin, kun  $2^n + n | n^3 - n$ : luvut  $8^n$  kasvavat nopeasti melko suuriksi, mutta  $n^3$  kasvaa verrattain hitaasti. Saadaan ratkaisut  $n = 1, 2, 4, 6$ .

Kommentti: Monesti jaollisuusehdon tullessa vastaan kannattaa ensiksi katsoa, voisiko sen esittää luonnollisesti jossain muussa muodossa. Tässä tehtävässä jaollisuusehdon muotoilu  $2^n + n | n^3 - n$  on sekä luonnollinen että hyödyllinen.

### 13.3 Polynomien arvot ja kertoma

Seuraavana esitetään hyödyllinen tulos polynomien arvojen suuruuden arvioimiseksi. Tulos on intuitiivinen, vaikkakin todistus on aavistuksen tekninen.

#### Lemma

Olkoon  $P(x) = a_d x^d + a_{d-1} x^{d-1} + \dots + a_1 x + a_0$ . Oletetaan, että  $a_d > 0$ . Kaikilla tarpeeksi suurilla  $x$  pätee  $0.99 \cdot a_d x^d < P(x) < 1.01 \cdot a_d x^d$ .

Lemman vakiot 0.99 ja 1.01 voidaan tietysti korvata vakioilla  $1 - \epsilon$  ja  $1 + \epsilon$ , missä  $\epsilon$  on mikä tahansa positiivinen (pieni) luku. Lisäksi vastaava väite on luonnollisesti olemassa, jos  $a_d < 0$ . Pointtina on, että polynomin aste ja korkeimman asteen termin kerroin määrää polynomin arvojen kasvunopeuden.

Todistetaan lemma. Ideana on kirjoittaa  $P(x) = a_d x^d + \dots + a_1 x + a_0$  muotoon

$$P(x) = a_d x^d \left( 1 + \frac{a_{d-1}}{a_d x} + \frac{a_{d-2}}{a_d x^2} + \dots + \frac{a_0}{a_d x^d} \right).$$

Nähdään, että kun  $x$  on hyvin suuri, niin suluissa oleva termi tulee olemaan lukujen 0.99 ja 1.01 välillä. Tarkan todistuksen ylärajalle voi todistaa vaikka seuraavasti: Valitaan  $x$  niin, että kaikilla  $0 \leq i \leq d-1$  pätee

$$\frac{a_i}{a_d x^{d-i}} < \frac{0.01}{d}$$

eli

$$\sqrt[d-i]{\frac{100a_id}{a_d}} < x.$$

Tämä selvästi onnistuu (haluamme siis vain, että  $x$  on suurempi kuin jotkin  $d$  lukua). Luku  $x$  valittiin näin, jotta saadaan seuraava epäyhtälö:

$$\begin{aligned} & 1 + \frac{a_{d-1}}{a_dx} + \frac{a_{d-2}}{a_dx^2} + \dots + \frac{a_0}{a_dx^d} \\ & < 1 + \frac{0.01}{d} + \frac{0.01}{d} + \dots + \frac{0.01}{d} = 1.01. \end{aligned}$$

Alaraja saadaan aivan vastaavaan tapaan. Yksityiskohdat on hyvä käydä läpi ainakin mielessä.

Käydään sitten läpi esimerkkitehtävä. Tehtävä on esiintynyt Suomen IMO-joukkueen valintakokeessa.

### Tehtävä

Määritä kaikki kokonaislukukertoimiset polynomit  $P$ , joilla kaikilla positiivisilla kokonaisluvuilla  $n$  pätee sekä  $P(n) > 0$  että

$$P(n!) = (P(n))!.$$

Ratkaisu perustuu oleellisesti ottaen siihen, että yhtälön oikean puolen  $P(n)!$  kasvaa huomattavasti nopeammin kuin vasemman puolen  $P(n!)$  kaikissa paitsi hyvin pienessä määrässä tapauksia. Lukija voi halutessaan yrittää todistaa tämän polynomille  $P(x) = x^2$  ennen kuin lukee ratkaisun.

Olkoon  $P(x) = a_dx^d + \dots + a_0$ . Kertoimet  $a_i$  ovat oletuksen nojalla kokonaislukuja. Lisäksi pätee  $a_d > 0$  (miksi?), joten  $a_d \geq 1$ . Käyttämällä edellistä lemmaa saadaan, että kaikilla tarpeeksi suurilla  $x$  pätee

$$0.99a_dx^d \leq P(x) \leq 1.01a_dx^d.$$

Yritetään käyttää tätä yhtälön vasemman ja oikean puolen arvioimiseen. Molempien puolien arvioimisessa tulee vastaan sama ongelma: kuinka suuri kertoma  $n!$  on? Tähän vastaa seuraava lemma. Lemman antamat ala- ja ylärajat ovat melko huonot, mutta ne kuitenkin riittävät tarkoituksiimme. Tarkempia tuloksia antaa ns. Stirlingin approksimaatio, mutta tälle on harvemmin käyttöä kilpailumatematiikassa.<sup>61</sup>

### Lemma

Kaikilla  $n \geq 1$  pätee

$$2^{n-1} \leq n! \leq n^n.$$

<sup>61</sup>Stirlingin approksimaatio käytännössä kertoo, että  $n! \approx \left(\frac{n}{e}\right)^n$ , missä  $e \approx 2.718$  on Eulerin luku. Täten tulon  $n! = 1 \cdot 2 \cdot \dots \cdot n$  termit ovat "tulon suhteen" keskimäärin  $\frac{n}{e}$  (eli lukujen  $1, 2, \dots, n$  ns. geometrinen keskiarvo on noin  $\frac{n}{e}$ , kun taas aritmeettinen eli "tavallinen" keskiarvo on  $\frac{n+1}{2}$ ). Tämä keskiarvo on kokoluokkaa  $0.4n$ .

Todistus on varsin helppo: pätee

$$n! = 1 \cdot 2 \cdot 3 \cdot \dots \cdot n \geq 1 \cdot 2 \cdot 2 \cdot \dots \cdot 2 = 2^{n-1},$$

ja

$$n! = 1 \cdot 2 \cdot 3 \cdot \dots \cdot n \leq n \cdot n \cdot n \cdot \dots \cdot n = n^n.$$

Etsitään nyt luvulle  $P(n!)$  yläraja. Koska kaikilla tarpeeksi suurilla  $n$  pätee epäyhtälö  $P(n) \leq P(n+1)$  (harjoitustehtävä), ja pätee  $n! \leq n^n$ , niin pätee myös

$$P(n!) \leq P(n^n).$$

Käyttämällä arviota  $P(x) < 1.01 \cdot a_d x^d$  saadaan

$$P(n^n) \leq 1.01 \cdot a_d n^{nd}.$$

Etsitään sitten luvulle  $P(n)!$  alaraja. Vastaavasti kuin edellä saadaan

$$P(n)! \geq \lfloor 0.99 a_d n^d \rfloor! \geq 2^{\lfloor 0.99 a_d n^d \rfloor - 1}.$$

Haluamme siis todistaa, että

$$1.01 a_d n^{nd} < 2^{\lfloor 0.99 a_d n^d \rfloor - 1}.$$

Otetaan puolittain 2-kantainen logaritmi ja käytetään logaritmien laskusääntöjä:

$$\log_2(1.01 a_d) + nd \log_2(n) < \lfloor 0.99 a_d n^d \rfloor - 1.$$

Vasen puoli on enintään vaikkapa  $n\sqrt{n}$ , kun  $n$  on suuri (koska  $\log_2(1.01 a_d)$  on vakio ja  $d \log_2(n)$  kasvaa hitaammin kuin  $\sqrt{n}$ ), ja oikea puoli on vähintään  $0.98 a_d n^d$ , kun  $n$  on suuri. Jos  $d \geq 2$ , niin epäyhtälö pätee tarpeeksi suurilla  $n$ .

Olemme päässeet jo pitkälle: tiedämme, että kaikkien ratkaisujen  $P$  asteet ovat enintään 1. Edelliset arviot ovat kuitenkin liian huonoja ratkaisemaan tapauksen  $\deg(P) \leq 1$ , joten tämä pitää tutkia vielä erikseen. Kirjoitetaan  $P(x) = ax + b$ . Vakiotapaus on helppo ( $b = 1$  tai  $b = 2$ ), joten oletetaan, että  $a \geq 1$ . Yhtälö

$$P(n!) = P(n)!$$

muuttuu muotoon

$$a \cdot n! + b = (an + b)!.$$

On uskottavaa, että oikea puoli kasvaa nopeammin kuin vasen puoli, jos  $a \geq 2$ . Tämän saa todistettua vaikkapa seuraavasti: kaikilla tarpeeksi suurilla  $n$  pätee

$$(an + b)! \geq (2n + b)! \geq (n + 1)! = (n + 1) \cdot n! > (a + 1) \cdot n! = a \cdot n! + n! > a \cdot n! + b.$$

Olemme taas poissulkeneet suuren määrän polynomeja. Enää on jäljellä tapaus  $a = 1$  eli tapaus  $P(x) = x + b$ . Tutkitaan ensiksi tapaus  $b \geq 1$ : tällöin saadaan

$$P(n)! = (n + b)! \geq (n + 1)! = (n + 1) \cdot n! = n \cdot n! + n! > n! + b = P(n!)$$

kaikilla suurilla  $n$ .

Jos taas  $P(x) = x + b$ , missä  $b < 0$ , niin suurilla  $n$  pätee

$$P(n)! = (n + b)! \leq (n - 1)! < n! + b = P(n!).$$

Ainoa jäljellä oleva tapaus on  $b = 0$ , ja tämä antaa ratkaisun  $P(x) = x$ . Kokonaisuudessaan kaikki ratkaisut ovat siis  $P(x) = 1$ ,  $P(x) = 2$  ja  $P(x) = x$ .

Kommentti: Ratkaisussa on melko paljon laskemista, mutta mikään tehdyistä arvioista ei kuitenkaan ole erityisen vaikea, eikä mikään arvioista ole erityisen ”tiukka”. Lähinnä jokaisessa vaiheessa ratkaisua riittää keksiä jokin siedettävän hyvä arvio. Esitetyt epäyhtälöt eivät siis todellakaan ole ainoat tavat saada todistettua halutut väitteet.

### 13.4 Vaikea esimerkki

Seuraavana esitetään tehtävä, jossa tarvitaan melko vaikeita arvioita. Ratkaisu on hyvin pitkä, ja sen aikana nähdään monia erilaisia tapoja tehdä arvioita. Tehtävä on vuoden 2018 ELMO-kilpailusta.

#### Tehtävä

Olkoot  $a_1, a_2, \dots, a_m$  positiivisia kokonaislukuja. Osoita, että on olemassa epänegatiiviset kokonaisluvut  $b, c$  ja  $N$ , joilla

$$\left\lfloor \sum_{i=1}^m \sqrt{n + a_i} \right\rfloor = \lfloor \sqrt{bn + c} \rfloor$$

kaikilla kokonaisluvuilla  $n > N$ .

Summaa neliöjuurilausekkeista voidaan siis arvioida hyvin yhdellä neliöjuurilausekkeella, mikä on melko mielenkiintoista.

On luontevaa yrittää ensin keksiä, mitä luvut  $b$  ja  $c$  ovat, ja sen jälkeen yrittää todistaa tämän arvauksen toimivuus. Luku  $N$  kuvastaa tässä tietysti vain sitä, että tutkitaan vain suuria luvun  $n$  arvoja.

Yhtälön vasen puoli on suurilla  $n$  karkeasti kokoluokkaa  $m \cdot \sqrt{n}$  eli  $\sqrt{m^2 n}$ . Tämän takia arvaus  $b = m^2$  vaikuttaa hyvältä. Tämä on oikeastaan ainoa luvun  $b$  arvo, joka voisi mitenkään toimia: Vasenta puolta voidaan arvioida seuraavasti:

$$\left\lfloor \sum_{i=1}^m \sqrt{n + a_i} \right\rfloor > \left\lfloor \sum_{i=1}^m \sqrt{n + 0} \right\rfloor = \lfloor m\sqrt{n} \rfloor = \lfloor \sqrt{m^2 n} \rfloor > \sqrt{m^2 n} - 1.$$

Yhtälön oikea puoli saadaan vastaavasti arvioitua ylöspäin: isoilla  $n$  pätee

$$\lfloor \sqrt{bn + c} \rfloor < \sqrt{bn + c} + 1 < \sqrt{bn + 0.5n} + 1 = \sqrt{(b + 0.5)n} + 1.$$

Nyt nähdään, että mikäli  $b \leq m^2 - 1$ , niin  $\sqrt{(b + 0.5)n} + 1 < \sqrt{m^2 n} - 1$  kaikilla suurilla  $n$ , mikä on ristiriita. Siispä tulee päteä  $b \geq m^2$ . Vastaavasti saadaan  $b \leq m^2$ . Tätä ei osoiteta tässä, koska todistusta ei oikeastaan edes tarvita tehtävän ratkaisemiseksi.

Yritetään sitten arvata luvun  $c$  arvo. Tämä ei ole aivan yhtä helppoa kuin luvun  $b$  arvaaminen, koska nyt tarvitaan parempia arvioita neliöjuurilausekkeille. Tähän on kuitenkin yksi kikka, jota voisi yrittää:

Lukujen  $k^2, k^2 + 1, k^2 + 2, \dots, k^2 + 2k + 1 = (k + 1)^2$  neliöjuuret ovat välillä  $[k, k + 1]$ . Voisi olettaa, että nämä neliöjuuret ovat melko tasaisesti jakautuneita eli että nämä  $2k + 2$  lukua jakavat välin  $[k, k + 1]$  suunnilleen yhtä suuriin väleihin, joita on  $2k + 1$  kappaletta. Voidaan siis arvioida

$$\sqrt{k^2 + x} \approx k + \frac{x}{2k + 1},$$

kun  $0 \leq x \leq 2k + 1$ .

Tämän avulla voidaan veikata luvun  $c$  arvo. Tutkitaan ensin vain tilanteita, joissa  $n$  on neliöluku  $k^2$ . Nyt

$$\left\lfloor \sum_{i=1}^m \sqrt{k^2 + a_i} \right\rfloor \approx \left\lfloor \sum_{i=1}^m k + \frac{a_i}{2k + 1} \right\rfloor = \left\lfloor mk + \frac{a_1 + a_2 + \dots + a_m}{2k + 1} \right\rfloor.$$

Vastaavasti saadaan

$$\lfloor \sqrt{bn + c} \rfloor = \lfloor \sqrt{(mk)^2 + c} \rfloor \approx \left\lfloor mk + \frac{c}{2mk + 1} \right\rfloor.$$

Vaikuttaa siis siltä, että veikkaus  $c = m(a_1 + a_2 + \dots + a_m)$  tai jokin tämäntyylinen toimisi. Edellä esitetyt arviot eivät kuitenkaan ole missään nimessä formaaleja todistuksia, joten tämä veikkaus ei välttämättä edes toimi. Kannattaa siis tutkia jotain erikoistapausta ja sen perusteella tarkistaa, toimiiko arvaus vai pitääkö luvun  $c$  arvoa muuttaa.

Huomataan, että jos kaikki luvut  $a_i$  ovat yhtä suuria, niin tehty valinta  $c = m(a_1 + \dots + a_m)$  todella toimii: tällöin yhtälön molemmat puolet ovat yhtä suuria kuin  $\lfloor \sqrt{m^2(n + a_1)} \rfloor$ . Entä vaikkapa tapaus  $m = 2, a_1 = 1$  ja  $a_2 = 3$ ? Tällöin epäyhtälön vasen puoli on  $\lfloor \sqrt{n + 1} + \sqrt{n + 3} \rfloor$  ja oikea puoli on  $\lfloor \sqrt{4n + 8} \rfloor$ .

Ei ole selvää, toimiiko arvaus tässä tapauksessa. Lienee kuitenkin hyödyllistä ratkaista tämä erikoistapaus ennen yleiseen tapaukseen siirtymistä. Miten tämän toimivuus (tai epätoimivuus) todistetaan? Yksi idea on asettaa  $\lfloor \sqrt{4n + 8} \rfloor = k$ , ja toivoa, että pätee myös  $\lfloor \sqrt{n + 1} + \sqrt{n + 3} \rfloor = k$ . Pätee siis

$$k \leq \sqrt{4n + 8} < k + 1,$$

eli neliöinnin ja uudelleenjärjestelyn jälkeen

$$\frac{k^2 - 8}{4} \leq n < \frac{k^2 + 2k - 7}{4}.$$

Funktio  $f(n) = \sqrt{n + 1} + \sqrt{n + 3}$  on kasvava, joten funktion  $\lfloor f(n) \rfloor$  arvojen määrittämiseksi riittää tutkia sen arvoja, kun  $n$  saa maksimi- ja minimiarvonsa. Tutkitaan ensiksi minimiarvoa, joka on

$$\left\lfloor \sqrt{\frac{k^2 - 8}{4} + 1} + \sqrt{\frac{k^2 - 8}{4} + 3} \right\rfloor = \left\lfloor \frac{1}{2} \left( \sqrt{k^2 - 4} + \sqrt{k^2 + 4} \right) \right\rfloor.$$

Tämä on alle  $\lfloor 4n + 8 \rfloor = k$ , eli meillä on ongelma. Huomataan, että  $n$  todella saa arvon  $\frac{k^2-8}{4}$  äärettömän usein, nimittäin silloin kun  $4n + 8$  on neliö. Siis veikkaus  $c = m(a_1 + \dots + a_m)$  ei toimi kaikissa tapauksissa.

Kaikki työ ei ole kuitenkaan mennyt hukkaan: Ensinnäkin esimerkki vihjaa pienentämään lukua  $c$  hieman, joten voimme seuraavaksi yrittää valita  $c = m(a_1 + a_2 + \dots + a_m) - 1$  (veikkauksemme luvusta  $c$  oli kuitenkin vain melko vähän pielessä). Toiseksi saimme idean siitä, miten epäyhtälön voisi todistaa yleisessä tapauksessa. Jos tämäkään luvun  $c$  veikkaus ei toimi, niin se tullaan huomaamaan todistusta yrittäessä, ja voimme yrittää keksiä vielä uuden suunnitelman.

Tutkitaan siis yleistä tapausta luvuilla  $a_1, a_2, \dots, a_m$ . Veikkaamme, että valinta  $b = m^2$  ja  $c = m(a_1 + a_2 + \dots + a_m) - 1$  toimii. Asetetaan  $\lfloor \sqrt{bn + c} \rfloor = k$ , eli

$$k \leq \sqrt{bn + c} < k + 1.$$

Kuten edellä tästä voidaan ratkaista  $n$ :

$$\frac{k^2 - c}{b} \leq n < \frac{(k + 1)^2 - c}{b}.$$

Ja kuten edellä riittää todistaa, että

$$k \leq \left\lfloor \sum_{i=1}^m \sqrt{n + a_i} \right\rfloor < k + 1,$$

kun  $n$  saa pienimmän ja suurimman arvonsa.

Tutkitaan ensiksi maksimitapausta. Koska  $n$  on kokonaisluku, on sen suurin arvo enintään

$$\frac{(k + 1)^2 - c - 1}{b},$$

joten haluamme, että

$$\sum_{i=1}^m \sqrt{\frac{(k + 1)^2 - c - 1}{b} + a_i} < k + 1.$$

Sijoitetaan tähän arvauksen mukaiset lukujen  $b$  ja  $c$  arvot. Saamme

$$\sum_{i=1}^m \sqrt{\frac{(k + 1)^2 - m(a_1 + a_2 + \dots + a_m)}{m^2} + a_i} < k + 1$$

eli

$$\sum_{i=1}^m \sqrt{(k + 1)^2 + m^2 a_i - m(a_1 + \dots + a_m)} < (k + 1)m.$$

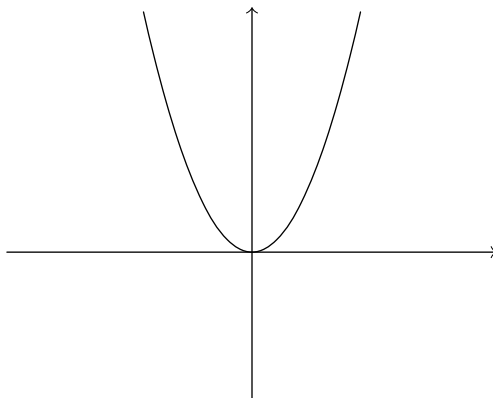
Haluamme siis todistaa ylärajan sille, kuinka suuri summa neliöjuurilausekkeista voi olla.

Apuun tulee Jensenin epäyhtälö. Sen esittämistä varten tarvitaan seuraava määritelmä.

**Määritelmä**

Funktiota  $f : \mathbb{R} \rightarrow \mathbb{R}$  kutsutaan konveksiksi, jos seuraava ehto pätee: jos funktion  $f$  kuvaajalta valitaan mitkä tahansa kaksi pistettä  $P_A = (a, f(a))$  ja  $P_B = (b, f(b))$ , niin kuvaaja kulkee pisteiden  $P_A$  ja  $P_B$  välillä näiden pisteiden välisen janan alapuolella (tai janan päällä).

Esimerkiksi paraabeli  $f(x) = x^2$  on konveksi, koska sen kuvaaja näyttää tältä:



Määritelmä ei tällaisenaan ole vielä kovin käyttökelpoinen. Ehdon voi kuitenkin kirjoittaa muodossa

$$f(ax + b(1 - x)) \leq f(a)x + f(b)(1 - x),$$

missä  $0 \leq x \leq 1$  ja  $a$  ja  $b$  ovat mielivaltaisia. Tämä on vain algebrallinen muoto ehdon graafiselle muodolle. Toinen, käytännössä hyödyllisin muotoilu konveksisuudelle on ehto  $f''(x) \geq 0$  kaikilla  $x \in \mathbb{R}$ .

Jensenin epäyhtälö liittyy konvekseihin funktioihin.

**Lause (Jensenin epäyhtälö)**

Olkoon  $f : \mathbb{R} \rightarrow \mathbb{R}$  konveksi funktio. Kaikilla reaaliluvuilla  $x_1, x_2, \dots, x_m$  pätee

$$\frac{f(x_1) + f(x_2) + \dots + f(x_m)}{m} \geq f\left(\frac{x_1 + x_2 + \dots + x_m}{m}\right).$$

Pari kommenttia epäyhtälöön liittyen: Jos  $f$  on ns. aidosti konveksi eli  $f''(x) > 0$  kaikilla<sup>62</sup>  $x$ , niin epäyhtälössä pätee yhtäsuuruus vain silloin, kun  $x_1 = x_2 = \dots = x_m$ . Lisäksi jos  $f$  on konkaavi funktio, eli  $f''(x) \leq 0$  kaikilla  $x$ , niin epäyhtälö pätee toiseen suuntaan. (Tämän voi todistaa tutkimalla konkaavin funktion  $f$  sijasta konveksia funktiota  $g(x) = -f(x)$ .)

Idea epäyhtälön takana on intuitiivinen. Tutkitaan esimerkiksi tapausta  $f(x) = e^x$ .

<sup>62</sup>Tätä ehtoa voi oikeastaan vielä lieventää: riittää olettaa, että  $f''(x) \geq 0$  kaikilla  $x$  ja  $f''(x) = 0$  pätee vain yksittäisissä pisteissä. Esimerkiksi funktio  $f(x) = x^4$  on aidosti konveksi.



Tällöin  $f''(x) = e^x > 0$ , eli  $f$  on aidosti konvekksi. Nyt pätee

$$\frac{e^{x_1} + e^{x_2}}{2} \geq e^{\frac{x_1+x_2}{2}}.$$

Jos  $x_1$  on hyvin suuri verrattuna lukuun  $x_2$ , niin yhtälön vasen puoli on kokoluokkaa  $\frac{1}{2}e^{x_1}$  ja oikea puoli vain kokoluokkaa  $e^{x_1/2}$ . Termi  $e^{x_1}$  on ”dominoiva” termi, ja sen jakaminen kahdella vaikuttaa paljon vähemmän kuin eksponentin  $x_1$  jakaminen kahdella. Kun  $x_1$  ja  $x_2$  ovat lähellä toisiaan, tapahtuu vastaava ilmiö, vaikkakin pienemmässä mittakaavassa.<sup>63</sup>

Funktio  $f(x) = \sqrt{x}$  on aidosti konkaavi funktio:

$$f''(x) = -\frac{1}{4x\sqrt{x}} < 0.$$

Siispä Jensenin epäyhtälö pätee toiseen suuntaan, ja pätee esimerkiksi

$$\frac{\sqrt{3} + \sqrt{5}}{2} \leq \sqrt{\frac{3+5}{2}} = \sqrt{4}.$$

Tämä on luonnollista: mitä isompi luku  $x$  on, sitä hitaammin  $\sqrt{x}$  kasvaa (tämä on käytännössä konkaaviuden määritelmä, ja neliöjuuren tapauksessa väite käy muutenkin järkeen). Siispä  $\sqrt{3}$  on kauempana luvusta  $\sqrt{4}$  kuin mitä  $\sqrt{4}$  on luvusta  $\sqrt{5}$ , mistä seuraa edellä esitetty epäyhtälö.

Huomautus: Sovelsimme tässä Jensenin neliöjuurifunktiolle, vaikka funktio  $f(x) = \sqrt{x}$  ei ole määritelty kaikilla reaaliluvuilla. Tämä ei kuitenkaan ole ongelma: Jensenin saa soveltaa yleisesti tapauksessa, jossa  $f$  on määritelty jollain reaalilukujen välillä (kunhan funktio on tällä välillä konvekksi tai konkaavi). Tällöin epäyhtälön luvuiksi  $x_i$  saa tietysti valita lukuja vain tältä väliltä, eli esimerkiksi neliöjuurifunktiolle tulee valita  $x_i \geq 0$ . (Miksi näin saadaan tehdä? Jensenin epäyhtälön todistus toimii samaan tapaan funktioille  $f: \mathbb{R} \rightarrow \mathbb{R}$  kuin vaikkapa funktioille  $f: \mathbb{R}^+ \rightarrow \mathbb{R}^+$ .)

Palataan tehtävän ratkaisuun. Suoraviivainen Jensenin epäyhtälön soveltaminen antaa arvion

$$\begin{aligned} & \frac{\sum_{i=1}^m \sqrt{(k+1)^2 + m^2 a_i} - m(a_1 + \dots + a_m)}{m} \\ & \leq \sqrt{\frac{\sum_{i=1}^m (k+1)^2 + m^2 a_i - m(a_1 + \dots + a_m)}{m}} \\ & = \sqrt{(k+1)^2} = k+1. \end{aligned}$$

Haluamme kuitenkin, että summa termeistä  $\sqrt{(k+1)^2 + m^2 a_i} - m(a_1 + \dots + a_m)$  on aidosti pienempää kuin  $(k+1)m$ . Miten poissuljemme yhtäsuuruustapauksen?

<sup>63</sup>Jensenin epäyhtälön tapaus  $n = 2$  seuraa suoraan piirtämällä kuvaajan ja käyttämällä konveksisuuden geometrista määritelmää. Yksi tapa todistaa Jensenin epäyhtälö on todistaa siitä painotettu versio epäyhtälöstä induktiolla muuttujan  $n$  suhteen.

Jensenin epäyhtälön yhteydessä mainittiin, että aidosti konvekseilla tai aidosti konkaveilla funktioilla epäyhtälössä pätee yhtäsuuruus vain silloin, kun kaikki luvut, joille epäyhtälöä sovelletaan, ovat samat. Siispä edellä pätee yhtäsuuruus vain silloin, kun kaikki luvut  $a_i$  ovat samoja. Tämä on kuitenkin helppo tapaus (jonka käsitelimme jo aiemmin), koska tällöin voidaan valita  $c = m(a_1 + a_2 + \dots + a_m)$ . Täten tapaus, joissa kaikki luvut  $a_i$  ovat samat, on käsitelty, ja muissa tapauksissa saimme halutun epäyhtälön.

Olemme nyt käsitelleet maksimitapauksen, mutta vielä on tekemättä minimitarastelu. Haluamme, että

$$k \leq \left\lfloor \sum_{i=1}^m \sqrt{n + a_i} \right\rfloor$$

kaikilla käsiteltävillä  $n$ . Sijoitetaan luvun  $n$  paikalle aiemmin saatu alaraja  $\frac{1}{b}(k^2 - c)$  ja sijoitetaan myös lukujen  $b$  ja  $c$  lausekkeet paikalleen. Edellinen epäyhtälö palautuu väitteeseen

$$km \leq \sum_{i=1}^m \sqrt{k^2 + m^2 a_i - m(a_1 + \dots + a_m) + 1},$$

joka on vastaavan tyyppinen kuin maksimitapauksen yhteydessä saatu epäyhtälö. Tällä kertaa kuitenkin haluamme alarajan neliöjuurien summalle.

Ennen kuin yritetään todistaa tämä epäyhtälö, katsellaan sitä hieman kauempaa. Epäyhtälö on muotoa

$$km \leq \sum_{i=1}^m \sqrt{k^2 + b_i},$$

missä luvut  $b_i = m^2 a_i - m(a_1 + \dots + a_m) + 1$  ovat kokonaislukuja, jotka eivät riipu luvusta  $k$ . Osa luvuista  $b_i$  voi olla negatiivisia ja osa positiivisia. Lisäksi todetaan, että lukujen summa on  $m$  (eli positiivinen), mikä antaa hieman liikkumavaraa.

Meillä on ongelma: Jensenin epäyhtälö antaa neliöjuurien summalle ylärajan muotoa

$$\sqrt{a} + \sqrt{b} \leq 2\sqrt{\frac{a+b}{2}} = \sqrt{2a+2b},$$

mutta se ei anna alarajaa.

Haluaisimme ikään kuin soveltaa Jensenin epäyhtälöä toiseen suuntaan neliöjuurille luvuista  $k^2 + b_i$ . Sellaisenaan epäyhtälö ei tietenkään päde haluttuun suuntaan, mutta ehkä sitä voitaisiin muuttaa hieman halutun epäyhtälön saamiseksi.

Seuraava lemma demonstroi tätä kahdella muuttujalla.

### Lemma

Olkoot  $a$  ja  $b$  reaalilukuja. Kaikilla tarpeeksi suurilla  $k$  pätee

$$\sqrt{k^2 + a} + \sqrt{k^2 + b} \geq 2\sqrt{k^2 + \frac{a+b}{2}} - 1.$$

Luku  $k$  siis valitaan suureksi verrattuna lukuihin  $a$  ja  $b$ . Huomaa, että Jensenin epäyhtälön nojalla pätee

$$\sqrt{k^2 + a} + \sqrt{k^2 + b} \leq 2\sqrt{k^2 + \frac{a+b}{2}},$$

eli termi  $-1$  oikean puolen neliöjuuren sisällä on todella tarpeen. Termi  $-1$  voitaisiin oikeastaan korvata millä tahansa negatiivisella vakiolla.

Lemman voi todistaa naiivisti neliöimällä: Haluamme, että

$$(k^2 + a) + (k^2 + b) + 2\sqrt{k^2 + a}\sqrt{k^2 + b} \geq 4\left(k^2 + \frac{a+b}{2} - 1\right)$$

eli

$$\sqrt{k^2 + a}\sqrt{k^2 + b} \geq k^2 + \frac{a+b}{2} - 2.$$

Neliöidään uudestaan. Saadaan

$$k^4 + (a+b)k^2 + ab \geq k^4 + k^2(a+b-4) + \left(\frac{a+b}{2} - 2\right)^2$$

eli

$$4k^2 \geq \left(\frac{a+b}{2} - 2\right)^2 - ab.$$

Tämä selvästi pätee suurilla  $k$ .

Lemman tulos ei oikeastaan ole yllättävä: Jensenin epäyhtälön antama arvio on varsin hyvä silloin, kun käytetyt luvut  $x_i$  ovat lähellä toisiaan. Lemman tuloksessa luvut  $k^2 + a$  ja  $k^2 + b$  ovat (suhteessa lukujen kokoon) hyvin lähellä toisiaan, kun  $k$  on suuri, ja tällöin

$$\sqrt{k^2 + a} + \sqrt{k^2 + b} \approx 2\sqrt{k^2 + \frac{a+b}{2}} > 2\sqrt{k^2 + \frac{a+b}{2} - 1}.$$

Lemma ei kuitenkaan itsessään vielä riitä, vaan haluaisimme siitä seuraavan monen muuttujan variantin.

### Lemma

Olkoot  $x_1, x_2, \dots, x_m$  reaalitykijöitä. Kaikilla tarpeeksi suurilla  $k$  pätee

$$\sum_{i=1}^m \sqrt{k^2 + x_i} \geq m\sqrt{k^2 + \frac{x_1 + \dots + x_m}{m} - 1}.$$

Tämä lemma todistaisi haluamamme väitteen, koska tämän tehtävän tapauksessa lukujen  $x_i$  summa on  $m$ , joten epäyhtälön oikea puoli on yhtä kuin  $mk$ . Lemman todistaminen ei kuitenkaan ole kovin helppoa: naiivi neliöiminen vain lisäisi termien määrää. Seuraavaksi esitettävä ratkaisu vaatii jonkin verran töitä.

Epäyhtälön voi kirjoittaa muodossa

$$\sum_{i=1}^m \left( \sqrt{k^2 + x_i} - \sqrt{k^2 + A - 1} \right) \geq 0,$$

missä  $A = \frac{1}{m}(x_1 + \dots + x_m)$  on lukujen  $x_i$  keskiarvo.

Epäyhtälön todistamista varten haluamme arvioida erotuksia muotoa

$$\sqrt{b} - \sqrt{a}.$$

Tähän on (ainakin) kaksi tapaa. Ensimmäinen tapa on pieni jippo: pätee

$$\sqrt{b} - \sqrt{a} = \frac{b - a}{\sqrt{b} + \sqrt{a}},$$

joka on vain tuttu kaava  $x^2 - y^2 = (x - y)(x + y)$  kirjoitettuna muuttujille  $x = \sqrt{b}$  ja  $y = \sqrt{a}$ . Toinen tapa on esittää erotus  $\sqrt{b} - \sqrt{a}$  integraalina

$$\int_a^b \frac{1}{2\sqrt{x}} dx,$$

kun  $a < b$ . Tätä integraalia voidaan arvioida yksinkertaisesti toteamalla  $\frac{1}{\sqrt{b}} \leq \frac{1}{\sqrt{x}} \leq \frac{1}{\sqrt{a}}$ , joten

$$\frac{1}{2\sqrt{b}} \cdot (b - a) \leq \int_a^b \frac{1}{2\sqrt{x}} dx \leq \frac{1}{2\sqrt{a}} \cdot (b - a).$$

Tässä tapauksessa yhtälö

$$\sqrt{b} - \sqrt{a} = \frac{b - a}{\sqrt{b} + \sqrt{a}}$$

antaa helpomman tavan käsitellä erotuksia (mutta yleisesti integraalimenetelmä voi auttaa, kun selvää jippoa ei ole). Nyt pätee

$$\sum_{i=1}^m \left( \sqrt{k^2 + x_i} - \sqrt{k^2 + \frac{x_1 + \dots + x_m}{m} - 1} \right) = \sum_{i=1}^m \left( \frac{x_i - A + 1}{\sqrt{k^2 + x_i} + \sqrt{k^2 + A - 1}} \right).$$

Aiomme arvioida positiivisia ja negatiivisia termejä erikseen. Jos  $x_i - A + 1 \leq 0$ , niin suurilla  $k$  pätee  $k^2 + x_i \geq (k - 1)^2$  ja  $k^2 + (A - 1) \geq (k - 1)^2$ , jolloin pätee myös

$$\frac{x_i - A + 1}{\sqrt{k^2 + x_i} + \sqrt{k^2 + A - 1}} \geq \frac{x_i - A + 1}{\sqrt{(k - 1)^2} + \sqrt{(k - 1)^2}} = \frac{x_i - A + 1}{2k - 2}.$$

Jos  $x_i - A + 1 \geq 0$ , niin vastaavalla logiikalla pätee

$$\frac{x_i - A + 1}{\sqrt{k^2 + x_i} + \sqrt{k^2 + A - 1}} \geq \frac{x_i - A + 1}{\sqrt{k^2 + 2k + 1} + \sqrt{k^2 + 2k + 1}} = \frac{x_i - A + 1}{2k + 2},$$

kun  $k$  on riittävän suuri.

Olkoon  $S_-$  summa termeistä muotoa

$$\frac{x_i - A + 1}{\sqrt{k^2 + x_i} + \sqrt{k^2 + A - 1}},$$

missä  $x_i - A + 1$  on negatiivinen. Määritellään  $S_+$  vastaavasti. (Termit, joissa  $x_i - A + 1$  on nolla, ovat nollia, joten niistä ei tarvitse välittää.)

Nyt

$$\begin{aligned} & \sum_{i=1}^m \left( \frac{x_i - A + 1}{\sqrt{k^2 + x_i} + \sqrt{k^2 + A - 1}} \right) = S_+ + S_- \\ & \geq \sum_{x_i - A + 1 > 0} \frac{x_i - A + 1}{2k + 2} + \sum_{x_i - A + 1 < 0} \frac{x_i - A + 1}{2k - 2}. \end{aligned}$$

Jos  $S'_-$  on niiden termien  $x_i - A + 1$  summa, joilla  $x_i - A + 1 < 0$ , ja  $S'_+$  määritellään vastaavasti, niin pätee

$$S_- + S_+ = x_1 + x_2 + \dots + x_m - Am + m = m,$$

eli  $S_- = m - S_+$ . Nyt saadaan

$$\begin{aligned} & \sum_{x_i - A + 1 > 0} \frac{x_i - A + 1}{2k + 2} + \sum_{x_i - A + 1 < 0} \frac{x_i - A + 1}{2k - 2} \\ &= \frac{S_+}{2k + 2} + \frac{S_-}{2k - 2} \\ &= \frac{S_+}{2k + 2} + \frac{m - S_+}{2k - 2} \\ &= \frac{m}{2k - 2} - \left( \frac{S_+}{2k - 2} - \frac{S_+}{2k + 2} \right). \end{aligned}$$

Tämä on positiivinen suurilla  $k$ . Intuitiivisesti tämä johtuu siitä, että termit  $\frac{S_k}{2k-2}$  ja  $\frac{S_+}{2k+2}$  ovat hyvin lähellä toisiaan, joten niiden erotus on hyvin pieni verrattuna termiin  $\frac{m}{2k-2}$ . Tarkemmin väitteen saa todistettua seuraavasti:

$$\begin{aligned} & \frac{m}{2k - 2} - \left( \frac{S_+}{2k - 2} - \frac{S_+}{2k + 2} \right) \\ &= \frac{m}{2k - 2} - \frac{S_+(2k + 2) - S_+(2k - 2)}{(2k - 2)(2k + 2)} \\ &= \frac{m}{2k - 2} - \frac{S_+}{(k - 1)(k + 1)} \\ &= \frac{1}{k - 1} \left( \frac{m}{2} - \frac{S_+}{k + 1} \right). \end{aligned}$$

Tämä puolestaan selvästi on positiivinen suurilla  $k$ . Olemme näin ollen valmiit.

Kommentti: Ratkaisu koostui seuraavista osista:

1. Arvataan (oikein) lukujen  $b$  ja  $c$  arvot.
2. Muutetaan haluttu väite epäyhtälöiksi lattiafunktioyhtälön sijasta.
3. Todistetaan ylärajaa koskeva väite.
4. Todistetaan alarajaa koskeva väite.

Ensimmäinen askel on hyvin luonnollinen, mutta oikean arvauksen tekeminen vaatii varovaisuutta, varsinkin luvun  $c$  kohdalla. Ei ole kovin helppoa huomata, että arvaus  $c = m(a_1 + \dots + a_m)$  ei toimi, vaan että tästä tulee vähentää vielä 1. Esitetyssä ratkaisussa tätä käytiin läpi erikoistapauksen kautta, mutta toinen luonnollinen tapa on vain yrittää todistaa väitettä virheellisellä luvun  $c$  arvolla ja huomata sen toimimattomuus. Ongelma virheellisellä arvolla tulee yritettäessä todistaa alarajaa, joka näyttää tältä:

$$\sum_{i=1}^m \sqrt{k^2 + b_i} \geq m \sqrt{k^2 + \frac{b_1 + \dots + b_m}{m}}.$$

Tämä on Jensen neliöjuurifunktiolle, mutta väärään suuntaan, eli epäyhtälö ei voi päteä (paitsi jos kaikki  $b_i$  ovat yhtä suuria). Tästä myös nähdään, että lukua  $c$  tulee pienentää hieman, joten on luonnollista yrittää valintaa  $c = m(a_1 + \dots + a_m) - 1$ .

Toinen askel on varsin tyypillinen lattiafunktioita sisältävissä ehdoissa: lattiafunktion määritelmähän on  $\lfloor x \rfloor = k$  jos ja vain jos  $k \leq x < k + 1$ . Jossain kohdassa lattiafunktioita koskeva epäyhtälö pitää purkaa auki.

Kolmas askel on suhteellisen helppo, jos tietää etukäteen joitain klassisia epäyhtälöitä. Tässä tapauksessa käytettiin Jensenin epäyhtälöä (joka on yleisesti hyvin käyttökelpoinen epäyhtälö), mutta myös parilla muulla yleisellä epäyhtälöllä saa todistettua väitteen (ks. alla).

Neljäs askel tuotti minulle ratkaisua miettiessäni selvästi eniten vaikeuksia. Todistettava epäyhtälö on hyvin uskottava, mutta toimivan arvion tekeminen ei ole kovin helppoa. Lisätyötä aiheuttaa negatiivisten ja positiivisten lukujen käsittely erikseen. Erilaisten arviointimenetelmien esittelyyn ratkaisu on kuitenkin hyvä.

Summan paloittelu erikseen positiivisiin ja negatiivisiin termeihin on luonnollinen ja yleisestikin usein harkinnanarvoinen idea. Tässä tehtävässä motivaationa toimii seuraava ajatus:<sup>64</sup> Jos  $x_i > A + 1$ , niin  $\sqrt{k^2 + x_i}$  on suurempi kuin  $\sqrt{k^2 + A - 1}$ , ja haluamme tietää, kuinka paljon suurempi se on (tai ainakin saada jokin alaraja), eli haluamme tietää, kuinka paljon hyödynnämme tästä termistä  $x_i$ . Jos taas  $x_i < A + 1$ , niin  $\sqrt{k^2 + x_i}$  on pienempi kuin  $\sqrt{k^2 + A - 1}$ , ja haluamme jonkin alarajan näiden termien erotuksen itseisarvolle, jotta tiedämme tästä termistä  $x_i$  koituvan haitan.

<sup>64</sup>Tämä on mielestäni ratkaisun kriittinen idea. Idean voi varmasti toteuttaa monella tavalla.

### 13.5 Klassiset epäyhtälöt

Usein puhuttaessa epäyhtälöistä kilpailumatematiikan yhteydessä tarkoitetaan ”perinteisiä” epäyhtälöitä: aritmeettis-geometrinen, Cauchy-Schwarz, Hölder, Schur, Jensen, Muirhead, potenssikeskiarvot, Minkowski ja niin edelleen. Puhtaat epäyhtälötehtävät olivat kilpailuissa melko yleisiä vielä vaikkapa pari vuosikymmentä sitten, mutta niiden yleisyys on laskenut vuosien varrella. Yksi selitys tälle on, että epäyhtälöiden ratkaisemiseksi rakennettu kalusto on muuttunut hyvin raskaaksi ja tehokkaaksi, joten on vaikeaa saada hyvää kilpailutehtävää epäyhtälöistä: toisaalta tehtävän ei tulisi vaatia syvällistä epäyhtälöiden osaamista, jotta sen voi ratkaista, toisaalta tehtävän ei tulisi ratketa triviaalisti tunnetuilla (tai hieman vähemmän tunnetuilla) työkaluilla.

Henkilökohtaisesti kilpatehtäviä ratkoessani olen mieltänyt epäyhtälöiden soveltamiseni ennemminkin arvioiden tekemisenä kuin klassisten epäyhtälöiden soveltamisena, mikä heijastuu tämän luvun sisällössä. En väitä, etteikö klassisten epäyhtälöiden osaaminen olisi hyödyksi (päinvastoin, tätä kautta oppii tekemään erilaisia arvioita), mutta minulle on tullut useammin vastaan (esimerkiksi tehtävän osatehtävänä) ongelmia muotoa<sup>65</sup> ”arvio lukujen  $n!$  ja  $P(n)$  suuruuksia, kun  $P$  on polynomi” kuin klassisia epäyhtälöitä muotoa ”Todista, että kaikilla positiivisilla reaaliluvuilla  $a, b$  ja  $c$  pätee  $\frac{a}{\sqrt{a^2+8bc}} + \frac{b}{\sqrt{b^2+8ac}} + \frac{c}{\sqrt{c^2+8ab}} \geq 1$ .”<sup>66</sup>

Tässä on esitetty pari yleisintä ja tärkeimpiin kuuluvaa epäyhtälöä. Nämä kannattaa osata hyvin. Esimerkki- ja harjoitustehtäviä löytyy Lisämateriaaleja-luvussa mainitusta epäyhtälömateriaalista.

#### Lause (Aritmeettis-geometrinen epäyhtälö)

Olkoot  $a_1, a_2, \dots, a_n$  positiivisia reaalilukuja. Pätee

$$\frac{a_1 + a_2 + \dots + a_n}{n} \geq \sqrt[n]{a_1 a_2 \dots a_n}.$$

Yhtälön vasen puoli on lukujen  $a_i$  aritmeettinen keskiarvo ja oikea puoli geometrisen keskiarvo, mikä perustelee epäyhtälön nimen.

Yksi lukuisista tavoista todistaa aritmeettis-geometrinen epäyhtälö on käyttää Jensenin epäyhtälöä. Koska  $a_i$  on positiivinen kaikilla  $i$ , voidaan kirjoittaa  $a_i = e^{b_i}$  jollain sopivalla reaaliluvulla  $b_i$  (joka voi olla negatiivinen). Epäyhtälö voidaan nyt kirjoittaa muodossa

$$\frac{e^{b_1} + e^{b_2} + \dots + e^{b_n}}{n} \geq e^{\frac{b_1 + b_2 + \dots + b_n}{n}},$$

mikä on vain Jensenin epäyhtälö aidosti konveksille funktiolle  $f(x) = e^x$ . Tästä näemme myös, että yhtäsuuruus pätee vain, jos kaikki luvut  $b_i$  ovat yhtä suuria eli

<sup>65</sup>Esimerkkejä tästä löytyy lukuteorian lisätehtävistä (”arvioi summaa  $\sum \frac{1}{p^2}$ , kun  $p$  käy läpi kaikki alkuluvut  $p \equiv 1 \pmod{4}$ ” ja ”analysoi lukujonoa, jossa seuraava termi on enintään edellisten keskiarvo plus jokin vakio”) ja algebran lisätehtävistä (”todista epäyhtälö  $a_i + \lfloor \sqrt{b_i} \rfloor \geq b_i + \lfloor \sqrt{a_i} \rfloor$ , kun  $a_i \geq b_i$  ja  $a_i, b_i \in \mathbb{Z}_+$ ” ja ”arvioi polynomin  $pf + g$  juurien kokoa”).

<sup>66</sup>Tämä tehtävä on vuoden 2001 IMOn tehtävä 2.

jos  $a_1 = \dots = a_n$ .

Tapaus  $n = 2$  antaa  $a + b \geq 2\sqrt{ab}$ . Tämä on varsin helppo epäyhtälö, mutta se antaa kätevän ylärajan kahden luvun tulon koolle (tai vastaavasti alarajan lukujen summalle).

Tutkitaan epäyhtälön tapausta  $n = 3$  eli epäyhtälöä  $\frac{a+b+c}{3} \geq \sqrt[3]{abc}$ . Perustellaan, miksi epäyhtälö pätee. Ideana on, että tulo  $abc$  maksimoituu suhteessa summaan  $a + b + c$  täsmälleen silloin, kun  $a = b = c$ . Todistetaan tämä. Oletetaan, että  $a, b$  ja  $c$  eivät ole kaikki yhtä suuria, eli pätee vaikkapa  $a \neq b$ . Tällöin korvaamalla luvut  $a, b$  ja  $c$  luvuilla  $\frac{a+b}{2}, \frac{a+b}{2}$  ja  $c$  lukujen summa pysyy samana, mutta tulo kasvaa, pätee

$$\frac{a+b}{2} \cdot \frac{a+b}{2} > ab$$

kaikilla  $a \neq b$ . (Tämä on aritmeettis-geometrisen epäyhtälö tapauksessa  $n = 2$ .) Siis jos kaikki luvuista  $a, b$  ja  $c$  eivät ole samoja, voidaan lukujen tuloa kasvattaa samalla pitäen lukujen summan samana. Tämän vuoksi tulo maksimoituu, kun  $a = b = c$ .<sup>67</sup>

Huomaa, että edellinen perustelu epäyhtälön pätevyydelle toimii myös muillekin luvun  $n$  arvoille.

Yleensä aritmeettis-geometrisen epäyhtälö esitetään vielä yhteydessä muihin keskiarvoihin:

#### Lause (QM-AM-GM-HM)

Olkoot  $a_1, a_2, \dots, a_n$  positiivisia reaalilukuja. Pätee

$$\sqrt{\frac{a_1^2 + a_2^2 + \dots + a_n^2}{n}} \geq \frac{a_1 + a_2 + \dots + a_n}{n} \geq \sqrt[n]{a_1 a_2 \dots a_n} \geq \frac{n}{\frac{1}{a_1} + \frac{1}{a_2} + \dots + \frac{1}{a_n}}.$$

Yleisemmin pätee, että summa  $\sqrt[k]{\frac{a_1^k + \dots + a_n^k}{n}}$  kasvaa luvun  $k$  kasvaessa. Tämä tunnetaan potenssikeskiarvojen epäyhtälönä. Edellisessä epäyhtälössä QM eli kvadraattinen keskiarvo (engl. quadratic mean) vastaa arvoa  $k = 2$ , aritmeettinen keskiarvo AM arvoa  $k = 1$  ja harmoninen keskiarvo HM arvoa  $k = -1$ . Geometrisen keskiarvo GM vastaa arvoa  $k = 0$ . Tämä ei ole ilmeistä, mutta voidaan osoittaa, että kun  $k$  lähestyy arvoa 0 (huomaa, että  $k$  voi olla myös epäkokonaisluku), niin eksponentin  $k$  potenssikeskiarvo lähestyy geometrisen keskiarvoa. Potenssikeskiarvojen epäyhtälön voi todistaa Jensenillä vastaavaan tapaan kuin aritmeettis-geometrisen epäyhtälön.

Huomaa, että sijoittamalla  $a_i = \sqrt{b_i}$  saadaan QM-AM-epäyhtälöstä neliöjuurien summalle sama yläraja kuin Jensenillä.

Potenssikeskiarvojen epäyhtälö on esimerkki symmetrisestä polynomiepäyhtälöstä. Toinen voimakas epäyhtälö näihin liittyen on Muirheadin epäyhtälö, joka kertoo

<sup>67</sup>Tämä ei ole aivan formaali todistus epäyhtälölle. Todistuksen idea on siis aina tuoda lukuja  $a, b$  ja  $c$  lähemmäs toisiaan operaatioilla, joissa kaksi lukua korvataan niiden (aritmeettisellä) keskiarvolla. Emme kuitenkaan koskaan pääse aivan tapaukseen  $a = b = c$ , vaan ainoastaan tapaukseen, jossa  $a, b$  ja  $c$  ovat miltei samat. Tämän ongelman voi paikata toteamalla, että lukujen  $a, b$  ja  $c$  summa ja tulo muuttuvat vain hieman, jos lukuja muuttaa pikkuriikkisen (summa ja tulo ovat siis jatkuvia funktioita). Yksityiskohtiin ei syvennytä tässä tämän enempää.



esimerkiksi, että epäyhtälö

$$\sum a^7 b^3 c^2 \geq \sum a^6 b^3 c^3$$

pätee kaikilla positiivisilla  $a, b$  ja  $c$ , missä summat käyvät läpi kaikki  $3! = 6$  permutaatioita muuttujista  $a, b$  ja  $c$ . Täten siis vasen puoli epäyhtälöstä on

$$a^7 b^3 c^2 + a^7 b^2 c^3 + a^3 b^7 c^2 + a^3 b^2 c^7 + a^2 b^7 c^3 + a^2 b^3 c^7.$$

Yleisesti Muirheadin epäyhtälö tiivistää ajatuksen siitä, milloin jotkin symmetriset polynomit ovat suurempia kuin toiset. Tässä eksponentit 7, 3 ja 2 antavat suuremman lausekkeen kuin eksponentit 6, 3 ja 3. Epäyhtälön tarkkaa muotoilua varten viitataan jälleen Lisämateriaaleja-luvussa mainittuun epäyhtälömateriaaliin.

Viimeisenä mainitaan vielä yksi hyvin tärkeä epäyhtälö.

#### Lause (Cauchy-Schwarzin epäyhtälö)

Olkoot  $a_1, a_2, \dots, a_n$  ja  $b_1, b_2, \dots, b_n$  reaalityyppiset luvut. Pätee

$$\left( \sum_{i=1}^n a_i^2 \right) \left( \sum_{i=1}^n b_i^2 \right) \geq \left( \sum_{i=1}^n a_i b_i \right)^2.$$

Huomaa, että luvut  $a_i$  ja  $b_i$  voivat olla negatiivisia, koska vasemman puolen arvo ei riipu lukujen merkeistä ja oikea puoli voi vain pienentyä, jos jonkin luvun muuttaa positiivisesta negatiiviseksi.

Tässä on lyhyesti esitetty yksi tapa todistaa epäyhtälö: Kerrotaan kaikki auki. Epäyhtälön vasemmalle puolelle syntyy summa termeistä  $a_i^2 b_j^2$  kaikkien  $1 \leq i, j \leq n$  yli ja oikealle puolelle summa termeistä  $a_i b_i a_j b_j$  (missä termi esiintyy kertoimella 2 jos  $i \neq j$  ja muuten kertoimella 1). Siis molemmille puolille syntyy ainakin termit  $a_i^2 b_i^2$ , kummallekin puolelle kertoimella 1. Supistetaan nämä pois. Huomataan, että vasemman puolen termien  $a_i^2 b_j^2$  ja  $a_j^2 b_i^2$  (missä  $i \neq j$ ) summa on vähintään oikean puolen termi  $2a_i b_i \cdot a_j b_j$  (aritmeettis-geometrisen epäyhtälön tapauksen  $n = 2$  nojalla). Siis ryhmittelemällä termit sopivasti saadaan aina pareja, joissa vasemman puolen termit ”voittavat” oikean puolen termit.

Myös Cauchy-Schwarzin epäyhtälön avulla saa arvion neliöjuurien summalle asettamalla  $b_i = 1$  ja  $a_i = \sqrt{x_i}$  kaikilla  $i$ .

## 14 Summia (Algebra)

Tässä luvussa käydään lyhyesti läpi, miten erilaisia summia voidaan laskea.

### 14.1 Teleskooppisumma

Ensimmäinen tehtävä on tunnettu klassikko, joka demonstroi yleistä menetelmää summien laskemiseksi.

#### Tehtävä

Laske

$$\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \frac{1}{3 \cdot 4} + \dots + \frac{1}{99 \cdot 100}.$$

Yksi tapa ratkaista tehtäviä on löytämällä säännönmukaisuus pieniä tapauksia tutkimalla:

$$\begin{aligned} \frac{1}{1 \cdot 2} &= \frac{1}{2}, \\ \frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} &= \frac{2}{3}, \\ \frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \frac{1}{3 \cdot 4} &= \frac{2}{3} + \frac{1}{12} = \frac{3}{4}, \\ \frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \frac{1}{3 \cdot 4} + \frac{1}{4 \cdot 5} &= \frac{3}{4} + \frac{1}{20} = \frac{4}{5}. \end{aligned}$$

Tämän perusteella ei ole vaikea veikata, että vastaus on  $\frac{99}{100}$ . Todistamisen voi hoitaa esimerkiksi induktiolla.

Tehtävään on kuitenkin toinen ratkaisu, joka on hieman vaikeampi keksiä, mutta joka on varsin elegantti. Ideana on kirjoittaa

$$\frac{1}{n(n-1)} = \frac{1}{n-1} - \frac{1}{n},$$

jolloin annettu summa muuttuu muotoon

$$\left(\frac{1}{1} - \frac{1}{2}\right) + \left(\frac{1}{2} - \frac{1}{3}\right) + \left(\frac{1}{3} - \frac{1}{4}\right) \dots + \left(\frac{1}{99} - \frac{1}{100}\right).$$

Miltei kaikki supistuu pois, ja jäljelle jää  $\frac{1}{1} - \frac{1}{100} = \frac{99}{100}$ .

Jälkimmäisen ratkaisun ideaa kutsutaan teleskooppisummaksi, koska summa kuituu kasaan kuten teleskooppi.

### 14.2 Polynomisummia

Tutkitaan sitten seuraavaa esimerkkiä.

**Tehtävä**

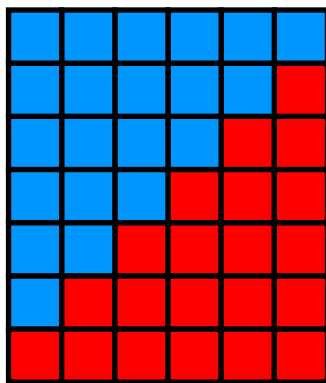
Laske

$$1 + 2 + 3 + \dots + 100.$$

Tässä voisi tutkia pieniä tapauksia, ja saada lukujonon  $1, 3, 6, 10, 15, 21, \dots$ , mutta tästä on vaikea arvata sadatta termiä.

Yksi ratkaisuun johtava idea on ajatella, että luvut ovat keskimäärin noin 50, ja niitä on sata kappaletta, joten summa on noin 5000. Tarkemmin sanoen lukujen keskiarvo on 50.5 – luvuthan voi jakaa pareihin  $(1, 100), (2, 99), (3, 98), \dots, (50, 51)$ , joista kunkin keskiarvo on 50.5. Siis summa on 5050.

Toinen ratkaisu on geometrinen: Ajatellaan ruuduista koostuvaa portaikkoa, jonka ruutujen määrä on tehtävän vastaus. Tehdään ruudukosta kopio, ja asetetaan portaikot niin, että ne muodostavat suorakulmion. Suorakulmion pinta-ala on helppo laskea.



Summa  $1 + 2 + \dots + 6$  on puolet  $6 \times 7$ -suorakulmion pinta-alasta.

Tällä menetelmällä päädytään vastaukseen  $\frac{100 \cdot 101}{2} = 5050$ . Yleisesti summa  $1 + 2 + \dots + n$  on samalla logiikalla  $n(n+1)/2$ .

Tutkitaan sitten vaikeampaa esimerkkiä.

**Tehtävä**

Laske

$$1^2 + 2^2 + 3^2 + \dots + 100^2.$$

Tähän on vaikea keksiä edes suuruusluokalta oikeaa arviota tai geometrsta tulkin-taa. Tehtävä onkin hyvin vaikea, ellei ole aiemmin nähnyt vastaavaa esimerkkiä.

Ideana on käyttää aiemmin esitettyä teleskooppisummaa. Ideana on siis yrittää kirjoittaa summan termit erotuksina, jotka sitten kumoavat toisiaan. Tarkemmin etsitään lauseketta  $f(n)$ , jolla pätee

$$n^2 = f(n) - f(n-1).$$

Jos nimittäin keksimme tällaisen lausekkeen, niin sitten summa saadaan laskettua:

$$\begin{aligned} 1^2 + 2^2 + 3^2 + \dots + 100^2 = \\ (f(1) - f(0)) + (f(2) - f(1)) + (f(3) - f(2)) + \dots + (f(100) - f(99)) = \\ f(100) - f(0). \end{aligned}$$

Mutta miten keksimme tällaisen lausekkeen?

On pari asiaa, jotka auttavat tällaisen lausekkeen etsintää. Ensinnäkin aiemmassa esimerkissä laskimme summaa murtolausekkeista  $\frac{1}{n(n-1)}$ , ja tällöin vastaava lauseke oli myös murtolauseke  $\frac{1}{n}$ . Tämä vihjaa siihen, että  $f$  kannattaa valita "samantyylliseksi" lausekkeeksi kuin  $n^2$ , esimerkiksi polynomiksi.

Toisekseen voidaan tutkia hieman yksinkertaisempaa esimerkkiä. Entä jos etsisimme lauseketta  $g$ , jolla pätee

$$n = g(n) - g(n-1)?$$

Huomataan, että tähän kelpaa aiemman tehtävän vastauksen lauseke  $g(n) = n(n+1)/2$ . Tämä ei yllätä, koska teleskooppisummaidealla saadaan, että

$$1 + 2 + \dots + n = g(n) - g(0),$$

ja aiemmin laskimme vasemman puolen olevan  $n(n+1)/2$ . Haluttu lauseke  $g$  on siis polynomi, mikä vihjaa siihen, että myös vaikeammassa tapauksessa  $n^2 = f(n) - f(n-1)$  etsitty lauseke on polynomi.

Etsintää voi vielä rajata hieman ottamalla huomioon, että jos  $f$  on polynomi, niin sen tulee olla enintään kolmannen asteen polynomi. Nimittäin summa  $1^2 + 2^2 + \dots + n^2$  on varmasti enintään  $n^3$ , koska jokainen termi on enintään  $n^2$  ja termejä on  $n$  kappaletta.

Kirjoitetaan siis  $f(n) = an^3 + bn^2 + cn + d$  ja ratkaistaan saatavat kertoimet. Tämä vaatii hieman laskemista:

$$\begin{aligned} f(n) - f(n-1) = \\ an^3 + bn^2 + cn + d - (a(n-1)^3 + b(n-1)^2 + c(n-1) + d) = \\ an^3 + bn^2 + cn + d - (an^3 - 3an^2 + 3an - a + bn^2 - 2bn + b + cn - c + d) = \\ 3an^2 - (3a - 2b)n - (-a + b - c). \end{aligned}$$

Tämän tulee olla  $n^2$ , joten  $a = 1/3$ ,  $b = 1/2$  ja  $c = 1/6$ . Vakiotermi  $d$  voidaan valita olemaan vaikkapa 0. Täten

$$f(n) = \frac{n^3}{3} + \frac{n^2}{2} + \frac{n}{6},$$

ja haluttu summa on  $f(100) - f(0) = f(100)$ . Lausekkeen voi kirjoittaa hieman siistimmin muotoon

$$f(n) = \frac{n(n+1)(2n+1)}{6}.$$

### 14.3 Binomikerroinpolynomit

Luonteva yleistys on tutkia kuutioiden summaa.

#### Tehtävä

Laske

$$1^3 + 2^3 + 3^3 + \dots + 100^3.$$

Yllä esitetty menetelmä toimii edelleen, mutta oikean lausekkeen  $f$  kertoimien laskeminen muuttuu työlääksi, varsinkin jos kuutioiden summan sijasta tutkii vielä korkeampia potensseja.

Tämän vuoksi tässä esitetään hieman toisenlainen tapa katsoa asiaa. Tälläkin tavalla laskemista tulee jonkin verran, mutta idea on hyvin käyttökelpoinen.

Tapa perustuu binomikerrointen ominaisuuksiin. Niin sanottu Pascalin identiteetti sanoo, että binomikertoimilla pätee

$$\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}.$$

(Katso Yläkoulu- ja lukiotietoja.) Täten

$$\binom{n}{k} = \binom{n+1}{k+1} - \binom{n}{k+1}.$$

Jos esimerkiksi  $k = 2$ , niin vasemman puolen binomikerroin on toisen asteen polynomi  $n(n-1)/2$ . Oikea puoli puolestaan on sellainen lauseke, johon teleskooppisumma toimii. Täten saadaan esimerkiksi

$$\sum_{n=1}^{100} \frac{n(n-1)}{2} = \binom{101}{3}.$$

Tämä ei ole kovin kaukana summan

$$\sum_{n=1}^{100} n^2$$

laskemisesta – molemmissa nimittäin summataan jotakin toisen asteen polynomia.<sup>68</sup>

Tässä on yksityiskohtaisempi tarkastelu. Lasketaan siis summa  $1^3 + 2^3 + \dots + 100^3$ . Ideana on esittää ensiksi lauseke  $n^3$  binomikertoimien avulla. Ensimmäinen arvaus on käyttää binomikerrointa

$$\binom{n}{3} = \frac{n(n-1)(n-2)}{6}.$$

<sup>68</sup>Yleensä puhuttaessa binomikertoimista  $\binom{a}{b}$  oletetaan, että  $a \geq b$ , koska  $a$  alkioista ei voi valita  $b$  alkioita, jos  $a < b$ . Tässä luvussa kuitenkin tutkimme binomikertoimia polynomeina. Esimerkiksi polynomi  $n(n-1)/2$  (joka vastaa binomikerrointa  $\binom{n}{2}$ ) on hyvin määriteltä, vaikka  $n$  olisi pienempää kuin 2 (tai vaikkei  $n$  edes olisi kokonaisluku).

Kertomalla kuudella saadaan korkeimman asteen termin  $n^3$  kerroin oikein. Siis

$$6\binom{n}{3} = n(n-1)(n-2) = n^3 - 3n^2 + 2n.$$

Toisen asteen termin kerroin menee väärin: sen tulisi olla nolla. Korjataan tilanne lisäämällä sopiva määrä binomikerrointa  $\binom{n}{2} = n(n-1)/2$ . Tähänkin sopiva kerroin on 6:

$$6\binom{n}{3} + 6\binom{n}{2} = n^3 - 3n^2 + 2n + (3n^2 - 3n) = n^3 - n.$$

Ensimmäisen asteen termi saadaan korjattua lisäämällä yksi kappale binomikerrointa  $\binom{n}{1}$ . Ensimmäinen vaihe on valmis: olemme saaneet esitettyä polynomin  $n^3$  binomikerroinpolynomien avulla:

$$n^3 = 6\binom{n}{3} + 6\binom{n}{2} + \binom{n}{1}.$$

Toinen vaihe on käyttää Pascalin identiteettiä ja teleskooppisummaa:

$$\begin{aligned} \sum_{n=1}^{100} n^3 &= \\ \sum_{n=1}^{100} 6\binom{n}{3} + 6\binom{n}{2} + \binom{n}{1} &= \\ 6\sum_{n=1}^{100} \binom{n}{3} + 6\sum_{n=1}^{100} \binom{n}{2} + \sum_{n=1}^{100} \binom{n}{1} &= \\ 6\binom{101}{4} + 6\binom{101}{3} + \binom{101}{2}. \end{aligned}$$

Yleisesti siis summa  $1^3 + 2^3 + \dots + n^3$  on  $6\binom{n+1}{4} + 6\binom{n+1}{3} + \binom{n+1}{2}$ . Nämä binomikerroinpolynomit voi vielä halutessaan esittää ”tavallisessa” muodossa. Laskemalla hieman vastaus voidaan esimerkiksi esittää muodossa

$$6\binom{n+1}{4} + 6\binom{n+1}{3} + \binom{n+1}{2} = \left(\frac{n(n+1)}{2}\right)^2.$$

(Tästä näkee esimerkiksi, että  $1^3 + 2^3 + \dots + n^3$  on aina neliöluku:  $1^3 = 1$ ,  $1^3 + 2^3 = 9$ ,  $1^3 + 2^3 + 3^3 = 36$ ,  $1^3 + 2^3 + 3^3 + 4^3 = 100$  ja niin edelleen.)

Idea tietysti yleistyy. Vastaavaan tapaan voidaan laskea vaikkapa kymmenensien potenssien summa  $1^{10} + 2^{10} + \dots + n^{10}$  esittämällä  $n^{10}$  binomikerroinpolynomien  $\binom{n}{1}, \binom{n}{2}, \dots, \binom{n}{10}$  avulla, vaikkakin tämä vaatii enemmän laskemista.

## 14.4 PolynomiekspONENTTISUMMIA

Olemme tähän mennessä tutkineet polynomisummaa. Lisäksi lukiosta on tuttu geometrisen lukujonon summakaava

$$1 + x + \dots + x^n = \frac{x^{n+1} - 1}{x - 1}$$

(kun  $x \neq 1$ ). Luonteva jatkokysymys on tutkia summaa, jossa on sekä polynomi- että eksponenttifunktioita, kuten esimerkiksi summia muotoa

$$\sum_n nx^n$$

tai

$$\sum_n n^2 x^n.$$

Näiden summien lähestymiseksi palautetaan mieleen geometrisen jonon summakaavan johtaminen. Merkitään  $S = 1 + x + \dots + x^n$ . Nyt  $xS$  voidaan kirjoittaa summana, jossa on miltei samat termit kuin summassa  $S$ :

$$xS = x + x^2 + \dots + x^{n+1} = (1 + x + \dots + x^n) + x^{n+1} - 1 = S + x^{n+1} - 1.$$

Vähentämällä puolittain  $S$  ja jakamalla termillä  $x - 1$  saadaan  $S = (x^{n+1} - 1)/(x - 1)$ .

Samalla idealla saa laskettua summan  $S = x + 2x^2 + 3x^3 + 4x^4 + \dots + nx^n$ : jälleen  $xS$  saadaan esitettyä summan  $S$  ja muutaman muun termin avulla:

$$\begin{aligned} xS &= x^2 + 2x^3 + 3x^4 + 4x^5 + \dots + nx^{n+1} = \\ &= (2x^2 + 3x^3 + \dots + nx^n + (n+1)x^{n+1}) - (x^2 + x^3 + x^4 + \dots + x^{n+1}) = \\ &= (S + (n+1)x^{n+1} - x) - x^2(1 + x + \dots + x^{n-1}). \end{aligned}$$

Sievennetään vielä käyttämällä geometrista summakaavaa, vähennetään puolittain  $S$  ja jaetaan luvulla  $x - 1$ . Saadaan

$$S = \frac{(n+1)x^{n+1} - x}{x - 1} - x^2 \frac{x^n - 1}{(x - 1)^2}.$$

Vastaavalla menetelmällä saadaan laskettua summa muotoa  $S = \sum_n n^2 x^n$  tutkimalla summa  $xS$ . Ylimääräisiksi termeiksi tulee geometrinen summa (joka osataan laskea) ja summa muotoa  $\sum_n nx^n$  (joka laskettiin yllä). Menetelmä yleistyy vielä pidemmälle summille muotoa  $\sum_n n^k x^n$ , missä  $k$  on positiivinen kokonaisluku.

Tässä on toinen, hieman visuaalisempi tapa hahmottaa esimerkiksi summaa  $\sum_{i=1}^n i2^i$ : Summan voi kirjoittaa kolmioksi

$$\begin{array}{r} 2^1 + 2^2 + 2^3 + 2^4 + \dots + 2^{n-1} + 2^n \\ + 2^2 + 2^3 + 2^4 + \dots + 2^{n-1} + 2^n \\ + 2^3 + 2^4 + \dots + 2^{n-1} + 2^n \\ \vdots \\ + 2^{n-1} + 2^n \\ + 2^n. \end{array}$$

Huomaa siis, että termi  $2^i$  esiintyy kolmiossa  $i$  kertaa. Ideana on, että jokainen rivi on geometrinen summa, joka osataan laskea. Myös geometrysten summien summa osataan laskea.

Yksityiskohdat: Rivillä  $k$  on summa  $2^{k+1} + 2^{k+1} + \dots + 2^n$ , joka on geometriseen summakaavaan nojautuen  $2^{n+1} - 2^k$ . Täten vastaus on

$$\sum_{k=1}^n 2^{n+1} - 2^n = n2^{n+1} - (2^{n+1} - 2) = (n-1)2^{n+1} - 2,$$

missä käytettiin vielä kerran geometrisen jonon summaa.

Vastaavasti visuaalisella tavalla voidaan laskea summa termeistä muotoa  $i^2 2^i$ , tosin samantyyllisesti kuin polynomisummien tapauksessa, on helpompaa laskea summa  $\binom{i}{2} 2^i$ . Ideana on jälleen kirjoittaa summa kolmioksi, mutta tällä kertaa antaa painottaa kutakin kertoimilla  $1, 2, 3, \dots, n$ .

$$\begin{aligned} &2^1 + 2^2 + 2^3 + 2^4 + \dots + 2^{n-1} + 2^n \\ &+ 2(2^2 + 2^3 + 2^4 + \dots + 2^{n-1} + 2^n) \\ &+ 3(2^3 + 2^4 + \dots + 2^{n-1} + 2^n) \\ &\quad \vdots \\ &+ (n-1)(2^{n-1} + 2^n) \\ &+ n2^n. \end{aligned}$$

Huomataan siis, että termin  $2^i$  kerroin on  $\binom{i}{2}$ , mistä saadaan laskettua summa termeistä muotoa  $\binom{i}{2} 2^i$ . Tästä ei enää ole vaikeaa saada laskettua summaa termeistä  $i^2 2^i$ . Vastaava idea yleistyy: jos halutaan laskea  $\sum \binom{i}{k} 2^i$ , annetaan riveille kertoimia  $\binom{1}{k-1}, \binom{2}{k-1}, \dots, \binom{n}{k-1}$ .

## 14.5 Diskreetti derivaatta ja integraali

Yllä on esitetty verrattain suoraviivaisia tapoja laskea polynomi- ja polynomieksponenttisummia. Tavat voivat kuitenkin vaikuttaa kasalta erilaisia temppuja eikä yleiseltä metodilta, joka soveltuisi myös muiden summien laskemiseen. Siksi tässä esitetään toinen tapa ajatella asiaa, joka yhdistää eri osat yhdeksi kokonaisuudeksi. Pienenä haittapuolena on se, että kokonaisuuden selittämistä varten on luontevaa verrata tilannetta lukion differentiaali- ja integraalilaskentaan, joten lukijalta vaaditaan esitietoja näihin liittyen.

Lyhyesti tiivistettynä funktion derivaatta kertoo funktion muutoksesta ja integraalifunktio on funktio, jonka derivaatta on annettu funktio.

Tarkalleen funktion  $f(x)$  derivaatta  $f'(x)$  määritellään raja-arvona

$$f'(x) = \lim_{h \rightarrow 0} \frac{f(x+h) - f(x)}{h}.$$

Tämän osion avainidea on seuraava: Entä jos emme annakaan  $h$ :n lähestyä nollaa, vaan valitsemme yksinkertaisesti  $h = 1$ ? Eli entä jos määrittelemme funktiolle  $f$  derivaatan variantin  $f^*(x)$  kaavalla

$$f^*(x) = \frac{f(x+1) - f(x)}{1} = f(x+1) - f(x)?$$



Kutsutaan tätä versiota derivaatasta diskreetiksi<sup>69</sup> derivaataksi ja tavallista versiota jatkuvaksi derivaataksi.

Tarvitsemme vielä integraalille diskreetin version. Funktion  $f$  diskreetti integraali  $F$  on sellainen funktio, jolla

$$F^*(x) = f(x),$$

eli  $F(x+1) - F(x) = f(x)$ . (Huomaa, että kuten tavallisen integraalin tapauksessa, integraalifunktioon voi lisätä jonkin vakion, ja se on edelleen integraalifunktio.)

Mitä hyödyimme näistä määritelmistä? Olkoon  $f(x)$  jokin funktio, vaikkapa  $f(x) = x^2$ . Lukiossa ollaan totuttu laskemaan funktion  $f$  alle jäävä pinta-ala määrättynä integraalina

$$\int_a^b f(x)dx = F(b) - F(a),$$

missä  $F$  on  $f$ :n integraalifunktio. Pinta-alan laskeminen vastaa siis integraalifunktion keksimistä. Tässä tapauksessa integraalifunktio on  $x^3/3$  (plus vakio), joten pinta-ala on  $\frac{1}{3}(b^3 - a^3)$ .

Diskreetissä tapauksessa pinta-ala vastaa summaa. Siis jos  $F$  on sellainen funktio, jolla  $F^*(x) = f(x)$ , niin

$$\sum_{n=a}^b f(n) = F(b+1) - F(a),$$

koska kyseessä on teleskooppisumma. (On myös hyvä pitää mielessä, että integraali eli käyrän alle jäävä pinta-ala voidaan ajatella eräiden pylväiden pinta-alojen summana, eli integraali on itsessään eräänlainen jatkuva summa.)

Idea on siis, että summien laskeminen vastaa integroimista. Integrointiin käytettävät menetelmät soveltuvat summien laskemiseen.

Todetaan ensiksi, että jatkuvassa tapauksessa funktioiden  $f(x) = x^n$  derivointi on helppoa: jatkuva derivaatta on  $f'(x) = nx^{n-1}$ . Diskreetissä tapauksessa funktion  $f(x) = x^n$  diskreetti derivaatta ei ole kovin yksinkertaisen näköinen. Sen sijaan binomikerroinpolynomien diskreetit derivaatat toimivat kivasti: jos  $f$  on  $k$ :s binomikerroinpolynomi

$$f(x) = \binom{x}{k} = \frac{x(x-1)(x-2)\cdots(x-(k-1))}{k!},$$

---

<sup>69</sup>Diskreetin voi matematiikassa ajatella olevan jatkuvan vastakohta. Voi esimerkiksi ajatella, että reaali lukujen joukko on jatkuva, kun taas kokonaislukujen joukko on diskreetti.

niin laskemalla saadaan

$$\begin{aligned} f^*(x) &= \binom{x+1}{k} - \binom{x}{k} = \\ &= \frac{(x+1)x(x-1)\cdots(x-(k-2))}{k!} - \frac{x(x-1)(x-2)\cdots(x-(k-1))}{k!} = \\ &= \frac{x(x-1)(x-2)\cdots(x-(k-2))}{k!} \left( (x+1) - (x-(k-1)) \right) = \\ &= \frac{x(x-1)(x-2)\cdots(x-(k-2))}{k!} \cdot k = \\ &= \binom{x}{k-1}. \end{aligned}$$

(Tämä on Pascalin identiteetti.) Eli jatkuvassa tapauksessa funktioiden

$$1, x, x^2, x^3, \dots$$

jatkuvat derivaatat toimivat yksinkertaisesti, kun taas diskreetissä tapauksessa funktioiden

$$1, x, \frac{x(x-1)}{2}, \frac{x(x-1)(x-2)}{6}, \dots$$

diskreetit derivaatat toimivat mukavasti.

Tästä syystä esimerkiksi aiemmin laskettaessa summaa  $\sum_{n=1}^{100} n^3$  oli hyvä idea kirjoittaa funktio  $n^3$  binomikerroinpolynomien avulla. Yleisemminkin binomikerroinpolynomit ovat käteviä summia laskettaessa. Voi oikeastaan ajatella, että summan  $\sum_{n=1}^{100} n^3$  laskeminen on samankaltainen tehtävä kuin integraalin  $\int_1^{100} \frac{x(x-1)(x-2)}{6} dx$  laskeminen: Integraalin tapauksessa on järkevää kertoa polynomi auki ja täten kirjoittaa se termien  $1, x, x^2, x^3, \dots$  avulla, koska näitä termejä on helppo integroida. Vastaavasti summan tapauksessa on järkevää kirjoittaa  $n^3$  binomikerroinpolynomien  $1, n, \binom{n}{2}, \binom{n}{3}, \dots$  avulla, koska näitä termejä on helppo summata.

Tutkitaan sitten eksponenttifunktioita. Jatkuvassa tapauksessa tiedämme, että funktion  $f(x) = e^x$  derivaatta on funktio itse, missä  $e = \lim_{n \rightarrow \infty} \left(1 + \frac{1}{n}\right)^n \approx 2.718$ . Entä mikä on funktio, jonka diskreetti derivaatta on funktio itse? Jos  $f$  on tällainen funktio, niin  $f(x) = f^*(x) = f(x+1) - f(x)$ , eli  $f(x+1) = 2f(x)$ . Huomataan siis, että funktion  $f(x) = 2^x$  diskreetti derivaatta on funktio itse, eli jatkuvan derivaatan  $e^x$  vastaa diskreetin derivaatan funktiota  $2^x$ .

Pohditaan sitten summan  $\sum_{n=1}^{100} n2^n$  laskemista. Koska  $2^n$  on diskreetti vastine funktiolle  $e^x$ , on tämä summa diskreetti versio integraalista

$$\int_1^{100} xe^x dx.$$

Summan laskemista varten on siis hyödyllistä miettiä, miten laskisi tämän integraalin. Lukiosta tuttu menetelmä on osittaisintegrointi, joka perustuu derivaatan ominaisuuteen  $(fg)' = f'g + fg'$ , mistä seuraa

$$\int_1^{100} f'(x)g(x)dx = f(100)g(100) - f(1)g(1) - \int_1^{100} f(x)g'(x)dx,$$

eli funktion  $f'g$  integrointi palautuu funktion  $fg'$  integrointiin. Voisi toivoa, että osittaisintegroinnille on diskreetti analogia. Analogia todella löytyy. Ideana on tutkia summaa

$$\sum_{n=1}^{100} f^*(n)g(n),$$

ja yrittää kirjoittaa se summana funktiosta  $f(n)g^*(n)$ . Tämä vaatii hieman laskemista ja varovaisuutta:

$$\begin{aligned} \sum_{n=1}^{100} f^*(n)g(n) &= \\ (f(2) - f(1))g(1) + (f(3) - f(2))g(2) + \dots + (f(101) - f(100))g(100) &= \\ -f(1)g(1) - f(2)(g(2) - g(1)) - f(3)(g(3) - g(2)) - \dots &= \\ -f(100)(g(100) - g(99)) + f(101)g(100) &= \\ f(101)g(100) - f(1)g(1) + \sum_{n=2}^{100} f(n)g^*(n-1). \end{aligned}$$

Nyt siis esimerkiksi summan  $\sum_{n=1}^{100} n2^n$  laskeminen sujuu kirjoittamalla  $f^*(n) = 2^n$ ,  $g(n) = n$ , jolloin  $f(n) = 2^n$  ja  $g(n) = 1$ . “Osittaissummaamalla” summan laskeminen palautuu summan  $\sum_{n=2}^{100} 2^n$  laskemiseen.

Menetelmä tietysti yleistyy polynomieksponenttisummille yleisemmin käyttämällä useamman kerran osittaissummaamista, aivan kuten soveltamalla osittaisintegrointia useamman kerran saa laskettua integraaleja muotoa  $\int x^k e^x dx$ .

Tässä on vielä pari kommenttia koskien aihetta. Ensinnäkään diskreetti derivaatta ja integraali eivät toki sovellu kaikkien summien laskemiseen. Esimerkiksi summalle

$$\sum_{n=1}^k \sqrt{n}$$

ei ole mitään kovin yksinkertaista kaavaa. Aivan kuten kaikille funktioille ei ole yksinkertaista jatkuvaa integraalifunktioita (klassinen esimerkki  $f(x) = e^{x^2}$ ), ei neliöjuurifunktiolle ole yksinkertaista diskreettiä integraalifunktiota. (Sen sijaan summaa voi approksimoida integraalina  $\int_1^k \sqrt{x} dx$ , joka osataan integroida.)

Toisekseen voisi yleisemmin tutkia diskreettejä derivaattoja, joissa luvun  $h$ :n arvoksi valitaan jotakin muuta kuin 1. Voitaisiin esimerkiksi tutkia arvoa  $h = 1/100$ , jolloin

$$f^*(x) = \frac{f(x+h) - f(x)}{h} = 100(f(x+1/100) - f(x)).$$

Ei ole kovin vaikea nähdä, että tällöin polynomien

$$1, x, \frac{x(x-h)}{2}, \frac{x(x-h)(x-2h)}{3!}, \frac{x(x-h)(x-2h)(x-3h)}{4!}, \dots$$

diskreetit derivaatat ovat aina jonon edellinen polynomi. Arvolla  $h = 1$  nämä ovat binomikerroinpolynomit, ja kun  $h$  on hyvin pieni, ovat nämä polynomit suunnilleen

polynomit  $x^n/n!$ . Huomataankin, että jonon

$$1, x, \frac{x^2}{2!}, \frac{x^3}{3!}, \frac{x^4}{4!}, \dots$$

polynomien jatkuvat derivaatat ovat aina jonon edellinen polynomi.

Eksponenttifunktion  $e^x$  diskreetti analogia on taas muotoa  $f(x) = a^x$  jollain vakiolla  $a$ . Ehdosta  $f^*(x) = f(x)$  saadaan yhtälö  $a$ :lle, mistä ratkaisemalla saadaan

$$a = (1 + h)^{1/h}.$$

Esimerkiksi jos  $h = 1$ , antaa tämä  $a = 2$ , ja jos  $h = 1/2$ , antaa tämä  $a = 2.25$ . Kun  $h$  on hyvin pieni, on  $a$  suunnilleen  $e$  (luvun  $e$  määritelmän nojalla). Tämä antaa hieman ymmärrystä siihen, miksi juuri  $e$  on se luku, jolla funktion  $e^x$  jatkuva derivaatta on funktio itse.

## 15 Lineaariset rekursiot (Algebra)

Tässä luvussa esitetään menetelmä lineaarisen rekursioyhtälön ratkaisemiseksi. Esi-  
merkki lineaarisesta rekursiosta on Fibonaccin lukujono  $0, 1, 1, 2, 3, 5, 8, \dots$

### 15.1 Fibonaccin luvut

Fibonaccin luvut määritellään yhtälöillä  $F_0 = 0$ ,  $F_1 = 1$  ja  $F_{n+2} = F_{n+1} + F_n$  kaikilla  $n \geq 0$ .

Yritetään etsiä yleinen kaava Fibonaccin luvuille. Fibonaccin luvut kasvavat suunnilleen eksponentiaalisesti, joten veikkataan  $F_n = r^n$  kaikilla  $n$ , missä  $r$  on sopiva vakio. Veikkaus ei tietenkään ole täysin oikea, mutta katsotaan, mihin se johtaa.

Jotta  $F_n = r^n$  toimisi, tulee olla  $F_{n+2} = F_{n+1} + F_n$ , eli  $r^{n+2} = r^{n+1} + r^n$ . Tietysti  $r = 0$  toteuttaa yhtälön, mutta tämä ei ole kovin kiinnostavaa. Oletetaan, että  $r \neq 0$ , jolloin jakamalla puolittain pois  $r^n$  saadaan

$$r^2 = r + 1.$$

Tällä yhtälöllä on ratkaisut  $r = \frac{1 \pm \sqrt{5}}{2}$ . Nämä toimivat rekursioyhtälön puolesta, mutta alkuarvot  $F_0 = 0$  ja  $F_1 = 1$  menevät pieleen.

Kriittiset huomiot ovat seuraavat:

- Jos  $F_n = f(n)$  toimii rekursioyhtälön puolesta, niin myös  $F_n = c \cdot f(n)$  toimii rekursioyhtälön puolesta kaikilla vakiolla  $c$ .
- Jos  $F_n = f(n)$  ja  $F_n = g(n)$  toimivat rekursioyhtälön puolesta, niin myös  $F_n = f(n) + g(n)$  toimii rekursioyhtälön puolesta.

Jälkimmäisellä pointilla tarkoitetaan sitä, että mikäli  $f(n+2) = f(n+1) + f(n)$  ja  $g(n+2) = g(n+1) + g(n)$  pätevät kaikilla  $n$ , niin silloin tietysti  $f(n+2) + g(n+2) = (f(n+1) + g(n+1)) + (f(n) + g(n))$  kaikilla  $n$ .

Huomioiden seurauksena saadaan seuraava väite:

Olko  $r_1$  ja  $r_2$  yhtälön  $r^2 = r + 1$  kaksi ratkaisua, ja olko  $c_1$  ja  $c_2$  mielivaltaisia vakioita. Tällöin  $F_n = c_1 r_1^n + c_2 r_2^n$  toteuttaa rekursioyhtälön  $F_{n+2} = F_{n+1} + F_n$ .

Enää tulee valita vakiot  $c_1$  ja  $c_2$  niin, että alkuarvot osuvat kohdilleen. Tällöin sekä alkuarvot että rekursioyhtälöt menevät oikein ja olemme valmiit.

Haluamme siis, että  $F_0 = 0 = c_1 a_1^0 + c_2 a_2^0 = c_1 + c_2$  ja että  $F_1 = 1 = c_1 r_1 + c_2 r_2$ . Tästä saadaan yhtälöpari

$$\begin{cases} c_1 + c_2 = 0 \\ c_1 r_1 + c_2 r_2 = 1. \end{cases}$$

Luvut  $r_1$  ja  $r_2$  ovat  $\frac{1+\sqrt{5}}{2}$  ja  $\frac{1-\sqrt{5}}{2}$ . Sijoitetaan ne paikoilleen, ja ratkotaan yhtälöpari. Saadaan ratkaisu

$$c_1 = \frac{1}{\sqrt{5}}, c_2 = -\frac{1}{\sqrt{5}},$$

eli

$$F_n = \frac{1}{\sqrt{5}} \left( \frac{1+\sqrt{5}}{2} \right)^n - \frac{1}{\sqrt{5}} \left( \frac{1-\sqrt{5}}{2} \right)^n.$$

Kuten aiemmin todettiin, tämä toteuttaa sekä alkuarvoehdot että rekursioyhtälön, joten olemme valmiit.

## 15.2 Yleinen tapaus

Määritellään ensiksi, mitä tarkoitetaan lineaarisella rekursiolla.

### Määritelmä

Olkoon  $a_0, a_1, a_2, \dots$  lukujono. Sanotaan, että luvut  $a_0, a_1, \dots$  muodostavat lineaarisen rekursion, jos on olemassa positiivinen kokonaisluku  $k$  ja luvut  $b_0, b_1, \dots, b_{k-1}$  niin, että

$$a_{n+k} = a_{n+k-1}b_{k-1} + \dots + a_{n+1}b_1 + a_nb_0$$

kaikilla kokonaisluvuilla  $n \geq 0$ .

Määritellään samalla lineaarisen rekursion karakteristinen polynomi.

### Määritelmä

Olkoon  $a_0, a_1, \dots$  lineaarinen rekursio, ja olkoot  $b_0, b_1, \dots, b_{k-1}$  kuten edellä. Lukujonon  $a_0, a_1, \dots$  karakteristinen polynomi on

$$P(x) = x^k - b_{k-1}x^{k-1} - b_{k-2}x^{k-2} - \dots - b_1x - b_0.$$

### Esimerkki

Fibonaccin lukujonon  $F_{n+2} = F_{n+1} + F_n$  karakteristinen polynomi on  $x^2 - x - 1$ .

Fibonaccin lukujonon ratkaisun yhteydessä karakteristisen polynomin nollakohdat antoivat sellaiset luvut  $r_1$  ja  $r_2$ , että  $F_n = r_i^n$  toteuttaa Fibonaccin lukujen rekursioyhtälön. Karakteristisen polynomin määritelmä on valittu niin, että näin käy yleisestikin.

Yleinen tapaus toimii siis käytännössä samalla tavalla: Veikataan, että

$$a_n = c_1r_1^n + c_2r_2^n + \dots + c_kr_k^n,$$

missä  $r_1, \dots, r_k$  ovat karakteristisen polynomin nollakohdat ja  $c_1, \dots, c_k$  ovat joitain vakioita. Tällöin  $a_n$  toteuttaa halutun rekursioyhtälön, jolloin enää tulee valita luvut  $c_i$  siten, että alkuarvot osuvat kohdalleen. Saamme yhtälöryhmän, jossa on  $k$

yhtälöä ja  $k$  muuttujaa, joten sillä on ratkaisu.<sup>70</sup> Tässä päättelyssä jätettiin kuitenkin huomioimatta kaksin- ja moninkertaiset nollakohdat, joihin keskitytään seuraavaksi.

### 15.3 Kaksinkertainen nollakohta

Tutkitaan rekursiota  $a_{n+2} = 4a_{n+1} - 4a_n$  (ei kiinnitetä huomiota alkuarvoihin). Karakteristinen polynomi on  $x^2 - 4x + 4 = (x - 2)^2$ . Tällä on vain yksi nollakohta  $x = 2$ . Mitä tapahtuu?

Jos jatkaisimme kuten edellä, saisimme  $a_n = c_1 2^n + c_2 2^n$  sopivilla vakioilla  $c_1$  ja  $c_2$  eli  $a_n = c 2^n$ . Kaikki ratkaisut eivät kuitenkaan ole tätä muotoa: Valitaan  $a_0 = 0$  ja  $a_1 = 1$ . Jos  $a_n = c 2^n$ , tulisi ehdon  $a_0 = 0$  vuoksi olla  $c = 0$ , mutta tällöin  $a_n = 0$  kaikilla  $n$ .

Kaksinkertaiset nollakohdat käyttäytyvät eri tavalla kuin yksinkertaiset. Huomataan, että  $a_n = n 2^n$  toteuttaa rekursioyhtälön:

$$(n+2)2^{n+2} = (4n+8)2^n = (8n+8)2^n - 4n2^n = 4(n+1)2^{n+1} - 4n2^n.$$

Siispä yleisesti  $a_n = c_1 2^n + c_2 n 2^n$  on ratkaisu rekursioyhtälöön. Olivat alkuarvot  $a_0$  ja  $a_1$  mitkä tahansa, niin yhtälöryhmällä

$$\begin{cases} c_1 = a_0 \\ 2c_1 + 2c_2 = a_1 \end{cases}$$

on ratkaisu.

Yleisen lineaarisen rekursioyhtälön ratkaisun toimintamekanismin kertoo seuraava lause.

#### Lause (Yleisen lineaarisen rekursioyhtälön ratkaisu)

Olkoon  $a_0, a_1, \dots$  lineaarisesti rekursiivinen lukujono, jonka karakteristinen polynomi on  $P$ . Olkoot  $r_1, r_2, \dots, r_m$  kaikki  $P$ :n erisuuret juuret, ja olkoot niiden kertaluvut  $e_1, e_2, \dots, e_m$ . On olemassa polynomit  $Q_1, Q_2, \dots, Q_m$ , joilla

$$a_n = Q_1(n)r_1^n + Q_2(n)r_2^n + \dots + Q_m(n)r_m^n.$$

Lisäksi näillä  $Q_i$  pätee ehto  $\deg(Q_i) < e_i$ .

Vastaavasti mikä tahansa tällä kaavalla määritelty lukujono  $a_n$  toteuttaa lineaarisen rekursion, jonka karakteristinen polynomi on  $P$ .

(Polynomin  $P$  nollakohdan  $r$  kertaluku on  $e$ , jos  $r$  on  $e$ -ertainen nollakohta, muttei  $e+1$ -ertainen nollakohta.)

<sup>70</sup>Vielä tulisi perustella, että tämän yhtälöryhmän yhtälöt ovat lineaarisesti riippumattomia. Tämä ei ole suoraviivaista. Tämä todistetaan (epäsuorasti) luvun lopussa lineaaristen rekursioiden päätuloksen yhteydessä.

Lauseen todistus on vaikea. Lisäksi se käyttää hieman lineaarialgebraa ja polynomin derivaatan ominaisuuksia, joita ei käsitellä tässä kirjassa. Todistus on näistä syistä piilotettu luvun loppuun.

## 15.4 Esimerkkejä

Esitetään neljä esimerkkiä etenemällä helposta vaikeaan.

### Tehtävä

Olkoot  $a_0 = 0$ ,  $a_1 = 5$  ja  $a_{n+2} = 7a_{n+1} - 6a_n$ . Määritä yleinen lauseke termille  $a_n$ .

Ratkaisut muotoa  $r^n$  saadaan karakteristisen polynomin  $x^2 - 7x + 6$  nollakohdista: ratkaisut ovat  $x = 1$  ja  $x = 6$ . Siis vakiofunktio  $1^n$  toteuttaa rekursioyhtälön, kuten myös eksponenttifunktio  $6^n$ . Yleinen ratkaisu lukujonolle onkin

$$a_n = x6^n + y1^n = x6^n + y,$$

missä  $x$  ja  $y$  ovat joitain vakioita. Tässä tapauksessa halutaan, että  $a_0 = 0$  ja  $a_1 = 5$ , joten

$$0 = a_0 = x6^0 + y = x + y$$

ja

$$5 = a_1 = x6^1 + y = 6x + y.$$

Tällä yhtälöparilla on yksikäsitteinen ratkaisu  $x = 1$ ,  $y = -1$ . Siis lauseke termille  $a_n$  on

$$a_n = 6^n - 1.$$

Ratkaisun toimivuuden voi vielä tarkistaa helpolla induktiolla.

### Tehtävä

Olkoon  $n \geq 0$  kokonaisluku, Osoita, että

$$2^n \mid \lceil (3 + \sqrt{5})^n \rceil$$

(Kattofunktio  $\lceil x \rceil$  kuvaa pienintä kokonaislukua, joka on vähintään  $x$ .)

Tätä tehtävää on vaikea lähestyä, ellei ole nähnyt vastaavaa aiemmin. On kuitenkin kaksi ideaa, jotka voivat tulla mieleen:

1. Kerrotaan luku  $(3 + \sqrt{5})^n$  auki binomilauseen avulla:

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

Joka toinen termi on kokonaisluku ja joka toinen on muotoa  $k\sqrt{5}$  kokonaisluvulla  $k$ . Muotoa  $k\sqrt{5}$  olevat termit voisi yrittää saada kumottua tutkimalla summaa



$(3 + \sqrt{5})^n + (3 - \sqrt{5})^n$ . Tämä toimii: lopputulos on kokonaisluku. Huomataan, että tämä kokonaisluku on se, jonka haluamme:  $0 < (3 - \sqrt{5})^n < 1$ , eli  $\lceil (3 + \sqrt{5})^n \rceil = (3 + \sqrt{5})^n + (3 - \sqrt{5})^n$ .

- Muistetaan, että vaikkapa Fibonaccin lukujonon yleisen termin lausekkeessa on muotoa  $r^n$  olevien termien erotus ja että erotus jaettuna luvulla  $\sqrt{5}$  on kokonaisluku  $F_n$ . Erotuksessa toinen termeistä  $r^n$ , siis  $(\frac{1-\sqrt{5}}{2})^n$ , on hyvin pieni. Tämä kertoo, että luku  $\frac{1}{\sqrt{5}}(\frac{1+\sqrt{5}}{2})^n$  on lähellä kokonaislukua suurilla luvun  $n$  arvoilla. Voisiko lineaarisia rekursioita hyödyntää tässä tehtävässä?

Edellisten ideoiden innoittamana yksi idea ratkaisuun voisi olla seuraava: muodostetaan lukujono  $a_n$ , jonka yleinen jäsen on suunnilleen  $(3 + \sqrt{5})^n$ , ja tutkitaan tämän lukujonon jäsenten jaollisuutta luvulla  $2^n$ .

Lukujonon karakteristinen polynomi  $x^2 + ax + b$  kannattaisi valita niin, että sillä on nollakohdat  $3 \pm \sqrt{5}$ . Kertomalla auki  $(x - (3 + \sqrt{5}))(x - (3 - \sqrt{5}))$  saadaan polynomi  $x^2 - 6x + 4$ . Idean 1 perusteella on luontevaa valita lukujonon alkuarvot niin, että yleinen termi on täsmälleen luvut muotoa  $(3 + \sqrt{5})^n + (3 - \sqrt{5})^n$ . Alkuarvoiksi tulee tällöin  $a_0 = 2$  ja  $a_1 = 6$ .

Saadaan siis rekursioyhtälö  $a_{n+2} = 6a_{n+1} - 4a_n$  alkuarvoilla  $a_0 = 2$  ja  $a_1 = 6$ . Nyt on hyvin helppoa osoittaa induktiolla, että  $2^n \mid a_n$ . Tämä todistaa väitteen.

Seuraava tehtävä on esiintynyt vuoden 2018 tammikuun valmennustehtävissä.

### Tehtävä

Määritellään  $a_0 = a_1 = 3$  ja  $a_{n+1} = 7a_n - a_{n-1}$  jokaisella  $n \in \mathbb{Z}_+$ . Osoita, että  $a_n - 2$  on neliöluku jokaisella  $n \in \mathbb{Z}_+$ .

Luonnollinen ensimmäinen askel on listata muutama ensimmäinen arvo. Saadaan  $a_2 = 18$ ,  $a_3 = 123$  ja  $a_4 = 843$ . Tutkitaan sitten, minkä lukujen neliöitä luvut  $a_n - 2$  ovat: merkitään näitä lukuja merkinnöillä  $b_n$ . Lukujonon  $b_0, b_1, \dots$  ensimmäiset termit ovat siis 1, 1, 4, 11, 29. Pienellä mielikuvituksella (ja tarvittaessa laskemalla vielä lisää termejä) tästä näkee rekursion  $b_{n+1} = 3b_n - b_{n-1}$ , paitsi kun  $n = 1$ . Tapaus  $n = 1$  voidaan kuitenkin korjata valitsemalla  $b_0 = -1$ , jolloin  $a_0 - 2 = b_0^2$  pätee edelleen ja  $b_2 = 3b_1 - b_0$ .

Meillä on nyt arvaus siitä, mitä luvut  $\sqrt{a_0 - 2}$  ovat: jonkin lineaarisesti rekursiivisen lukujonon jäsenet. Miten tämä todistetaan? Luonnollinen idea olisi käyttää induktiota. (Väite onkin mahdollista todistaa induktiolla, mutta tämä ei ole aivan suoraviivaista.) Tässä esitetään kuitenkin toisenlainen ratkaisu, joka ei vaadi minkäänlaista luovuutta. Ideana on yksinkertaisesti määrittää yleinen lauseke lukujonojen  $a_n$  ja  $b_n$  termeille, ja todistaa väite siitä.

Ennen kuin edetään pidemmälle, voidaan jopa todeta, että tämä ratkaisu tulee toimimaan. Tiedämme nimittäin jo etukäteen, että jonon  $a_n$  termit saadaan suoraan kaavalla muotoa

$$a_n = c_1 r_1^n + c_2 r_2^n,$$

missä  $c_1$  ja  $c_2$  ovat sopivia vakiota ja  $r_1$  ja  $r_2$  ovat lukujonon  $a_n$  karakteristisen

polynomin  $x^2 - 7x + 1$  nollakohdat (huomaa, että nollakohdat eivät ole kaksinkertaisia). Vastaavasti saadaan

$$b_n = d_1 s_1^n + d_2 s_2^n$$

sopivilla vakiolla  $d_1, d_2, s_1$  ja  $s_2$ . Todistettavaan väitteeseen

$$a_n - 2 = b_n^2$$

voidaan sijoittaa edellä saadut lausekkeet luvuille  $a_n$  ja  $b_n$ , ja tämän jälkeen termi  $b_n^2$  voidaan kertoa auki. Miltä jäljelle jäävä yhtälö näyttää? Se koostuu termeistä muotoa  $a \cdot q^n$ , joita summaamalla saadaan 0:

$$\sum a_i \cdot q_i^n = 0.$$

Kuinka vaikeaa tällaisen yhtälön todistaminen voi olla? Vastaus: yhtälön todistamiseksi riittää vain sieventää se. Oletetaan nimittäin, että yhtälö on sievennetyssä muodossa, eli oletetaan, että  $q_i \neq q_j$  kaikilla  $i \neq j$  ja kaikki  $a_i$  ovat nollasta eroavia. Pointtina on, että se summan termeistä  $a_i \cdot q_i^n$ , jolla  $|q_i|$  on isoin, tulee ”dominoimaan” summaa, eli se määrää summan kasvunopeuden. Esimerkiksi summassa  $3^n - 100 \cdot 2^n$  termi  $3^n$  tulee dominoimaan ennen pitkää. Summan tulee kuitenkin olla 0, mikä tarkoittaa, että dominoivaa termiä ei ole ja että sievennetyssä muodossa on 0 termiä.<sup>71</sup>

Enää jäljelle jää laskeminen. Edellä kuvailtujen vakioiden  $c_1, c_2, r_1, r_2, d_1, d_2, s_1$  ja  $s_2$  laskeminen ei ole vaikeaa (vaikkakin se on hieman työlästä), joten esitetään vain vastaukset: pätee

$$a_n = \frac{3 - \sqrt{5}}{2} \left( \frac{7 + 3\sqrt{5}}{2} \right)^n + \frac{3 + \sqrt{5}}{2} \left( \frac{7 - 3\sqrt{5}}{2} \right)^n$$

ja

$$b_n = \frac{\sqrt{5} - 1}{2} \left( \frac{3 + \sqrt{5}}{2} \right)^n - \frac{\sqrt{5} + 1}{2} \left( \frac{3 - \sqrt{5}}{2} \right)^n.$$

Koska lausekkeet ovat melko ikäviä, käytetään vielä hetken aikaa eksplisiittisten esitysten sijasta kirjaimia.

Tutkitaan yhtälöä  $a_n - 2 = b_n^2$ . Tämä muuttuu muotoon

$$c_1 r_1^n + c_2 r_2^n - 2 = d_1^2 (s_1^2)^n + 2d_1 d_2 (s_1 s_2)^n + d_2^2 (s_2^2)^n,$$

missä oikealla puolella on kerrottu neliö  $(d_1 s_1^n + d_2 s_2^n)^2$  auki. Yritetään sieventää tätä hillitysti: emme halua sijoittaa kaikkien muuttujien paikoille niiden arvoja, koska laskeminen muuttuisi ikäväksi.

Kuten aiemmin todettiin, yhtälön todistamiseksi riittää vain sen sieventäminen. Siispä termien  $q^n$  kantalukujen  $q$  pitäisi olla samoja yhtälön molemmilla puolilla.

<sup>71</sup>Esimerkiksi summan  $2^n + (-2)^n$  analysoinnissa tulee olla hieman varovaisempi, koska tämä on nolla parittomilla  $n$ . Yleisessä tapauksessa todistaminen ei ole helppoa, mutta tämä tehdään luvun lopussa todistettaessa lineaaristen rekursioiden päätulosta.

Tästä motivoituneena tehdään seuraavat havainnot: Pätee

$$s_1^2 = \left( \frac{3 + \sqrt{5}}{2} \right)^2 = \frac{7 + 3\sqrt{5}}{2},$$

joka on yhtä suuri kuin  $r_1$ . Lisäksi kertoimet ovat oikeat:

$$d_1^2 = \left( \frac{\sqrt{5} - 1}{2} \right)^2 = \frac{3 - \sqrt{5}}{2} = c_1.$$

Täten termit  $c_1 r_1^n$  ja  $d_1^2 (s_1^2)^n$  kumoavat toisensa. Vastaavasti nähdään, että termit  $c_2 r_2^n$  ja  $d_2^2 (s_2^2)^n$  kumoavat toisensa. Todistettavana on enää yhtälö

$$-2 = 2d_1 d_2 (s_1 s_2)^n.$$

Jotta tämä pätesi kaikilla  $n$ , tulee päteä  $s_1 s_2 = 1$ . Ja niin pätee:

$$s_1 s_2 = \frac{3 + \sqrt{5}}{2} \cdot \frac{3 - \sqrt{5}}{2},$$

joka saadaan sievennettyä (käyttämällä yhtälöä  $(x - y)(x + y) = x^2 - y^2$ ) muotoon

$$\frac{3^2 - 5}{2^2} = 1,$$

joka on mitä haluttiinkin. (Väite  $s_1 s_2 = 1$  seuraa myös käyttämällä Vietan kaavoja lukujonon  $b_n$  karakteristiselle polynomille  $x^2 - 3x + 1$ .)

Vielä lopuksi todetaan, että  $d_1 d_2 = -1$ , ja ratkaisu on valmis: kaikilla  $n$  pätee  $a_n - 2 = b_n^2$ , eli  $a_n - 2$  on aina kokonaisluvun  $b_n$  neliö. Kuten alussa mainittiin, yhtälön  $a_n - 2 = b_n^2$  todistamiseksi riitti helpot sievennykset.

Yleisesti ennen kuin lähtee ratkaisemaan tehtävää paljon manuaalisia laskuja vaativalla tavalla, on hyvä vakuuttua siitä, että ratkaisu todella tulee toimimaan.

Viimeinen tehtävä on myös esiintynyt valmennustehtävänä.

### Tehtävä

Selvitä joukon  $\{1, 2, \dots, 2000\}$  niiden osajoukkojen lukumäärä, joiden sisältämien lukujen summa on viidellä jaollinen.

Tutkitaan ensin mitä tapahtuu, jos 5 korvataan jollain muulla luvulla, koska yksinkertaisemman tapauksen tarkastelu varmaankin auttaa tehtävää ratkoessa. Tutkitaan yleisesti joukkoa  $\{1, 2, \dots, n\}$ .

*Tapaus 1: Yhdellä jaollisuus.* Tällöin osajoukkojen määrä on  $2^n$  joukon koon ollessa  $n$ .

*Tapaus 2: Kahdella jaollisuus.* Osoitetaan, että tasan puolet osajoukoista ovat sellaisia, joissa osajoukon alkioiden summa on parillinen. Valitaan jokin osajoukko  $X$ . Jos  $1 \in X$ , muodostetaan joukko  $X'$  poistamalla joukosta  $X$  alkio 1. Tällöin

joukon  $X'$  alkioden summan parillisuus on eri kuin joukon  $X$ . Vastaavasti jos  $1 \notin X$ , muodostetaan  $X'$  lisäämällä joukkoon  $X$  alkio 1. Näin saadaan muodostettua osajoukoista pareja, joiden alkioilla on eri summat modulo 2. Tämä osoittaa väitteen.

*Tapaus 3: Kolmella jaollisuus.* Nyt ongelmaksi tulee se, ettei kohdan 2 kaltaista yksinkertaista paritusta voida tehdä. Ideaa voi kuitenkin jalostaa. Valitaan jokin joukon  $\{4, 5, \dots, n\}$  osajoukko  $X$ . Voimme luoda tästä 8 erilaista joukon  $\{1, 2, \dots, n\}$  osajoukkoa sen mukaan, mitä alkioita joukosta  $\{1, 2, 3\}$  lisätään joukkoon  $X$ .

Eri valinnat muuttavat joukon  $X$  alkioden summaa eri tavalla modulo 3. On neljä vaihtoehtoa, jotka eivät muuta summaa: ei lisätä mitään, lisätään 1 ja 2, lisätään 3 ja lisätään 1, 2 ja 3. Vastaavasti voidaan käsitellä muita tapauksia. Tästä voidaan rakentaa rekursioyhtälöitä.

Tutkitaan sitten viidellä jaollisuutta. Tapauksen 3 idea voisi soveltua tähänkin tapaukseen. Idea on siis seuraava: Oletetaan, että arvolla  $n = k$  tiedetään, kuinka monta sellaista joukon  $\{1, 2, \dots, k\}$  osajoukkoa on, joiden alkioden summa on  $0 \pmod{5}, 1 \pmod{5}, \dots, 4 \pmod{5}$ . Tällöin vastaavat tiedot saadaan ratkaistua arvolle  $n = k + 5$ .

Koska tehtävänannon joukon koko on 2000, tutkitaan vain viiden kokoisia joukkoja. Merkitään  $5n$ -kokoisen joukon  $\{1, 2, \dots, 5n\}$  niiden osajoukkojen määrää, joiden alkioden summa on  $0 \pmod{5}$ , luvulla  $a_n$ . Määritellään vastaavasti lukujonot  $b_n, c_n, d_n$  ja  $e_n$  jakojäännöksille 1, 2, 3 ja 4.

Intuitio sanoo, että jäännökset 1 ja 4 eivät juurikaan poikkea toisistaan; ne ovat ikään kuin toistensa komplementteja. Tämä on helppo muotoilla ja todistaa formaalisti: Olkoon  $X$  joukko, jonka alkioden summa  $S(X)$  on  $1 \pmod{5}$ . Tällöin  $X$ :n komplementin, eli niiden  $y \in \{1, 2, \dots, 5n\}$  joukko, joilla  $y \notin X$ , alkioden summa on  $1 + 2 + \dots + 5n - S(X) = \frac{5n(5n+1)}{2} - S(X) \equiv 4 \pmod{5}$ . Tämä osoittaa, että  $b_n \leq e_n$  kaikilla  $n$ . Vastaavasti saadaan  $e_n \leq b_n$ , joten  $e_n = b_n$ .<sup>72</sup> Samoin todistetaan, että  $c_n = d_n$  kaikilla  $n$ .

Ongelma on nyt palautettu kolmeen lukujonoon viiden sijasta, mikä on hyvää edistystä. Muodostetaan sitten rekursioyhtälöt.<sup>73</sup>

Käyttämällä tapauksen 3 ideaa saadaan siis seuraava rekursioyhtälö:

$$a_{n+1} = a_1 a_n + e_1 b_n + d_1 c_n + c_1 d_n + b_1 e_n.$$

Lyhyt perustelu, joka on kuin edellä: Valitaan jokin joukon  $\{6, 7, \dots, 5(n+1)\}$  osajoukko  $X$ . Jos  $S(X) \equiv 0 \pmod{5}$ , voidaan joukkoa  $X$  täydentää  $a_1$  tavalla. Jos  $S(X) \equiv 1 \pmod{5}$ , niin täydentäminen voidaan tehdä  $e_1$  tavalla, ja niin edelleen.

Pieni laskeminen antaa  $a_1 = 8$  ja  $b_1 = c_1 = d_1 = e_1 = 6$ . Käyttämällä vielä ehtoja  $e_n = b_n$  ja  $d_n = c_n$  saadaan

$$a_{n+1} = 8a_n + 12b_n + 12c_n.$$

<sup>72</sup>Teimme siis samankaltaisen parituksen kuin mitä käytettiin ongelman varianttiin, jossa käsiteltiin osajoukkojen alkioden summien parillisuuksia.

<sup>73</sup>Rekursioyhtälöt olisi voinut muodostaa myös ennen kuin todistaa  $b_n = e_n$ . Lisäksi rekursioyhtälöistä näkisi suoraan, että  $b_n = e_n$  pätee kaikilla  $n$ .

Vastaavasti saadaan

$$b_{n+1} = 6a_n + 14b_n + 12c_n$$

ja

$$c_{n+1} = 6a_n + 12b_n + 14c_n.$$

Nyt on triviaalia osoittaa induktiolla, että  $b_n = c_n$  kaikilla  $n$ . Ongelma redusoituu enää kahteen lukujonoon, eli tutkittavina ovat nyt yhtälöt

$$a_{n+1} = 8a_n + 24b_n$$

ja

$$b_{n+1} = 6a_n + 26b_n.$$

Nyt ei ole ilmeistä, miten jatkaa. Kyseessä on lineaaristen rekursioiden ja yhtälöparin yhdistelmä. Kuten lineaarisissa yhtälöpareissa voisi tässäkin kuvitella olevan mahdollista eliminoida toinen muuttuja (eli lukujono), jolloin ongelma palautuu yhden lukujonon tutkimiseen. Yksi tapa tähän on toistuva sijoittaminen:

$$\begin{aligned} a_{n+1} &= 8a_n + 24b_n \\ &= 8a_n + 24(6a_{n-1} + 26b_{n-1}) \\ &= 8a_n + 24(6a_{n-1} + 26(6a_{n-2} + 26b_{n-2})) \\ &\vdots \end{aligned}$$

Lopputulos on jotain kauheaa, mutta ideana on, että kyseessä on jokin summa termeistä  $a_i$ . Lisäksi summan kertoimet vaikuttavat olevan likimain jonkin geometrisen lukujonon jäsenet. Jos kertoimet muodostaisivat geometrisen lukujonon, jonka suhdevakio on  $c$ , olisi erotuksen  $a_{n+1} - ca_n$  tutkiminen hyödyllistä: tällöinhän miltei kaikki supistuisi pois. Nyt tilanne ei tunnu olevan aivan otollisin tälle, mutta yritetään silti:

$$a_{n+1} - ca_n = (8a_n + 24b_n) - ca_n = (8 - c)a_n + 24b_n.$$

Vielä ei saatu mitään hyödyllistä, joten jatketaan iterointia:

$$a_{n+1} - ca_n = (8 - c)(8a_{n-1} + 24b_{n-1}) + 24(6a_{n-1} + 26b_{n-1}).$$

Luku  $c$  halutaan valita niin, että termi  $b_{n-1}$  supistuu pois. Tämä onnistuu, kun  $24(8 - c) + 24 \cdot 26 = 0$  eli kun  $c = 34$ . Tällöin saadaan

$$a_{n+1} - 34a_n = 64a_{n-1}.$$

Tämä on tavallinen lineaarinen rekursioyhtälö, joka osataan ratkaista. Alkuarvo  $a_1 = 8$  on tiedossa. Lisäksi voidaan ajatella, että  $a_0 = 1$ , jolloin saadaan ratkaisu:

$$a_n = \frac{2^{n+2} + 2^{5n}}{5}.$$

Arvolla  $n = 400$  saadaan tehtävän ratkaisu  $\frac{2^{402} + 2^{2000}}{5}$ . Vastaus on oikeaa kokoluokkaa, onhan  $a_n \approx b_n = c_n = d_n = e_n \approx \frac{2^{2000}}{5}$ . Summa  $0 \pmod{5}$  sattuu olemaan muita hieman yleisempi.

Edellisessä esimerkissä nähtiin, miten tietynlainen kahden lukujonon rekursiivinen yhtälöpari ratkaistiin. Luonnollinen jatkokysymys on, voiko yleisesti lineaaristen rekursioiden yhtälöryhmän ratkaista. Tähän kysymykseen vastataan luvun lopussa.

## 15.5 Lauseen todistus

Olkoon  $P(x) = x^k - b_{k-1}x^{k-1} - \dots - b_0$  karakteristinen polynomi, jonka nollakohdat ovat  $r_1, \dots, r_m$  kertaluvuilla  $e_1, \dots, e_m$ . Osoitamme seuraavat kaksi tulosta.

- Jos jono  $a$  määritellään asettamalla

$$a_n = Q_1(n)r_1^n + \dots + Q_m(n)r_m^n,$$

missä polynomien  $Q_1, \dots, Q_m$  asteet ovat pienempiä kuin  $e_1, \dots, e_m$ , niin jono  $a_n$  toteuttaa rekursioyhtälön

$$a_{n+k} = a_{n+k-1}b_{k-1} + \dots + a_nb_0.$$

- Jos jono  $a$  toteuttaa rekursioyhtälön

$$a_{n+k} = a_{n+k-1}b_{k-1} + \dots + a_nb_0,$$

niin se on edellä kuvailtua muotoa.

Sanotaan, että lukujono  $(a_n)$  on hyvä, jos se toteuttaa polynomia  $P$  vastaavan rekursioyhtälön, ja erinomainen, jos se on muotoa  $Q_1(n)r_1^n + \dots + Q_m(n)r_m^n$ . Haluamme siis osoittaa, että jokainen hyvä jono on erinomainen ja päinvastoin.

Osoitetaan ensiksi, että jokainen erinomainen jono on hyvä. Kuten jo aiemmin totesimme: mikäli kaksi rekursiota  $f(n)$  ja  $g(n)$  toteuttavat karakteristista polynomia  $P$  vastaavan rekursioyhtälön, niin myös  $c \cdot f(n)$  ja  $f(n) + g(n)$  toteuttavat sen. Siis kahden hyvän jonon summa on hyvä, ja hyvä jono kerrottuna vakiolla on hyvä. Huomataan myös, että erinomaisilla jonoilla on sama ominaisuus.

Tämän vuoksi riittää todistaa, että jono  $n^e r_i^n$  on hyvä kaikilla  $0 \leq e < e_i$  ja  $1 \leq i \leq m$ , koska tämän jälkeen voimme rakentaa minkä tahansa lukujonon muotoa

$$Q_1(n)r_1^n + \dots + Q_m(n)r_m^n$$

kertomalla jonoja  $n^e r_i^e$  sopivilla vakioilla ja summaamalla näin saatuja jonoja.

Olemmekin jo todenneet, että jono  $r_i^n$  toteuttaa rekursioyhtälön (tämä seuraa suoraan karakteristisen polynomin määritelmästä). Tutkitaan sitten tapausta  $nr_i^n$ . Haluamme osoittaa, että

$$(n+k)r_i^{n+k} = (n+k-1)r_i^{n+k-1}b_{k-1} + \dots + nr_i^n b_0.$$

Toisaalta tiedämme, että

$$nr_i^{n+k} = nr_i^{n+k-1}b_{k-1} + \dots + nr_i^n b_0,$$

koska jakamalla termillä  $nr_i^n$  yhtälö palautuu muotoon  $P(r_i) = 0$ . Haluamamme väite muuttuu siis muotoon

$$kr_i^{n+k} = (k-1)r_i^{n+k-1}b_{k-1} + \dots + r_i^{n+1}b_1.$$

Supistamalla tästä  $r_i^{n+1}$  saadaan

$$kr_i^{k-1} = (k-1)r_i^{k-2}b_{k-1} + \dots + b_1.$$

Mitä tiedämme luvusta  $r_i$ ? Se on polynomin  $P$  kaksinkertainen nollakohta (halutaan todistaa, että  $n^e r_i^n$  on hyvä kaikilla  $0 \leq e < e_i$ , joten tapauksessa  $e = 1$  luku  $e_i$  on vähintään 2). Siispä se on myös polynomin  $P$  derivaatan  $P'$  nollakohta. Mutta

$$P'(x) = kx^{k-1} - (k-1)b_{k-1}x^{k-2} + \dots + b_1,$$

joten yhtälö  $P'(r_i) = 0$  vastaa haluamaamme väitettä.

Samaan tapaan voidaan todistaa jonon  $n^e r_i^n$  toteuttavan karakteristista polynomia vastaavan rekursioyhtälön kaikilla  $0 \leq e < e_i$ . Tämä ei kuitenkaan ole kovin mielenkiintoista (uusia ideoita ei tarvita), joten tarkistaminen sivuutetaan.

Olemme siis todistaneet, että jokainen erinomainen jono on hyvä.

Todistetaan sitten toinen puoli, eli todistetaan, että jokainen hyvä jono on erinomainen. Tutkitaan jotakin hyvää jonoa  $a$ . Selvästikin sen ensimmäiset  $\deg(P) = k$  termiä määräävät jonon yksikäsitteisesti. Meillä on ikään kuin  $k$  eri ”vapausastetta”: valitsemalla  $k$  eri lukua päätämme, minkä lukujonon luomme. Formaalisimmin ajatus on seuraava: hyvien jonojen joukko on vektoriavaruus, jonka ulottuvuus on  $k$ . (Kuten on jo mainittu, kahden hyvän jonon summa on hyvä, ja hyvän jonon kertominen vakiolla antaa taas hyvän jonon.)

Erinomaiset jonot muodostavat niin ikään vektoriavaruuden. Erinomaiset jonot muodostavat siis aliavaruuden hyvien jonojen vektoriavaruudelle. Ideana on osoittaa, että tämä aliavaruus on itse asiassa koko avaruus. Toisin sanoen erinomaisia jonoja on ”yhtä paljon” kuin hyviä jonoja, minkä vuoksi jokainen hyvä jono on erinomainen.<sup>74</sup> Tämän todistaminen puolestaan palautuu siihen, että erinomaisten jonojen vektoriavaruuden ulottuvuus on  $k$ .

Tutkitaan erinomaisia jonoja muotoa  $n^e r_i^n$ , missä  $0 \leq e < e_i$  ja  $1 \leq i \leq m$ . Yhteensä näitä on  $k$  kappaletta. Olkoot nämä jonot  $v_1, \dots, v_k$ . Osoitetaan, että jonot  $v_i$  ovat lineaarisesti riippumattomia. Tällöin niiden virittämän aliavaruuden ulottuvuus on  $k$ , mikä on haluttu väite.

Lineaarinen riippumattomuus tarkoittaa, että mikäli luvut  $c_1, \dots, c_k$  ovat vakioita ja jono  $c_1 v_1 + \dots + c_k v_k$  on nollajono (eli sen jokainen jäsen on 0), niin jokainen kertoimista  $c_i$  on nolla. Toisin sanoen haluamme todistaa seuraavan tuloksen.

<sup>74</sup>Varoituksen sana: Äärettömyyksien kanssa tulee tietää, mitä tekee. Esimerkiksi parillisia kokonaislukuja on tietystä miehestä yhtä paljon kuin kaikkia kokonaislukuja, mutta kaikki kokonaisluvut eivät silti ole parillisia. Vektoriavaruuksien tapauksessa asiat kuitenkin toimivat melko mukavasti.

**Lemma**

Olkooot  $r_1, r_2, \dots, r_m$  nollasta eroavia erisuuria kompleksilukuja ja olkooot  $Q_1, \dots, Q_m$  (kompleksikertoimisia) polynomeja. Oletetaan, että kaikilla positiivisilla kokonaisluvuilla  $n$  pätee

$$Q_1(n)r_1^n + \dots + Q_m(n)r_m^n = 0.$$

Tällöin jokainen polynomeista  $Q_1, \dots, Q_m$  on nollapolynomi.

(Huomaa, että voimme olettaa, ettei karakteristisella polynomilla  $P$  päde  $P(0) = 0$ , eli oletamme että  $r_i \neq 0$  kaikilla  $i$ .)

Tämä lemma on koko homman juju. Lemma ei ole aivan ilmeinen, koska lemmän lausekkeet voivat olla ”usein” nollia, vaikka ne eivät olisi aina nollia: esimerkiksi  $2^n + (-2)^n$  on nolla kaikilla parittomilla luvuilla.

Todistetaan lemmän väite induktiolla muuttujan  $m$  suhteen. Tapaus  $m = 1$  on ilmeinen: jokaisella nollasta eroavalla polynomilla on vain asteensa verran nollakohtia. Oletetaan, että väite pätee arvolla  $m = M$ , ja todistetaan se arvolla  $m = M + 1$ . Oletetaan siis, että lukujonon

$$a_n = Q_1(n)r_1^n + \dots + Q_{M+1}(n)r_{M+1}^n$$

jokainen termi on 0, ja todistetaan, että jokainen polynomeista  $Q_i$  on nollapolynomi. Merkitään  $\deg(Q_i) = e_i$ . Riittää todistaa, että  $Q_{M+1}$  on nollapolynomi, koska tämän jälkeen olemme induktiolla valmiit. Tähdätään siis tähän.

Todistuksen pääidea on seuraava: voidaan kirjoittaa

$$a_n = b_n + c_n,$$

missä

$$b_n = Q_1(n)r_1^n + \dots + Q_M(n)r_M^n$$

ja

$$c_n = Q_{M+1}(n)r_{M+1}^n.$$

Jono  $b$  toteuttaa tietyn lineaarisen rekursioyhtälön. Jono  $a$  toteuttaa saman rekursioyhtälön, koska jokainen jonon  $a$  termi on 0. Siten myös jono  $c$  toteuttaa tämän rekursioyhtälön. Siis  $c$  toteuttaa rekursioyhtälön, jota sen ei ”pitäisi” toteuttaa. Vertaamalla tätä siihen rekursiojonoon, jonka  $c$ :n pitäisi toteuttaa, saadaan  $c_n = 0$  kaikilla  $n$ .

Tässä on ajatuksen toteutus. Olkoon

$$P_M(x) = (x - r_1)^{e_1} \dots (x - r_M)^{e_M},$$

ja kirjoitetaan

$$P_M(x) = x^d - f_{d-1}x^{d-1} - \dots - f_0.$$

Koska erinomaiset jonot ovat hyviä, tiedämme, että jono  $b$  toteuttaa rekursioyhtälön

$$b_{n+d} = f_{d-1}b_{n+d-1} + \dots + f_0b_n.$$



Koska  $a_n = 0$  kaikilla  $n$ , niin pätee tietysti

$$a_{n+d} = f_{d-1}a_{n+d-1} + \dots + f_0a_n.$$

Nyt myös  $c_n = a_n - b_n$  toteuttaa vastaavan yhtälön:

$$c_{n+d} = f_{d-1}c_{n+d-1} + \dots + f_0c_n.$$

Siis  $c$  toteuttaa rekursioyhtälön, jonka karakteristinen polynomi on  $P_M$ .

On olemassa yksinkertaisempikin rekursioyhtälö, jonka jono  $c$  toteuttaa. Olkoon

$$P_{M+1}(x) = (x - r_{M+1})^{e_{M+1}}.$$

Koska erinomaiset jonot ovat hyviä, jono  $c$  toteuttaa rekursioyhtälön, jonka karakteristinen polynomi on  $P_{M+1}$ . Tämä on se rekursioyhtälö, joka jonon  $c_n$  pitäisi toteuttaa, kun taas polynomia  $P_M$  vastaavaa rekursioyhtälöä jonon  $c_n$  ei pitäisi toteuttaa.

Tarvitsemme vielä seuraavan lemmän.

### Lemma

Olkoot  $A$ ,  $B$  ja  $C$  polynomeja. Olkoon  $x$  jono, joka toteuttaa rekursioyhtälöt, joiden karakteristiset polynomit ovat  $A$  ja  $B$ . Tällöin  $x$  toteuttaa rekursioyhtälön, jonka karakteristinen polynomi on  $A + B$ . Lisäksi  $x$  toteuttaa rekursioyhtälön, jonka karakteristinen polynomi on  $AC$ .

Viimeistellään ensiksi lauseen todistus ja keskitytään sitten tähän lemmaan.

Polynomeilla  $P_M$  ja  $P_{M+1}$  ei ole yhteisiä nollakohtia (koska luvut  $r_1, \dots, r_{M+1}$  ovat erisuuria). Täten ne ovat yhteistekijättömiä, joten Bezout'n lemmän polynomiversion nojalla on olemassa sellaiset (kompleksikertoimiset) polynomit  $A$  ja  $B$ , että

$$AP_M + BP_{M+1}$$

on vakiopolynomi 1. Koska jono  $c_n$  toteuttaa polynomeja  $P_M$  ja  $P_{M+1}$  vastaavat rekursioyhtälöt, toteuttaa se nyt lemmän nojalla vakiopolynomia 1 vastaavan rekursioyhtälön. Siis  $c_n = 0$  kaikilla  $n$ , eli  $Q_{M+1}$  on nollapolynomi.

Koska oletuksen nojalla  $a_n = 0$  kaikilla  $n$ , niin nyt  $b_n = a_n - c_n = 0$  kaikilla  $n$ . Induktio-oletuksen nojalla polynomit  $Q_1, \dots, Q_M$  ovat nollapolynomeja. Näin ollen lause on todistettu.

Tutkitaan sitten lemmaa. Tehdään seuraava ajatusleikki: Sanotaan, että jono  $a$  on polynomin  $P$  nollakohta, jos  $a$  toteuttaa rekursion, jonka karakteristinen polynomi on  $P$ . Nyt lemma sanoo, että jos  $a$  on polynomien  $A$  ja  $B$  nollakohta, niin se on myös polynomien  $A + B$  ja  $AC$  nollakohta millä tahansa polynomilla  $C$ . Vastaavat tulokset pätevät tietysti silloin, kun puhutaan tavallisisat nollakohdista. Tämä ajatus johdattelee oikeiden ideoiden jäljille.

Ennen lemmän todistusta mainitaan tekninen, tylsä yksityiskohta: Tähän mennessä olemme tutkineet rekursioyhtälöitä muotoa

$$x_{n+k} = c_{k-1}x_{n+k-1} + \dots + c_0x_n$$

ja näitä vastaavia karakteristisia polynomeja. Tällöin karakterististen polynomien korkeimman asteen termin kerroin on aina 1. Lemmaa varten tarvitsemme kuitenkin myös muita polynomeja (jos  $A$ :n ja  $B$ :n korkeimman asteen termin kertoimet ovat 1 ja  $\deg(A) = \deg(B)$ , niin summan  $A + B$  korkeimman asteen termin kerroin on 2). Tämä ei tietenkään ole ongelma: polynomi  $P(x) = c_k x^k - c_{k-1} x^{k-1} - \dots - c_0$  voidaan ajatella rekursion

$$c_k x_{n+k} = c_{k-1} x_{n+k-1} + \dots + c_0 x_n$$

karakteristisena polynomina.

Todistetaan sitten lemma. Kirjoitetaan  $A(x) = a_A x^A + a_{A-1} x^{A-1} + \dots + a_0$  ja käytetään polynomeille  $B$  ja  $C$  vastaavia merkintöjä. Tiedämme, että

$$a_A x_{n+A} + a_{A-1} x_{n+A-1} + \dots + a_0 x_n = 0$$

ja

$$b_B x_{n+B} + b_{B-1} x_{n+B-1} + \dots + b_0 x_n = 0$$

kaikilla  $n$ . Summaamalla yhtälöt saadaan, että jono  $x$  toteuttaa rekursion, jonka karakteristinen polynomi on  $A + B$ .

Tutkitaan sitten tuloa  $AC$ . Tiedämme kuten edellä, että

$$a_A x_{n+A+i} + a_{A-1} x_{n+A-1+i} + \dots + a_0 x_{n+i} = 0.$$

kaikilla  $n$  ja  $i$ . Kerrotaan yhtälö puolittain luvulla  $c_i$  ja summataan saadut yhtälöt arvoilla  $i = 0, 1, \dots, C$  yhteen. Termin  $x_{n+t}$  kerroin syntyneessä yhtälössä on

$$a_t c_0 + a_{t-1} c_1 + \dots + a_0 c_t,$$

missä määrittelemme  $a_i = 0$  jos  $i > A$  ja  $c_i = 0$  jos  $i > C$ . Tämä on termin  $x^t$  kerroin polynomissa  $AC$ . Olemme valmiit.

## 15.6 Jälkipuinti

Olemme nähneet paljon vaivaa päälauseen todistamiseksi. Tämä on kuitenkin sen arvoista: tulos on todella vahva. Saamme esimerkiksi todistettua seuraavat tulokset vain toteamalla, että kahden erinomaisen lukujonon summa ja tulo ovat erinomaisia.

- Jos  $a$  ja  $b$  ovat lineaarisesti rekursiivisia lukujonoja, niin myös lukujono  $c_n = a_n + b_n$  on lineaarisesti rekursiivinen.
- Jos  $a$  ja  $b$  ovat lineaarisesti rekursiivisia lukujonoja, niin myös lukujono  $c_n = a_n b_n$  on lineaarisesti rekursiivinen.

Summan tapauksessa jonon  $c$  karakteristiseksi polynomiksi voidaan valita jonojen  $a$  ja  $b$  karakterististen polynomien tulo, mutta jonojen tulo tapauksessa jonon  $c$  karakteristinen polynomi on paljon vaikeampi määrittää.

Sitten esitetään hieman vaikeampi sovellus, joka on kuitenkin varsin mielenkiintoinen. Tämän luvun viimeisessä esimerkkit tehtävässä ratkaistiin lineaaristen rekursioyhtälöiden yhtälöpari. Ratkaisun jälkeen luvattiin, että luvun lopussa esitetään menetelmä, jolla voi yleisesti ratkaista tällaisia yhtälöryhmiä. On aika lunastaa lupaus.

Ensin täytyy määritellä hieman notaatiota.

Jos  $a = (a_0, a_1, a_2, \dots)$  on lukujono, määritellään sitä vastaava ns. generoiva funktio olemaan  $A(x) = a_0 + a_1x + a_2x^2 + \dots$ . Siis  $A(x)$  on ikään kuin ääretönasteinen polynomi. Painotetaan kuitenkin, että generoivaa funktiota  $A(x)$  ei kannata ajatella polynomina tai edes funktiona – emme sijoita  $x$ :n paikalle mitään arvoja. Generoivat funktiot ovat siis vain yksi tapa kuvailla lukujonoja eikä mitään sen ihmeempää.

Miksi generoivat funktiot sitten ovat hyödyllinen tapa kuvailla lukujonoja? Voimme suorittaa generoivilla funktioilla laskutoimituksia vastaavaan tapaan kuin polynomeilla. (Tarkalleen ottaen määrittelemme laskutoimitukset vastaavaan tapaan kuin polynomeille.) Eli kun jonoja ajattelee generoivina funktioina, niille on helppoa suorittaa operaatioita.

Jonoja  $a = (a_0, a_1, \dots)$  ja  $b = (b_0, b_1, \dots)$  vastaavien generoivien funktioiden  $A(x)$  ja  $B(x)$  summa  $A(x) + B(x)$  määritellään olemaan

$$(a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \dots,$$

ja summa vastaa täten lukujonon  $(a_0 + b_0, a_1 + b_1, \dots)$  generoivaa funktiota.

Tulo määritellään niin ikään vastaavasti kuin polynomeille. Funktioiden  $A(x)$  ja  $B(x)$  tulo  $A(x)B(x)$  on

$$a_0b_0 + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + \dots$$

Yleisesti termin  $x^n$  kerroin on

$$\sum_{m=0}^n a_m b_{n-m},$$

mikä vastaa polynomien kertolaskua.

Miten generoivat funktiot liittyvät lineaarisiin rekursioihin? Ideana on, että jos jono  $a$  toteuttaa rekursioyhtälön karakteristisella polynomilla  $P$ , niin tulossa

$$A(x)(x^{\deg(P)}P(1/x))$$

termin  $x^n$  kerroin on 0 kaikilla  $n \geq \deg(P)$ . (Termien  $1, x, x^2, \dots, x^{\deg(P)-1}$  kertoimet voivat olla nollasta eroavia.) Tämä on suora seuraus tehdyistä määritelmistä. Alla on yksityiskohdat.

Oletetaan, että  $a$  toteuttaa yhtälön

$$a_{n+k} + c_{k-1}a_{n+k-1} + \dots + c_0a_n = 0$$

kaikilla  $n \geq 0$ , missä  $c_0, \dots, c_{k-1}$  ovat vakioita. Nyt  $x^{\deg(P)}P(1/x) = 1 + c_{k-1}x + \dots + c_0x^k$ . Termin  $x^{n+k}$ , missä  $n \geq 0$ , kerroin tulossa  $A(x)(x^{\deg(P)}P(1/x))$  on

$$a_{n+k} + a_{n+k-1}c_{k-1} + \dots + a_{n+1}c_1 + a_n.$$

Tämä on oletuksen nojalla 0.

(Huomataan, että  $x^{\deg(P)}P(1/x)$  on polynomi  $P$  ”väärin päin”. Yksinkertaisuuden vuoksi käytetään merkintää  $\overline{P(x)} = x^{\deg(P)}P(1/x)$ , jolloin  $\overline{P(x)}$  on  $P(x)$  väärin päin.)

Vastaavasti kuin yllä todetaan, että jos generoivan funktion  $A(x)\overline{P(x)}$  lausekkeessa termin  $x^n$  kerroin on 0 kaikilla  $n \geq \deg(P)$ , niin jono  $a$  toteuttaa karakteristista polynomia  $P$  vastaavan rekursioyhtälön.

Aiemmin käytetty termistö ”lukuono  $a$  on nollakohta polynomille  $P$ ” voidaan nyt ajatella niin, että generoivan funktion  $A(x)\overline{P(x)}$  termit  $x^n, n \geq \deg(P)$ , ovat nollia.

Tutkitaan sitten lineaaristen rekursioiden yhtälöparia.

Olkoot  $a$  ja  $b$  kaksi jonoa, jotka toteuttavat yhtälöparin

$$a_{n+k_1} = c_{k_1-1}a_{n+k_1-1} + d_{k_1-1}b_{n+k_1-1} + \dots + c_0a_n + d_0b_n,$$

$$b_{n+k_2} = C_{k_2-1}a_{n+k_2-1} + D_{k_2-1}b_{n+k_2-1} + \dots + C_0a_n + D_0b_n,$$

missä  $k_1$  ja  $k_2$  ovat rekursioiden syvyydet ja luvut  $c_i, d_i, C_i, D_i$  ovat vakioita. Olkoon

$$P_1(x) = x^{k_1} - c_{k_1-1}x^{k_1-1} - \dots - c_0$$

ensimmäisen yhtälön jonoa  $a$  vastaava karakteristinen polynomi ensimmäisessä yhtälössä, ja olkoon vastaavasti

$$Q_1(x) = -(d_{k_1-1}x^{k_1-1} + \dots + d_0)$$

ensimmäisen yhtälön jonoa  $b$  vastaava karakteristinen polynomi. Määritellään vastaavasti  $P_2$  ja  $Q_2$  katsomalla toista yhtälöä.

Yhtälöpari voidaan nyt kirjoittaa muodossa

$$\begin{cases} a(x)\overline{P_1(x)} + b(x)\overline{Q_1(x)} = 0 \\ a(x)\overline{P_2(x)} + b(x)\overline{Q_2(x)} = 0. \end{cases}$$

Tässä ja myöhemmin yhtälö muotoa  $f(x) = 0$  kuvaa sitä, että generoivan funktion  $f$  termin  $x^n$  kerroin on 0 kaikilla tarpeeksi suurilla  $n$ . (Emme tässä keskity kovin tarkasti alkuarvoihin tai ylipäättään pieniin indekseihin, mutta niiden käsittely onnistuu samoilla menetelmillä.)

Yhtälöpari on tietysti mielessä lineaarinen, ja se ratkeaa vastaavasti kuin normaali lineaarinen yhtälöpari.

Kerrotaan ensimmäinen yhtälö generoivalla funktiolla  $\overline{Q_2(x)}$  ja toinen yhtälö funktiolla  $\overline{Q_1(x)}$ , ja vähennetään tulokset toisistaan.<sup>75</sup> Saadaan

$$A(x)(\overline{P_1(x)}\overline{Q_2(x)} - \overline{Q_1(x)}\overline{P_2(x)}) = 0.$$

<sup>75</sup>Tässä käytetään sitä tietoa, että generoivilla funktioilla  $A, B, C$  pätee  $(A(x)B(x))C(x) = A(x)(B(x)C(x))$ , ts. tulon järjestyksellä ei ole väliä. Todistus on sama kuin normaaleillakin polynomeilla (eli suora lasku). Yleisesti generoivia funktioita voi käsitellä pitkälti kuten polynomeja.

Ideana on, että nyt  $a$  toteuttaa rekursioyhtälön, jonka karakteristinen polynomi on  $P_1(x)Q_2(x) - Q_1(x)P_2(x)$ . Tämä perustuu siihen, että polynomin kääntäminen on kiva operaatio: sillä on ominaisuudet

$$\overline{P(x) + Q(x)} = \overline{P(x)} + \overline{Q(x)}$$

ja

$$\overline{P(x)} \overline{Q(x)} = \overline{P(x)Q(x)}.$$

(Tämä ei ole kovin yllättävää ja todistus on taas vain suora, helppo lasku.) Saamme siis, että

$$A(x)\overline{P_1(x)Q_2(x) - Q_1(x)P_2(x)} = 0,$$

eli  $a$  tosiaan toteuttaa polynomia  $P_1(x)Q_2(x) - Q_1(x)P_2(x)$  vastaavan rekursioyhtälön.

Todetaan vielä, että polynomien määritelmästä seuraa  $\deg(P_1) = k_1 > \deg(Q_1)$  ja  $\deg(Q_2) = k_2 > \deg(P_2)$ . Siis polynomia  $P_1(x)Q_2(x) - Q_1(x)P_2(x)$  vastaava lineaarinen rekursioyhtälö ei ole triviaali  $0 = 0$ , eli jono  $a$  toteuttaa epätriviaalin lineaarisen rekursioyhtälön. Olemme valmiit.

Samalla laskulla saadaan, että myös jono  $b$  toteuttaa polynomia  $P_1(x)Q_2(x) - Q_1(x)P_2(x)$  vastaavan rekursioyhtälön. Siis sen lisäksi, että jonot  $a$  ja  $b$  ovat molemmat lineaarisesti rekursiivisia, ne toteuttavat saman rekursioyhtälön.<sup>76</sup>

Menetelmä toimii vastaavasti useammalle kuin kahdelle rekursiolle. Tällöin jonot toteuttavat rekursioyhtälön, jonka karakteristinen polynomi vastaa muodostuvan yhtälöryhmän determinanttia.

<sup>76</sup>Jos jonot  $a$  ja  $b$  toteuttavat karakteristisia polynomeja  $A$  ja  $B$  vastaavat lineaariset rekursiot, niin ne molemmat toteuttavat polynomia  $AB$  vastaavan rekursion. Voimme siis teennäisesti luoda rekursioyhtälön, jonka molemmat jonot toteuttavat. Yhtälöparin tapauksessa jonot kuitenkin toteuttavat ”luonnollisesti” saman rekursioyhtälön: jos jonojen  $a$  ja  $b$  alkuarvot valitaan satunnaisesti, niin hyvin todennäköisesti jonot eivät toteuta rekursioyhtälöä, joka olisi lyhyempi kuin polynomia  $P_1Q_2 - Q_1P_2$  vastaava yhtälö.

## 16 Funktionaaliyhtälöt (Algebra)

Tässä luvussa käydään läpi funktionaaliyhtälötehtäviä sekä yleisimpiä ratkaisuideoita.

Tavallisin funktionaaliyhtälötehtävä on seuraavanlainen: on annettu yhtälö, ja haluamme määrittää kaikki funktiot, jotka toteuttavat annetun yhtälön. Tässä on yksinkertainen esimerkkitehtävä.

### Tehtävä

Määritä kaikki funktiot  $f : \mathbb{R} \rightarrow \mathbb{R}$ , joilla

$$f(x) - f(y) = x - y$$

kaikilla reaaliluvuilla  $x$  ja  $y$ .

Ratkaisu: Olkoon  $f$  jokin funktio, joka toteuttaa ehdot. Pyritään saamaan tietoa funktiosta  $f$ . Yhtälö  $f(x) - f(y) = x - y$  toteutuu kaikilla luvuilla  $x$  ja  $y$ , joten se toteutuu arvolla  $y = 0$ . Siispä  $f(x) - f(0) = x - 0$ , eli

$$f(x) = x + f(0).$$

Luku  $x$  on mielivaltainen, eli  $f(x)$  on yleisesti muotoa  $x + c$  jollain vakiolla  $c$  (joka on tässä  $f(0)$ ). Miten voimme määrittää tämän vakion  $c$ ? Emme mitenkään, koska kaikki tätä muotoa olevat funktiot ovat ratkaisuja: oli  $x$  ja  $y$  mitä tahansa reaalilukuja, niin pätee

$$f(x) - f(y) = (x + c) - (y + c) = x - y.$$

Siis vastaus tehtävään on: kaikki funktiot muotoa  $x + c$ , missä  $c$  on jokin reaaliluku.

---

Funktionaaliyhtälötehtävissä on kaksi osaa:

1. Osoitetaan, että kaikkien ehdot toteuttavien funktioiden tulee olla tiettyä muotoa. Esimerkiksi edellisessä tehtävässä todistettiin, että ehdon toteuttavien  $f$  tulee olla muotoa  $x + c$ .
2. Osoitetaan, että nämä tiettyä muotoa olevat funktiot todella ovat ratkaisuja. Esimerkiksi edellisessä tehtävässä tarkistettiin, että muotoa  $x + c$  olevat funktiot todella toteuttavat alkuperäisen ehdon.

Osa 2 on vain rutiininomaista laskemista, ja tehtävien vaikeus perustuu osan 1 vaikeuteen.

Funktionaaliyhtälöt ovat melko yleisiä kilpailutehtävissä. Yksi syy tälle on, että funktionaaliyhtälöihin on hyvin vähän yleistä teoriaa – ennemminkin on yleisiä temppuja, joita voi yrittää soveltaa. Tämä näkyy tämän luvun sisällössä.

## 16.1 Cauchyn funktionaaliyhtälö

Cauchyn funktionaaliyhtälö on ehkäpä ainoa teoriaa muistuttava asia, jota funktionaaliyhtälöistä voi sanoa. Se on hyvä pitää mielessä.

Cauchyn funktionaaliyhtälöksi kutsutaan funktionaaliyhtälöä

$$f(x + y) = f(x) + f(y).$$

Yleensä oletetaan, että  $f : \mathbb{Q} \rightarrow \mathbb{Q}$  tai  $f : \mathbb{R} \rightarrow \mathbb{R}$ . Esitetään ensiksi ratkaisu rationaaliluvuille.

Osoitetaan, että  $f(x) = cx$  kaikilla  $x$ , missä  $c$  on sopiva vakio. Selvästi tätä muotoa olevat funktiot ovat ratkaisuja (osa 2), joten osoitetaan, että kaikki ratkaisut ovat tätä muotoa (osa 1).

Ensinnäkin  $f(0 + 0) = f(0) + f(0)$ , eli  $f(0) = 0$ . Sijoitetaan  $x = y = 1$ , saadaan  $f(2) = 2f(1)$ . Sijoittamalla  $x = 2, y = 1$  saadaan  $f(3) = f(2) + f(1) = 3f(1)$ . Sijoittamalla  $x = 3, y = 1$  saadaan  $f(4) = f(3) + f(1) = 4f(1)$ . Yleisesti induktiolla saadaan  $f(n) = nf(1)$ , kun  $n$  on positiivinen kokonaisluku.

Sijoituksella  $y = -x$  saadaan  $f(0) = f(x) + f(-x)$ , eli  $f(-x) = -f(x)$ . Täten  $f(-n) = -f(n) = -nf(1)$ , kun  $n$  on positiivinen kokonaisluku. Siis  $f(k) = kf(1)$  kaikilla kokonaisluvuilla  $k$ .

Valitaan sitten jokin rationaaliluku  $\frac{p}{q}$ , ja pyritään osoittamaan, että  $f\left(\frac{p}{q}\right) = \frac{p}{q}f(1)$ . Oletetaan, että  $q > 0$ .

Induktiolla nähdään, että  $f(x_1 + x_2 + x_3 + \dots + x_n) = f(x_1) + f(x_2) + \dots + f(x_n)$  kaikilla rationaaliluvuilla  $x_i$ . Siispä

$$\begin{aligned} pf(1) &= f(p) = f\left(q \cdot \frac{p}{q}\right) \\ &= f\left(\frac{p}{q} + \frac{p}{q} + \dots + \frac{p}{q}\right) \\ &= f\left(\frac{p}{q}\right) + f\left(\frac{p}{q}\right) + \dots + f\left(\frac{p}{q}\right) \\ &= qf\left(\frac{p}{q}\right). \end{aligned}$$

Täten  $f\left(\frac{p}{q}\right) = \frac{p}{q}f(1)$ , ja olemme valmiit.

---

Reaalilukujen tapaus eroaa merkittävästi rationaalilukujen tapauksesta. Vastaa- vasti kuin rationaalilukujen tapauksessa saadaan  $f(r) = rf(1)$  kaikilla  $r \in \mathbb{Q}$ . Matka päättyy tähän: miten ihmeessä saadaan käsiteltyä irrationaalilukuja? Miten saadaan määritettyä vaikkapa  $f(\sqrt{2})$ ? Vastaus: ei mitenkään.

On olemassa ”ikäviä” ratkaisuja Cauchyn funktionaaliyhtälölle, kun  $f : \mathbb{R} \rightarrow \mathbb{R}$ . Nämä ratkaisut ovat erittäin kummallisia: ne ovat esimerkiksi tiheitä siinä mielessä,

että tulostettu kuva niiden kuvaajasta olisi täysin musta.<sup>77</sup> Toistetaan vielä: Cauchyn funktionaaliyhtälön ikävät ratkaisut ovat todella ikäviä.

Jos funktionaaliyhtälöön tehdään esimerkiksi lisäoletus  $f(x) \geq 0$ , kun  $x \geq 0$ , niin silloin ainoat ratkaisut ovat ”mukavat” lineaariset ratkaisut  $f(x) = cx$  vakioilla  $c \geq 0$ . Muita riittäviä lisäoletuksia ovat jatkuvuus jossain pisteessä tai rajoittuneisuus jostain suunnasta jollain välillä  $[a, b]$ , jossa  $a < b$ .

Monet funktionaaliyhtälöt ovat samantyyliä kuin Cauchyn yhtälö, ja on hyvä taito nähdä, milloin ongelman voi palauttaa Cauchyn yhtälöön. Tutkitaan esimerkiksi yhtälöä

$$g(x + y) = g(x)g(y).$$

Tämä voidaan palauttaa Cauchyn funktionaaliyhtälöön seuraavasti.

Sijoittamalla  $x = y$  saadaan  $g(2x) = g(x)^2 \geq 0$ , eli  $g(t) \geq 0$  kaikilla  $t$ . Jos  $g(t) = 0$  jollain  $t$ , niin  $g(t + y) = g(t)g(y) = 0$  kaikilla  $y$ , eli  $g$  on nollafunktio. Muussa tapauksessa  $g(x) > 0$  kaikilla  $x$ . Tällöin voidaan asettaa  $f(x) = \ln(g(x))$ , jolloin  $g(x) = e^{f(x)}$ . Sijoitetaan tämä alkuperäiseen yhtälöön. Saadaan  $e^{f(x+y)} = e^{f(x)+f(y)}$ , eli

$$f(x + y) = f(x) + f(y).$$

## 16.2 Yleisiä ratkaisuiideoita

Vaikka funktionaaliyhtälöihin ei ole yleistä ratkaisumenetelmää, on olemassa muutamia yleinen kikka, joista jokin yleensä antaa jotain hyödyllistä. Tässä luvussa esitetään joitain yleisiä ratkaisuiideoita.<sup>78</sup>

Ensiksi katsellaan funktionaaliyhtälöä ja tehdään helppoja sijoituksia.

**Tärkeää on saada asioita supistumaan.**

Ensimmäisenä tehtävät sijoitukset ovat ne, joilla saa ilmeisiä termejä supistumaan: esimerkiksi  $x = 0$  on usein tällainen sijoitus. Jos yhtälössä esiintyy vaikkapa termi  $f(y - f(x))$ , niin voi sijoittaa  $y = f(x)$ . Tavoitteena on saada ”työkalupakkiin” jotain hyödyllistä funktiosta  $f$ , esimerkiksi  $f(f(x)) = f(x)$ . Yleisesti halutaan jotakin, joka voi auttaa myöhemmin.

Työkalupakissa hyvin usein tärkeäksi osoittautuvat injektiivisyys ja surjektiivisyys.<sup>79</sup>

### Määritelmä

Olkoon  $f$  funktio. Sanotaan, että  $f$  on injektio, jos ehdosta  $f(x) = f(y)$  seuraa  $x = y$ .

<sup>77</sup>Formaalimmin tämä tarkoittaa sitä, että kaikilla tason pisteillä  $P$  on olemassa mielivaltaisen lähellä  $P$ :tä olevia kuvaajan pisteitä  $(x, f(x))$ .

<sup>78</sup>Teksti kuvaa suunnilleen sitä, miten itse lähdän ratkomaan funktionaaliyhtälötehtäviä.

<sup>79</sup>Henkilökohtaisesti teen aina ensimmäisenä nopean injektiivisyys- ja surjektiivisuustarkastelun ja vasta sitten helpot sijoitukset.



**Esimerkki**

Funktio  $f(x) = x$  on injektio, mutta  $g(x) = x^2$  ei ole, koska  $g(-1) = g(1)$ .

Huomautus: Todellisuudessa ominaisuudet riippuvat funktion lähtö- ja maalijoukosta. Esimerkiksi  $g : \mathbb{R} \rightarrow \mathbb{R}$ , jolla  $g(x) = x^2$ , ei ole injektio, mutta  $h : \mathbb{R}_+ \rightarrow \mathbb{R}_+$ , jolla  $h(x) = x^2$ , on injektio. Termien kanssa tulee olla tarkkana.

**Määritelmä**

Olkoon  $f : A \rightarrow B$  funktio. Sanotaan, että  $f$  on surjektio, jos kaikilla  $b \in B$  on olemassa  $a \in A$ , jolla  $f(a) = b$ .

**Esimerkki**

Funktio  $f : \mathbb{R} \rightarrow \mathbb{R}$ , jolla  $f(x) = x$  kaikilla  $x$ , on surjektio. Funktio  $g : \mathbb{R} \rightarrow \mathbb{R}$ , jolla  $g(x) = x^2$ , ei ole surjektio, koska se ei saa esimerkiksi arvoa  $-1$ .

**Määritelmä**

Sanotaan, että funktio  $f$  on bijektio, jos  $f$  on sekä injektio että surjektio.

Injektiivisyyttä tai surjektiivisuutta ei tietenkään kannata yrittää todistaa, jos funktionaaliyhtälöllä ei ole injektivisiä tai surjektiivisiä ratkaisuja. Siksi alussa kannattaa suunnilleen keksiä, mitä ratkaisuja yhtälöllä on. Yleisesti jos yhtälön kaikilla ratkaisuilla pätee vaikkapa  $f(0) = 0$ , voi tämä olla hyvä asia yrittää todistaa.

Kun kaikki ”helpot” sijoitukset ja huomiot on tehty, on kaksi tapausta: tehtävä joko on ratkennut tai ei ole ratkennut. Jälkimmäisessä tapauksessa on usein kuitenkin saatu käsitys siitä, mistä tehtävässä todella on kyse, miksi ongelma on vaikea ja mikä estää ratkaisemasta koko ongelmaa.

## 16.3 Esimerkkitehtäviä

Aloitamme helpommista tehtävistä ja etenemme vaikeampiin.

Ensimmäinen tehtävä on kohtuullisen tunnettu.

**Tehtävä**

Määritä kaikki jatkuvat funktiot  $f : \mathbb{R} \rightarrow \mathbb{R}$ , joilla

$$f(f(x+y)) = f(x) + f(y)$$

kaikilla  $x, y \in \mathbb{R}$ .

Sijoitetaan  $y = 0$ : saamme  $f(f(x)) = f(x) + f(0)$ . Tämä tarkoittaa, että  $f(f(x))$  saadaan ilmoitettua muuttujan  $f(x)$  avulla. Korvataan tämä alkuperäiseen yhtälöön, jolloin saamme

$$f(x+y) + f(0) = f(x) + f(y).$$

Tämä saadaan sijoituksella muutettua Cauchyn funktionaaliyhtälöksi: olkoon  $g(x) = f(x) - f(0)$ . Edellisestä yhtälöstä saadaan  $g(x + y) = g(x) + g(y)$ . Koska  $f$  on jatkuva, niin myös  $g$  on, ja täten ainoa ratkaisu on mukava lineaarinen ratkaisu  $g(x) = kx$ . Nyt  $f(x) = kx + c$  jollain vakiolla  $c$ . Sijoitetaan tämä alkuperäiseen yhtälöön:

$$k(k(x + y) + c) + c = kx + c + ky + c.$$

Vertailemalla muuttujan  $x$  kerrointa saadaan  $k^2 = k$ , eli joko  $k = 0$  tai  $k = 1$ . Jos  $k = 0$ , niin  $c = 0$ , eli ratkaisuksi saadaan nollafunktio. Jos  $k = 1$ , kelpaa luvuksi  $c$  mikä vain, ja saadaan ratkaisu  $f(x) = x + c$ .

Siis kaikki ratkaisut ovat nollafunktio ja  $f(x) = x + c$ .

Seuraava tehtävä on Pohjoismaisesta matematiikkakilpailusta vuodelta 2011.

### Tehtävä

Määritä kaikki funktiot  $f : \mathbb{R} \rightarrow \mathbb{R}$ , joille

$$f(f(x) + y) = f(x^2 - y) + 4yf(x)$$

kaikilla reaaliluvuilla  $x$  ja  $y$ .

Yhtälöllä on ratkaisunaan ainakin nollafunktio. Termi  $x^2$  vihjaa siihen, että  $f(x) = x^2$  tai jokin variantti (jokin toisen asteen polynomi) voisi olla ratkaisu. Helppo tarkistus osoittaaakin, että  $f(x) = x^2$  on ratkaisu:

$$f(f(x) + y) = (x^2 + y)^2 = x^4 + 2x^2y + y^2 = (x^2 - y)^2 + 4yx^2 = f(x^2 - y) + 4yf(x).$$

Tässä saattaa olla kaikki ratkaisut. Tehdään helppoja sijoituksia. Ensiksi  $y = 0$ , josta saadaan

$$f(f(x)) = f(x^2).$$

Luonnollisia yrityksiä ovat myös  $x = 0$ ,  $y = x^2$  ja  $y = -f(x)$ , joilla saadaan asioita supistumaan. Esitettävässä ratkaisussa ei kuitenkaan käytetä näitä, vaan tehdään jotain muuta.

Emme ole löytäneet yhtäkään injektiivistä ratkaisua, joten injektiivisyyttä ei kannata yrittää todistaa. Voidaan kuitenkin katsoa, mitä ehdosta  $f(a) = f(b)$  seuraa. Olkoon  $f(a) = f(b) = c$ . Sijoitetaan vuorotellen  $x = a$  ja  $x = b$  ja annetaan  $y$ :n olla mielivaltainen. Saadaan

$$f(c + y) = f(a^2 - y) + 4yc$$

ja

$$f(c + y) = f(b^2 - y) + 4yc,$$

eli

$$f(a^2 - y) = f(b^2 - y).$$

Tätä voi vielä selkeyttää muuttujanvaihto  $y = a^2 - z$ , jolloin yhtälö on siis

$$f(z) = f(z - (a^2 - b^2)).$$

Tämä yhtälö pätee kaikilla reaaliluvuilla  $z$ . Jos  $a^2 - b^2 \neq 0$ , tarkoittaa tämä, että  $f$  on jaksollinen: funktion  $f$  arvot toistuvat tietyin väliajoin. Jakaudutaan tapauksiin sen mukaan, onko  $f$  jaksollinen vai ei.

*Tapaus 1:  $f$  on jaksollinen.*

Olko  $f(x) = f(x + T)$  kaikilla  $x \in \mathbb{R}$ . Löytämistämme ratkaisusta ainoastaan nollafunktio on jaksollinen, joten pyritään todistamaan, että  $f$ :n tulee olla nollafunktio. Sijoitetaan alkuperäiseen yhtälöön muuttujan  $y$  paikalle  $y + T$ , jolloin

$$f(f(x) + y + T) = f(x^2 - y - T) + 4(y + T)f(x),$$

eli  $f(f(x) + y) = f(x^2 - y) + 4yf(x) + 4Tf(x)$ . Vertaamalla tätä alkuperäiseen yhtälöön saadaan  $4Tf(x) = 0$ . Koska  $x$  oli mielivaltainen, saadaan  $f(x) = 0$  kaikilla  $x$ , eli  $f$  on nollafunktio.

Motivaatio sijoituksen  $y \rightarrow y + T$  takana on se, että tällä saadaan muutettua osaa alkuperäisen yhtälön kohdista ja osa pysyy muuttumattomina.<sup>80</sup> Tällöin saadaan uutta tietoa, kuten yllä.

*Tapaus 2:  $f$  ei ole jaksollinen.*

Päädyimme jatkuvuuskysymykseen ehdosta  $f(a) = f(b)$ , josta seurasi  $f(z) = f(z - (a^2 - b^2))$ . Jos  $f$  ei ole jaksollinen, niin ehdosta  $f(a) = f(b)$  seuraa  $a^2 = b^2$  eli  $a = \pm b$ : ei aivan injektivisyys, mutta melkein.

Miten voisimme hyödyntää tätä ehtoa? Haluamme  $f(\text{jotain}_1) = f(\text{jotain}_2)$ , josta saisimme  $\text{jotain}_1 = \pm \text{jotain}_2$ . Alkuperäistä yhtälöä tutkimalla nähdään, että tähän päästään (jo ratkaisun alussa tehdyllä sijoituksella)  $y = 0$ : saamme

$$f(f(x)) = f(x^2),$$

eli  $f(x) = \pm x^2$  kaikilla  $x$ .

Huomaa, että tiedämme, että jokaisella  $x$ :n arvolla pätee  $f(x) = x^2$  tai  $f(x) = -x^2$ . **Emme vielä tiedä, voiko merkki vaihtua kesken kaiken.** Voisi vaikkapa olla, että  $f(x) = x^2$ , kun  $x > 123$ , ja muulloin  $f(x) = -x^2$ . On hyvin yleinen virhe vain tarkistaa, että  $f(x) = -x^2$  ei ole ratkaisu alkuperäiseen yhtälöön, ja todeta, että  $f(x) = x^2$ . Virhe on oikeastaan niin yleinen, että sillä on oma nimensä: Pointwise trap.

Miten ansalta vältetään? Lähdetään siitä, mitä haluamme todistaa: haluamme osoittaa, että  $f(a) \neq -a^2$  kaikilla  $a$  (jotka eivät ole 0). Oletetaan, että tällainen  $a$  on, ja pyritään saamaan ristiriita. Sijoitetaan vaikka  $x = a$ , jolloin saadaan

$$f(y - a^2) = f(a^2 - y) - 4ya^2$$

eli

$$\pm(y - a^2) = \pm(a^2 - y) - 4ya^2$$

---

<sup>80</sup>Tämä on yleinen ajatus: "Mikä muuttuu ja mikä ei muutu?"

Jokainen merkkien yhdistelmä johtaa yhtälöön muotoa

$$c(y - a^2) = 4ya^2,$$

missä  $-2 \leq c \leq 2$  on kokonaisluku. Tämä voidaan ajatella polynomiyhtälönä muuttujan  $y$  suhteen. Vakioiden tulee olla puolittain samat, eli  $-a^2c = 0$ . Oletimme, että  $a \neq 0$ , eli  $c = 0$ . Mutta tällöin  $4ya^2 = 0$  kaikilla  $y$ , mikä ei tietenkään käy.

Olemme siis todistaneet, että  $f(a) \neq -a^2$  kaikilla  $a$ , joten tulee olla  $f(a) = a^2$  kaikilla  $a$ . Tämä päättää ratkaisun.

Kommentti: Tehtävän ratkaisu oli suhteellisen pitkä, mutta tämä ei kerro suoraan ratkaisun vaativuudesta. Monet kohdista ovat tyyppiä ”tulee vain tehdä jotain”. Esimerkiksi tapauksessa 1 riittää vain jotenkin käyttää jaksollisuutta. Yksi luonnollisimmista tavoista on juuri  $y \rightarrow y + T$ , ja tämä toimi. Toinen esimerkki on tapauksessa 2 käytetty ”melkein injektiivisyyden” soveltaminen, ja tässäkin  $y = 0$  on yksi luonnollisimmista vaihtoehdoista.

Itse injektiivisyydestä tarkastelun kokeileminen voi tuntua vaikealta kohdalta. Injektiivisyys on hyvin yleinen työkalu, joten tämäkin askel on jossain määrin vain ”yleinen temppu”.

Seuraava tehtävä on esiintynyt lukuisissa eri kilpailuissa.

### Tehtävä

Määritä kaikki funktiot  $f : \mathbb{Z} \rightarrow \mathbb{Z}$ , joilla

$$f(m - n + f(n)) = f(m) + f(n)$$

kaikilla kokonaisluvuilla  $m$  ja  $n$ .

Harjoitus lukijalle: keksitkö, mitkä ratkaisut funktionaaliyhtälöllä on?

Jälleen voidaan tehdä helppoja sijoituksia, kuten  $m = 0$ ,  $n = 0$ ,  $m = n$  tai  $m = n - f(n)$ . Henkilökohtaisesti tykkään injektiivisyys- ja surjektiivisuustarkasteluista, joten aloitetaan niillä.

Surjektiivisuutta yhtälöstä on vaikea saada: kaikki on funktion  $f$  sisässä. (Lisäksi tulemme näkemään, että yhtälöllä ei ole yhtäkään surjektiivista ratkaisua.) Tutkitaan siis injektiivisyyttä: oletetaan, että  $f(a) = f(b) = c$ . Sijoitetaan  $m = a$  ja  $m = b$ . Saadaan

$$f(a - n + f(n)) = c + f(n)$$

ja

$$f(b - n + f(n)) = c + f(n).$$

Saamme siis  $f(a - n + f(n)) = f(b - n + f(n))$ . Tämä on jaksollisuuden henkinen, mutta tällä on vaikea tehdä mitään, koska emme tiedä, mitä arvoja  $f(n) + n$  saa. Yritetään sittenkin sijoituksia  $n = a$  ja  $n = b$ . Saadaan

$$f(m - a + c) = f(m) + c$$

ja

$$f(m - b + c) = f(m) + c.$$

Nämä antavat jaksollisuuden, jos  $f$  ei ole injektio. Voimme jälleen jakautua kahteen tapaukseen.

*Tapaus 1:  $f$  on jaksollinen.*

Olkoon  $f(n) = f(n + T)$  kaikilla  $n \in \mathbb{Z}$ . Voisimme yrittää tehdä sijoituksia  $m \rightarrow m + T$  tai  $n \rightarrow n + T$ . Tämä ei kuitenkaan hyödytä mitään: emme saa mitään uutta tietoa.

Mitä jaksollisuus kertoo? Funktion  $f$  arvot toistuvat tietyin väliajoin. Koska  $f$  on funktio  $\mathbb{Z} \rightarrow \mathbb{Z}$ , saa  $f$  vain äärellisen monta eri arvoa. Voidaanko näistä arvoista sanoa jotain?

Olkoon  $y$  suurin arvo, jonka  $f$  saa, ja olkoon  $f(x) = y$ . Sijoitetaan  $m = n = x$ , jolloin yhtälö antaa

$$f(y) = 2y.$$

Siis  $f$  saa arvon  $2y$ . Koska  $y$  oli suurin arvo, saadaan  $2y \leq y$  eli  $y \leq 0$ . Funktio  $f$  ei täten saa positiivisia arvoja. Vastaavasti voidaan tutkia pienintä arvoa  $z$ , ja saada  $2z \geq z$  eli  $z \geq 0$ . Täten  $f$  ei saa negatiivisia arvoja. Siispä  $f$ :n tulee olla nollafunktio.

*Tapaus 2.  $f$  on injektio.*

Haluaisimme soveltaa injektiiivisyyttä. Jos jollain  $m$  pätee  $f(m) = 0$ , saadaan

$$f(m - n + f(n)) = f(n)$$

eli  $m - n + f(n) = n$ . Tästä seuraisi  $f(n) = 2n - m$ , ja olisimme käytännössä valmiit (sijoitetaan alkuperäiseen yhtälöön  $f(x) = 2x + c$ , ja todetaan arvon  $c = 0$  olevan ainoa ratkaisu). Ei kuitenkaan ole ilmeistä, miten tällaisen  $m$  olemassaolo todistetaan.

Toinen lähestymistapa olisi valita kaksi lukuparia  $(m_1, n_1)$  ja  $(m_2, n_2)$  niin, että  $f(m_1) + f(n_1) = f(m_2) + f(n_2)$ . Tällöin annetun yhtälön oikean puolen arvo on sama parien välillä, joten myös vasemman puolen arvo on sama. Tästä saamme

$$f(m_1 - n_1 + f(n_1)) = f(m_2 - n_2 + f(n_2)),$$

ja pääsemme käyttämään injektiiivisyyttä.

Miten voidaan varmistaa ehto  $f(m_1) + f(n_1) = f(m_2) + f(n_2)$ ? Helppo valinta  $m_1 = n_2 = a$  ja  $n_1 = m_2 = b$  ainakin toimii, ja tästä saamme

$$f(a - b + f(b)) = f(b - a + f(a)).$$

Nyt  $a - b + f(b) = b - a + f(a)$ . Sijoitetaan vaikkapa  $a = 0$ , jolloin  $f(b) = 2b + f(0)$ . Koska  $b$  oli mielivaltainen, tämä pätee kaikilla  $b$ . Sijoittamalla tämän alkuperäiseen yhtälöön saadaan ratkaisu  $f(n) = 2n$ .

Yhtälöllä on siis kaksi ratkaisua: nollafunktio ja  $f(x) = 2x$  kaikilla  $x$ .

Kommentti: Kokonaisluvuilla määritellyt funktionaaliyhtälöt toimivat eri tavalla kuin reaaliluvuilla määritellyt. Tapauksessa 1 todettiin jaksollisuudesta seuraavan, että  $f$  saa vain äärellisen monta arvoa: tämä ei päde reaaliluvuilla, ja tangenttifunktio jopa saa kaikki reaalilukuarvot jaksollisuudestaan huolimatta.

Tapauksessa 2 käytetty muuttujien  $m$  ja  $n$  vaihtaminen päittäin on yleinen temppu, jota voi käyttää silloin, kun yhtälön toinen puoli on symmetrinen muuttujien suhteen, mutta toinen puoli ei ole.

Luvun viimeinen ja vaikein esimerkki on vuoden 2012 Turkin kansallisessa kilpailussa esiintynyt tehtävä. Tehtävä on esiintynyt myös Suomen IMO-joukkueen valintakokeessa.

### Tehtävä

Määritä kaikki kasvavat funktiot  $f : \mathbb{R} \rightarrow \mathbb{R}$ , joilla

$$f(f(x^2) + y + f(y)) = x^2 + 2f(y)$$

kaikilla reaaliluvuilla  $x$  ja  $y$ .

Yhtälöllä on ratkaisu  $f(x) = x$ , ja tämä on varmaankin ainoa ratkaisu.

Huomataan, että termit  $x^2$  voidaan vain korvata muuttujalla  $x$  ja vaatia  $x \geq 0$ . Siis

$$f(f(x) + y + f(y)) = x + 2f(y)$$

kaikilla reaaliluvuilla  $x \geq 0$  ja  $y$ . Tutkitaan loppuratkaisun ajan vain tätä yhtälöä.

Aloitetaan injektiivisyydestä ja surjektiivisuudesta. Injektiivisyys seuraa suoraan epänegatiivisille luvuille: jos  $f(a) = f(b)$  joillain  $a, b \geq 0$ , niin sijoittamalla  $x = a$  ja  $x = b$  ja vertaamalla saadaan  $a = b$ .

Toinen lähestymistapa on sijoittaa  $y = a$  ja  $y = b$ . Saadaan

$$f(f(x) + a + c) = f(f(x) + b + c).$$

Emme vielä tiedä, mitä arvoja  $f(x)$  saa, joten tutkitaan surjektiivisuutta ja palataan sitten tähän.

Hyödynnetään vapaata muuttujaa  $x$  ja asetetaan  $y = 0$ . Antamalla  $x$ :n käydä läpi kaikki epänegatiiviset arvot yhtälön oikea puoli käy läpi arvot väliltä  $[2f(0), \infty[$ . Siispä  $f$  saa kaikki tarpeeksi suuret arvot.

Palataan yhtälöön  $f(f(x) + a + c) = f(f(x) + b + c)$ . Jos  $f$  ei ole injektio, niin  $f$  on jaksollinen tarpeeksi suurilla arvoilla muuttujan  $x$  arvoilla. Voimme jakautua tapauksiin...

Jaksollisuus suurilla arvoilla ei käy, koska  $x \rightarrow x + T$  pitää vasemman puolen puolen vakiona, mutta oikea puoli kasvaa arvolla  $T$ . Siispä  $f$  on injektio.

Yritetään soveltaa injektiivisyyttä. Naiivi tapa tälle on valita  $x = -f(y)$  (tämä

vaatii  $f(y) \leq 0$ , jolloin saadaan

$$f(f(-f(y)) + y + f(y)) = f(y),$$

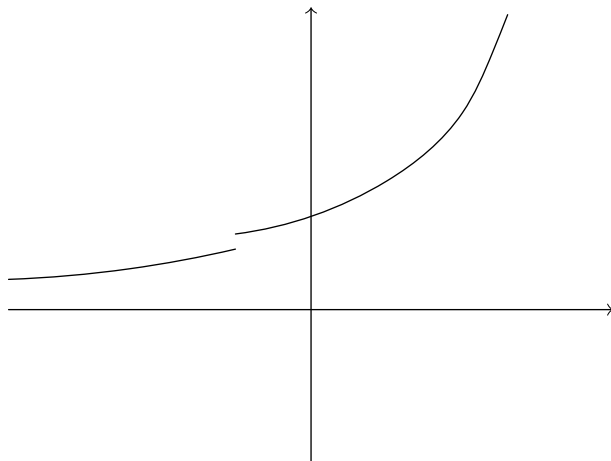
eli injektiivisyydellä  $f(-f(y)) + f(y) = 0$ . Kirjoitetaan tämä muodossa  $f(-f(y)) = -f(y)$ . Siis  $f(z) = z$  kaikilla arvoilla  $z$ , jotka  $-f(y)$  saa – paitsi että pitää huomioida tehty oletus  $f(y) \leq 0$ . Jos tietäisimme, että  $f$  on surjektio, saisimme  $f(z) = z$  kaikilla  $z \geq 0$ . Tutkitaan ensiksi, saako tästä  $f(z) = z$  kaikille  $z$ , ja keskitytään sitten surjektiivisuuteen.

Oletetaan, että  $f(x) = x$  kaikilla  $x \geq 0$ . Haluamme tehdä annettuun yhtälöön sijoituksen, jolla saadaan  $f(x) = x$  arvoilla  $x < 0$ . Koska emme saa asettaa muuttujan  $x$  arvoksi negatiivisia lukuja, on luontevaa antaa  $y$ :n olla mielivaltainen negatiivinen luku ja valita  $x$  sopivasti. Tämä toimii: Olkoon  $y$  mielivaltainen, ja olkoon  $x$  sellainen, että  $x \geq \max(-(y + f(y)), 0)$ . Nyt

$$f(f(x) + y + f(y)) = f(x + y + f(y)),$$

ja koska  $x \geq -(y + f(y))$ , saadaan  $f(x + y + f(y)) = x + y + f(y)$ . Vertaamalla tätä annetun yhtälön oikeaan puoleen  $x + 2f(y)$  saadaan vihdoin  $y = f(y)$ .

Enää on jäljellä surjektiivisuuden todistaminen. Jos  $f$  saa arvon  $t$ , niin valitsemalla  $y$  niin, että  $f(y) = t$ , voidaan todeta, että  $f$  saa kaikki arvot, jotka ovat vähintään  $2t$ . Jos  $f$  siis saisi arvon  $-1$ , se saisi myös arvot, jotka ovat vähintään  $\geq -2$ , eli myös arvot vähintään  $-4$  ja niin edelleen. Siis jos  $f$  ei ole surjektio, niin  $f$ :n arvoilla on jokin epänegatiivinen alaraja. Lisäksi koska  $f$  on kasvava, tarkoittaisi tämä sitä, että  $f$ :n kuvaaja näyttäisi joltain tämän tyyliseltä:



Kuvaajassa siis voisi olla hyppäyksiä, mutta arvot lähellä  $-\infty$  lähestyisivät jotain alarajaa.

Merkitään tätä alarajaa arvolla  $c$ . Siis  $f$  saa arvoja, jotka ovat mielivaltaisen lähellä lukua  $c$ , mutta arvot eivät mene koskaan luvun  $c$  alle. Annetaan funktionaaliyhtälössä muuttujan  $y$  lähestyä pistettä  $-\infty$  ja pidetään  $x$  jonakin vakiona. Vasen puoli lähestyy nyt arvoa

$$f(f(x) + y + f(y)) \rightarrow f(f(x) + (-\infty) + c) \rightarrow c$$

ja oikea puoli arvoa

$$x + 2f(y) \rightarrow x + 2c.$$

Kunhan  $x \neq -c$ , olemme saaneet ristiriidan. Alarajaa ei siis voi olla, joten  $f$  saa mielivaltaisen pieniä arvoja ja täten kaikki arvot. Näin ollen  $f$  on surjektio, ja olemme valmiit.

Kommentti: Tämä on esimerkki vaikeasta tehtävästä, jossa pelkästään rutiininomaiset sijoitukset eivät riitä ratkaisuun. Niillä kuitenkin sai injektiivisyyden, ja lisäksi saatiin selville, mistä on todella kyse: funktion  $f$  surjektiivisuudesta. Tutkimalla funktion  $f$  käyttäytymistä saatiin myös surjektiivisuus.



## 17 Lisätehtäviä (Algebra)

Tässä luvussa käydään läpi haastavampia algebran tehtäviä.

Ensimmäinen tehtävä on vuoden 2012 ELMOn lyhytlistalta.

### Tehtävä

Olkoot  $a_0$  ja  $b_0$  positiivisia kokonaislukuja. Määritellään  $a_{i+1} = a_i + \lfloor \sqrt{b_i} \rfloor$  ja  $b_{i+1} = b_i + \lfloor \sqrt{a_i} \rfloor$  kaikilla  $i \geq 0$ . Osoita, että on olemassa positiivinen kokonaisluku  $n$ , jolla  $a_n = b_n$ .

Jos  $a_i$  on paljon suurempi kuin  $b_i$ , niin mentäessä luvusta  $b_i$  lukuun  $b_{i+1}$  kasvu on suurempaa kuin mentäessä luvusta  $a_i$  lukuun  $a_{i+1}$ . Idea on siis, että  $a_i$  ja  $b_i$  lähenevät aina toisiaan ja jostain pisteestä lähtien lukujonot ovat samat.

Ennen kuin mennään asioiden edelle, todistetaan pari luonnollista huomiota lukujonoista  $a_i$  ja  $b_i$ . Ensimmäinen huomio on, että jos  $a_i \geq b_i$ , niin silloin myös  $a_{i+1} \geq b_{i+1}$ . Tämän todistaminen vaatii hieman työtä, mutta se ei ole erityisen vaikeaa. Epäyhtälö  $a_{i+1} \geq b_{i+1}$  on ekvivalentti epäyhtälön

$$a_i + \lfloor \sqrt{b_i} \rfloor \geq b_i + \lfloor \sqrt{a_i} \rfloor$$

kanssa. Neliöjuurien lattiafunktioiden käsittelyä varten kirjoitetaan  $b_i = k^2 + r$ , missä  $k$  ja  $0 \leq r \leq 2k$  ovat kokonaislukuja. Nyt siis  $k^2 \leq b_i < (k+1)^2$ , eli  $\lfloor \sqrt{b_i} \rfloor = k$ . Tutkitaan paria tapausta.

*Tapaus 1:* Pätee  $k^2 \leq a_i < (k+1)^2$ . Tällöin  $\lfloor \sqrt{a_i} \rfloor = \lfloor \sqrt{b_i} \rfloor$ , joten väite seuraa oletuksesta  $a_i \geq b_i$ .

*Tapaus 2:* Pätee  $a_i \geq (k+1)^2$ . Ideana on, että nyt  $a_i$  on niin paljon suurempi kuin  $b_i$ , että pätee  $a_i + \lfloor \sqrt{b_i} \rfloor \geq b_i + \lfloor \sqrt{a_i} \rfloor$ , vaikka oikean puolen termi  $\lfloor \sqrt{a_i} \rfloor$  on suurempi kuin vasemman puolen termi  $\lfloor \sqrt{b_i} \rfloor$ . Kirjoitetaan  $(k+m)^2 \leq a_i < (k+m+1)^2$ , missä  $m \geq 1$ . Nyt epäyhtälö saadaan muotoon

$$a_i \geq b_i + m.$$

Käydään nopeasti läpi kaksi osatapausta.

*Tapaus 2.1:*  $m = 1$ . Tällöin epäyhtälö pätee, koska  $a_i > b_i$ .

*Tapaus 2.2:*  $m \geq 2$ . Tässä tapauksessa  $a_i - b_i$  on jo hyvin suuri ja tarvittavat helpot arviot saa vaikka seuraavasti:

$$a_i \geq (k+m)^2 = k^2 + 2mk + m^2 \geq k^2 + 2k + m^2 \geq k^2 + 2k + m + 1 = (k+1)^2 + m > b_i + m.$$

Oletetaan tästä lähtien, että  $a_0 \geq b_0$ , jolloin kaikilla  $i$  pätee  $a_i \geq b_i$ .

Seuraava luonnollinen huomio on, että erotukset  $a_i - b_i$  eivät koskaan kasva. Tämän todistaminen on helpompaa kuin aiemman huomion. Väite seuraa yksinkertaisesti oletuksella  $a_i \geq b_i$ :

$$a_{i+1} - b_{i+1} = a_i - b_i + (\lfloor \sqrt{b_i} \rfloor - \lfloor \sqrt{a_i} \rfloor) \leq a_i - b_i.$$

Tiedämme siis, että  $a_i - b_i \geq 0$  kaikilla  $i$  ja että  $a_i - b_i$  ei koskaan kasva. Olemme melkein ratkaisseet tehtävän: enää tulee poissulkea tilanne, jossa erotukset  $a_i - b_i$  pysyvät (nollasta eroavana) vakiona jostain kohdasta lähtien. Tehdään vastaoletus: oletetaan, että kaikilla tarpeeksi suurilla  $i$  pätee  $a_i - b_i = c$  jollain  $c \neq 0$  (jolloin  $c > 0$ ).

Sijoitetaan rekursioyhtälöihin saatu yhtälö  $a_i = b_i + c$ . Saadaan

$$b_{i+1} + c = b_i + c + \lfloor \sqrt{b_i} \rfloor$$

ja

$$b_{i+1} = b_i + \lfloor \sqrt{b_i + c} \rfloor.$$

Tämä tarkoittaa, että  $\lfloor \sqrt{b_i + c} \rfloor = \lfloor \sqrt{b_i} \rfloor$  kaikilla tarpeeksi suurilla  $i$ . Toisin sanoen välillä  $(b_i, b_i + c]$  ei ole neliölukua millään suurella  $i$ . Jotta vaikein tapaus  $c = 1$  saataisiin poissuljettua, tulisi luvun  $b_i + 1$  olla neliöluku jollain  $i$ .

Lähdetään siis ylemmän yhtälön määritelmästä  $b_{i+1} = b_i + \lfloor \sqrt{b_i} \rfloor$  ja yritetään todistaa, että  $b_i + 1$  on neliöluku jollain  $i$ . Yksi idea on tutkia erikoistapauksia ja saada tätä kautta intuitiota.

*Erikoistapaus 1:* Luku  $b_i$  on neliöluku jollain  $i$ . Kirjoitetaan  $b_i = k^2$ . Nyt  $b_{i+1} = k^2 + k$  ja  $b_{i+2} = k^2 + 2k$ , mikä on yhden vaille neliöluku  $(k+1)^2 = k^2 + 2k + 1$ . Tämä tapaus on kunnossa.

*Erikoistapaus 2:* Luku  $b_i$  on muotoa  $k^2 + 1$  jollain  $i$ . Laskemalla saadaan  $b_{i+1} = b_i + k = k^2 + k + 1$  ja  $b_{i+2} = k^2 + 2k + 1 = (k+1)^2$ . Ongelma on palautettu ensimmäiseen erikoistapaukseen.

Tutkimalla tarvittaessa vielä erikoistapausta  $b_i = k^2 + 2$  huomataan säännönmukaisuus: luvusta  $k^2 + t$  siirrytään kahdella askeleella lukuun  $(k+1)^2 + (t-1)$ . Jos tämä pätee, niin olemme valmiit, koska lopulta kaikki palautuu erikoistapaukseen 1. Seuraavaksi todistetaan tämä väite.

Kirjoitetaan siis  $b_i = k^2 + t$ , missä  $t \leq 2k$ . Saadaan

$$b_{i+1} = b_i + k = k^2 + (t+k).$$

Haluaisimme vetää johtopäätöksen  $b_{i+2} = b_{i+1} + k = (k+1)^2 + (t-1)$ . Tämä pätee kuitenkin vain silloin, kun  $\lfloor \sqrt{b_{i+1}} \rfloor = k$  eli kun  $t \leq k$ . Ongelma on kuitenkin helppo ratkaista: Jos yhtälössä  $b_i = k^2 + t$  pätee  $t > k$ , niin kirjoitetaan  $s = t - k$ . Nyt

$$b_{i+1} = k^2 + (t+k) = k^2 + (s+2k) = (k+1)^2 + (s-1)$$

ja  $0 \leq s-1 \leq (k+1)$ , joten päädyimme edellä käsitellyyn tapaukseen, jossa  $t$  on pieni. Olemme valmiit.

Kommentti: Ratkaisussa esitetyt väitteet ”erotus  $a_i - b_i$  ei koskaan kasva”, ”erotus  $a_i - b_i$  on aina vähintään 0” ja ”erotus  $a_i - b_i$  ei voi olla positiivinen vakio jostain kohdasta lähtien” kertovat paljon lukujonojen  $a_i$  ja  $b_i$  käyttäytymisestä. Jokaisen yksittäisen väitteen todistus on suhteellisen helppo, mutta kokonaisessa ratkaisussa tulee huomata jokainen näistä tuloksista, mistä syntyy osa tehtävän vaikeudesta.

Viimeistä kysymystä koskien tilannetta  $a_i - b_i = c$  varten ratkaisussa tutkittiin erikoistapauksia  $b_i = k^2$  ja  $b_i = k^2 + 1$ , joiden kautta huomattiin säännönmukaisuus. Konkreettisten erikoistapauksien käsitteleminen ei välttämättä vaadi pienillä luvuilla kokeilujen tekemistä. Mielestäni tässä tilanteessa on oikeastaan helpompaa huomata säännönmukaisuus tutkimalla yleisesti tapausta  $b_i = k^2$  kuin tutkimalla vaikkapa tapausta  $b_i = 9$ . Lisäksi laskuvirheen mahdollisuus on pienempi (ainakin jos on hyvä rutiini lausekkeiden käsittelystä).

Seuraava tehtävä on vuoden 2018 European Mathematical Cup -kilpailusta.

### Tehtävä

Mille reaailuvuille  $k > 1$  on olemassa rajoitettu, positiivisista reaailuvuista koostuva joukko  $S$ , jossa on vähintään 3 alkioita ja jolla

$$k(a - b) \in S$$

kaikilla  $a, b \in S$ , joilla  $a > b$ ?

(Positiivisista reaailuvuista koostuvaa joukkoa  $S$  kutsutaan rajoitetuksi, jos on olemassa sellainen reaailuku  $M$ , että kaikilla  $x \in S$  pätee  $x < M$ .)

Aloitetaan ratkaisuprosessi tutkimalla joitain erikoistapauksia. Ensin on esitetty sekalaisia ajatuksia.

Mitä tapahtuu, jos  $S$  sisältää vaikkapa luvut 1 ja 2? Tällöin saadaan esimerkiksi  $k(2 - 1) = k \in S$ ,  $k(2 - k) \in S$  ja  $k(k - 1) \in S$ . Tämä ei vaikuta kovin hyödylliseltä, joten yritetään jotain muuta.

Tehtävänannossa vaaditaan, että  $S$  sisältää vähintään kolme lukua. Onko olemassa kahden kokoista esimerkkiä? Jos  $S = \{a, b\}$ , missä  $a > b$ , tulee olla

$$k(a - b) \in S = \{a, b\}.$$

Jos  $k(a - b) = a$ , pätee  $b = \frac{k-1}{k}a$ , mistä saadaan yksi ratkaisu. Jos taas  $k(a - b) = b$ , niin

$$a = b \frac{k+1}{k},$$

mistä saadaan toinen ratkaisu.

Huomaamme, että kelpaavasta joukosta  $S$  saa uuden kelpaavan joukon kertomalla kaikki joukon  $S$  alkioit jollain (positiivisella) vakiolla.

Onko olemassa kolmen kokoista kelpaavaa joukkoa  $S$ ? Kirjoitetaan  $S = \{a, b, c\}$ , missä  $a > b > c$ . Luvut

$$k(a - b), k(a - c) \text{ ja } k(b - c)$$

ovat kaikki joukon  $S$  alkioita. Näiden lukujen keskinäisistä suuruusjärjestyksistä voidaan sanoa  $k(a - c) > k(b - c)$  ja  $k(a - c) > k(a - b)$ . Täten luku  $k(a - c)$  on joko  $a$  tai  $b$ , ja vastaavasti luvut  $k(b - c)$  ja  $k(a - b)$  ovat joko  $b$  tai  $c$ .

Ongelma jakautuu melko moneen tapaukseen:

1.  $k(a - c) = b$ ,  $k(b - c) = c$  ja  $k(a - b) = c$ .
2.  $k(a - c) = a$ ,  $k(b - c) = b$  ja  $k(a - b) = b$ .
3.  $k(a - c) = a$ ,  $k(b - c) = b$  ja  $k(a - b) = c$ .
4.  $k(a - c) = a$ ,  $k(b - c) = c$  ja  $k(a - b) = b$ .
5.  $k(a - c) = a$ ,  $k(b - c) = c$  ja  $k(a - b) = c$ .

Tapauksissa 1, 2 ja 5 pätee, että  $b - c = a - b$  eli että luvut  $a$ ,  $b$  ja  $c$  muodostavat aritmeettisen lukujonon. Oletetaan vaikka, että  $b = 1$ , jolloin pätee  $c = 1 - d$  ja  $a = 1 + d$ , missä  $d$  on lukujonon erotusvakio. Tulee päteä  $kd \in S$  ja  $2kd \in S$ . Pieni tapauskäsittely (jonka yksityiskohdat sivuutetaan) antaa ratkaisun  $k = 2$ . Tämä vastaa erotusvakiota  $d = \frac{1}{3}$ .

Tapaukset 3 ja 4 voi käsitellä vaikka seuraavasti. Tapauksessa 3 pätee

$$k(a - c) - k(b - c) - k(a - b) = a - b - c.$$

Vasen puoli on yhtä kuin 0, joten  $a = b + c$ . Tapauksessa 4 saadaan vastaavasti  $a = b + c$ . Molemmissa tapauksissa voimassa oleva ehto  $k(a - c) = a$  antaa nyt  $kb - b = c$ , jolloin  $a = kb$ . Tästä ei ole enää vaikeaa viedä laskuja maaliin. Yksityiskohdat sivuutetaan, mutta luvulle  $k$  saadaan yhtälö  $k^2 - k = 1$ , ja ratkaisemalla toisen asteen yhtälö saadaan ratkaisu

$$k = \frac{1 + \sqrt{5}}{2}.$$

(Luvun  $k$  tulee olla yli 1, joten toinen yhtälön  $k^2 - k = 1$  ratkaisusta ei käy.)

Hengähdetään hetki. Edellä tutkittiin tapausta  $|S| = 3$  ja löydettiin kaksi ratkaisua. Tämä on tietysti edistystä: löysimme joitain kelpaavia luvun  $k$  arvoja. Laskeminen on kuitenkin raskasta, ja yleistä tapausta ei voi vain laskea läpi. Yritetään keksiä jokin strategia, jolla tehtävän voisi saada ratkaistua kokonaan.

Olemme tähän mennessä käsitelleet vain äärellisiä joukkoja  $S$ . Tehtävässä on kuitenkin myös mahdollista, että  $S$  on ääretön. Ehto ”joukko  $S$  on rajoitettu” onkin mielenkiintoinen ainoastaan äärettömillä joukoilla  $S$ .

Tästä motivoituneena voisimme ensiksi yrittää ratkaista tapauksen, jossa  $S$  on ääretön. Palataan tämän jälkeen äärellisten joukkojen tapaukseen, ja yritetään löytää näille jokin yleisesti toimiva menetelmä.

Oletetaan, että  $S$  sisältää äärettömän monta alkioita.

Selvästikin joukon  $S$  rajoittuneisuus on tärkeä oletus (eihän sitä muuten olisi annettu).<sup>81</sup> Oletetaan siis, että kaikilla  $x \in S$  pätee  $x < M$ .

<sup>81</sup>On oikeastaan hyvin yksinkertaista luoda äärettömiä joukkoja  $S$ , joilla  $k(a - b) \in S$  kaikilla  $a, b \in S$ ,  $a > b$ . Yksi esimerkki:  $k$  on kokonaisluku,  $S = \{1, 2, 3, 4, \dots\}$ . Toinen esimerkki: lisätään joukkoon  $S$  alkio 1 ja 2, ja lisätään aina luku  $k(a - b)$  joukkoon  $S$ , kun  $a$  ja  $b$  ovat joukon  $S$  alkioita.

Mietitään joukon  $S$  alkioden sijoittumista reaaliakselille. Tiedämme, että näitä pisteitä on äärettömästi ja että jokainen piste on välillä  $(0, M)$ . Näiden pisteiden joukossa on sellaisia pisteitä, jotka ovat enintään etäisyydellä  $\frac{1}{1000}$  toisistaan (muutenhan pisteitä olisi enintään  $1000M$ ). Jos pätee  $|a - b| < \frac{1}{1000}$  ja  $a > b$ , kun  $a, b \in S$ , niin nyt ehdon nojalla  $k(a - b) \in S$ , eli  $S$  sisältää jonkin alkion, joka on alle  $\frac{k}{1000}$ . Korvaamalla luvun 1000 yleisesti jollain mielivaltaisen suurella luvulla saadaan, että  $S$  sisältää mielivaltaisen pieniä lukuja.

Entä sitten? Miksei  $S$  voisi sisältää vaikka kaikkia lukuja väliltä  $(0, M)$ ? Tämän esimerkin toimimattomuus nähdään valitsemalla  $a$  olemaan hyvin suuri luku (noin  $M$ ) ja  $b$  olemaan hyvin pieni luku (noin 0). Tällöin ehdon  $k > 1$  avulla saadaan

$$k(a - b) \approx kM > M,$$

eli tällöin  $k(a - b)$  ei ole enää joukossa  $S$ . Tämän idean voi yleistää kaikille äärettömille  $S$  seuraavasti.

Olkoon  $M$  sellainen reaaliluku, jolla  $x < M$  kaikilla  $x \in S$ . Valitaan tämä  $M$  lisäksi niin, että on olemassa jokin luku  $x$ , jolla  $x > \frac{M}{k}$  ja jolla  $x \in S$  (haluamme siis, että  $M$  on suunnilleen samaa kokoluokkaa kuin joukon  $S$  suurimmat alkiot).<sup>82</sup> Olkoon  $y$  sellainen joukon  $S$  alkio, jolla  $y < x - \frac{M}{k}$  (tällainen  $y$  on olemassa, koska  $S$  sisältää mielivaltaisen pieniä lukuja). Nyt

$$k(x - y) > k \cdot \frac{M}{k} > M,$$

joten  $k(x - y) \notin S$ , mikä on ristiriita.

Oletetaan sitten, että  $S$  sisältää vain äärellisen monta alkioita  $a_1, a_2, \dots, a_n$ . Oletetaan, että  $a_1 > a_2 > \dots > a_n$ . Tiedämme siis, että  $k(a_i - a_j)$  on jokin luvuista  $a_1, \dots, a_n$ , olivat  $i$  ja  $j$  ( $i < j$ ) mitä tahansa.

Voisimme yrittää soveltaa kolmen luvun joukkojen käsittelyssä käytettyä ideaa: Pätee

$$k(a_1 - a_2) > k(a_1 - a_3) > \dots > k(a_1 - a_n).$$

Tämä antaa melko paljon tietoa siitä, mitä luvut  $k(a_1 - a_i)$  voivat olla. Yhteensä tapauksia on  $n$  kappaletta:

- $k(a_1 - a_2) = a_2, k(a_1 - a_3) = a_3, k(a_1 - a_4) = a_4, \dots, k(a_1 - a_n) = a_n.$
- $k(a_1 - a_2) = a_1, k(a_1 - a_3) = a_3, k(a_1 - a_4) = a_4, \dots, k(a_1 - a_n) = a_n.$
- $k(a_1 - a_2) = a_1, k(a_1 - a_3) = a_2, k(a_1 - a_4) = a_4, \dots, k(a_1 - a_n) = a_n.$
- $\vdots$

<sup>82</sup>Ratkaisun selittämistä vaikeuttaa se, ettemme voi puhua joukon  $S$  suurimmasta alkioista. Jos esimerkiksi  $S$  sisältää kaikki luvut väliltä 0 ja 1, muttei lukuja 0 eikä 1, niin joukossa  $S$  ei ole suurinta eikä pienintä lukua. Tämän ongelman voi kiertää puhumalla joukon  $S$  pienimmästä ylärajasta (merkitään usein  $\sup(S)$ ). On fakta, että kaikilla reaalilukujen joukoilla on olemassa pienin yläraja (joka on mahdollisesti ääretön). Tämä on oikeastaan (yksi) syy sille, miksi reaaliluvut on määritelty: rationaaliluvuilla ei ole tätä ominaisuutta, mutta analyysin kannalta ominaisuus on tärkeä.

- $k(a_1 - a_2) = a_1, k(a_1 - a_3) = a_2, k(a_1 - a_4) = a_3, \dots, k(a_1 - a_n) = a_{n-1}$ .

On siis olemassa jokin ”hyppäyskohta”  $h$ , jolla pätee  $k(a_1 - a_i) = a_{i-1}$  kaikilla  $i \leq h$  ja  $k(a_1 - a_i) = a_i$  kaikilla  $i > h$ . Edellisen listan hyppäyskohdat ovat ylhäältä alas luvut  $1, 2, \dots, n$ .

Miltä lukujono sitten näyttää? Tapauksessa  $h = 1$  kaikilla  $i \geq 2$  pätee

$$k(a_1 - a_i) = a_i$$

eli

$$a_i = a_1 \frac{k}{k+1}.$$

Tällöinhän  $a_2 = a_3 = \dots = a_n$ , mikä ei selvästi käy.

Vastaavalla idealla huomataan, että hyppäyskohta ei voi olla mikään luvuista  $2, 3, \dots, n-2$ : muuten arvoilla  $i = n-1$  ja  $i = n$  pätsivät sama yhtälö

$$a_i = a_1 \frac{k}{k+1}$$

kuin yllä arvolla  $h = 1$ . Tästä seuraisi  $a_{n-1} = a_n$ , mutta tämä ei käy.

Olemme siis kahden tapauksen päässä tehtävän ratkaisemisesta.

*Tapaus 1:*  $h = n$ . Tällöin kaikilla  $i \geq 2$  pätee

$$k(a_1 - a_i) = a_{i-1}.$$

Arvolla  $i = 2$  tästä saadaan  $k(a_1 - a_2) = a_1$  eli

$$a_2 = a_1 \frac{k-1}{k}.$$

Nyt arvolla  $i = 3$  pätee  $k(a_1 - a_3) = a_2$ . Sijoittamalla tähän luvun  $a_2$  arvon saadaan

$$a_3 = \frac{ka_1 - a_2}{k} = a_1 \frac{k - \frac{k-1}{k}}{k} = a_1 \frac{k^2 - k + 1}{k^2}.$$

Lasketaan vielä yksi arvo:

$$a_4 = \frac{ka_1 - a_3}{k} = a_1 \frac{k - \frac{k^2 - k + 1}{k^2}}{k} = a_1 \frac{k^3 - k^2 + k - 1}{k^3}.$$

Tästä nähdään, miten lukujonon termi  $a_i$  lasketaan. Tämä toki lisää uskoa ratkaisun toimivuuteen, mutta nyt herää kysymys: mitä seuraavaksi?

Tutkitaan jotain erotusta, joka ei ole muotoa  $a_1 - a_i$ . Ehkäpä yksinkertaisin näistä on  $a_2 - a_3$ . Nyt luvun  $k(a_2 - a_3)$  pitäisi kuulua joukkoon  $S$ . Tämä luku voidaan laskea:

$$k(a_2 - a_3) = a_1 k \left( \frac{k^2 - k}{k^2} - \frac{k^2 - k + 1}{k^2} \right) = -\frac{a_1}{k}.$$

Tämähän on negatiivinen – teimmekö jossain laskuvirheen? Emme: tämä vain tarkoittaa, että  $h = n$  ei anna ratkaisuja.

*Tapaus 2:*  $h = n - 1$ .

Saadaan siis  $k(a_1 - a_i) = a_{i-1}$  kaikilla  $2 \leq i \leq n - 1$ . Huomataan, että jos  $n \geq 4$ , niin edellisen tapauksen käsittely toimii ilman ongelmia: voimme laskea luvut  $a_2$  ja  $a_3$  ja todeta, että  $a_3 > a_2$ . Tapaus  $n = 3$  onkin käsitelty jo.

Olemme siis valmiit: tehtävän kaikki ratkaisut ovat  $k = 2$  ja  $k = \frac{1+\sqrt{5}}{2}$ .

Kommentti: Tehtävässä on paljon tekemistä. Tapauksen  $|S| = 3$  käsittely vaatii jonkin verran laskemista, tapaus  $|S| = \infty$  vaatii muutaman erilaisen huomion ja tapaus  $4 \leq |S| < \infty$  ei myöskään ole triviaali. Tästä ei kuitenkaan pidä lannistua, vaan kannattaa vain aloittaa jostain. Lisäksi huomattiin, että vaikka tapaus  $|S| = 3$  voi aluksi näyttää vain turhulta ja työläältä erikoistapauksien läpikäymiseltä, saatiin tästä hyödyllinen idea yleiseen tapaukseen. Tapaus  $|S| = 3$  oli tavallaan myös vaikeampi kuin tapaus  $4 \leq |S| < \infty$ , jossa kaikki tapaukset sai käsiteltyä samalla tavalla. (Tämä on loogista: Kun  $|S| = n$ , niin ehtoja muotoa  $k(a_i - a_j) \in S$  on  $\binom{n}{2}$  kappaletta, ja mitä suurempi  $n$  on, sitä suurempi  $\binom{n}{2}$  on joukon  $S$  kokoon verrattuna. Täten tuntuu uskottavalta, että ratkaisuja löytyy silloin, kun  $|S|$  on pieni, mutta ei silloin, kun  $|S|$  on suuri.)

Seuraavana on esimerkki vaikeasta funktionaaliyhtälöstä. Tehtävä on esiintynyt vuoden 2018 APMOssa.

### Tehtävä

Määritä kaikki funktiot  $f : \mathbb{R} \rightarrow \mathbb{R}$ , joilla

$$f(x^2 + f(y)) = f(f(x)) + f(y^2) + 2f(xy)$$

kaikilla reaaliluvuilla  $x$  ja  $y$ .

Ryhdytään hommiin. Tehdään helppo sijoitus  $x = 0$ . Saadaan

$$f(f(y)) = f(y^2) + 2f(0) + f(f(0)).$$

Saamme siis laskettua, mitä on  $f(f(y))$ . Sijoituksella  $y = 0$  saadaan  $f(0) = 0$ , joten  $f(f(y)) = f(y^2)$  pätee kaikilla  $y$ . Sijoittamalla tämän alkuperäiseen yhtälöön saadaan

$$f(x^2 + f(y)) = f(x^2) + f(y^2) + 2f(xy). \quad (1)$$

Yhtälön oikea puoli on symmetrinen muuttujien  $x$  ja  $y$  suhteen, joten tästä saadaan

$$f(x^2 + f(y)) = f(y^2 + f(x)). \quad (2)$$

Jos saisimme injektiivisyyden, niin tehtävä olisi ratkaistu: nyt olisi  $x^2 + f(y) = y^2 + f(x)$  eli  $f(x) = x^2 + f(0) = x^2$ . Helppo tarkastus osoittaa, että  $f(x) = x^2$  on ratkaisu. Emme kuitenkaan mitenkään voi saada injektiivisyyttä, koska  $f(x) = x^2$  ei ole injektio.

Vaikka injektiivisyys on liikaa toivottu, niin voi silti auttaa tutkia, mitä ehdosta  $f(a) = f(b)$  saadaan irti. Sijoittamalla yhtälöön 1 vuorotellen  $y = a$  ja  $y = b$  saadaan

$$f(a^2) + 2f(xa) = f(b^2) + 2f(xb).$$

Sijoittamalla tähän  $x = 0$  saadaan edelleen  $f(a^2) = f(b^2)$ , eli kaikilla  $x$  pätee  $f(xa) = f(xb)$ . Täten (sijoituksella  $x \rightarrow \frac{x}{b}$ ) pätee

$$f(cx) = f(x) \quad (3)$$

kaikilla  $x$ , missä  $c = \frac{a}{b}$  on vakio. (Jos  $b = 0$ , niin  $f$  on vakio, mistä saadaan ratkaisu  $f = 0$ .) Tämä on hyvin voimakas ehto.

Tästä saamme muodostettua strategian tehtävän ratkaisemiseksi. Oletetaan, että on olemassa jokin luku  $c$  ( $c \neq \pm 1$ ), jolla  $f(cx) = f(x)$  kaikilla  $x$ , ja yritetään osoittaa, että  $f$  on vakiofunktio. Tällöin epävakioilla  $f$  ehdosta  $f(a) = f(b)$  seuraa  $a = \pm b$  (mikä vastaa tapausta  $c = \pm 1$ ). Tästä ”melkein injektiivisyydestä” tehtävän luulisi ratkeavan.

Tutkimme siis joukkoa  $C = \{\frac{a}{b} \mid f(a) = f(b)\}$ . Kysymys kuuluu: mitä lukuja joukossa  $C$  on?

Ensinnäkin, jos  $f(x) = f(cx)$  kaikilla  $x$ , niin  $f(x) = f(cx) = f(c^2x) = \dots$ . Täten  $f(x) = f(c^n x)$  kaikilla  $n$  ja  $x$ , eli  $c^n \in C$  kaikilla  $c \in C$ , ja muun muassa  $\frac{1}{c} \in C$ .

Toiseksi yhtälöstä 2 saadaan

$$\frac{x^2 + f(y)}{y^2 + f(x)} \in C$$

kaikilla  $x, y \in \mathbb{R}$  (joilla  $y^2 + f(x) \neq 0$ ). Esimerkiksi valinnalla  $y = 0$  saadaan  $\frac{x^2}{f(x)} \in C$ .

On tietysti hyvä, että saadaan  $c^n \in C$  kaikilla  $c \in C$  ja että  $\frac{x^2}{f(x)} \in C$ , koska nämä antavat lisätietoa joukosta  $C$ . Ongelmana on kuitenkin, etteivät nämä ehdot vielä läheskään riitä todistamaan, että  $C$  sisältää kaikki reaaliluvut. Esimerkiksi ehto  $\frac{x^2}{f(x)} \in C$  ei loppujen lopuksi kerro kovin paljoa.

Millainen olisi hyvä tieto joukosta  $C$ ? Olisi hyvä, jos saataisiin ehto muotoa  $L(x, y) \in C$ , jossa  $L$  on jokin lauseke muuttujista  $x$  ja  $y$ : tämä antaa enemmän tietoa kuin ”yksiulotteinen” väite  $\frac{x^2}{f(x)} \in C$ .<sup>83</sup> Toinen tärkeä huomio on, että ehtojen tulee olla sellaisia, jotka poissulkevat esimerkiksi tapauksen  $C = \mathbb{Q}$ . Pelkästään ehdot muotoa  $c^n \in C$  tai  $c_1 + c_2 \in C$  kaikilla  $c, c_1, c_2 \in C$  eivät riittäisi poissulkemaan tätä tapausta. Tästä motivoituneena lähdetään todistamaan, että joukko  $C$  sisältää kaikki reaaliluvut joltain väliltä  $[a, b]$ .<sup>84</sup>

Käyttämällä yhtälöä 2, sijoitusta  $x \rightarrow cx$  ja yhtälöä 3 saadaan yhtälöketju

$$f(c^2x^2 + f(y)) = f(y^2 + f(cx)) = f(y^2 + f(x)) = f(x^2 + f(y)),$$

eli pätee

$$\frac{c^2x^2 + f(y)}{x^2 + f(y)} \in C.$$

<sup>83</sup>Esimerkkinä tällaisesta ”kaksiulotteisesta” tiedosta on yhtälöstä 2 saatu ehto  $\frac{x^2 + f(y)}{y^2 + f(x)} \in C$ , mutta tätäkin on vielä turhan hankala käyttää.

<sup>84</sup>Tätä strategiaa ei välttämättä edes tarvitse keksiä, jotta voi päätyä esitettyyn ratkaisuun, mutta strategialle on selkeä motivaatio.



Tämä voidaan kirjoittaa muodossa

$$c^2 - \frac{(c^2 - 1)f(y)}{x^2 + f(y)} \in C.$$

Oletetaan hetkeksi, että pätee  $c^2 > 1$  ja  $f(y) > 0$ . Huomataan, että kun  $x$  kulkee läpi arvot nolasta äärettömään, niin tämä lauseke saa kaikki arvot väliltä  $[1, c^2]$ . Tässä  $c$  on mikä tahansa luku, joka toteuttaa ehdon  $c^2 > 1$ . Koska  $c$  voidaan tarvittaessa korottaa potenssiin  $n$ , niin  $C$  sisältää edellisen nojalla kaikki luvut, jotka ovat vähintään 1. Tästä seuraa, että  $f$  on vakio.<sup>85</sup>

Edellä tehtiin kaksi oletusta:  $c^2 > 1$  ja  $f(y) > 0$ . Nämä eivät ole kovin oleellisia rajoituksia, ja niistä päästään eroon vaikkapa seuraavasti: Jos  $c^2 < 1$ , niin luvun  $c^2$  sijasta voidaan käsitellä lukua  $c^{-2} > 1$ . Oletus  $f(y) > 0$  voidaan myös tehdä. Todistetaan tämä vastaoletuksella, eli oletetaan, että kaikilla  $y$  pätee  $f(y) \leq 0$ . Aiemmin yhtälön 3 yhteydessä todettiin, että mikäli  $f$  ei ole injektiivinen nollassa (eli funktiolla  $f$  on useampi nollakohta), niin  $f$  on vakio. Siis  $f(y) < 0$  kaikilla  $y \neq 0$ . Valitaan jokin  $y \neq 0$ . Nyt yhtälöstä 1 saadaan sijoituksella  $x = \sqrt{-f(y)}$  ehto

$$0 = f(x^2) + f(y^2) + 2f(xy),$$

eli  $f(y^2) = f(x^2) = 2f(xy) = 0$ , eli muun muassa  $y^2 = 0$ . Tästä seuraa, että  $y = 0$ , mikä on ristiriidassa oletuksen  $y \neq 0$  kanssa. (Sijoitus  $x = \sqrt{-f(y)}$  on luonnollinen, koska sillä saadaan asioita supistumaan.)

Edellä siis oletettiin, että on olemassa  $c \neq \pm 1$ , jolla  $c \in C$ . Muussa tapauksessa  $f$  on melkein injektio, eli ehdosta  $f(a) = f(b)$  seuraa  $a = \pm b$ . Soveltamalla tätä yhtälöön 2 saadaan

$$x^2 + f(y) = \pm(y^2 + f(x)),$$

eli sijoittamalla  $y = 0$  saadaan

$$f(x) = \pm x^2$$

kaikilla  $x$ . Vielä pitää poissulkea pointwise trap, eli halutaan, että etumerkki yhtälössä  $f(x) = \pm x^2$  ei riipu luvusta  $x$ . Tämä ei ole erityisen vaikeaa.

Oletetaan, että  $f(y) = -y^2$  jollain reaalityyppisellä  $y \neq 0$ . Yhtälöstä 2 saadaan

$$f(x^2 - y^2) = f(y^2 + f(x)).$$

Tutkitaan paria tapausta:

*Tapaus 1:*  $f(x) = x^2$  jollain  $x$ . Nyt  $f(x^2 - y^2) = f(x^2 + y^2)$ , eli  $\pm(x^2 - y^2) = \pm(x^2 + y^2)$  jollain etumerkkien valinnoilla.

Jos etumerkit ovat samat, saadaan  $y = 0$  vastoin oletusta.

Jos etumerkit eivät ole samat, saadaan  $x = 0$ . Tämä tarkoittaa, että ehdosta  $f(x) = x^2$  seuraa  $x = 0$ , eli  $f(x) = -x^2$  kaikilla  $x$ . Sijoittamalla tämä alkuperäiseen yhtälöön on helppoa tarkistaa, ettei tämä ole ratkaisu.

<sup>85</sup>Teoriassa olisi mahdollista, että  $f$  olisi eri vakio positiivisilla ja negatiivisilla luvuilla. Helpot sijoitukset alkuperäiseen yhtälöön kuitenkin todistavat, ettei tämä ole mahdollista.

*Tapaus 2:*  $f(x) = -x^2$  kaikilla  $x$ . Kuten edellä todettiin, tämä ei ole ratkaisu.

Täten ainoat ratkaisut ovat  $f(x) = 0$  kaikilla  $x$  ja  $f(x) = x^2$  kaikilla  $x$ .

Kommentti: Pidän tästä tehtävästä. Standarditempuilla ja -sijoituksilla päädytään tutkimaan joukkoa  $C$ , ja tämän jälkeen pitää hoksata jotain joukon  $C$  rakenteesta. Ainoa keksimäni tapa todistaa, että  $C$  sisältää kaikki reaalityluvut, oli yrittää pakottaa joukko  $C$  sisältämään jokin väli. Tehtävän ratkaiseminen voi mennä pahasti pieleen, jos yhtälöihin tekee sokeasti yksiulotteisia sijoituksia, koska näistä on hyvin vaikeaa saada mitään järkevää tietoa joukosta  $C$ . Ratkaisun löytämiseksi ei ole pakko lähteä todistamaan nimenomaan sitä, että  $C$  sisältää jonkin välin, mutta on hyvä olla jokin käsitys siitä, millainen olisi riittävä tieto joukosta  $C$ .

Viimeinen esimerkkitehtävä on vuoden 2012 IMO-lyhytlistalta.

### Tehtävä

Olkoot  $f$  ja  $g$  sellaisia kokonaislukukertoimisia polynomeja, jotka eivät ole nollapolynomeja ja joilla  $\deg(f) > \deg(g)$ . Oletetaan, että äärettömän monella alkuluvulla  $p$  polynomilla  $pf + g$  on rationaalinen juuri. Osoita, että polynomilla  $f$  on rationaalinen juuri.

Ensimmäisenä muistetaan, että polynomin rationaaliset nollakohdat ovat muotoa ”vakiotermin tekijä jaettuna korkeimman asteen termin tekijällä”. Tämän soveltamiseksi kirjoitetaan  $f$ :n ja  $g$ :n kertoimet auki: Olkoot

$$f(x) = a_d x^d + \dots + a_0$$

ja

$$g(x) = b_{d-1} x^{d-1} + \dots + b_0.$$

Tässä  $d = \deg(f)$  ja  $a_d \neq 0$ , mutta  $b_{d-1}$  voi olla 0.

Olkoon  $p$  jokin tehtävänannon mukainen alkuluku. Jos  $\frac{m}{n}$  on jokin polynomin

$$pf + g = pa_d x^d + (pa_{d-1} + b_{d-1})x^{d-1} + \dots + (pa_0 + b_0)$$

nollakohta, niin seuraavien (tärkeiden) jaollisuusehtojen tulee päteä:

$$m | pa_0 + b_0$$

ja

$$n | pa_d.$$

On kaksi mahdollisuutta: joko  $p \nmid n$  tai  $p \mid n$ . Ensimmäisessä tapauksessa  $n$  on jokin luvun  $a_d$  tekijä. Toisessa tapauksessa  $n$  on vastaavasti muotoa  $c \cdot p$ , missä  $c | a_d$ . Oleellista tässä on, että ensimmäisessä tapauksessa  $n$  on enintään jokin vakio ja toisessa tapauksessa  $n$  kasvaa lineaarisesti muuttujan  $p$  mukana. Jakaudutaan kahteen tapaukseen.

*Tapaus 1:* Äärettömän monella  $p$  pätee  $p \nmid n$ .

Täten  $n$  on enintään vakio. Toisaalta polynomin  $pf + g$  juurien tulee olla melko pieniä: jos luvun  $x$  itseisarvo on hyvin suuri, niin luvun  $pf(x) + g(x)$  arvo on

suunnilleen sama kuin luvun  $pf(x)$  (koska  $\deg(f) > \deg(g)$ ). Täten minkä tahansa polynomin  $pf + g$  juuren tulee olla enintään jokin vakio, joka ei riipu luvusta  $p$ .

Täten jos  $\frac{m}{n}$  on polynomin  $pf + g$  juuri, niin koska  $n$  on enintään vakio, on myös  $m$  enintään jokin vakio. Tästä seuraa, että luvulle  $\frac{m}{n}$  on vain äärellisen monta eri vaihtoehtoa. Ei ole vaikeaa nähdä, että jonkin tällaisen rationaaliluvun  $\frac{m}{n}$  tulee olla polynomin  $f$  (ja täten myös  $g$ ) juuri. Yksi tapa tämän todistamiseksi on seuraava: Koska  $\frac{m}{n}$  on polynomin  $pf + g$  nollakohta, niin

$$p = -\frac{g\left(\frac{m}{n}\right)}{f\left(\frac{m}{n}\right)}$$

olettaen, että  $f\left(\frac{m}{n}\right) \neq 0$ . Luvulle  $\frac{m}{n}$  on vain äärellisen monta vaihtoehtoa, mutta luvulle  $p$  on äärettömän monta eri vaihtoehtoa. Tämä johtaa ristiriitaan.

*Tapaus 2: Äärettömän monella  $p$  pätee  $p \mid n$ .*

Voimme käyttää tapauksen 1 tuloksia: Jos  $\frac{m}{n}$  on polynomin  $pf + g$  juuri, niin  $\frac{m}{n}$  on enintään jokin vakio. Pätee myös

$$p = -\frac{g\left(\frac{m}{n}\right)}{f\left(\frac{m}{n}\right)},$$

jos  $\frac{m}{n}$  ei ole polynomin  $f$  juuri.

Mitä tästä seuraa? Koska yhtälön vasemman puolen  $p$  voi kasvaa mielivaltaisen suureksi, tulee myös oikean puolen lausekkeen  $-\frac{g(x)}{f(x)}$  (itseisarvon) kasvaa mielivaltaisen suureksi. Koska juuret  $\frac{m}{n}$  ovat enintään jokin vakio, on myös arvo  $g\left(\frac{m}{n}\right)$  enintään jokin vakio. Jotta luku

$$-\frac{g\left(\frac{m}{n}\right)}{f\left(\frac{m}{n}\right)}$$

voi kasvaa mielivaltaisen suureksi, tulee juurten  $\frac{m}{n}$  lähestyä jotain polynomin  $f$  juurta.

Miten tämä mahdollisuus poissuljetaan? Edellisessä tapauksessa tämä olisi ollut helppoa, koska siinä luvulle  $\frac{m}{n}$  oli vain äärellisen monta eri vaihtoehtoa. Tässä tapauksessa tiedämme, että  $p \mid n$ , joten luvulle  $n$  on vain äärellisen monta vaihtoehtoa, mutta luvusta  $m$  tiedetään vain

$$m \mid pa_0 + b_0.$$

Voimme ainakin tehdä vastaoletuksen ja katsoa, mitä tapahtuu. Oletetaan siis, että polynomilla  $f$  on jokin juuri  $\alpha$ , jota luvut  $\frac{m}{n}$  lähestyvät. Täten

$$\frac{m}{n} \approx \alpha.$$

Käytetään nyt tietoa siitä, että luku  $m$  on luvun  $pa_0 + b_0$  tekijä. Voidaan kirjoittaa

$$m = \frac{pa_0 + b_0}{C}$$

jollain kokonaisluvulla  $C$ . Saamme nyt

$$\frac{pa_0 + b_0}{nC} \approx \alpha.$$

Käytetään vielä tietoa siitä, että  $n$  on jaollinen luvulla  $p$ . Kirjoitetaan siis  $n = pc$ , missä  $c$  on jokin kokonaisluku (jolle on vain äärellisen monta vaihtoehtoa). Saadaan

$$\frac{pa_0 + b_0}{pcC} \approx \alpha.$$

Tämän approksimaation vasen puoli voidaan kirjoittaa muodossa

$$\frac{a_0}{cC} + \frac{b_0}{pcC}.$$

Kun  $p$  kasvaa suureksi, niin termi  $\frac{b_0}{pcC}$  lähestyy nollaa. Täten juuret  $\frac{n}{m}$  eivät voi lähestyä mitään irrationaalista lukua  $\alpha$ , koska tällöin myös lukujen  $\frac{a_0}{cC}$  tulisi lähestyä lukua  $\alpha$ . Tämä ei ole selvästi ole mahdollista: Jos  $\alpha$  on irrationaalinen, niin  $|\alpha| > 0$ . On kuitenkin olemassa vain äärellisen monta kokonaislukujen  $c$  ja  $C$  arvoa, joilla luvun  $|\frac{a_0}{cC}|$  koko on suunnilleen kokoluokkaa  $|\alpha|$ , joten näillä ei voi approksimoida irrationaalilukua  $\alpha$  mielivaltaisen hyvin.

Kommentti: Ratkaisussa huomionarvoista on, ettei siinä tarvinnut tehdä raskaita laskuja, vaan oleellisinta oli korkean tason ymmärrys juurten  $\frac{m}{n}$  käyttäytymisestä. Kuvailen tätä ongelmanratkaisumenetelmää usein sanomalla ”zoom in, zoom out”. (Tämä on hieman toisenlainen näkökulma aiemmin käsiteltyyn aiheeseen kokonaiskuvasta ja yksityiskohdista.) Tässä *zoom out* kuvaa suurien kuvioiden suunnittelua, heuristiikkojen keksimistä ja erilaisten ideoiden punnitsemista. Usein en *zoom out*-tilassa edes koske kynään. *Zoom in* puolestaan tapahtuu silloin, kun keskitytään yksityiskohtiin, käydään pieniä tapauksia läpi tai manuaalisesti lasketaan jotain. Monesti silloin, kun en ole saanut ratkaistua tehtävää, olen ollut liikaa *zoom in*-mielentilassa.

Sanoisin myös, että neljän ja puolen tunnin kilpailuissa (kuten IMOssa) ei ole tarkoituksenakaan olla koko aikaa *zoom in*-tilassa – tehtävät eivät ratkea pelkästään raa’alla voimalla, ja lisäksi monta tuntia *zoom in*-tilaa olisi varmasti hyvin raskasta. Lisää tästä aiheesta löytyy kehittymistä käsittelevästä tekstistäni sekä siellä linkatusta blogipostauksesta.

## 18 Pelit (Kombinatoriikka)

Tässä luvussa esitetään menetelmiä kombinatoristen pelien analysoimiseksi. Kilpailutehtävien peleissä tilanne on usein seuraava: kaksi pelaajaa pelaavat peliä, ja haluamme määrittää, kumpi voittaa molempien pelatessa optimaalisesti.

Aloitetaan suhteellisen yksinkertaisella esimerkillä, joka on esiintynyt vuoden 2012 MAOLin alkukilpailussa.

### Tehtävä

Kasassa on 2012 tulitikkua. Anna ja Bella poistavat vuorotellen kasasta tikkuja. Jokaisella vuorolla poistettujen tulitikkujen määrän tulee olla joko 1, 2 tai 3. Viimeisen tulitikun poistanut pelaaja voittaa. Kumpi voittaa, kun molemmat pelaavat optimaalisesti ja Anna aloittaa?

2012 on hyvin suuri luku, mutta peliä voi pelata myös pienemmällä määrällä tikkuja. Huomataan, että tikkumäärillä 1, 2 ja 3 Anna voittaa valitsemalla kaikki tikut. Jos taas kasassa on 4 tikkuja, Anna ei voi voittaa ensimmäisellä siirrolla, ja Bella saa seuraavalla siirrolla tyhjennettyä kasan.

Tikkumäärillä 5, 6 ja 7 Anna voi toimia seuraavasti: hän poistaa kasasta sen verran tikkuja, että jäljelle jää 4 tikkuja. Nyt peliä voikin ajatella niin, että Bella aloittaa ja että kasassa on tällöin 4 tikkuja. Tämä tilanne käsiteltiin jo: aloittaja, eli nyt Bella, häviää ja Anna voittaa.

Huomataan, että tikkumäärällä 8 Anna joutuu siirtymään johonkin tikkumääristä 5, 6 ja 7. Edellä todettiin, että näillä määrillä aloittava pelaaja, eli nyt Bella, voittaa ja siispä Anna häviää.

Jatkamalla samaa ideaa nähdään, että aloittava pelaaja häviää täsmälleen silloin, kun kasassa on neljällä jaollinen määrä tikkuja. Tämän voi todistaa helposti induktiolla (mikä jätetään lukijalle). Siispä 2012 tulitikulla aloittaja häviää, eli Bella voittaa molempien pelatessa optimaalisesti.

Edellinen esimerkkitehtävä motivoi voitto- ja häviötilojen käsitteet.

### Määritelmä

Kahden pelaajan pelin voittotiloiksi kutsutaan niitä tiloja, joissa vuorossa oleva pelaaja voittaa, ja häviötiloiksi puolestaan niitä tiloja, joissa vuorossa oleva pelaaja häviää.

Haluaisimme tietysti tavan määrittää voitto- ja häviötilat. Tässä auttaa seuraava tulos.

### Lemma

Kahden pelaajan pelin tila on voittotila täsmälleen silloin, kun siitä pääsee johonkin häviötilaan. Tila on häviötila täsmälleen silloin, kun siitä pääsee vain voittotiloihin.

Lemman todistus perustuu samaan havaintoon kuin esimerkkitehtävässä. Jos pelissä on Annan vuoro ja hän pystyy siirtymään tilaan, jossa aloittava pelaaja (eli tällöin Bella) häviää varmasti, niin Anna voittaa tekemällä tämän siirron. Jos taas kaikki mahdolliset Annan siirrot johtavat tilanteeseen, jossa seuraavana siirtävä Bella voittaa, niin Anna häviää.

Tämä idea on varsin yleinen ja antaa helpon tavan laskea voitto- ja häviötiloja monissa erilaisissa peleissä. Tikkupelin tapauksessa käydään läpi tikkumääriä  $1, 2, 3, \dots$  ja pidetään kirjaa pelin voitto- ja häviötiloista. Tikkumäärän  $n$  status riippuu vain tilojen  $n - 1, n - 2, n - 3$  statuksista.

Esitetään vielä toinen vastaavanlainen tehtävä. Tämä tehtävä on Suomen IMO-joukkueen valintakokeesta.

### Tehtävä

Liitutaululle on kirjoitettu luku 2019. Anna ja Bella tekevät vuorotellen seuraavanlaisia operaatioita: jos taululla on luku  $n$ , niin se voidaan korvata luvulla  $n - d$ , missä  $d < n$  on jokin luvun  $n$  tekijä. Pelin voittaa se, joka saa muutettua taululla olevan luvun ykköseksi. Anna aloittaa. Kumpi voittaa, kun molemmat pelaavat optimaalisesti?

Aloitetaan pienillä tapauksilla: Tila 2 on aloittavalle pelaajalle voittoisa, koska luvusta voidaan vähentää  $d = 1$ . Tila 3 on häviötila, koska tästä voidaan siirtyä vain voittotilaan 2. Tila 4 on taas voittotila, koska siitä voidaan siirtyä häviötilaan 3.

Tiloja voidaan laskea rutiininomaisesti eteenpäin vaikkapa kymmeneen asti. Saa daan, että 3, 5, 7 ja 9 ovat häviötiloja ja 2, 4, 6, 8 ja 10 ovat voittotiloja. Logiikka on selvä: voittotiloja ovat täsmälleen parilliset luvut.

Väitteen voi todistaa induktiolla. Oletetaan, että tiloista  $2, 3, \dots, n - 1$  voittotiloja ovat täsmälleen parilliset luvut. Todistetaan sama väite tilalle  $n$ . Tutkitaan kahta tapausta luvun  $n$  parillisuuden mukaan.

*Tapaus 1: Luku  $n$  on parillinen.* Tällöin  $n - 1$  on (induktio-oletuksen nojalla) häviötila ja tilasta  $n$  voidaan siirtyä tilaan  $n - 1$  valinnalla  $d = 1$ . Siis  $n$  on voittotila, kuten halusimmekin.

*Tapaus 2: Luku  $n$  on pariton.* Haluamme todistaa, että tila  $n$  on häviötila eli että tilasta  $n$  pääsee vain voittotiloihin eli parillisiin lukuihin. Tämä on selvää: Koska  $n$  on pariton, kaikki luvun  $n$  tekijät  $d$  ovat parittomia. Tällöin seuraava tila on  $n - d$ , joka on kahden parittoman luvun erotus ja täten parillinen. Luvusta  $n$  ei siis pääse voittotiloihin, joten lukua  $n$  vastaa häviötila.

Väite on todistettu kaikille  $n$ , ja täten Anna häviää aloitettaessa luvusta 2019.

Edellisissä ongelmissa pelin tiloja pystyi helposti kuvaamaan yhdellä positiivisella kokonaisluvulla, mikä mahdollisti voittotilojen listaamisen ja tätä kautta säännön-mukaisuuden löytämisen. Sama menetelmä ei kuitenkaan toimi kaikkiin tehtäviin, koska tiloja voi olla hyvin paljon. Johdantokappaleessa esitetty tehtävä on tästä oiva

esimerkki. Tehtävä on esiintynyt Suomen valmennuksen harjoituskokeessa.

### Tehtävä

Anna ja Berg pelaavat dominopalikoilla ( $2 \times 1$ ) peliä  $n \times 1$  ruudun laudalla. Pelissä pelaajat laittavat vuorotellen yhden dominopalikan laudalle niin, että palikka peittää täsmälleen kaksi ruutua eikä mene yhdenkään muun palikan päälle. Peli loppuu, kun tällaisia siirtoja ei pystytä enää tekemään. Viimeisen siirron tehnyt pelaaja voittaa pelin. Osoita, että jos Anna ja Berg pelaavat yhden pelin jokaisella luvun  $n$  arvolla  $2, 3, \dots, 2007$ , Anna aloittaa jokaisen pelin ja molemmat pelaajat pelaavat optimaalisesti, niin Anna voittaa ainakin 1505 peliä.

Pelissä on paljon muitakin mahdollisia tiloja kuin tyhjät laudat kokoa  $n \times 1$  (vertaa aiempiin esimerkkeihin, joissa näin ei ollut). Tämän vuoksi voitto- ja häviötilojen laskeminen ei toimi suoraan.<sup>86</sup>

Hankitaan hieman tuntumaa tehtävästä pienien tapauksien kautta, niin kuin aiemmissa tehtävissä. Arvoilla  $n = 2, 3, 4$  Anna voi pakottaa voiton heti ensimmäisellä siirrolla. Arvolla  $n = 5$  tämä ei kuitenkaan onnistu: Berg voi aina tehdä vähintään yhden siirron, minkä jälkeen laudasta on peitetty jo neljä ruutua viidestä eikä enempää siirtoja voida enää tehdä.

Arvolla  $n = 6$  huomataan, että Anna voittaa laittamalla palikan kahteen keskimäiseen ruutuun. Pienellä mielikuvituksella huomataan, että tämä toimii kaikilla parillisilla  $n$ : Anna aloittaa laittamalla palikan kahden keskimmäisten ruudun päälle. Tämän jälkeen Anna vain matkii Bergiä: kun Berg laittaa palikan, Anna laittaa palikan toiselle puolelle keskimmäistä palikkaa ja yhtä kauaksi keskikohdasta kuin Berg. Nyt lauta on aina symmetrinen Annan siirron jälkeen, joten ei voi syntyä tilannetta, jossa Berg saisi tehtyä siirron ja Anna ei. Täten Anna voittaa.

Anna siis voittaa parillisilla  $n$ , joten arvoilla  $n = 2, 3, \dots, 2007$  Anna voittaa vähintään 1003 peliä. Tämä ei vielä riitä, joten pitää tutkia myös parittomia  $n$ .

Parittomilla luvun  $n$  arvoilla ei ole selvää tapaa jakaa lautaa kahteen eri osaan, ja kuten aiemmin totesimme arvon  $n = 5$  kohdalla, Anna ei edes voita kaikkia pelejä. Tarvitsisimme Annalle kuitenkin vielä 502 voittotilaa parittomilla luvuilla eli noin puolet parittomien lukujen tapauksista. Tämä antaakin pienen vihjeen: tehtävänannossa ei pyydetä määrittämään kaikkia voittotiloja, vaan halutaan vain, että noin puolilla parittomista  $n$  Anna voittaa. Tämä motivoi seuraavan idean.

Oletetaan, että arvolla  $n = 2k - 1$  Anna häviää. Jos saamme todistettua, että esimerkiksi arvolla  $n = 2k + 1$  Anna voittaa, niin saamme jokaista häviötilaa vastaamaan jonkin voittotilan, jolloin vähintään puolet parittomista  $n$  ovat aloittajan voittoja.

Idea on helppo toteuttaa. Tutkitaan peliä arvolla  $n = 2k + 1$ . Anna voi laittaa

<sup>86</sup>Voidaan kuitenkin ajatella, että ensimmäisen siirron jälkeen pelilauta jakautuu kahdeksi pienemmäksi pelilaudaksi, joilla pelataan samanaikaisesti (ja pelaaja saa päättää, kummalla laudalla tekee siirron). Tämä ei kuitenkaan suoraan johda ratkaisuun.

palikan kahden ensimmäisen ruudun kohdalle, jolloin peli käytännössä vastaa  $(2k - 1) \times 1$ -kokoista lautaa. Mutta  $n = 2k - 1$  vastasi häviötilaa, eli vuorossa oleva Berg häviää pelin molempien pelatessa optimaalisesti. Siis  $n = 2k + 1$  todella on voittotila.

Enää täytyy tehdä tarkat laskut voittotilojen määristä. Totesimme jo, että  $n = 3$  on voittotila. Nähdään, että vähiten parittomien  $n$  voittotiloja on siinä tapauksessa, että tilat

$$n = 5, 9, 13, 17, \dots, 2001, 2005$$

vastaisivat häviötiloja ja tilat

$$n = 3, 7, 11, 15, \dots, 2003, 2007$$

vastaisivat voittotiloja. Tällöin voittotiloja olisi 502 kappaletta. Olivat voittotilat siis mitä tahansa, saimme haluamamme 502 voittotilaa, joten olemme valmiit.

Kommentti: ratkaisussa käsiteltiin parilliset ja parittomat  $n$  eri tavoilla. Parilliset  $n$  saatiin käsiteltyä symmetrian avulla, ja parittomat  $n$  saatiin ns. strategianvarastuksella. Molemmat ideat ovat hyvin yleisiä pelejä käsittelevissä tehtävissä.

Seuraava tehtävä on klassinen esimerkki strategianvarastamisesta. Netistä lisää pelistä löytää nimellä Chomp.

### Tehtävä

Olkoon  $n$  positiivinen kokonaisluku. Liitutaululle on kirjoitettu luvun  $n$  kaikki positiiviset tekijät (mukaan lukien 1 ja  $n$ ). Anna ja Bella tekevät vuorotellen seuraavanlaisia siirtoja: pelaaja valitsee taululta luvun  $d$  ja poistaa taululta kaikki luvut muotoa  $kd$ , missä  $k = 1, 2, \dots$ . Pelaaja, joka poistaa taululta luvun 1, häviää pelin. Anna aloittaa. Osoita, että Anna voittaa kaikilla  $n > 1$ .

Esimerkiksi arvolla  $n = 6$  taululla on aluksi luvut 1, 2, 3 ja 6. Anna voi aloittaa poistamalla luvun 6. Tällöin Bella joutuu valitsemaan toisen luvuista 2 ja 3, minkä jälkeen Anna valitsee näistä jäljelle jääneen. Lopulta Bella joutuu poistamaan luvun 1.

Jos  $n$  on alkuluvun potenssi  $p^k$ , niin tehtävän väite on triviaali: Anna valitsee luvun  $p$ . Mutta jo tapaus  $n = p^a q^b$  joillain alkuluvuilla  $p \neq q$  ja kokonaisluvuilla  $a, b \geq 1$  on vaikea. Tätä tilannetta voi hahmottaa pelinä, jossa on annettuna  $a \times b$ -suklaalevy, jonka kohta  $(x, y)$  vastaa luvun  $n$  tekijää  $p^x q^y$ . Pelaajat lohkaisevat vuorotellen levystä jonkin ”ylänurkan” (eli valitsevat kohdan  $(x, y)$ , ja poistavat kaikki sen yläpuolella, oikealla puolella tai ylempänä ja oikeammalla olevat kohdat). Jos luvulla  $n$  on kolme erisuurta alkutekijää, niin suklaalevy muuttuu kolmiulotteiseksi kappaleeksi, ja yleisellä  $n$  suklaalevy voi olla vielä moniulotteisempi.

Vaikuttaa siis melko vaikealta ratkaista tehtävä suoraan keksimällä voittostrategia Annalle. Idea onkin todistaa epäsuorasti strategianvarastusidealla voittavan strategian olemassaolo. Tutkimme kahta tapausta:

*Tapaus 1: Anna voittaa valitsemalla aluksi luvun  $n$ .* Tässä tapauksessa Anna voittaa.



*Tapaus 2: Anna ei voita valitsemalla aluksi luvun  $n$ .* Tämä tarkoittaa, että mikäli Anna valitsisi luvun  $n$ , niin Bellalla olisi voittava strategia. Olkoon  $d$  luvun  $n$  tekijä, jonka Bella valitsisi heti Annan ensimmäisen siirron jälkeen. Anna voikin varastaa Bellan strategian: sen sijaan, että Anna valitsisi ensimmäisellä siirrollaan luvun  $n$ , hän valitseekin luvun  $d$ . Syntynyt tila on sama kuin mikä syntyisi Annan valitessa ensin luvun  $n$  ja Bellan vastatessa luvulla  $d$ , mutta nyt vuorossa oleva pelaaja on vaihtunut. Siispä Anna voittaa.

Seuraavana esitetään tehtävä vuoden 2011 MAOLin loppukilpailusta.

### Tehtävä

Kaksi pelaajaa, rakentaja ja hajottaja, pelaavat seuraavanlaista peliä. Rakentaja aloittaa, ja pelaajat valitsevat vuorotellen joukon  $\{0, 1, \dots, 10\}$  eri alkioita. Rakentaja voittaa, jos jotkin neljä hänen valitsemistaan kuudesta alkioista muodostavat aritmeettisen jonon. Hajottaja puolestaan voittaa, jos hän pystyy estämään rakentajaa muodostamasta tällaista aritmeettista nelikkoo. Kummalla pelaajista on voittostrategia?

Miten tehtävää lähestytään? Jos ei keksi mitään järkevää, niin voi ainakin tutkia, mitä erilaisia neljän pituisia aritmeettisia jonoja on. Jos jonon erotusvakio on 1, niin jonot ovat  $(0, 1, 2, 3)$ ,  $(1, 2, 3, 4)$ ,  $\dots$ ,  $(7, 8, 9, 10)$ . Erotusvakion ollessa kaksi jonot ovat  $(0, 2, 4, 6)$ ,  $(1, 3, 5, 7)$ ,  $(2, 4, 6, 8)$ ,  $(3, 5, 7, 9)$  ja  $(4, 6, 8, 10)$ . Jonoilla  $(0, 3, 6, 9)$  ja  $(1, 4, 7, 10)$  erotusvakio on 3. Muita jonoja ei ole.

Jotta rakentaja voittaisi, tulisi hänen saada valittua jokin näistä jonoista. Hyvä idea olisi valita aluksi sellaisia lukuja, jotka kuuluvat mahdollisimman moneen näistä jonoista. Tämä on hyvä strategia myös hajottajalle.

Mitkä sitten ovat usein jonoissa esiintyviä lukuja? Tarkastelemalla edellä tehtyä listausta nähdään, että luvut 4 ja 6 esiintyvät eniten. Myös luvut 3 ja 7 ovat yleisiä. Rakentaja saa varmasti valittua näistä luvuista vähintään kaksi kappaletta, samoin hajottaja.

Nyt voisi tutkia paria eri tapausta sen mukaan, mitä lukuja rakentaja saa valittua. Tämä ei kuitenkaan tunnu helpolta: vaikka rakentaja saisi valittua luvut 3 ja 4, niin ei ole selvää, miten hän voittaisi.

Sen sijaan huomataan, että mikäli hajottaja saa valittua luvut 3 ja 4, niin hänellä on jo erittäin hyvä asema: jokaisessa kahden tai kolmen erotusvakion jonossa on joko luku 3 tai 4, kuten listauksesta nähdään. Tämä ei kuitenkaan aivan riitä: Jos rakentaja valitsee luvut 6 ja 7, niin hajottaja ei valittuaan luvut 3 ja 4 voi enää estää rakentajan voittoa. Rakentaja voisi valita luvun 8, ja hän saa vielä valittua joko luvun 5 tai luvun 9.

Edellinen idea kuitenkin toimii luvuilla 3 ja 6: tämä estää jo kaikki erotusvakioden 1 ja 2 jonot, ja jäljelle jää enää jono  $(1, 4, 7, 10)$ . Nyt hajottaja saa varmasti valittua vielä jonkin luvuista 1, 4, 7 ja 10, joten hän voittaa pelin. Vastaava väite tietysti pätee symmetrian nojalla lukujen 3 ja 6 sijasta myös luvuilla 4 ja 7. Alkaa vaikuttaa siltä, että hajottajalla on voittostrategia.

Voimme jatkaa samaa ideaa vielä eteenpäin. Jos hajottaja saa valittua luvut 3 ja 8, niin jäljelle jäävät jonot  $(4, 5, 6, 7)$ ,  $(0, 2, 4, 6)$  ja  $(1, 4, 7, 10)$ , mikä vaikuttaa hyvältä tilanteelta hajottajalle. Vastaavanlainen tilanne pätee hajottajan saadessa haltuunsa luvut 2 ja 7.

Nämä ideat varmaankin riittävät ratkaisuun, ja kyse on enää ideoiden yhdistämisestä. Alla on esitetty ratkaisu.

Osoitetaan, että hajottajalla on voittostrategia. Symmetrian nojalla voidaan olettaa, että rakentajan ensimmäisen vuoron luku on enintään 5. Tutkitaan kolmea tapausta.

1. Rakentaja ei aluksi valitse kumpaakaan luvuista 3 ja 4. Tällöin hajottaja voi valita luvun 3, ja rakentajan tulee yllä esitetyn päättelyn nojalla vastata luvulla 6. Hajottaja valitsee luvun 4, ja rakentajan tulee vastaavalla logiikalla vastata luvulla 7. Hajottaja voi nyt valita luvun 8. Huomataan, että hajottaja on saanut estettyä kaikki nelikot.
2. Rakentaja valitsee aluksi luvun 3. Tällöin hajottaja voi vastata valitsemalla luvun 7, jolloin rakentajan tulee valita luku 4. Hajottaja valitsee luvun 2. Jäljelle jääneet nelikot ovat  $(3, 4, 5, 6)$ ,  $(4, 6, 8, 10)$  ja  $(0, 3, 6, 9)$ . Jakaudutaan vielä pariin helppoon osatapaukseen.
  - (a) Rakentaja ei valitse lukua 6. Tällöin hajottaja valitsee seuraavaksi luvun 6 ja voittaa.
  - (b) Rakentaja valitsee luvun 6. Hajottaja vastaa luvulla 5. Nähdään, ettei rakentaja voi enää pakottaa voittoa: hänellä on nelikoista  $(4, 6, 8, 10)$  ja  $(0, 3, 6, 9)$  valittuna alkio 3, 4 ja 6, joten hajottaja voi aina estää uhkaukset.
3. Rakentaja valitsee aluksi luvun 4. Hajottaja vastaa luvulla 3, ja rakentajan tulee valita luku 6. Hajottaja valitsee luvun 8. Jäljelle jääneet nelikot ovat  $(4, 5, 6, 7)$ ,  $(0, 2, 4, 6)$  ja  $(1, 4, 7, 10)$ . Jos rakentaja ei seuraavalla vuorolla valitse mitään luvuista 0, 2 ja 7, voi hajottaja valita seuraavalla vuorollaan luvun 7 ja voittaa. Tutkitaan loput tapaukset.
  - (a) Rakentaja valitsee luvun 7. Tällöin hajottaja valitsee luvun 5, ja kuten kohdassa 2b hajottaja voi aina estää rakentajan uhkaukset.
  - (b) Rakentaja valitsee luvun 0. Tällöin hajottaja valitsee luvun 2. Jos rakentaja ei seuraavaksi valitse lukua 7, voi hajottaja valita luvun 7, jolloin hän voittaa. Muuten hajottaja valitsee luvun 5 ja selvästikin voittaa pelin.
  - (c) Rakentaja valitsee luvun 2. Hajottaja valitsee luvun 0, ja tilanne on sama kuin edellisessä kohdassa.

Täten hajottajalla on voittostrategia.

Kommentti: Tehtävästä voi olla vaikea saada otetta ennen ensimmäistä hyödyllistä huomiota. Tämän jälkeen tehtävä kuitenkin murenee palasiin: voimme löytää

(yrityksen ja erehdyksen kautta) monenlaisia hajottajalle edullisia asetelmia ja käydä näiden pohjalta läpi kaikki mahdolliset siirtosarjat. Tapauskäsittely itsessään ei ole vaikea, eikä sen tekeminen vie paljoakaan aikaa.

Osoittautuu myös, että mikäli hajottaja saa valittua molemmat luvuista 4 ja 9 ensimmäisellä kahdella siirrollaan, niin hän voittaa. Tämän voi todistaa suoraan tutkimalla paria eri tapausta. Vastaavasti hajottaja voittaa saamalla luvut 1 ja 6, ja kuten aiemmin todettiin, myös lukujen 3 ja 6 tai lukujen 4 ja 7 saaminen voittaa pelin. Ei ole vaikeaa nähdä, että hajottaja saa pakotettua jonkin näistä pareista itselleen ensimmäisten kahden siirtonsa aikana. Tämä antaa vaihtoehtoisen viimeistelyn ratkaisulle.

Viimeisenä esitettävä tehtävä on vuoden 2015 IMO-lyhytlistalta Suomen ehdottama tehtävä.

### Tehtävä

Olkoon  $n$  positiivinen kokonaisluku. Anna ja Bella pelaavat peliä, jossa he valitsevat positiivisia kokonaislukuja  $k \leq n$ . Säännöt ovat seuraavat:

1. Pelaaja ei saa valita lukua, jonka jompikumpi pelaajista on valinnut jollain aiemmalla vuorolla.
2. Pelaaja ei saa valita lukua, joka on yhden päässä tämän pelaajan jo aiemmin valitsemasta luvusta.
3. Peli on tasapeli, jos kaikki luvut on valittu. Muussa tapauksessa pelaaja, joka ei voi siirtää, häviää pelin.

Anna aloittaa. Määritä pelin lopputulos, kun molemmat pelaavat optimaalisesti.

Huomaa, että pelaaja voi valita luvun  $k$ , vaikka vastustaja olisi valinnut jommankumman (tai molemmat) luvuista  $k - 1$  ja  $k + 1$ , mutta ehto 2 kieltää uuden luvun valitsemisen oman luvun vierestä.

Nopea pienten tapausten tarkastelu antaa, että arvoilla  $n = 1, 2, 4$  peli on tasapeli ja arvolla  $n = 3$  Bella voittaa. Tästä ei vielä voida vetää kovin suuria johtopäätöksiä.

Huomataan helppo symmetria-argumentti: parillisilla  $n$  Bella ei ainakaan häviä. Bella voi nimittäin aina peilata Annan valintoja, eli jos Anna valitsee luvun  $i$ , niin Bella valitsee luvun  $n + 1 - i$ . Tämä todistus ei kuitenkaan yleisty parittomille  $n$ .

Yleisesti ottaen Bellalla on pieni etu: pelissä on huono asia, jos joutuu tekemään siirron, koska tämä poissulkee myöhempien siirtojen mahdollisia valintoja. Vastaavalla logiikalla on hyvä idea valita luku 1 tai luku  $n$  eikä antaa näitä vastustajalle, koska näiden lukujen valitseminen poissulkee vain yhden luvun jatkosta.

Tästä motivoituneena yritetään todistaa, että Bella ei ainakaan häviä, keksimällä strategia, jossa Bella valitsee ensimmäisellä vuorollaan joko luvun 1 tai  $n$ . Oletetaan, että  $n \geq 2$ , jolloin Bella todella saa valittua jommankumman luvuista 1 ja  $n$ . Symmetrian vuoksi voidaan olettaa, että Anna valitsee ensimmäisellä vuorollaan

jonkin luvun, joka on enintään  $\frac{n+1}{2}$ , jolloin Bella voi valita luvun  $n$ .

Tutkitaan tilannetta Annan toisen siirron jälkeen. Anna on valinnut luvut  $a_1$  ja  $a_2$ , joilla  $1 \leq a_1 < a_2 < n$ , ja Bella on valinnut luvun  $n$ . Nyt Bella voi ainakin valita itselleen luvun lukujen  $a_1$  ja  $a_2$  välistä. Annan valitsee seuraavalla vuorollaan jonkin luvun  $a_3$ , minkä seurauksena Annan lukuihin syntyy uusi väli, josta Bella voi valita itselleen seuraavan luvun. Jos esimerkiksi  $a_1 < b < a_3 < a_2$ , niin lukujen  $a_3$  ja  $a_2$  väliin syntyy uusi väli, josta Bella voi valita toisen lukunsa. Yleisesti Annan siirrot luovat aina uuden välin, josta Bella ei ole vielä valinnut yhtään lukua ja josta Bella voi näin ollen valita uuden luvun.

Bella ei siis häviä, joten enää pitää tutkia, milloin peli päättyy tasapeliin Bellan pelatessa edellä kuvaillulla strategialla. On uskottavaa, että oikeastaan peli päättyy hyvin harvoin tasapeliin: tämä vaatisi, että Annan ja Bellan valitsemat luvut olisivat täsmälleen parittomat ja parilliset luvut, vastaavasti.

Täten Bella voi estää tasapelin valitsemalla jonkin parittoman luvun samalla, kun pelaa edellä kuvaillulla strategialla. Jos  $n$  on pariton, niin tämä selvästi onnistuu, koska Bella tulee heti ensimmäisellä vuorollaan valitsemaan luvun  $n$ . Parillisilla  $n$  pyritään valitsemaan pariton luku toisella vuorolla.

Arvolla  $n = 6$  tämä ei vielä onnistu: Anna voi aloittaa valitsemalla luvun 1, jolloin Bella strategiansa vuoksi valitsee luvun 6. Anna vastaa valitsemalla luvun 3, mikä varmistaa mahdollisuuden valita luvun 5 Annan kolmannella eli viimeisellä siirrolla.

Arvoilla  $n \geq 8$  tämä kuitenkin onnistuu. Tutkitaan tilannetta, jossa Bella on valinnut luvun  $n$  ja Anna luvut  $a$  ja  $b$ ,  $1 \leq a < b < n$ . Luvut  $a$  ja  $b$  voivat itsessään peittää maksimissaan kaksi paritonta lukua, ja lisäksi luku  $n - 1$  on pariton luku, jota Bella ei voi valita toisella vuorollaan. Koska parittomia lukuja välillä  $[1, n]$  on  $\frac{n}{2} \geq 4$  kappaletta, on jäljellä vielä vähintään yksi pariton luku, jonka Bella voi valita. Täten Bella voittaa, jos  $n \geq 8$ .

Olemme siis tapauksia  $n = 6$  vaille valmiit. Todistetaan, että tapauksessa  $n = 6$  Anna voi varmistaa tasapelin valitsemalla ensiksi luvun 1. Tutkitaan tapauksia sen mukaan, mitä Bella vastaa.

- Jos Bella valitsee luvun 2, Anna vastaa valitsemalla luvun 5. Anna saa varmasti myöhemmin valittua luvun 3.
- Jos Bella valitsee luvun 3, Anna vastaa valitsemalla luvun 6. Anna saa varmasti myöhemmin valittua luvun 4.
- Bella: 4, Anna: 6, myöhemmin Anna: 3.
- Bella: 5, Anna: 6, myöhemmin Anna: 4.
- Bella: 6, Anna: 3, myöhemmin Anna: 5.

Siis tapauksessa  $n = 6$  sekä Anna että Bella voivat varmistaa, etteivät he häviä, joten peli on tasapeli.

Täten peli on tasapeli täsmälleen silloin, kun  $n = 1, 2, 4$  tai  $6$ , ja muissa tapauksissa Bella voi varmistaa voiton.

Kommentti: Tehtävä ei ole helppo. Ensinnäkään vastausta ei ole helppoa arvata, koska arvoilla  $n = 2, 4, 6$  peli on tasapeli ja arvoilla  $n = 3, 5, 7$  peli on Bellan voitto. Luonnollinen arvaus siitä, että peli on tasapeli parillisilla  $n$  ja Bellan voitto parittomilla  $n$ , osoittautuu vääräksi. Tämän arvauksen vian voi intuitiivisesti nähdä näin: Bella ei häviä parillisilla  $n$  symmetria-argumentin takia. Jos peli olisi tasapeli arvolla  $n = 100$ , niin Annan tulisi saada kaikki parilliset tai parittomat luvut. Kuulostaa kuitenkin epäuskottavalta, että Bella ei voisi estää tätä tapahtumasta, kun Bellalla on hieman etua Annan aloittaessa.

Toisekseen ei ole kovin helppoa keksiä voittostrategiaa Bellalle. Tähän voi kuitenkin päätyä keksimällä ratkaisussa esitetyn idean lukujen  $1$  ja  $n$  hyödyllisyydestä. Tämän jälkeen luonnollinen kysymys on ”Miltä näyttäisi tilanne, jossa lauta ei ole vielä täynnä, mutta Bella ei voi tehdä yhtäkään siirtoa?” Tällaista tilannetta ei ole, ja syyn voi nähdä konkreettisia esimerkkejä tarkastelemalla: Anna on aina tehnyt enemmän siirtoja kuin Bella, ja tämän vuoksi on aina olemassa kaksi Annan lukua, joiden välissä ei ole Annan eikä Bellan lukuja. Tästä välistä voi siis valita luvun Bellalle.

## 19 Laskennallista kombinatoriikkaa (Kombinatoriikka)

Tässä luvussa esitetään kombinatoriikan tehtäviä, jotka ovat enemmän tai vähemmän laskennallisia.

### 19.1 Laatikkoperiaate

Laatikkoperiaate<sup>87</sup> on yksi tärkeimmistä kombinatoriikan tuloksista, mutta se on samalla yksi helpoimmista.

#### Lause (Laatikkoperiaate, muotoilu 1)

Olkoon  $n$  positiivinen kokonaisluku. Jos  $n$  laatikkoon laitetaan  $n + 1$  palloa, niin on olemassa vähintään yksi laatikko, jossa on vähintään kaksi palloa.

Väite käy järkeen. Ehkäpä helpoin tapa saada tulokselle formaali todistus on tehdä vastaoletus: Oletetaan, että vähintään kaksi palloa sisältävää laatikkoa ei ole. Nyt jokaisessa laatikossa on enintään yksi pallo, joten palloja on enintään  $n$ , mikä on ristiriita.

Laatikkoperiaatteesta on myös seuraava, hieman yleisempi muotoilu. Myös tämä väite on intuitiivisesti selvä, ja formaalin todistuksen saa tässäkin vastaoletuksella.

#### Lause (Laatikkoperiaate, muotoilu 2)

Olkoot  $n$  ja  $k$  positiivisia kokonaislukuja. Jos  $n$  laatikkoon laitetaan  $kn + 1$  palloa, niin on olemassa vähintään yksi laatikko, jossa on vähintään  $k + 1$  palloa.

Mikä laatikkoperiaatteesta tekee niin tärkeän? Oleellista on se, miten laatikkoperiaatetta soveltaa. Valitsemalla laatikot ja pallot sopivasti voidaan todistaa epätriviaaleja tuloksia, kuten seuraavista esimerkeistä nähdään. Ensimmäinen esimerkkitehtävä on esiintynyt valmennustehtävänä vuoden 2016 joulukuussa.

#### Tehtävä

51 pientä hyönteistä laitetaan yksikköneliön sisään. Osoita, että millä tahansa hetkellä neliössä on ainakin kolme hyönteistä, jotka voidaan peittää ympyrällä, jonka säde on  $\frac{1}{7}$ .

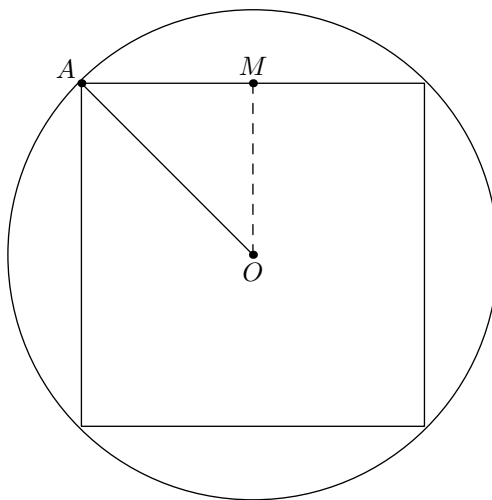
Tehtävään on luonnollista yrittää soveltaa laatikkoperiaatetta: jos saamme peitettyä yksikköneliön riittävän pienellä määrällä  $\frac{1}{7}$ -säteisiä ympyröitä, niin laatikkoperiaate kertoo, että jossain ympyrässä on varmasti riittävän paljon hyönteisiä (eli kolme hyönteistä).

<sup>87</sup>Laatikkoperiaatteesta käytetään myös nimitystä kyyhkyslakkaperiaate.

Kuinka monta ympyrää meillä on käytettävissä? Käytetään  $n$  kappaletta ympyröitä. Haluaisimme soveltaa laatikkoperiaatteen muotoilua 2 arvolla  $k = 2$ . Täten  $n$  laatikkoon (eli tässä tapauksessa ympyrään) laitetaan  $2n + 1$  palloa (eli tässä tapauksessa pientä hyönteistä). Koska hyönteisiä on 51, saadaan tästä  $2n + 1 = 51$ , eli  $n = 25$ . Käytössä on siis 25 ympyrää.

Ympyrät kannattaisi varminkin sijoittaa tasaisesti yksikköneliön sisälle. Yksi luonnollinen idea tämän saavuttamiseksi on jakaa yksikköneliö 25 neliöön, joiden jokaisen sivun pituus on  $\frac{1}{5}$ , ja asettaa ympyröiden keskipisteet näiden pikkuneliöiden keskelle. Nyt kysymys kuuluu: peittääkö jokainen ympyrä oman pikkuneliönsä?

Vastaus kysymykseen on myönteinen. Tilanne on esitettyä seuraavassa kuvassa.



Kuvaan on merkitty neliön ja ympyrän keskipiste  $O$  neliön kärkipiste  $A$  ja yhden neliön sivun keskipiste  $M$ . Riittää tietysti todistaa, että jokainen neliön kärkipisteistä on ympyrän sisäpuolella. Haluamme siis todistaa, että  $AO \leq \frac{1}{7}$ .

Pituus  $AO$  osataan laskea kolmiosta  $AMO$  käyttämällä Pythagoraan lausetta. Janat  $AM$  ja  $MO$  ovat pituudeltaan puolet neliön sivun pituudesta  $\frac{1}{5}$ , eli  $AM = MO = \frac{1}{10}$ . Pythagoraan lause antaa

$$AO^2 = AM^2 + MO^2 = \frac{1}{100} + \frac{1}{100} = \frac{1}{50}.$$

Täten  $AO = \frac{1}{\sqrt{50}}$ . Tämä on pienempi kuin  $\frac{1}{7}$ , koska  $\sqrt{50} > 7$ . (Ero on kuitenkin hyvin pieni, kuten kuvastakin nähdään.) Tehtävä on täten ratkaistu.

Seuraava tehtävä on vaikeampi esimerkki tehtävästä, jossa laatikkoperiaate on avuksi. Tehtävä on vuoden 2016 Baltian tie -kilpailusta. Ratkaisussa käytetään apuna Aritmetiikan peruslause -luvussa esitettyjä tuloksia.

### Tehtävä

Joukossa  $A$  on 2016 positiivista kokonaislukua. Kaikki joukon lukujen alkutekijät ovat pienempiä kuin 30. Todista, että joukossa  $A$  on neljä eri lukua  $a, b, c$  ja  $d$ , joille  $abcd$  on neliöluku.

Tehtävänannon osa ”Kaikki joukon lukujen alkutekijät ovat pienempiä kuin 30” ohjaa tutkimaan lukujen alkutekijähajotelmia. Lukua 30 pienempiä alkulukuja on 10 kappaletta:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29.$$

Aritmetiikan peruslausetta käsittelevän luvun perusteella tiedämme, että joukon  $A$  luvut voidaan esittää 10 kokonaisluvun avulla: lukua  $n$  vastaa luvut  $v_2(n), v_3(n), \dots, v_{29}(n)$ .

Milloin  $abcd$  on neliöluku? Täsmälleen silloin, kun  $v_p(abcd)$  on parillinen kaikilla alkuluvuilla  $p$ . Lisäksi tiedetään, että  $v_p(abcd) = v_p(a) + v_p(b) + v_p(c) + v_p(d)$ . Huomionarvoista on, että tehtävän kannalta lukujen  $v_p(a), v_p(b), v_p(c)$  ja  $v_p(d)$  tarkoilla arvoilla ei ole väliä, vaan ainoastaan niiden parillisuuksilla on väliä.

Lukua  $n$  vastaavien kymmenen luvun  $v_2(n), v_3(n), \dots, v_{29}(n)$  parillisuuksien yhdistelmille on  $2^{10} = 1024$  vaihtoehtoa. Jos tämä määrä olisi ollut pienempi, kuten vaikkapa 500 (tarkka raja on noin  $\frac{2016}{3}$ ), niin olisimme voineet soveltaa laatikkoperiaatetta seuraavasti: Laatikkoperiaatteen nojalla on olemassa jotkin neljä eri lukua  $a, b, c$  ja  $d$ , joilla lukujen  $v_p(a), v_p(b), v_p(c)$  ja  $v_p(d)$  parillisuudet ovat samat kaikilla alkuluvuilla  $p$  (jotka ovat alle 30). Tällöin  $v_p(a) + v_p(b) + v_p(c) + v_p(d)$  olisi aina joko neljän parittoman luvun summa tai neljän parillisen luvun summa ja siten parillinen. Luku  $2^{10} = 1024$  on kuitenkin liian iso, joten täytyy keksiä jotain muuta.

Kriittinen idea on, ettei ole välttämätöntä, että kaikkien lukujen  $v_p(a), v_p(b), v_p(c)$  ja  $v_p(d)$  parillisuudet ovat samat: riittää, että  $v_p(a)$  ja  $v_p(b)$  ovat samaa parillisuutta ja että  $v_p(c)$  ja  $v_p(d)$  ovat samaa parillisuutta. Toisin sanoen pyrimme valitsemaan luvut  $a, b, c$  ja  $d$  niin, että luvut  $ab$  ja  $cd$  ovat neliölukuja. Tällöin myös  $abcd$  on neliöluku.

Tällä idealla ratkaisu saadaankin toimimaan. Laatikkoina toimivat ne 1024 kymmenen pituisia kokonaisluvun jonoa, jotka koostuvat nolista ja ykkösistä, ja palloina toimivat joukon  $A$  alkiot. Joukossa  $A$  on  $2016 \geq 1024 + 1$  lukua, joten laatikkoperiaatteen nojalla on olemassa jotkin kaksi eri joukon  $A$  alkioita  $a$  ja  $b$ , joilla on samat alkutekijöiden eksponenttien parillisuudet. Tällöin  $ab$  on neliöluku.

Tutkitaan nyt kaikkia loppuja joukon  $A$  alkioita. Näitä on  $2014 \geq 1024 + 1$  kappaletta. Voimme jälleen soveltaa laatikkoperiaatetta todetaksemme, että on olemassa jotkin joukon  $A$  alkiot  $c$  ja  $d$  (jotka eivät ole yhtä suuria kuin  $a$  tai  $b$ ), joilla  $cd$  on neliöluku. Nyt  $abcd$  on neliöluku, ja olemme valmiit.

## 19.2 Inklusion ja eksklusion periaate

Inklusion ja eksklusion periaate (tai vain inklusio-eksklusio) on hyvä apuväline erilaisten joukkojen laskemiseen. Käydään menetelmän idea läpi verrattain helpon esimerkin kautta.

### Tehtävä

Määritä niiden positiivisten kokonaislukujen määrä, jotka ovat enintään 300 ja jotka ovat jaollisia vähintään yhdellä luvuista 2, 3 ja 5.



Niiden lukujen määrä, jotka ovat jaollisia kahdella, on  $\frac{300}{2} = 150$ . Vastaavasti kolmella ja viidellä jaollisten lukujen määrät ovat  $\frac{300}{3} = 100$  ja  $\frac{300}{5} = 60$ . Onko vastaus siis  $150 + 100 + 60 = 310$ ? Ei tietenkään: tähän on yli 300. Ongelma on, että esimerkiksi kuudella jaolliset luvut tulee laskettua sekä kahdella jaollisiin lukuihin että kolmella jaollisiin lukuihin.

Ongelman voi korjata vähentämällä vastauksesta kuudella jaollisten lukujen määrä. Lisäksi pitää vähentää myös luvuilla  $2 \cdot 5 = 10$  ja  $3 \cdot 5 = 15$  jaollisten lukujen määrät. Kuudella, kymmenellä ja viidellätoista jaollisten lukujen määrät ovat  $\frac{300}{6} = 50$ ,  $\frac{300}{10} = 30$  ja  $\frac{300}{15} = 20$ .

Onko vastaus siis  $150 + 100 + 60 - (50 + 30 + 20) = 210$ ? Ei aivan. Edellisessä päättelyssä on vielä se ongelma, että luvulla  $2 \cdot 3 \cdot 5 = 30$  jaolliset luvut lasketaan kolmesti mukaan kahdella, kolmella ja viidellä jaollisten lukujen määrään, ja ne vähennetään kolmesti kuudella, kymmenellä ja viidellätoista jaollisten lukujen määriä laskettaessa. Ne tulee siis laskea vielä mukaan. Näitä lukuja on  $\frac{300}{30} = 10$  kappaletta.

Ei ole vaikeaa nähdä, että nyt jokainen luku tulee laskettua täsmälleen kerran vastausta laskettaessa. Vastaus on siis

$$\frac{300}{2} + \frac{300}{3} + \frac{300}{5} - \frac{300}{6} - \frac{300}{10} - \frac{300}{15} + \frac{300}{30} = 220.$$

Inklusion ja ekskluusion periaate yleistää edellisen ratkaisun ideaa. Olkoot  $A_1, A_2, \dots, A_n$  mielivaltaisia joukkoja. Tavoitteenamme on laskea niiden alkioden määrä, jotka kuuluvat vähintään yhteen joukoista  $A_1, \dots, A_n$  (kun joukoista  $A_i$  tiedetään sopivat tiedot). Edellisessä tehtävässä joukkoja on kolme: joukko  $A_1$  sisältää ne luvut väliltä  $[1, 300]$ , jotka ovat jaollisia kahdella, ja joukot  $A_2$  ja  $A_3$  määritellään vastaavasti.

Ennen pidemmälle etenemistä määritellään hieman notaatiota.

### Määritelmä

Olkoot  $A$  ja  $B$  joukkoja. Joukkojen  $A$  ja  $B$  unioni on se joukko, joka sisältää kaikki ne alkiot, jotka kuuluvat vähintään toiseen joukoista  $A$  ja  $B$ . Tätä joukkoa merkitään  $A \cup B$ .

### Määritelmä

Olkoot  $A$  ja  $B$  joukkoja. Joukkojen  $A$  ja  $B$  leikkaus on se joukko, joka sisältää kaikki ne alkiot, jotka kuuluvat molempiin joukoista  $A$  ja  $B$ . Tätä joukkoa merkitään  $A \cap B$ .

Monella joukolla unionit ja leikkaukset määritellään vastaavasti. Esimerkiksi  $A \cup B \cup C$  sisältää ne alkiot, jotka kuuluvat vähintään yhteen joukoista  $A, B$  ja  $C$ .

Nyt pääsemme itse tuloksen pariin.

**Lause (Inklusion ja eksklusion periaate)**

Olkoot  $A_1, A_2, \dots, A_n$  mielivaltaisia joukkoja. Pätee

$$\begin{aligned} |A_1 \cup A_2 \cup \dots \cup A_n| = & \sum_{1 \leq i \leq n} |A_i| \\ & - \sum_{1 \leq i < j \leq n} |A_i \cap A_j| \\ & + \sum_{1 \leq i < j < k \leq n} |A_i \cap A_j \cap A_k| \\ & \vdots \\ & + (-1)^{n+1} |A_1 \cap A_2 \cap \dots \cap A_n|. \end{aligned}$$

Pieni selitys on paikallaan. Laskeaksemme niiden alkioden määrän, jotka kuuluvat johonkin joukoista  $A_i$  (eli suureen  $|A_1 \cup A_2 \cup \dots \cup A_n|$ ) summaamme ensin yhteen jokaisen joukon  $A_i$  koot  $|A_i|$ . Tämän jälkeen tulee vähentää niiden alkioden määrä, jotka on laskettu kahdesti, eli ne, jotka kuuluvat kahteen joukkoon  $A_i$  ja  $A_j$ . Tämän jälkeen tulee lisätä ne alkiot, joita ei nyt ole vielä laskettu, eli jotka kuuluvat kolmeen joukkoon  $A_i, A_j$  ja  $A_k$ . Idea on siis sama kuin edellisessä ratkaisussa. Tapauksessa  $n = 3$  inklusio-eksklusio antaa

$$|A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| + |A_1 \cap A_2 \cap A_3|.$$

Inklusio-eksklusio tapauksessa  $n = 2$  kertoo, että  $|A \cup B| = |A| + |B| - |A \cap B|$ . Jos siis haluamme laskea niiden alkioden määrän, jotka kuuluvat vähintään toiseen joukoista  $A$  ja  $B$ , riittää tietää joukkojen  $A$  ja  $B$  koko sekä niiden leikkauksen koko. Vastaavasti leikkauksen koko voidaan laskea, kun tiedetään unionin ja itse joukkojen koko.

Lauseen todistus vastaa päättelyä, joka tehtiin esimerkkitoteutuksessa. Valitaan jokin alkio  $a$ , joka kuuluu johonkin joukoista  $A_i$ . Tällöin se kontribuoi joukon  $A_1 \cup A_2 \cup \dots \cup A_n$  kokoon yhden verran. Se myös kontribuoi lauseen yhtälön toiseen puoleen yhden verran. Jos nimittäin  $a$  kuuluu joukkoihin  $A_{i_1}, A_{i_2}, \dots, A_{i_k}$  (muttei muihin joukoista  $A_1, \dots, A_n$ ), niin sen vaikutus summaan

$$\sum_{1 \leq i \leq n} |A_i|$$

on  $k$ , vaikutus summaan

$$\sum_{1 \leq i < j \leq n} |A_i \cap A_j|$$

on  $\binom{k}{2}$  ja niin edelleen. Ja koska binomilauseen nojalla

$$\binom{k}{1} - \binom{k}{2} + \binom{k}{3} - \dots = 1 - (1-1)^k = 1,$$

alkio  $a$  kontribuoi myös toisen puolen summaan yhden verran. Toisin sanoen, jokainen alkio  $a$  lasketaan tasan yhden kerran summia laskettaessa.

Esitetään vielä toinen esimerkki inklusio-ekskluusion soveltamisesta.

### Tehtävä

Laske niiden joukon  $\{1, 2, 3, 4, 5, 6\}$  permutaatioiden määrä, jotka eivät kuvaa mitään alkioita itselleen.

Kaikkien permutaatioiden määrä on  $6! = 720$ . Riittää määrittää niiden permutaatioiden määrä, jotka kuvaavat vähintään yhden alkion itselleen, koska lopuksi tämä määrä voidaan vähentää kaikkien permutaatioiden määrästä vastauksen saamiseksi.

Valitaan inklusio-ekskluusioon kuusi joukkoa. Joukko  $A_i$  sisältää ne permutaatiot, jotka kuvaavat alkion  $i$  itselleen, kun  $1 \leq i \leq 6$ . Selvästikin  $|A_i| = 5! = 120$  kaikilla  $i$ , koska alkion  $i$  kuvautuessa itselleen on muille viidelle alkioille  $5!$  eri mahdollisuutta kuvautua toisilleen. Vastaavasti saadaan  $|A_i \cap A_j| = 4! = 24$  kaikilla  $i \neq j$ ,  $|A_i \cap A_j \cap A_k| = 3! = 6$  ja niin edelleen. Sovelletaan nyt inklusio-ekskluusiota.

Inklusio-ekskluusiossa on summia muotoa

$$\sum_{1 \leq i_1 < i_2 < \dots < i_k \leq 6} |A_{i_1} \cap \dots \cap A_{i_k}|,$$

missä  $1 \leq k \leq 6$ . Tämä summa käy läpi  $\binom{6}{k}$  vaihtoehtoa, ja jokaisen summattavan termin arvo on (yllä tehdyn päättelyn nojalla)  $(6-k)!$ . Täten

$$|A_1 \cup A_2 \cup \dots \cup A_6| = \binom{6}{1} 5! - \binom{6}{2} 4! + \binom{6}{3} 3! - \binom{6}{4} 2! + \binom{6}{5} 1! - \binom{6}{6} 0!,$$

minkä voi laskea olevan 455. Täten alkuperäisen ongelman vastaus on  $6! - 455 = 265$ .

## 19.3 Kahdella tavalla laskeminen

Kahdella tavalla laskeminen on konseptina hyvin yksinkertainen: jos sama asia lasketaan kahdella eri tavalla, saadaan aikaan yhtäsuuruus. Tässä on yksinkertainen esimerkki: Osoita, että

$$\binom{n}{0} + \binom{n}{1} + \dots + \binom{n}{n} = 2^n.$$

(Tätä ongelmaa on käsitelty myös Estitietoja-luvussa.) Ideana on laskea joukon  $\{1, 2, \dots, n\}$  osajoukkojen määrä kahdella eri tavalla. Yksi tapa on laskea yhteen nollan kokoisten osajoukkojen määrä, sitten yhden kokoisten osajoukkojen määrä ja niin edelleen. Tästä saadaan yhtälön vasen puoli. Toinen, helpompi tapa laskea osajoukot on seuraava: osajoukot voidaan rakentaa päättämällä, kuuluuko luku 1 osajoukkoon, kuuluuko luku 2 osajoukkoon ja niin edelleen. Tästä saadaan yhtälön oikea puoli. (Väite seuraa myös binomilauseella lausekkeen  $(1+1)^n$  suhteen. Tämä ratkaisu on kuitenkin pohjimmiltaan sama kuin edellä esitetty.)

Edellä saatu tulos ei ole ilmeinen: summaa  $\binom{n}{0} + \dots + \binom{n}{n}$  ei ole helppoa sieventää luvuksi  $2^n$  lähtemällä binomikertoimien määritelmästä  $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ . Vaikka kahdella tavalla laskeminen on periaatteena hyvin yksinkertainen, voi sillä saada todistettua vaikeitakin tuloksia. Kuten laatikkoperiaatteen tapauksessa, kyse on nytkin siitä, miten periaatetta soveltaa. Käymme läpi kolme esimerkkiä.

Ensimmäinen tehtävä on klassikko, joka on esiintynyt myös valmennustehtävänä.

### Tehtävä

Olkoon  $n$  positiivinen kokonaisluku. Osoita, että

$$\sum_{i=0}^n \binom{n}{i}^2 = \binom{2n}{n}.$$

Kuten edellisessä esimerkissä, naiivi idea käyttää binomikertoimien algebrallista määritelmää ja sieventää lausekkeita ei johda ratkaisuun. Pitää siis keksiä jotain ovelampaa.

Tässä binomikertoimia on järkevämpää tulkita niiden merkityksen kautta ( $\binom{n}{k}$  kertoo, kuinka monella tavalla  $n$  alkioista voidaan valita  $k$  alkioita) kuin algebrallisen määritelmän kautta ( $\binom{n}{k}$  on yhtä suuri kuin  $\frac{n!}{k!(n-k)!}$ ). Annetun yhtälön oikea puoli siis kertoo, kuinka monella tavalla  $2n$  alkioista voidaan valita  $n$  alkioita. Vasen puoli taas käsittelee sitä, miten  $n$  alkioista voidaan valita jokin määrä alkioita.

Kriittinen idea tehtävän ratkaisemiseksi on jakaa tämä  $2n$ -alkioinen joukko kahdeksi  $n$ -alkioiseksi joukoksi. Motivaationa on yrittää saada yhtälön eri puolien merkitykset mahdollisimman lähelle toisiaan. Tutkitaan siis vaikkapa joukkoa  $S = \{1, 2, \dots, 2n\}$ , joka on jaettu kahdeksi  $n$  alkion joukoksi  $A = \{1, 2, \dots, n\}$  ja  $B = \{n+1, n+2, \dots, 2n\}$ .

Nyt kannattaa yrittää tulkita yhtälön vasenta puolta joukkojen  $A$  ja  $B$  kautta. Termin  $\binom{n}{i}^2$  voidaan tulkita kertovan, kuinka monta tapaa on valita  $i$  alkioita kummastakin joukosta  $A$  ja  $B$ . Yhteensä valitsemme siis  $2i$  alkioita. Olisi kuitenkin ollut parempi, jos alkioita olisi valittu  $n$  kappaletta kuten annetun yhtälön oikealla puolella. Tämä voidaan kuitenkin korjata:  $\binom{n}{i} = \binom{n}{n-i}$ , eli sen sijaan, että joukosta  $B$  valitaan  $i$  alkioita, voidaan ajatella, että joukosta  $B$  valitaan  $n-i$  alkioita.

Olemme siis valmiit: Yhtälön molemmat puolet laskevat  $2n$ -kokoisen joukon  $S$  kaikkien  $n$ -kokoisten osajoukkojen lukumäärän. Yhtälön oikea puoli tekee tämän ilmeisimmällä tavalla. Yhtälön vasen puoli tekee tämän laskemalla osajoukoista ne, joissa on  $i$  alkioita joukosta  $A$  ja  $n-i$  alkioita joukosta  $B$ , ja käymällä kaikki luvun  $i$  arvot läpi.

Kommentti: Alussa esitetty helpompi esimerkki  $\sum_{i=0}^n \binom{n}{i} = 2^n$  ratkeaa binomilauseella heti tulkitsemalla yhtälön puolet eri esityksinä luvulle  $(1+1)^n$ . Tätä tehtävää ei ole kuitenkaan aivan niin helppo ratkaista binomilauseella, koska binomilause ei anna binomikertoimien neliöitä  $\binom{n}{i}^2$ . Seuraava ratkaisu on kuitenkin mahdollinen.

Tutkitaan lauseketta  $(1+x)^{2n}$  ja erityisesti sen termin  $x^n$  kerrointa  $x$ :n ollessa muuttuja. Binomilauseen nojalla tämä on  $\binom{2n}{n}$ . Toisaalta voidaan kirjoittaa  $(1+x)^{2n} =$

$(1+x)^n \cdot (1+x)^n$ . Voimme nyt laskea ensimmäisestä tulontekijästä, mikä sen termin  $x^i$  kerroin on, ja toisesta tulontekijästä, mikä sen termin  $x^{n-i}$  kerroin on. Kun tämä tehdään kaikille  $i$ , polynomien kertolaskulla saadaan tulon  $(1+x)^{2n}$  termin  $x^n$  kerroin. Haluttu yhtäsuuruus seuraa.

Binomilauseeseen perustuva ratkaisu on (jälleen) pohjimmiltaan sama kuin kombinatorisempi ratkaisu. Algebrallinen lähestymistapa on kuitenkin usein varsin hyödyllinen. Menetelmä on niinkin yleinen, että sillä on oma nimensä: generoivat funktiot (engl. generating functions). Kahdella tavalla laskeminen -menetelmän tavoin tässäkin ei ole ideatasolla mitään ihmeellistä: tutkimme erilaisten polynomien kertoimia.<sup>88</sup> Hyöty tulee siitä, että generoivat funktiot antavat ympäristön, jossa tietynlaisia ongelmia on luonnollista käsitellä. Yksi esimerkkisovellus generoivista funktioista on annettu luvussa Lineaariset rekursiot.

Seuraava tehtävä on hieman erilainen esimerkki kahdella tavalla laskemisesta. Tehtävään esitetään ensiksi ”rehellinen” ratkaisu, minkä jälkeen esitetään elegantti kombinatorinen ratkaisu. Tämän kombinatorisen ratkaisun menetelmä tunnetaan nimellä ”tähdet ja tikut” (engl. stars and bars).

### Tehtävä

Olkoot  $k$  ja  $n$  positiivisia kokonaislukuja. Määritä yhtälön

$$x_1 + x_2 + \dots + x_k = n$$

niiden kokonaislukuratkaisujen määrä, joissa  $x_i \geq 0$  kaikilla  $i$ .

Tässä kaksi ratkaisua  $x_1, x_2, \dots, x_k$  ja  $x'_1, x'_2, \dots, x'_k$  ovat eri ratkaisut, jos  $x_i \neq x'_i$  jollain  $i$ . Esimerkiksi arvoilla  $n = 3$  ja  $k = 2$  ratkaisut  $1 + 2 = 3$  ja  $2 + 1 = 3$  ovat eri ratkaisut. Lisäksi  $3 + 0 = 3$  ja  $0 + 3 = 3$  ovat ratkaisuja.

Pienillä lukujen  $n$  ja  $k$  arvoilla vastauksen pystyy laskemaan helposti käsin, mutta suurilla arvoilla laskeminen on vaikeaa, ellei sitä tee järjestelmällisesti. Yksi idea tehdä tapausten laskemista systemaattista on tutkia ensiksi tapaus  $x_1 = 0$ , sitten tapaus  $x_1 = 1$  ja jatkaa vastaavasti, kunnes lopulta tutkitaan tapaus  $x_1 = n$ . Tästä saamme samalla seuraavan, yleisen tuloksen.

Olkoon  $f(k, n)$  haluttu arvo. Päte

$$f(k, n) = \sum_{i=0}^n f(k-1, n-i).$$

Tässä summan termi  $i$  vastaa ratkaisuja, joissa  $x_1 = i$ .

Nyt arvoja on oikeastaan melko helppo laskea. Alla  $i$ :s vaakarivi vastaa arvoa  $k = i$ , ja tälle riville on lueteltu arvot  $f(i, 0), f(i, 1), \dots, f(i, 5)$ . Tällöin rivin  $i$  kohdan  $j$  luku on rivin  $i - 1$  lukujen summa kohtaan  $j$  asti.

<sup>88</sup>Generoivilla funktiolla tutkitaan yleensä myös ääretönasteisia polynomeja, eli ns. potenssisarjoja (engl. power series). Niiden ei kannatakaan ajatella olevan samoja kuin ”normaalit” äärellisasteiset polynomit, vaan käsitteet kannattaa pitää erillään. Potenssisarjojen ja polynomien käsittely on kuitenkin hyvin samankaltaista.

- 1, 1, 1, 1, 1, 1
- 1, 2, 3, 4, 5, 6
- 1, 3, 6, 10, 15, 21
- 1, 4, 10, 20, 35, 56

Näyttäisi siltä, että jokaisen kohdan luku on vain sen yläpuolella ja vasemmalla puolella olevien lukujen summa. Tämä on selvää siitä, miten luvut on määritelty, ja voidaan todistaa seuraavasti: käyttämällä kahdesti aiemmin saatua summayhtälöä luvuille  $f(k, n)$  saadaan

$$\begin{aligned}
 & f(k, n) \\
 &= \sum_{i=0}^n f(k-1, n-i) \\
 &= f(k-1, n) + \sum_{i=1}^n f(k-1, n-i) \\
 &= f(k-1, n) + \sum_{i=0}^{n-1} f(k-1, (n-1)-i) \\
 &= f(k-1, n) + f(k, n-1).
 \end{aligned}$$

Lisäksi näyttäisi siltä, että listan luvut ovat binomikertoimia. Binomikertoimet näyttäisivät olevan tarkalleen sellaiset, että

$$f(k, n) = \binom{n+k-1}{n}.$$

Tämä on hyvin helppoa todistaa induktiolla muuttujan  $n+k$  suhteen käyttämällä yllä saatua yhtälöä  $f(k, n) = f(k-1, n) + f(k, n-1)$  ja Pascalin identiteettiä  $\binom{m}{k} + \binom{m}{k+1} = \binom{m+1}{k+1}$ . Motivaatio tehdä induktio muuttujan  $n+k$  suhteen on se, että haluamme käydä lukuparit  $(k, n)$  sellaisessa järjestyksessä, että parit  $(k-1, n)$  ja  $(k, n-1)$  käydään läpi ennen paria  $(k, n)$ . Yksityiskohdat induktiosta jätetään lukijalle.

Huomaa, että yllä käytännössä katsoen todistettiin, että ns. Pascalin kolmiosta<sup>89</sup> löytyvät luvut ovat aina sopivia binomikertoimia. Tähän vihjattiin jo Esitietoja-luvussa binomikertoimia käsittelevässä osiossa.

Vastaus alkuperäiseen ongelmaan on siis  $\binom{n+k-1}{n}$ . Vastaus on yllättävän sievä, ja tälle on luonnollinen syy. Seuraavaksi esitetään tehtävälle lyhyt ratkaisu, joka kertoo, mistä nimitys ”tähdet ja tikut” tulee.

<sup>89</sup>Pascalin kolmio rakennetaan laittamalla ensiksi ylimmälle riville luku 1. Tämän jälkeen seuraava rivi rakennetaan aina niin, että siinä on yksi luku enemmän kuin edellisellä rivillä, ja jokainen uuden rivin luku on sen kahden yläpuolella olevan luvun summa (pois lukien reunimmaisiet luvut, joihin asetetaan arvo 1). Ensimmäiset rivit ovat siis (1), (1, 1), (1, 2, 1), (1, 3, 3, 1) ja (1, 4, 6, 4, 1). Huomaa, että nämä rivit saadaan aiemmin esitetystä listauksesta lukemalla sitä viistorivi kerrallaan. Aiemmin tehty listaus on siis Pascalin kolmio, vaikkakin se on kirjoitettu eri suuntaan kuin yleensä.

Asetetaan riviin  $n$  tähteä. Nyt sellaisia  $k$  kokonaisluvun  $x_1, x_2, \dots, x_k$  jonoja, joilla  $x_1 + x_2 + \dots + x_k = n$ , voidaan kuvata jakamalla nämä  $n$  tähteä  $k - 1$  tikulla  $k$  joukkoon. Tikkujen muodostama jako kertoo, mikä arvo kullekin muuttujalle asetetaan. Alla on esitetty yhtälön  $x_1 + x_2 + x_3 = 6$  ratkaisu  $x_1 = 2, x_2 = 1, x_3 = 3$ . Kuvassa tähdet on yksinkertaisuuden vuoksi korvattu ympyröillä.



Huomaa, että jonkin muuttujan  $x_i$  arvo voi olla nolla. Tällöin kuviosta löytyy kaksi tikkua, joiden välissä ei ole yhtään ympyrää.

Ratkaisun päähuomio on seuraava: jokainen  $n$  tähden ja  $k - 1$  tikun asetelma riviin vastaa yhtä yhtälön  $x_1 + x_2 + \dots + x_k = n$  ratkaisua ja päinvastoin. Tämä käy järkeen, mutta tässä on vielä lisää yksityiskohtia: Olkoon  $i$ :nnettä tikkua ennen  $a_i$  tähteä (kun tarkastelemme asetelmaa vasemmalta oikealle). Määritellään  $x_i = a_i - a_{i-1}$  kun  $2 \leq i \leq k - 1$ ,  $x_1 = a_1$  ja  $x_k = n - a_{k-1}$ . Nyt jokaista tikkuasetelmaa vastaa täsmälleen yksi yhtälön  $x_1 + \dots + x_k = n$  ratkaisu ja toisin päin.

Selvästikin  $n$  tähteä ja  $k - 1$  tikkua voidaan asettaa riviin  $\binom{n+k-1}{n}$  eri tavalla: Voidaan ajatella, että rivissä on valmiina  $n + k - 1$  paikkaa, joista  $n$  kohtaan tulee laittaa ympyrä ja  $k - 1$  kohtaan tulee laittaa tikku. On siis  $\binom{n+k-1}{n}$  eri tapaa valita ympyröiden sijainnit, jolloin tikkujen sijainnit määräytyvät yksikäsitteisesti. Tämä päättää ratkaisun.

Kommentti: Ensimmäisenä esitetty laskennallisempi ratkaisu on hyvin luonnollinen. Aluksi lähdetään siitä, miten ratkaisuja laskisi käsin, minkä kautta nähdään, miten vastaukset muuttujien  $n$  ja  $k$  eri arvoilla riippuvat toisiinsa. Listaus ja säännönmukaisuuden etsiminen on varsin yleinen strategia, ja monesti tehtävänannosta näkee hyvin nopeasti, onko tämä lähestymistapa mahdollinen.

Jälkimmäinen ratkaisu perustuu kahdella tavalla laskemiseen, mutta hieman eri tavalla kuin aiemmat esimerkit. Menetelmää voi kuvata tarkemmin bijektion<sup>90</sup> rakentamisena jonkin joukon koon laskemiseksi. Ratkaisussa bijektio rakennettiin yhtälön  $x_1 + x_2 + \dots + x_k = n$  epänegatiivisten kokonaislukuratkaisujen ja  $n$  tähden ja  $k - 1$  tikun asetelmien välille. Bijektion olemassaolon tärkein seuraus on, että näiden joukkojen koot ovat samat. Koska tähtien ja tikkujen asetelmien määrä on helppoa laskea, pystytään myös yhtälön ratkaisujen määrä laskemaan.

Viimeinen tehtävä kahdella tavalla laskemisesta on vuoden 2006 Pohjoismaisesta matematiikkakilpailusta.

### Tehtävä

100 × 100-shakkilaudan neliöt väritetään 100:lla eri värillä. Kuhunkin ruutuun käytetään vain yhtä väriä, ja joka väriä käytetään tasan sataan ruutuun. Osoita, että laudalla on jokin vaaka- tai pystyriivi, jonka ruutuihin on käytetty ainakin kymmentä väriä.

<sup>90</sup>Bijektio on määritelty tarkemmin luvussa Funktionaaliryhtälöt.

Ei ole vaikeaa nähdä, että asettamalla kunkin värin  $10 \times 10$  -neliöön saadaan luotua tapaus, jossa joka pysty- ja vaakarivillä on tasan kymmentä väriä. Tätä tietoa ei suoraan tarvita ratkaisussa, mutta se antaa intuitiota ongelmaan.

Voimme tehdä vastaoletuksen – siitä ei ainakaan ole haittaa. Oletetaan siis, että jokaisella pysty- ja vaakarivillä on enintään yhdeksää väriä.

Jokaisella pysty- ja vaakarivillä on siis vain vähän värejä. Tämän ei pitäisi olla mahdollista. Mikä on intuitiivinen selitys sille, miksi tämä on mahdotonta? Ajatuksena on, että jokainen väri jakautuu laajalle alueelle, tarkemmin sanoen monelle eri pysty- ja vaakariville.<sup>91</sup> Koska värejä on paljon (sata), niin siinä tapauksessa, että jokainen väri osuu riittävän monelle eri pysty- ja vaakariville, tulee jollain rivillä olla paljon värejä.

Kriittinen idea on keksitty, ja enää ”kvalitatiivinen” tarkastelu tulee muuttaa ”kvantitatiiviseksi”. Tutkitaan kaikkia 200 pysty- ja vaakariviä. Olkoon  $S$  summa määrästä ”kuinka montaa eri väriä tällä rivillä on” kaikkien 200 rivin yli. Koska jokaisella rivillä on vastaoletuksen vuoksi enintään 9 väriä, pätee  $S \leq 9 \cdot 200 = 1800$ .

Tutkitaan sitten sitä, kuinka paljon kukin yksittäinen väri kontribuoi summaan  $S$ . Tutkitaan jotain väriä, ja oletetaan, että sitä esiintyy  $a$  eri vaakarivillä ja  $b$  eri pystyrivillä. Tavoitteena on todistaa, että  $a+b$  on suuri. Intuitiivisesti kaikkein ”tiivein” asettelu värin ruuduille on asettaa ne  $10 \times 10$  -neliöksi, jolloin  $a = b = 10$  ja  $a+b = 20$ . Tätä ei ole kovin vaikea todistaa: Koska värin ruutuja on vain tietyillä  $a$  pystyrivillä ja  $b$  vaakarivillä, tulee näiden ruutujen olla pysty- ja vaakarivien leikkauspisteissä. Näitä leikkauspisteitä on  $ab$  kappaletta. Värin ruutuja on 100 kappaletta, joten tulee päteä  $ab \geq 100$ .

Haluamme siis todistaa, että ehdosta  $ab \geq 100$  seuraa, että  $a+b \geq 20$ . Tämä seuraa mm. aritmeettis-geometrisesta epäyhtälöstä ( $\frac{a+b}{2} \geq \sqrt{ab}$ ), joka seuraa epäyhtälöstä  $(\sqrt{a} - \sqrt{b})^2 \geq 0$ . Mikäli tätä ei näe, voi myös edetä suoraan lukiomenetelmin seuraavasti (käytännössä samalla todistaen aritmeettis-geometrisen epäyhtälön kahden muuttujan tapauksen).<sup>92</sup>

Todistetaan, että kaikilla positiivisilla reaalityyppisillä  $a$  ja  $b$ , joilla  $ab \geq 100$ , pätee  $a+b \geq 20$ . Jos  $ab > 100$ , voidaan muuttujaa  $b$  pienentää, jotta  $ab = 100$ . Tällöin summa  $a+b$  pienenee. Riittää siis tutkia vaikeinta tapausta, jossa  $ab = 100$ . Nyt  $b = \frac{100}{a}$ , joten todistettavana on  $a + \frac{100}{a} \geq 20$ . Kertomalla puolittain muuttujalla  $a$  tämä palautuu toisen asteen epäyhtälöksi, joka osataan ratkaista. Epäyhtälö muuttuu muotoon  $(a-10)^2 \geq 0$ .

Nyt siis jokainen väri lisää summaan  $S$  luvun, joka on ainakin 20 verran, joten  $S \geq 20 \cdot 100 = 2000$ . Tämä on ristiriita aiemman epäyhtälön  $S \leq 1800$  kanssa. Vasta oletus oli väärä, joten olemme valmiit.

<sup>91</sup>Tämä on nähdäkseni sellainen ajatus, joka tulee varsin helposti mieleen tehtävää ratkoessa, mutta jota on vaikea pukea sanoiksi. Lisäksi arveluttava tekijä on, voiko tehtävää saada ratkaistua tällä idealla eli voiko ideaa formalisoida.

<sup>92</sup>Voisimme myös käydä suoraan tapauksia läpi:  $a$  ja  $b$  ovat positiivisia kokonaislukuja. Oletetaan, että  $a \geq b$ . Nyt  $ab \geq 100$  tarkoittaa, että  $a \geq 10$ . Jos  $a \geq 20$ , olemme tietysti valmiit. Riittää enää tutkia kymmenen tapausta  $a = 10, 11, \dots, 19$ , ja tämä on helppoa.



## 19.4 Esimerkkitehtäviä

Ensimmäinen esimerkkitehtävä on vuoden 2017 IMO-lyhytlistalta.

### Tehtävä

Herra Alex pelaa seuraavaa peliä 9 ruudun rivistä koostuvalla laudalla: Aluksi jokainen ruutu on tyhjä. Jokaisella siirrolla herra Alex suorittaa toisen seuraavista kahdesta operaatiosta.

1. Valitse mikä tahansa luku muotoa  $2^j$ , jossa  $j$  on epänegatiivinen kokonaisluku, ja laita se johonkin tyhjään ruutuun.
2. Valitse kaksi (ei välttämättä vierekkäistä) ruutua, joissa on sama luku. Olkoon tämä luku  $2^j$ . Korvaa toisen ruudun luku luvulla  $2^{j+1}$  ja poista toisen ruudun luku.

Pelin lopuksi yhdessä ruudussa on luku  $2^n$ , jossa  $n$  on positiivinen kokonaisluku, ja muut ruudut ovat tyhjiä. Määritä suurin sellainen määrä siirtoja, jonka herra Alex on voinut tehdä, luvun  $n$  avulla ilmaistuna.

Luonnollinen ensiaskel on tietysti tutkia, mikä vastaus on pienillä luvun  $n$  arvoilla. Ei ole vaikeaa nähdä, että kun  $n \leq 8$ , niin vastaus on  $2^{n+1} - 1$ , koska voimme edetä ”optimaalisesti”: Lisäämme taululle aina pelkästään lukuja  $2^0 = 1$ , ja yhdistelemme näitä sopivasti. Aina jos taululla on kaksi samaa lukua, yhdistetään ne tyypin 2 operaatiolla. Koska  $n \leq 8$ , niin siinä tapauksessa, että peli ei ole vielä päättynyt, ovat taulun luvut aina joitain lukuja joukosta  $2^0, 2^1, \dots, 2^7$ . Täten aina voidaan joko yhdistää kaksi lukua tai lisätä uusi luku. Tyypin 1 operaatioita tehdään  $2^n$  kappaletta ja tyypin 2 operaatioita  $2^n - 1$ .

Vastaavasti huomataan, että suuremmilla luvun  $n$  arvoilla emme pysty lisäämään pelkkiä ykkösiä: jossain kohtaa tulisi vastaan tilanne, jossa taululla on luvut  $2^1, 2^2, \dots, 2^8$  ja yksi tyhjä ruutu. Tähän tyhjään ruutuun täytyykin laittaa luku  $2^1 = 2$ .

On siis vaikeaa arvata, mikä vastaus voisi olla. Ei ole edes selvää, kasvaako vastaus eksponentiaalisesti: arvoilla  $n \leq 8$  vastaus on  $2^{n+1} - 1$ , mutta suuremmilla luvun  $n$  arvoilla kasvu hidastuu merkittävästi, koska taululle tulee lisätä myös isoja lukuja.

Voimme kuitenkin lähestyä vastauksen arvaamista myös toisesta suunnasta. Tehtävässä on sanottu, että ruutuja on yhdeksän. Voimme tietenkin pelata peliä myös pienemmillä (tai isommilla) laudoilla. Jos ruutuja on 1, peli on tylsä: siirtoja voi tehdä aina vain yhden kappaleen. Jos ruutuja on 2, niin peli etenee seuraavasti: Taululle lisätään kaksi kappaletta lukuja  $2^0$ , jotka yhdistetään. Taululle lisätään luku  $2^1$ , ja taulun luvut yhdistetään. Taululle lisätään luku  $2^2$ , ja taulun luvut yhdistetään. Tämä on selvästikin optimaalinen tapa pelata peliä (kovin montaa muuta tapaa ei edes ole), ja siirtojen määräksi saadaan  $2n + 1$ .

Tutkitaan sitten kolmen ruudun lautaa. Miten peliä kannattaa pelata? On tietysti järkevintä laittaa laudalle aina mahdollisimman pieniä lukuja. Huomataankin, että

muilla tekijöillä ei ole väliä: jos tiedämme, mitkä luvut laudalle lisättiin, ja tiedämme laudan lopputilanteen (yhdessä ruudussa on luku  $2^n$  ja muut ovat tyhjiä), niin siirtojen määrä voidaan ainakin teoriassa laskea.

Pelaamalla peliä hiukan keksitään seuraava strategia: Pidetään ensimmäisessä ruudussa aina isointa lukua. Jos ensimmäisessä ruudussa on luku  $2^i$ , niin käytetään kahta muuta ruutua luomaan toinen luku  $2^i$ . Yhdistetään nämä, jolloin ensimmäisessä ruudussa on luku  $2^{i+1}$  ja muut ruudut ovat tyhjiä. Ei ole aivan selvää, onko tämä paras mahdollinen strategia, mutta se tuntuu optimaaliselta.

Lasketaan tehtyjen operaatioiden määrä. Kuinka monta operaatiota tehdään, kun siirrytään luvusta  $2^i$  lukuun  $2^{i+1}$ ? Kahden ruudun variantin nojalla toisen luvun  $2^i$  kopion tekemiseen kuluu  $2i + 1$  operaatiota. Lopuksi tehdään yhdistäminen, josta seuraa yksi lisäoperaatio. Täten operaatioita tehdään yhteensä

$$1 + \sum_{i=0}^{n-1} (2i + 2) = 1 + 2n + \sum_{i=0}^{n-1} 2i = 1 + 2n + n(n - 1) = n^2 + n + 1.$$

(Ensimmäinen ykkönen vastaa ensimmäistä siirtoa, jossa ensimmäiseen ruutuun lisätään luku  $2^0$ .)

Huomataan, että vastaus on toisen asteen polynomi. Kahdella ruudulla vastaus oli ensimmäisen asteen polynomi, ja yhdellä ruudulla nollannen asteen polynomi (eli vakio). Ei hämmästyttäisi, jos  $k$  ruudulla vastaus olisi  $k - 1$  asteen polynomi. Vastaus ei siis vaikuta kasvavan eksponentiaalisesti luvun  $n$  mukana.

Emme ole vielä todistaneet, että kolmen ruudun varianttiin käyttämämme strategia on optimaalinen. Strategialla on kuitenkin ilmeinen variantti  $k$  ruudulle: yhdessä ruudussa pidetään isointa lukua, ja lopuilla  $k - 1$  ruudulla luodaan aina kopio isoimmasta luvusta. Pystymme laskemaan vastauksen mille tahansa ruutujen määrälle tällä tavalla, kun oletetaan, että strategia on optimaalinen. Todistetaan suoraan yleisessä tapauksessa, että strategia on optimaalinen. Lasketaan tämän jälkeen itse vastaus.

Olkoon  $f(k, n)$  vastaus tehtävään  $k$  ruudulla. Strategiamme idea on siis ensiksi  $f(k, n - 1)$  operaatiolla saada rakennettua luku  $2^{n-1}$ , minkä jälkeen jäljelle jäävillä  $k - 1$  ruudulla tehdään  $f(k - 1, n - 1)$  operaatiota toisen luvun  $2^{n-1}$  muodostamiseksi. Lopuksi käytetään yksi operaatio yhdistämiseen. Tiedämme siis, että  $f(k, n) \geq f(k, n - 1) + f(k - 1, n - 1) + 1$ . Todistamme seuraavaksi, että tässä epäyhtälössä pätee yhtäsuuruus.

Tutkitaan luvun  $2^n$  saavuttamista  $k$  ruudulla. Tähän on kaksi tapaa. Ensimmäinen tapa on lisätä taululle luku  $2^n$  heti, jolloin tehdään yhteensä vain yksi siirto. Toinen on saada taululle aikaan kaksi kappaletta lukua  $2^{n-1}$  ja yhdistää ne.

Strategiassamme tehdään niin, että ensiksi luodaan luku  $2^{n-1}$  käyttämällä  $k$  ruutua niin, että loput  $k - 1$  ruutua ovat tyhjiä. Tämän jälkeen loppuja  $k - 1$  ruutua käytetään luomaan kopio luvusta  $2^{n-1}$ . Kysymys kuuluu: onko olemassa parempaa strategiaa, jossa ensimmäisen luvun  $2^{n-1}$  syntymisen jälkeen jokin loppuista  $k - 1$  ruudusta on epätyhjä? Intuitio sanoo, että tämä ei ole mahdollista: nämä ylimääräiset luvut vain vievät tilaa. Alla on tähän ideaan pohjautuva todistus.

Ennen pelin viimeistä siirto laudalla on kaksi kappaletta lukua  $2^{n-1}$ . Jokainen pelin aikana taululle lisättävä luku voidaan ajatella ennen pitkää yhdistyvän joko ensimmäiseen tai toiseen luvuista  $2^{n-1}$ . Voimme siis jakaa pelin aikana syntyvät luvut kahteen joukkoon  $A$  ja  $B$  niin, että emme (ennen pelin viimeistä siirtoa) yhdistä kahta lukua, joista toinen on joukossa  $A$  ja toinen on joukossa  $B$ .

Symmetrian vuoksi voidaan olettaa, että taululle ensimmäisenä lisättävä luku kuuluu joukkoon  $A$ . Selvästikin joukon  $A$  sisällä tehdään enintään  $f(k, n-1)$  operaatiota luvun  $2^{n-1}$  saavuttamiseksi. Koska taululla on aina vähintään yksi joukon  $A$  luku (paitsi pelin päätyttyä), niin joukon  $B$  luvuille on aina tilaa enintään  $k-1$  ruutua. Täten joukon  $B$  sisällä tehdään enintään  $f(k-1, n-1)$  operaatiota luvun  $2^{n-1}$  saavuttamiseksi. Operaatioita tehdään siis yhteensä enintään  $f(k, n-1) + f(k-1, n-1) + 1$ , missä viimeinen ykkönen tulee lukujen  $2^{n-1}$  yhdistämisestä.

Olemme siis todistaneet, että  $f(k, n) \leq f(k, n-1) + f(k-1, n-1) + 1$ . Nyt tämän ja aiemman toisen suunnan epäyhtälön nojalla pätee

$$f(k, n) = f(k, n-1) + f(k-1, n-1) + 1.$$

Lasketaan seuraavaksi vastaus. Tiedämme jo vastauksen arvoilla  $k = 1, 2$  ja  $3$ . Voimme tietysti jatkaa tästä eteenpäin arvoille  $k = 4, 5, \dots, 9$  ja saada näin vastauksen tehtävään. Tämä on ihan toimiva tapa, mutta olisi parempi, jos olisi mahdollista laskea vastaus yleisessä tapauksessa. Tällöin konkreettisilla luvuilla ei tarvitse laskea niin paljon, ja laskuvirheen riski on pienempi. (Lisäksi naiivi laskeminen antaa vastauksen suoraan polynomina, kun taas alla annetaan vastaus muodossa, joka on kuvailevampi.)

On (ainakin) kaksi tapaa saada laskettua  $f(k, n)$ . Ensimmäinen perustuu siihen, että huomataan rekursion olevan hyvin samankaltainen kuin binomikertoimilla (ks. ”tähdet ja tikut”). Ei ole kaukaa haettava arvata, että  $f(k, n)$  voidaan esittää binomikertoimien avulla. Tästä motivoituneena voi määrittää esimerkiksi mitä  $f(3, n)$  on binomikertoimien avulla lausuttuna.

Laskimme aiemmin, että  $f(3, n) = n^2 + n + 1$ . Esitetään tämä binomikertoimien  $\binom{n}{i}$  summana. Binomikerroin  $\binom{n}{i}$  voidaan tulkita polynomina muuttujan  $n$  suhteen:  $\binom{n}{i} = \frac{n(n-1)(n-2)\cdots(n-(i-1))}{i!}$ . (Huomaa, että tämä määritelmä toimii myös silloin, kun  $n$  ei ole kokonaisluku.) Tämän polynomin aste on  $i$ . Siis jos  $n^2 + n + 1$  on binomikertoimien summa, niin kaikissa termeissä tulee päteä  $i \leq 2$ . Jotta termin  $n^2$  kerroin saadaan oikein, tulee binomikertoimen  $\binom{n}{2}$  kertoimen olla 2. Nyt

$$2\binom{n}{2} = 2 \cdot \frac{n(n-1)}{2} = n^2 - n,$$

joten olemme  $2n+1$  päässä oikeasta vastauksesta  $n^2 + n + 1$ . Polynomi  $2n+1$  voidaan vastaavasti esittää binomikertoimien avulla korkeimman asteen termistä aloittaen. Lopulta saadaan

$$f(3, n) = n^2 + n + 1 = 2\binom{n}{2} + 2\binom{n}{1} + \binom{n}{0}.$$

Laskemalla tarvittaessa vielä lisää erikoistapauksia keksitään yleiselle tapaukselle arvaus

$$f(k, n) = 2\binom{n}{k-1} + 2\binom{n}{k-2} + \dots + 2\binom{n}{1} + 1.$$

On suoraviivaista tarkistaa, että tämä toteuttaa rekursioyhtälön, käyttäen Pascalin identiteettiä

$$\binom{n-1}{i-1} + \binom{n-1}{i} = \binom{n}{i}.$$

Tässä on toinen tapa, jolla rekursion voi saada selville. On saatu rekursioyhtälö  $f(k, n+1) - f(k, n) = f(k-1, n) + 1$ . Tästä seuraa induktiolla muuttujan  $k$  suhteen, että  $f(k, n)$  on astetta  $k-1$  oleva polynomi muuttujan  $n$  suhteen (katso Summia-luku, jossa käsitellään yleistä tilannetta  $f(x+1) - f(x) = Q(x)$ , missä  $Q$  on polynomi). Lisäksi tämän polynomin arvoista tiedetään, että  $f(k, n) = 2^{n+1} - 1$  kaikilla  $0 \leq n \leq k-1$  (tämä todistettiin aiemmin arvolla  $k=9$ , ja yleinen tapaus on täysin analoginen). Tiedämme siis astetta  $k-1$  olevan polynomin  $f(k, n)$  arvoista  $k$  arvoa  $f(k, 0), \dots, f(k, k-1)$ . Nämä arvot määräävät polynomin yksikäsitteisesti.<sup>93</sup>

Enää tulee löytää sellainen polynomi  $P(x)$ , jolla  $P(x) = 2^{x+1} - 1$  kaikilla  $x = 0, 1, \dots, k-1$ . Tämä vaatii hieman mielikuvitusta, ja auttaa, jos on huomannut, että binomikertoimista voisi olla hyötyä. Kaikilla kokonaisluvuilla  $x \geq 0$  pätee

$$\binom{x}{0} + \binom{x}{1} + \dots + \binom{x}{x} = 2^x.$$

Tästä seuraa

$$2\binom{x}{0} + 2\binom{x}{1} + \dots + 2\binom{x}{k-1} = 2^{x+1}$$

kaikilla  $0 \leq x \leq k-1$ . Vähentämällä puolittain ykkönen saadaan, että polynomi

$$P(x) = \binom{x}{0} + 2\binom{x}{1} + \dots + 2\binom{x}{k-1}$$

toteuttaa yhtälön  $P(x) = 2^{x+1} - 1$  kaikilla  $0 \leq x \leq k-1$ .

Vastaus tehtävään on siis

$$1 + 2\binom{n}{1} + 2\binom{n}{2} + \dots + 2\binom{n}{8}.$$

Kommentti: Tässä tehtävässä pienempien tapauksien tarkastelusta oli kahdestakin syystä hyötyä. Ensinnäkin sitä kautta saatiin intuitiota siihen, miten ongelma käyttäytyy. Toiseksi vastaus suuremmilla lukujen  $k$  ja  $n$  arvoilla riippuu suoraan pienemmistä arvoista. Tätä on vaikeaa huomata, jos keskittyy ongelmaan yhdeksällä ruudulla.

<sup>93</sup>Jos  $\deg(P) = \deg(Q) = k-1$  ja  $P$  ja  $Q$  saavat  $k$  samaa arvoa, niin polynomilla  $R(x) = P(x) - Q(x)$  on  $k$  nollakohtaa. Koska  $\deg(R) \leq k-1$ , tulee algebran peruslauseen nojalla polynomin  $R$  olla nollapolynomi.

Itse vastauksen laskemiseen käytettiin binomikertoimia. Binomikertoimet ovat tietysti kombinatoriikassa isossa roolissa, mutta niillä on myös algebran ja lukuteorian näkökulmasta mielenkiintoisia ominaisuuksia. Ratkaisussa binomikertoimia käytettiin rekursioyhtälön ratkaisujen esittämiseen. Summien muotoa  $1^k + 2^k + \dots + n^k$  laskemisessa voi käyttää binomikertoimia apuna (katso Summia-luku).

Lukuteorian puolelta mainitaan seuraava tulos: Jos  $P$  on rationaalilukukertoiminen polynomi ja  $P(n)$  on kokonaisluku kaikilla kokonaisluvuilla  $n$ , niin  $P(x)$  voidaan esittää summana polynomeista muotoa  $c_i \cdot \binom{x}{i}$ , jossa  $c_i$  ovat kokonaislukuja. (Huomaa, että esimerkiksi polynomin  $\frac{x(x-1)}{2}$  kertoimet eivät ole kokonaislukuja, mutta sen arvot kokonaislukupisteissä ovat kokonaislukuja.)

Luvun viimeinen tehtävä on vuoden 2011 Yhdysvaltojen kansallisesta kilpailusta.

### Tehtävä

Olkoon  $A$  joukko, jolla  $|A| = 225$ . Olkoot  $A_1, A_2, \dots, A_{11}$  sellaisia joukon  $A$  osajoukkoja, että  $|A_i| = 45$  kaikilla  $1 \leq i \leq 11$  ja  $|A_i \cap A_j| = 9$  kaikilla  $1 \leq i < j \leq 11$ . Osoita, että  $|A_1 \cup A_2 \cup \dots \cup A_{11}| \geq 165$ , ja anna esimerkki, jossa epäyhtälössä vallitsee yhtäsuuruus.

Ensimmäinen ajatus: sovelletaan inklusio-ekskluusiota. On helppoa nähdä, että se ei yksinään johda ratkaisuun, mutta se voisi toimia hyvänä työkaluna. Tiedämme joukkojen  $A_i$  koot sekä niiden parittaisten leikkausten koot, muttemme sellaisten leikkausten kokoja, joissa on suurempi määrä joukkoja. Saamme tätä kautta kuitenkin alarajan halutun unionin koolle: pätee

$$|A_1 \cup A_2 \cup \dots \cup A_{11}| \geq \sum_{1 \leq i \leq 11} |A_i| - \sum_{1 \leq i < j \leq 11} |A_i \cap A_j|.$$

Tämä ei ole ilmeistä itse inklusio-ekskluusiosta, vaan pikemminkin sen todistuksesta. Epäyhtälön oikea puoli laskee niiden lukujen määrää, jotka kuuluvat vähintään yhteen joukoista  $A_i$ . Jotkut luvut tulee laskettua useasti, joten ne vähennetään pois summalla  $\sum |A_i \cap A_j|$ . Jotkut luvut tulee (mahdollisesti) vähennettyä useasti, mutta nämä unohdetaan kokonaan. Näin saadaan alaraja unionin koolle.

Ikävä kyllä tästä saatava alaraja on huono:

$$\sum_{1 \leq i \leq 11} |A_i| - \sum_{1 \leq i < j \leq 11} |A_i \cap A_j| = 11 \cdot 45 - \binom{11}{2} \cdot 9 = 495 - 495 = 0.$$

Seuraava luonnollinen idea on yrittää parantaa inklusio-ekskluusioon perustuvaa arviotamme ottamalla lisää termejä huomioon. Aivan vastaavalla logiikalla kuin aiemmin saadaan

$$\begin{aligned} & |A_1 \cup \dots \cup A_{11}| \\ & \geq \sum_{1 \leq i \leq 11} |A_i| - \sum_{1 \leq i < j \leq 11} |A_i \cap A_j| + \\ & \quad \sum_{1 \leq i < j < k \leq 11} |A_i \cap A_j \cap A_k| - \sum_{1 \leq i < j < k < l \leq 11} |A_i \cap A_j \cap A_k \cap A_l|. \end{aligned}$$

(Huomaa, että mikäli ottaisimme huomioon vain ensimmäiset kolme summattavaa, niin saisimmekin unionin koolle ylärajan emmekä alarajaa.)

Kolminkertaisten leikkauksien  $|A_i \cap A_j \cap A_k|$  summaa on mahdollista arvioida melko hyvin. Tutkitaan leikkauksia muotoa  $A_1 \cap A_j$ . Nämä vastaavat joitain joukon  $A_1$  osajoukkoja, joiden koot ovat 9. Joukon  $A_1$  koko on 45. Indeksille  $j$  on 10 eri vaihtoehtoa, joten voisi ajatella, että joukon  $A_1$  alkiot kuuluvat keskimäärin kahteen muuhun joukkoon  $A_j$ .

Visualisoin tätä itse niin, että  $A_1$  on laatta, jonka leveys on 45 yksikköä. Leikkaukset  $A_1 \cap A_j$  ovat myös levyjä, joiden leveys on 9. Leikkaukset  $A_1 \cap A_j \cap A_k$  vastaavat niitä kohtia, jotka peittyvät vähintään kolmella levyllä. Luonnollisin tapa valita levyt on niin, että ensimmäistä 9 joukon  $A_1$  kohtaa peittävät joukot  $A_2$  ja  $A_3$ , seuraavaa 9 alkioita peittävät  $A_4$  ja  $A_5$  ja niin edelleen. Tämä tuntuu oikeastaan olevan paras tapa valita levyjen sijainnit, jos tavoitteena on minimoida summa termeistä  $|A_1 \cap A_j \cap A_k|$ , kun  $2 \leq j < k \leq 11$ . Tätä ei ole kovin vaikeaa todistaa. Emme kuitenkaan keskity todistukseen, koska tämä lähestymistapa ei tule toimimaan.

Saamme tästä siis

$$\sum_{2 \leq j < k \leq 11} |A_1 \cap A_j \cap A_k| \geq 5 \cdot 9 = 45.$$

Toistamalla vastaavan muillekin joukoille kuin  $A_1$  saadaan

$$\sum_{1 \leq i < j < k \leq 11} |A_i \cap A_j \cap A_k| = \frac{1}{3} \sum_{\substack{1 \leq i, j, k \leq 11 \\ i \neq j \neq k \neq i}} |A_i \cap A_j \cap A_k| \geq \frac{45 \cdot 11}{3} = 165.$$

Luku 165 on sama kuin tehtävässä. Emme kuitenkaan ole valmiit: vielä tulee vähentää nelinkertaisten leikkausten koot. Jos mikään alkio ei kuulu neljään eri joukkoon  $A_i$ , niin väite pätee, mutta muuten pätevyydestä ei ole tietoa.

Luonteva idea on merkitä nelinkertaisten leikkausten kokojen summaa muuttujalla  $x$  ja todistaa esimerkiksi, että

$$\sum_{1 \leq i < j < k \leq 11} |A_1 \cap A_j \cap A_k| \geq 165 + x.$$

Tämä ei kuitenkaan päde: joukot  $A_i$  voitaisiin valita niin, että on olemassa 9 alkioita, jotka kuuluvat kaikkiin joukoista  $A_1, \dots, A_{11}$ . Tällöin kolminkertaisten leikkauksien kokojen summa on  $\binom{11}{3} \cdot 9$  ja nelinkertaisten leikkauksien kokojen summa on  $\binom{11}{4} \cdot 9$ . Selvästi jälkimmäinen on suurempi.

Välikommentti: Oikeastaan tehtävässä on sanottu, että joukot  $A_i$  ovat jonkin 225-alkioisen joukon osajoukkoja. Tämä on kuitenkin puhtaasti hämäystä. Tehtävässä kaikki ”tapahtuu” unionissa  $A_1 \cup A_2 \cup \dots \cup A_{11}$ , ja millään muilla alkiolla ei ole merkitystä. Edellä esitetty konstruktio, jossa joukoilla  $A_i$  on kaikilla 9 yhteistä alkioita, vaatisi unioniin  $9 + 11 \cdot (45 - 9) = 405 > 225$  alkioita. Ehto 225-kokoisesta joukosta on kuitenkin täysin keinotekoinen, joten tästä ei kannata välittää.<sup>94</sup>

<sup>94</sup>Teoriassa olisi mahdollista, että ehdolla  $|A| = 225$  olisi väliä: tällaisella ehdolla voisi saada lisää

Inklusio-eksklusio ei enää vaikuta kovin hyvältä idealta. Täytyy keksiä jotain hienostuneempaa. Tässä vaiheessa voisi yrittää keksiä yhtäsuuruustapauksen ongelmaan. Tähän saadaan vinkkiä aiemmin todistetuista tuloksista: Aiemmin todistettiin, että mikäli mikään alkio ei kuulu vähintään neljään joukoista  $A_i$ , niin epäyhtälö pätee. Tutkimalla argumenttia tarkemmin voidaan oikeastaan todeta, että tehtävän epäyhtälössä vallitsee tällöin yhtäsuuruus.

Tästä saadaan strategia yhtäsuuruustapauksen luomiseksi: valitaan jokaiselle 165 alkiolle jotkin kolme joukkoa  $A_i, A_j$  ja  $A_k$ , joihin se kuuluu ja tehdään tämä niin, että ei ole kahta alkioita, jotka kuuluisivat samoihin kolmeen joukkoon. Tämä konstruktio toimii: Indeksit voidaan valita  $\binom{11}{3} = 165$  eri tavalla. Jokainen joukko  $A_i$  valitaan  $\binom{10}{2} = 45$  eri kolmikkoon, ja kaksi joukkoa  $A_i$  ja  $A_j$  ovat  $\binom{9}{1} = 9$  eri kolmikossa yhdessä.

Yhtäsuuruustapauksen löytyminen ei kuitenkaan tunnu auttavan itse ongelman ratkaisemiseen. Keksityssä yhtäsuuruustapauksessa ei ole nelinkertaisia leikkauksia, ja varmaan yhtäsuuruustapauksissa ei yleisestikään ole nelinkertaisia leikkauksia, mutta tämä tuntuu vaikealta todistaa. Ja kuten aiemmin jo todettiin, inklusio-eksklusio ei ole tarpeeksi tarkka, jotta siitä olisi hyötyä. Ideat ovat melko vähissä.

Pointtina on tosiaan keksiä jotain hienostunutta. Mitä tarkalleen? Mietitään ensiksi helpompaa kysymystä: miksi inklusio-eksklusio ei sovellu tehtävään? Ongelmana on, että inklusio-eksklusion soveltaminen vaatisi hyvin tarkkaa tietoa erilaisista muuttujista (kuten kolminkertaisten leikkauksien kokojen summa). Näiden muuttujien suuruudet voivat vaihdella hyvinkin paljon erilaisten joukkojen  $A_i$  valintojen välillä.

Ongelmana on siis liian suuri määrä muuttujia, joiden arvoista ei tiedetä paljoakaan. Yritetään korjata ongelma keksimällä muuttujat, joita on helpompi käsitellä ja joiden avulla voidaan esittää tehtävänannon kannalta oleelliset suureet (eli joukkojen koot, parittaisten leikkausten koot ja unionin koko). Emme voi lähestyä ongelmaa joukkojen kokojen näkökulmasta – tätä on yritetty jo. Toinen luonteva idea on tutkia jokaisella unionin  $A_1 \cup \dots \cup A_{11}$  alkiolla sitä, kuinka monessa joukossa se sijaitsee. (Aiemmin käsitelty inklusio-eksklusion perustuva argumentti sivuaa tätä näkökulmaa, mutta keskitytään tähän nyt syvemmin.)

Tutkitaan siis tilannetta, jossa joukot  $A_1, A_2, \dots, A_{11}$  sisältävät positiivisia kokonaislukuja vaikkapa väliltä  $[1, 1000]$ . Olkoon jokaisella  $1 \leq i \leq 1000$  luku  $x_i$  niiden indeksien  $j$  ( $1 \leq j \leq 11$ ) määrä, joilla  $i$  kuuluu joukkoon  $A_j$ .

Nähdään, että

$$495 = 11 \cdot 45 = \sum_{1 \leq j \leq 11} |A_j| = \sum_{1 \leq i \leq 1000} x_i,$$

koska jokainen alkio  $i$  kontribuoi  $x_i$  verran summaan  $\sum |A_j|$ . Vastaavasti nähdään, että voimme esittää parittaisten leikkausten kokojen summan muuttujien  $x_i$  avulla.

rakennetta osajoukkoihin  $A_i$ . Tässä tehtävässä näin ei kuitenkaan ole, kuten ratkaisusta nähdään. (Lisäksi 225 on paljon suurempi kuin haluttu raja 165, minkä vuoksi lisärajoitus  $|A| = 225$  ei tunnu antavan hyödyllistä lisätietoa.)

Pätee

$$495 = \binom{11}{2} \cdot 9 = \sum_{1 \leq j < k \leq 11} |A_j \cap A_k| = \sum_{1 \leq i \leq 1000} \binom{x_i}{2},$$

koska alkio  $i$  kontribuoi  $\binom{x_i}{2}$  verran parittaisten leikkausten kokojen summaan: voimme valita täsmälleen  $\binom{x_i}{2}$  paria indeksejä  $j$  ja  $k$ , joilla  $i \in A_j \cap A_k$ .

Kerrotaan binomikerroin auki. Saamme siis

$$495 = \sum_{1 \leq i \leq 1000} \binom{x_i}{2} = \frac{x_i(x_i - 1)}{2} = \frac{1}{2} \sum_{1 \leq i \leq 1000} x_i^2 - \frac{1}{2} \sum_{1 \leq i \leq 1000} x_i.$$

Koska lukujen  $x_i$  summa on 495, seuraa tästä, että lukujen  $x_i^2$  summa on  $3 \cdot 495 = 1485$ .

Muotoillaan muuttujien  $x_i$  avulla vielä tehtävänannon kolmas osa eli haluttu väite. Joukon  $A_1 \cup \dots \cup A_{11}$  koko on tietysti niiden indeksien  $i$  määrä, joilla  $x_i > 0$ .

Tiedämme siis joidenkin epänegatiivisten kokonaislukujen summan ja neliöiden summan, ja haluamme rajata positiivisten lukujen määrää. Tehtävä on siis muutettu kombinatoriikasta algebraan. Huomataan, että niillä muuttujilla  $x_i$ , joilla  $x_i = 0$ , ei ole mitään väliä: ne eivät vaikuta summaan, neliöiden summaan eikä positiivisten lukujen määrään. (Tätä käsiteltiin jo aiemmin, kun mainittiin, että ehto  $|A| = 225$  on turha ja keinotekoinen.)

Tutkitaan siis seuraavaa tilannetta: luvut  $y_1, y_2, \dots, y_k$  ovat positiivisia kokonaislukuja, joilla

$$\sum_{i=1}^k y_i = 495$$

ja

$$\sum_{i=1}^k y_i^2 = 495 \cdot 3.$$

Haluamme todistaa, että  $k \geq 165$ .

Miksi tuloksen pitäisi päteä? Ajatuksena on, että jos  $k$  on liian pieni, niin jotta lukujen  $y_i$  summa voisi olla 495, tulee jonkin luvun  $y_i$  olla melko suuri. Tällöin neliöiden summa  $y_i^2$  onkin yli  $495 \cdot 3$ . (Tämän huomion voi keksiä tarkastelemalla ääritapauksia  $k = 1, 2, 3$  ja niin edelleen.)

Ongelma ratkeakin suoraan Cauchy-Schwarzin epäyhtälöllä (katso Arviointi ja epäyhtälöt -luku): Cauchy-Schwarz sanoo, että kaikilla reaalityyppisillä  $a_1, a_2, \dots, a_k$  ja  $b_1, \dots, b_k$  pätee

$$\left( \sum a_i^2 \right) \left( \sum b_i^2 \right) \geq \left( \sum a_i b_i \right)^2.$$

Sijoitetaan tähän  $a_i = y_i$  ja  $b_i = 1$  kaikilla  $i$ . Saadaan

$$\left( \sum y_i^2 \right) \cdot k \geq \left( \sum y_i \right)^2.$$

Sijoitetaan arvot paikalleen. Saadaan

$$k \geq \frac{495^2}{495 \cdot 3} = \frac{495}{3} = 165,$$



ja olemme valmiit.

Edellisessä viimeistelyssä ei ole mitään vikaa, mutta seuraava kysymys herää: vaatiiko tehtävän viimeistely sen, että tajuaa soveltaa Cauchy-Schwarzia tai vastaavaa epäyhtälöä? Vastaus on kielteinen. Seuraavaksi esitetään tapa viimeistellä todistus ilman järeitä työkaluja. Todistuksen idealla voi todistaa yllä esitetyn epäyhtälön  $k \cdot \sum y_i^2 \geq (\sum y_i)^2$  (joka on jo Arviointi ja epäyhtälöt -luvussa esitetty kvadraattis-aritmeettinen epäyhtälö).

Huomataan ensiksi, että arvolla  $k = 165$  voidaan valita  $y_1 = y_2 = \dots = y_{165} = 3$ . Tämä vastaa tehtävään konstruointia yhtäsuuruustapausta. Oletetaan nyt, että  $k \leq 164$ . Osoitetaan, että ehdosta  $\sum y_i = 495$  seuraa väkisinkin, että  $\sum y_i^2 > 495 \cdot 3$ . Todistuksen idea on luonnollinen: osoitetaan, että neliöiden summa  $\sum y_i^2$  on minimissään silloin, kun luvut  $y_i$  ovat mahdollisimman lähellä toisiaan. Tällöin epäyhtälön todistamiseksi riittää tutkia tätä tapausta, jossa luvut  $y_i$  ovat miltei yhtä suuria.

Tutkitaan joitain positiivisia kokonaislukuja  $y_1, \dots, y_k$ , joilla  $\sum y_i = 495$ . Oletetaan, että  $y_i \geq y_j + 2$  jollain indekseillä  $i$  ja  $j$ . Osoitetaan, että korvaamalla luvun  $y_i$  luvulla  $y_i - 1$  ja luvun  $y_j$  luvulla  $y_j + 1$  lukujen  $y_1, \dots, y_k$  neliöiden summaa saadaan pienennettyä. Tämä on helppoa:

$$(y_i - 1)^2 + (y_j + 1)^2 = y_i^2 + y_j^2 + 2 - 2(y_i - y_j) \leq y_i^2 + y_j^2 + 2 - 4 = y_i^2 + y_j^2 - 2.$$

Huomaa, että lukujen summa 495 ei muutu tämän operaation seurauksena.

Voimme siis olettaa, että on olemassa jokin sellainen kokonaisluku  $n$ , että jokainen luvusta  $y_i$  on joko  $n$  tai  $n + 1$ . Koska  $\sum y_i = 495$  ja  $k \leq 164 < 165 = \frac{495}{3}$ , tulee päteä  $n \geq 3$ . Täten  $y_i^2 \geq n \cdot y_i \geq 3 \cdot y_i$  kaikilla  $i$ . Lisäksi kaikissa epäyhtälöissä ei voi päteä yhtäsuuruus, koska tällöin olisi  $y_i = 3$  kaikilla  $i$ , jolloin pätesi  $k = 165$ . Täten

$$\sum y_i^2 > 3 \cdot \sum y_i = 3 \cdot 495,$$

ja olemme valmiit.

Kommentti: Tehtävän alussa tehtyä tunnustelua ei tarvittu lopulliseen ratkaisuun, mutta se oli oleellinen osa ratkaisuprosessiani. Minulle inklusio-eksklusio oli asia, joka tuli heti mieleen tehtävän nähdessäni. Vaikka osasinkin epäillä, ettei ratkaisu tulisi tällä tuloksella helposti, ajattelin, että olisin käyttänyt sitä edes jossakin kohdassa ratkaisua.

Tehtävä paljastaakin inklusio-ekskluusion huonot puolet: mikäli joukkojen leikkauksien tarkkoja kokoja ei tiedetä, on menetelmää vaikea soveltaa järkevästi. Syynä tähän on inklusio-ekskluusiossa esiintyvien termien valtava määrä. Vahvimmillaan inklusio-eksklusio taas on silloin, kun leikkausten koot on mahdollista laskea tarkasti. Tästä nähtiin kaksi esimerkkiä inklusio-ekskluusiota käsittelevässä osiossa.

Ratkaisun kriittinen idea käsitellä muuttujia  $x_i$  liittyy aiemmin käsiteltyyn kahdella tavalla laskemiseen: laskemme joukkojen  $A_i$ ,  $A_i \cap A_j$  ja  $A_1 \cup \dots \cup A_{11}$  kokoja jollain muulla kuin ilmeisimmällä tavalla vaihtamalla näkökulmaa joukkojen sisältämistä alkioista siihen, mihin joukkoihin tietty alkio kuuluu. Kyseessä on siis varsin

perinteinen kahdella tavalla laskemisen sovellus. Minulta kului kuitenkin paljon aikaa ymmärtää, että lähestymistapaani ongelmaan tulisi vaihtaa. Helponkin idean keksiminen voi olla vaikeaa, mikäli ongelmaa katsoo väärällä tavalla (varsinkin jos ei tajua katsovansa ongelmaa väärällä tavalla).

Ratkaisun viimeistely tästä ei enää vaadi mitään kovin ihmeellistä. Ensin ongelma kirjoitetaan mahdollisimman puhtaaseen muotoon, minkä jälkeen ongelma palautuu suhteellisen helppoon epäyhtälöön. Käsitelty epäyhtälö koski lukujen summan yhdistämistä lukujen neliöiden summaan. Luvussa Arviointi ja epäyhtälöt käsiteltiin lukujen neliöjuurien summan yhteyttä lukujen summaan. Nämä ongelmat ovat (muuttujanvaihtoa vaille) samat, ja halutun väitteen saakin Cauchy-Schwarzilla, kvadraattis-aritmeettisella tai Jensenillä. Epäyhtälöt eivät olekaan pelkästään algebran tehtävissä esiintyvä asia. Monet lukuteorian ja kombinatoriikan ongelmat sisältävät epäyhtälöitä jossain muodossa, joten on hyvä osata epäyhtälöitä riittävästi, että osaa ratkaista näissä tehtävissä vastaan tulevat arviointia koskevat ongelmat.

Kirjoitin ratkaisuun kuitenkin myös sellaisen viimeistelyn, joka ei käytä mitään tunnettua epäyhtälöä. Tämän tarkoitus oli näyttää, että osan epäyhtälöitä käsittelevistä ongelmista voi ratkaista, vaikkei kovin vahvaa osaamista epäyhtälöistä omaisikaan. Ei siis kannata panikoida, mikäli tehtävässä tulee vastaan jotain, joka ei ole omalla mukavuusalueella (tämä koskee tietysti muitakin kuin epäyhtälötehtäviä), vaan kannattaa vain alkaa ratkoa ongelmaa. (Olen ainakin itse välillä syylistynyt panikointiin.)

Huomataan, että tehtävän tulosta voi yleistää. Lopullinen ratkaisu ei käytä sitä tietoa, että  $|A_i \cap A_j| = 9$  kaikilla  $i \neq j$ , vaan tietoa

$$\sum_{1 \leq i < j \leq 11} |A_i \cap A_j| = 495.$$

Vastaavasti ratkaisussa ei käytetty suoraan tietoa siitä, että joukkojen  $A_i$  koot ovat 45, vaan sitä, että kokojen summa on 495. Siispä joukkojen unionille saa varsin hyviäkin arvioita, kunhan tietää joukkojen kokojen summan ja joukkojen leikkausten kokojen summan. Tehtävän ratkaisu antaa seuraavan tuloksen: jos  $A_1, A_2, \dots, A_n$  ovat joukkoja, niin pätee

$$|A_1 \cup A_2 \cup \dots \cup A_n| \geq \frac{(\sum_{1 \leq i \leq n} |A_i|)^2}{\sum_{1 \leq i, j \leq n} |A_i \cap A_j|}.$$

(Huomaa, että nimittäjän summa käy läpi kaikki  $n^2$  paria  $i, j$ , mukaan lukien ne, joissa  $i = j$ .) Intuitiivisesti joukossa  $A_1 \cup A_2 \cup \dots \cup A_n$  on paljon alkioita, jos joukot  $A_i$  eivät leikkaa toisiaan kovin paljoa eli jos parittaisten leikkauksien kokojen summa  $\sum |A_i \cap A_j|$  on pieni. Tulos vahvistaa intuitiivisen käsityksen ja antaa alarajan unionin koolle.

## 20 Prosessit (Kombinatoriikka)

Tässä luvussa käydään läpi esimerkkitehtäviä, joissa tutkitaan erilaisia prosesseja. Aiheesta ei esitetä sen kummemmin teoriaa, vaan tehtävien ratkaisujen kautta esitetään erilaisia ideoita tällaisten ongelmien käsittelemiseen.

Ensimmäinen tehtävä on esiintynyt mm. Suomen valmennuksen harjoituskokeessa.

### Tehtävä

Pyöreän pöydän ympärillä istuu 25 poliitikkoa, jotka äänestävät. Ensimmäisellä äänestyskierroksella jokainen äänestää satunnaisesti joko ”Kyllä” tai ”Ei”. Jokaisella seuraavista kierroksista jokainen poliitikko äänestää seuraavasti:

- Jos vähintään toinen poliitikon vierustovereista äänesti edellisellä kerralla samoin kuin poliitikko itse, niin poliitikko äänestää samoin kuin edellisellä kerralla.
- Muussa tapauksessa poliitikko äänestää päinvastoin kuin edellisellä kierroksella.

Osoita, että jostain kierroksesta lähtien kenenkään poliitikon ääni ei enää muutu.

Numeroidaan poliitikot myötäpäivään  $1, 2, \dots, 25$ . Esimerkiksi jos ensimmäisellä kierroksella henkilöt  $1, 2, \dots, 24$  äänestävät ”Kyllä” ja henkilö  $25$  äänestää ”Ei”, niin toisella kierroksella kaikki äänestävät ”Kyllä”, samoin myös kolmannella kierroksella. Tällöin kenenkään ääni ei enää muutu.

Ongelmasta saa melko helposti tehtyä seuraavat havainnot: Jos henkilöt  $A$  ja  $B$  istuvat vierekkäin ja äänestävät samalla tavalla, niin kumpikaan ei tule vaihtamaan ääntään enää missään vaiheessa. Lisäksi koska  $25$  on pariton luku, niin ensimmäisellä kierroksella on olemassa jotkin kaksi vierekkäin istuvaa poliitikkoa, jotka äänestävät samoin. Muutoin kaikkien parittoman luvun saaneiden poliitikkojen tulisi äänestää samalla tavalla ja vastaavasti kaikkien parillisen luvun saaneiden tulisi äänestää samalla tavalla, mutta tällöin henkilöt  $1$  ja  $25$  äänestävät samalla tavalla.

Jokaisella äänestyskerralla löytyy siis vähintään yksi ryhmä, jonka jäsenet istuvat vierekkäin, eli muodostavat yhtenäisen osan pyöreän pöydän kehästä, ja äänestävät keskenään samalla tavalla. Enää tulee osoittaa, että jokaisesta poliitikosta tulee ennen pitkää osa jotakin tällaista ryhmää.

Tämä on oikeastaan melko helppoa. Valitaan jokin vierekkäisten poliitikkojen joukko  $S$ . Olkoon  $h$  poliitikko, joka kuuluu joukkoon  $S$  mutta jonka vierustoveri  $h'$  ei kuulu joukkoon  $S$ . (Jos tällaista poliitikkoa ei löydy, niin  $S$  sisältää kaikki 25 poliitikkoa ja olemme valmiit.) Jos poliitikko  $h'$  ei aiemmin kuulunut mihinkään ryhmään, on hän edellisellä äänestyskierroksella äänestänyt eri tavalla kuin  $h$ . Tällöin  $h'$  tulee äänestämään seuraavalla kierroksella samalla tavalla kuin  $h$ , joten hän liittyy joukkoon  $S$ .

Huomataan siis, että jokainen ryhmä  $S$  haalii joukkoonsa vieressään istuvia poli-

tikkoja, jos ne eivät jo valmiiksi kuulu johonkin ryhmään. Tämän vuoksi jokainen poliitikko tulee jossakin vaiheessa kuulumaan johonkin ryhmään, mikä todistaa väitteen.

Huomaa, että parillisilla määrillä poliitikkoja väite ei päde, koska tällöin ensimmäisellä äänestyskerralla ei välttämättä muodostu yhtään ryhmää.

Seuraava tehtävä on vuoden 2014 IMO-lyhytlistalta.

### Tehtävä

Olkoon  $m \geq 1$  kokonaisluku.  $2^m$  paperiarkille on jokaiseen kirjoitettu luku 1. Yhdellä operaatiolla voidaan valita kaksi eri paperiarkkia, joissa on luvut  $a$  ja  $b$ , pyyhkiä nämä luvut ja kirjoittaa molempiin arkkeihin luku  $a + b$ . Osoita, että  $m \cdot 2^{m-1}$  askeleen jälkeen papereihin kirjoitettujen lukujen summa on vähintään  $4^m$ .

Askelmäärä  $m \cdot 2^{m-1}$  ei oikein anna mitään vihjeitä. Kannattaa siis aluksi vain saada todistettua joitain hyviä alarajoja summalle prosessin edetessä. Summa kasvaa tietysti aina vähintään kahdella, mutta tämä ei tietenkään ole riittävä alaraja.

Luonnollinen idea on tutkia, kuinka monella operaatiolla summaa saadaan kasvatettua jollain pienellä määrällä. Esimerkiksi maksimissaan  $\frac{2^m}{2}$  operaatiolla summa voi kasvaa vain kahdella ja maksimissaan  $\frac{2^m}{2}$  operaatiolla summa voi kasvaa tasan kolmella.

Tämä lähestymistapa johtaa kuitenkin ongelmiin: emme voi samanaikaisesti saada  $\frac{2^m}{2}$  operaatiolla summaa kasvamaan vain kahdella ja  $\frac{2^m}{2}$  operaatiolla summaa kasvamaan vain kolmella. Tällä idealla saatavat alarajat eivät täten ole kovin hyviä.

Huomataan, että tehtävän alaraja todella on saavutettavissa: yhdistetään ensiksi  $2^{m-1}$  operaatiolla lappuja niin, että jokaisessa on luku 2, minkä jälkeen käytetään jälleen  $2^{m-1}$  operaatiota niin, että jokaisessa on luku 4, ja niin edelleen. Arvioiden tulee siis olla oikeasti melko tarkkoja.

Miksei edellinen lähestymistapa toimi? Syynä on se, että siinä katsotaan vain, mitä tapahtuu yksittäisille lapuille, eikä tutkita niinkään kokonaiskuvaa. Yritetään siis keksiä jokin ”globaalimpi” lähestymistapa ongelmaan.

Miltä näyttäisi globaali ratkaisu? Yritetään muodostaa paperilappujen luvuista jokin suure, joka kasvaa jokaisella operaatiolla ja jonka kautta saadaan lopulta alaraja summalle. Yksinkertaisesti ”lukujen summa” ei ole hyvä tällainen suure, kuten jo aiemmin totesimme – sitä on vaikea arvioida hyvin. Luonnollinen seuraava yritys on valita suureeksi lukujen tulo. Hankaluutena tässä valinnassa on se, ettei heti välttämättä näe, miten tulosta päästään lopussa takaisin summaan. On kuitenkin rohkaisevaa huomata, että tulo käyttäytyy hyvin operaatioita tehdessä, kuten seuraavaksi näemme.

Mitä lukujen tulolle tapahtuu yhdellä operaatiolla? Muut kuin operaatioon valitut luvut  $a$  ja  $b$  pysyvät samana ja tulo  $ab$  muuttuu tuloksi  $(a + b)^2$ . Miten näitä voi verrata? Pienellä kokeilemisella (tai aritmeettis-geometrisellä epäyhtälöllä) nähdään,

että saamme tuloon kertoimen 4: pätee

$$(a + b)^2 \geq 4ab,$$

koska tämä voidaan kirjoittaa muodossa  $a^2 - 2ab + b^2 \geq 0$  eli  $(a - b)^2 \geq 0$ .

Huomataan siis, että paperiarkkien lukujen tulo vähintään nelinkertaistuu, kun tehdään yksi operaatio. Koska aluksi tulo oli 1, niin  $k$  askeleen jälkeen tulo on vähintään  $4^k$ . Erityisesti kun  $k = m \cdot 2^{m-1}$ , on tulo vähintään

$$4^{m \cdot 2^{m-1}} = 2^{m \cdot 2^m}.$$

Viimeinen haaste ratkaisussa on: kuinka suuri lukujen summan tulee vähintään olla, jos tiedämme, että tulo on vähintään  $2^{m \cdot 2^m}$ ? Intuitiivisesti summa minimoituu silloin, kun kaikki luvut ovat suunnilleen yhtä suuria. Aritmeettis-geometrisen epäyhtälö sanoo nimenomaan tämän (ks. Arviointi ja epäyhtälöt -luku). Jos lopuksi papereilla olevat luvut ovat  $a_1, a_2, \dots, a_{2^m}$ , niin pätee

$$\frac{a_1 + a_2 + \dots + a_{2^m}}{2^m} \geq \sqrt[2^m]{a_1 a_2 \dots a_{2^m}}.$$

Oikean puolen tulo on  $2^{m \cdot 2^m}$ , joten epäyhtälön oikea puoli on vähintään  $\sqrt[2^m]{2^{m \cdot 2^m}} = 2^m$ . Saamme siis  $a_1 + a_2 + \dots + a_{2^m} \geq 4^m$ , mikä on haluttu arvio.

Edellinen ratkaisu perustui siihen, että jokin suure, tässä tapauksessa lukujen tulo, kasvoi jokaisella operaatiolla (ja vieläpä tarpeeksi nopeasti). Tällaista hallitusti muuttuvaa suuretta kutsutaan semi-invariantiksi. Invariantti puolestaan on suure, joka ei muutu ollenkaan. Seuraavan klassikkotehtävän ratkaisu sisältää helpon esimerkin tästä.

### Tehtävä

Kokoa  $8 \times 8$  olevan ruudukon kaksi vastakkaista kulmaa on leikattu pois. Voiko jäljelle jääneet 62 ruutua peittää  $2 \times 1$  ja  $1 \times 2$  -dominopalikoilla, kun kunkin palikan tulee peittää täsmälleen kaksi (vierekkäistä) ruutua ja mitkään kaksi laatua eivät saa mennä päällekkäin?

Ideana on värittää ruudukko shakkilautamaisesti. Nähdään, että leikatussa laudassa on 30 valkoista ja 32 mustaa ruutua (tai toisin päin). Kukin dominopalikka kuitenkin peittää täsmälleen yhden ruudun kumpaakin väriä, joten kaikkien ruutujen peittäminen on mahdotonta.

Jos invariantin haluaa tuoda eksplisiittisemmin esiin, voidaan sanoa, että suure ”peitettyjen valkoisten ruutujen määrä miinus peitettyjen mustien ruutujen määrä” ei muutu, kun dominopalikoita lisätään, ja että peittäminen on siksi mahdotonta.

Seuraavana on tehtävä vuoden 2018 IMO-lyhytlistalta.

**Tehtävä**

Olkoon  $n$  positiivinen kokonaisluku. Anna pelaa seuraavaa peliä laudalla, joka koostuu  $n+1$  laatikosta, jotka on numeroitu  $0, 1, \dots, n$ . Aluksi laatikossa 0 on  $n$  kiveä ja muut laatikot ovat tyhjiä. Jokaisella vuorolla Anna voi valita laatikon, jossa on  $k$  kiveä, ja siirtää yhtä laatikon kivistä enintään  $k$  ruutua eteenpäin (mutta kuitenkin niin, että kivi pysyy pelilaudalla). Annan tavoite on saada kaikki  $n$  kiveä laatikkoon  $n$ . Osoita, että Annan täytyy tehdä vähintään

$$\left\lceil \frac{n}{1} \right\rceil + \left\lceil \frac{n}{2} \right\rceil + \left\lceil \frac{n}{3} \right\rceil + \dots + \left\lceil \frac{n}{n} \right\rceil$$

siirtoa saavuttaakseen tavoitteensa.

Raja on mielenkiintoisen näköinen, ja se vaikuttaa luonnolliselta. Yksi idea olisi yrittää saada siirrettyä yhtä kiveä  $\left\lceil \frac{n}{1} \right\rceil$  kertaa, toista kiveä  $\left\lceil \frac{n}{2} \right\rceil$  kertaa ja niin edelleen. Toinen ajatus on siirtää jokaista kiveä aina niin pitkälle kuin mahdollista.

Pienillä tapauksilla on varsin helppoa saavuttaa raja. Yleinen tapaus tuntuu kuitenkin vaikeammalta. Tähän on luonnollinen syy: tehtävässä pyydetään todistamaan alarajaa, mutta se ei välttämättä ole tiukka.<sup>95</sup> Ei siis välttämättä ole olemassa sellaista strategiaa, joka saavuttaisi tämän minimisiirtomäärän.

Miten rajan pitävyyden voisi todistaa? Tutkimalla pelin kulkua konkreettisissa tapauksissa huomataan, että kaikilla  $i$  jokin kivi siirtyy jossain vaiheessa laatikosta  $i$  laatikkoon  $i+1$ . Tämän voi todistaa seuraavasti: Tutkitaan siirtoa, jonka jälkeen laatikoissa  $1, 2, \dots, i$  ei ole enää yhtään kiveä. Viimeisenä siirrettävän kiven täytyy olla ainoa kivi laatikossaan, joten se voi siirtyä vain yhdellä eteenpäin, eli se siirtyy laatikosta  $i$  laatikkoon  $i+1$ . Voidaan ajatella, että yhden askeleen eteenpäin siirtyvä kivi on aina sama kivi, koska kivien identiteeteillä ei ole väliä. Numeroidaan tämä kivi kiveksi numero 1. Kivi 1 on siis aina jonon viimeisenä.

Vastaavasti huomataan, että jokaisessa pelissä on ikään kuin kivi, joka hyppii aina maksimissaan kahden laatikon päähän ja joka ei ole kivi numero 1. Tämän voi todistaa samoin kuin edellä: Tutkitaan tilannetta, jossa laatikoissa  $1, 2, \dots, i$  on viimeisen kerran yhteensä kaksi kiveä. Tällöin kivi, joka ei ole kivi numero 1, joko hyppää laatikosta  $i-1$  kahden päähän tai hyppää laatikosta  $i$  yhden tai kahden päähän. Numeroidaan tämä kivi kiveksi 2, jolloin kivi numero 2 hyppää siis aina enintään kahden ruudun päähän.

Yleisesti nähdään, että kivet voidaan numeroida edellä kuvaillulla tavalla luvuilla  $1, 2, \dots, n$  niin, että kivi numero  $t$  hyppää aina enintään  $t$  laatikon päähän. Täten se tekee vähintään  $\left\lceil \frac{n}{t} \right\rceil$  hyppäystä. Summaamalla nämä luvut arvoilla  $t = 1, 2, \dots, n$  saadaan haluttu väite.

Kommentti: Idea on hyvin luonnollinen ja tulee esiin kokeilemalla pelin kulkua. Idean toteutusta tarvitsee miettiä hieman, mutta tämä ei ole erityisen vaikeaa.

Huomionarvoinen on idea siitä, että laskemme kullekin kivelle tehtyjä siirtoja emmekä esimerkiksi jokaisen laatikon tekemiä siirtoja. (Toteutus tämänkin lähesty-

<sup>95</sup>Kyseinen raja ei todella olekaan tiukka.

mistavan kautta on mahdollinen käyttämällä samanlaisia ideoita kuin edellä, mutta pidän kuitenkin kivien näkökulmaa luonnollisempana). Tämä on oikeastaan koko tehtävän pointti: vaihdamme näkökulmaa laatikoista kiviin. Idea näkökulman muuttamisesta ei ole harvinainen, ja esimerkiksi kahdella tavalla laskemisen periaate perustuu nimenomaan tähän ideaan.

Myös seuraava tehtävä on IMO-lyhytlistalta vuodelta 2013.

### Tehtävä

Riviin on kirjoitettu äärellinen määrä positiivisia kokonaislukuja. Yhdellä operaatiolla Anna voi valita kaksi vierekkäistä lukua  $x$  ja  $y$ , missä  $x$  on  $y$ :n vasemmalla puolella ja  $x > y$ , ja korvata parin  $(x, y)$  joko parilla  $(y + 1, x)$  tai parilla  $(x - 1, x)$ . Osoita, että Anna voi tehdä vain äärellisen monta operaatiota.

Huomataan, että jokaisella operaatiolla valittu oikeanpuoleinen luku kasvaa. Väite perustuukin tähän: hiljalleen rivin oikeassa päässä alkaa olla isoimmat luvut ja vasemmassa päässä pienimmät luvut. Enää pitää todistaa, että näin käy varmasti.

Sen lisäksi, että oikeanpuoleinen luku kasvaa, vasemmanpuoleinen luku joko pienenee tai pysyy samana.

Numeroidaan rivin luvut indekseillä  $1, 2, \dots, n$ , missä 1 vastaa vasemmanpuoleisinta lukua ja  $n$  vastaa oikeanpuoleisinta lukua. Yksi idea on tutkia, mitä tapahtuu kohdissa 1 ja  $n$  oleville luvuille. Tutkitaan kohtaa 1. Jokaisella operaatiolla kohdassa 1 oleva luku pienenee tai pysyy samana. Jos tietäisimme, että kaikki rivin luvut ovat aina positiivisia, niin saisimme, että vasemmanpuoleisin luku ei voi pienentyä äärettömän montaa kertaa. Mutta tämän voi todistaa seuraavasti: Aluksi kaikki luvut ovat positiivisia. Tarkastellaan ensimmäistä operaatiota, jonka seurauksena riviin tulee epäpositiivinen luku. Jos jollain askeleella jokin luku muuttuu nolaksi tai negatiiviseksi, niin sen tulee tapahtua operaation  $(x, y) \rightarrow (x - 1, x)$  seurauksena. Tällöin tulisi olla  $x \leq 1$ , mikä pakottaisi  $y \leq 0$ , joten jokin luku olisikin jo valmiiksi nolla tai negatiivinen, mikä on ristiriita.

Siis kohdan 1 luvulle voidaan tehdä vain äärellinen määrä operaatioita muotoa  $(x, y) \rightarrow (x - 1, x)$ , ja jos sille tehdään operaatio muotoa  $(x, y) \rightarrow (y + 1, x)$ , niin kaikilla paitsi äärellisen monella operaatiolla tulee päteä  $x = y + 1$ . Kohdan 1 luku ei siis enää muutu jostain pisteestä lähtien, ja aina, kun sille tehdään operaatio, niin kohdassa 2 oleva luku on yhtä pienempi kuin kohdan 1 luku.

Jos kohdille 1 ja 2 tehdään vain äärellinen määrä operaatioita, voimme kokonaan unohtaa kohdan 1 ja tutkia yhtä pienempää tapausta (tai kirjoittaa ratkaisun alkuun ”todistetaan väite induktiolla muuttujan  $n$  suhteen”, ja todeta, että tässä tapauksessa ollaan valmiit). Oletetaan siis, että kohdille 1 ja 2 tehdään äärettömän monta operaatiota. Tehdään vastaava oletus myös muille kohtapareille  $i$  ja  $i + 1$ .

Seuraava luonnollinen kysymys on: mitä arvoja kohdassa 2 oleva luku voi saada? Jos kohdassa 1 on luku  $x$ , niin kun kohdille 1 ja 2 suoritetaan operaatio, tulee kohdassa 2 olla tätä ennen luku  $x - 1$ . Tämän jälkeen kohdassa 2 on luku  $x$ . Kohdille 1 ja 2 tehtävien operaatioiden välillä kohdan 2 luvun tulee siis pienentyä yhdellä.

Toteamme, että kohdassa 2 on aina joko luku  $x$  tai  $x - 1$  (riittävän monen siirron jälkeen).

Mitä sitten on kohdassa 3? Jollain ajanhetkellä kohdille 2 ja 3 tulee tehdä operaatio, joka vähentää kohdan 2 lukua arvosta  $x$  arvoon  $x - 1$ . Tämän jälkeen kohdassa 3 tulee olemaan luku  $x$ . Toisaalta kohdan 3 arvo ei voi koskaan enää muuttua suuremmaksi kuin  $x$ .

Jatkamalla tätä päättelyä huomataan, että jokaisessa kohdassa lukujen arvot ovat aina enintään  $x$  (jostain ajanhetkestä lähtien). Erityisesti todetaan, että kohdassa  $n$  oleva arvo on jostain pisteestä lähtien aina enintään  $x$ . Mutta aina, kun kohdille  $n - 1$  ja  $n$  tehdään operaatio, kasvaa kohdassa  $n$  oleva luku vähintään yhdellä. Täten kohdille  $n - 1$  ja  $n$  tehdään vain äärellisen monta operaatiota, ja kaikki loput operaatiot tehdään kohdissa  $1, 2, \dots, n - 1$ .

Olemme siis saaneet redusoitua ongelman yhtä pienempään tapaukseen. Toistamalla tätä (tai kuten aiemmin mainittiin, käyttämällä induktiota) tehtävä saadaan ratkaistua.

Kommentti: Tehtävän voi ratkaista myös suoraan semi-invarianteilla. Määritellään lukurivin arvo seuraavasti: jos rivissä on vasemmalta oikealle luvut  $x_1, x_2, \dots, x_n$ , niin sen arvo on  $\frac{x_1}{2^n} + \frac{x_2}{2^{n-1}} + \dots + \frac{x_n}{2}$ . Helppo tarkastelu osoittaa, että jokaisella siirrolla arvo kasvaa vähintään luvun  $\frac{1}{2^n}$  verran. Koska rivin lukujen maksimi  $M$  ei kasva, on rivin arvo kuitenkin enintään  $\frac{M}{2^n} + \frac{M}{2^{n-1}} + \dots + \frac{M}{2} < M$ , joten operaatioita voidaan tehdä vain äärellisen monta.

Tämän ratkaisun voi motivoida niin, että lähdetään heti etsimään jotain semi-invarianttia ja kokeillaan erilaisia suureita kunnes jokin toimii. Lisäksi monesti semi-invariantti rakennetaan antamalla kullekin luvulle jokin painokerroin ja summaamalla saadut termit yhteen,<sup>96</sup> joten esitetty rivin arvon määritelmä on melko tyypillinen ja siksi verrattain helppo keksiä. Toinen toimiva tapa valita painokertoimet on valita termille  $x_i$  kerroin  $i$ .

Viimeinen esimerkki on niin ikään IMO-lyhytlistalta, tällä kertaa vuodelta 2017.

### Tehtävä

Olko  $n$  positiivinen kokonaisluku. Määritellään kameleontti olemaan mikä tahansa  $3n$  merkin pituinen merkkijono, jossa on tasan  $n$  kappaletta kutakin kirjaimista  $a, b$  ja  $c$ . Yhdellä operaatiolla kameleontista saa vaihtaa kahden vierekkäisen kirjaimen paikat. Osoita, että mille tahansa kameleontille  $X$  on olemassa sellainen kameleontti  $Y$ , että  $X$ :ää ei voi muuttaa  $Y$ :ksi alle  $\frac{3n^2}{2}$  operaatiolla.

Ei ole ilmeistä, miten  $Y$  tulee valita. Tämän vuoksi voisi olla hyödyllistä tutkia ensiksi jotain yksittäistä  $Y$  ja katsoa, mille  $X$  tehtävänannon ehto toteutuu. (Voitaisiin myös valita jokin  $X$  ja katsoa, mitkä  $Y$  sille kelpaa.)

<sup>96</sup>Tämä on tietysti ihan luonnollinen idea.



Yksinkertaisin esimerkkitapaus saadaan valitsemalla kameleontiksi  $Y$  merkkijono

$$aa \dots aabb \dots bbcc \dots cc.$$

Tehtävän voi nyt hahmottaa seuraavasti: jotta kameleontista  $X$  päästään jollain operaatiosarjalla kameleonttiin  $Y$ , tulee meidän saada järjestettyä  $X$ :n merkit aakkosjärjestykseen. Intuitiivisesti tämä onnistuu helpoiten silloin, kun  $X$ :n merkit ovat valmiiksi jo melkein oikeassa järjestyksessä. Vastaavasti vaikein tapaus on se, jossa  $X$  on  $Y$  takaperin.

Tulisi siis keksiä jokin tapa mitata sitä, kuinka kaukana oikeaa järjestystä kameleontti  $X$  on. Miten tämän suureen tulee käyttäytyä? Sen pitäisi pienentyä silloin, kun menemme ”oikeaan suuntaan” eli teemme  $X$ :lle operaation, joka saa sen lähemmäs oikeaa järjestystä. Vastaavasti suureen tulee kasvaa, jos teemme huonon siirron.

Millaisia ovat siirrot, joilla menemme oikeaan suuntaan? Siirrot, joilla vaihdamme kaksi vierekkäistä merkkiä  $ba$  järjestykseen  $ab$  ovat hyviä siirtoja. Jos  $X$ :ssä on aluksi jossain kohdassa  $i$  merkki  $b$  ja jossain  $i$ :stä vasemmalla olevassa kohdassa merkki  $a$ , niin jossain vaiheessa tulee tehdä siirto, joka vaihtaa juuri nämä kirjaimet  $a$  ja  $b$  toisin päin. Vastaavasti operaatiot, jotka vaihtavat vierekkäiset merkit  $ca$  järjestykseen  $ac$  ja merkit  $cb$  järjestykseen  $bc$ , ovat hyviä siirtoja.

Merkkijono on eniten epäjärjestyksessä silloin, kun on paljon sellaisia pareja  $i$  ja  $j$ , että kohta  $i$  on kohdan  $j$  vasemmalla puolella ja kohdan  $i$  kirjain on aakkosissa kohdan  $j$  jälkeen. Tämä voisi siis olla haluamamme suure. Kutsutaan tällaisia pareja kameleontin inversioiksi. Suuremme on siis kameleontin inversioiden määrä.

Edellisten huomioiden avulla ei ole vaikeaa nähdä, että jokaisella aiemmin kuvatulla ”hyvällä” siirrolla inversioiden määrä pienenee yhdellä ja jokaisella ”huonolla” siirrolla (joka esimerkiksi vaihtaisi merkit  $ab$  merkeiksi  $ba$ ) inversioiden määrä kasvaa yhdellä. Jos operaatio vaihtaa kaksi samaa merkkiä keskenään, niin merkkijono ei muutu ja myöskään inversioiden määrä ei muutu.

Siis jos kameleontissa  $X$  on vähintään  $\frac{3n^2}{2}$  inversiota, niin sitä ei voi muuttaa kameleontiksi  $Y$  alle  $\frac{3n^2}{2}$  operaatiolla, koska jokainen siirto vähentää inversioiden määrää enintään yhdellä. Kuinka suuren osan merkkijonoista tämä käsittelee? Noin puolet. Suurin määrä inversioita, mitä kameleontissa voi olla, saadaan nimittäin silloin, kun se on  $Y$  takaperin. Tällöin inversioiden määrä on  $3n^2$ .

Tästä huomaammekin, että tutkimalla kameleonttia

$$Y' = cc \dots ccbb \dots bbba \dots aa$$

saadaan vastaavasti käsiteltyä ne  $X$ , joissa on enintään  $\frac{3n^2}{2}$  inversiota suhteessa kameleonttiin  $Y$ .

Tehtävä on siis ratkaistu: jokaiselle  $X$  voimme aina valita kameleontiksi  $Y$  joko merkkijonon, joka on aakkosjärjestyksessä, tai merkkijonon, joka on käänteisessä aakkosjärjestyksessä.

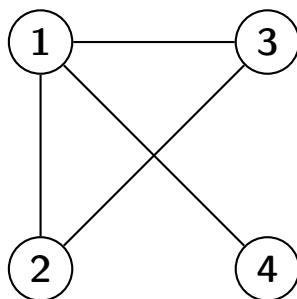
Kommentti: Merkkijonon inversioihin saattaa törmätä joissain muissa tehtävissä. Tämän idean tietäminen valmiiksi tietysti helpottaa tehtävän ratkaisemista huomattavasti.

## 21 Verkot (Kombinatoriikka)

Tutkitaan jotakin ihmisjoukkoa. Kuvitellaan, että jotkut henkilöistä ovat kavereita keskenään ja jotkut eivät ole. Tilannetta voidaan kuvastaa verkkona: verkossa on joukko solmuja (vertaa ihmisiin), joiden välillä on kaaria (vertaa ystävyssuhteisiin). Tässä luvussa esitetään perusteet verkoista ja käydään läpi esimerkkitehtäviä.

Tutkimme luvussa vain ns. suuntaamattomia verkkoja. Käytännössä tämä tarkoittaa sitä, että jos henkilö  $A$  on henkilön  $B$  kaveri, niin myös henkilö  $B$  on henkilön  $A$  kaveri.

Verkkoa merkitään usein kirjaimella  $G$ , ja joskus voidaan merkitä  $G = (V, E)$ , missä  $V$  on jokin joukko solmuja ja  $E$  on näiden solmujen välillä olevien kaarien joukko.



Verkko, jossa on neljä solmua ja neljä kaarta.

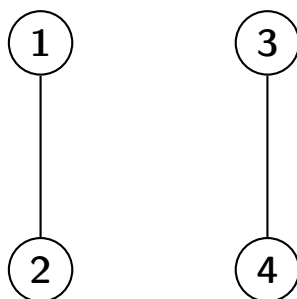
Yllä esitetyssä verkossa solmujen joukko on  $\{1, 2, 3, 4\}$  ja kaarien joukko on  $\{(1, 2), (1, 3), (1, 4), (2, 3)\}$ .

Aloitetaan verkon yhtenäisyyden käsitteellä.

### Määritelmä

Verkkoa  $G$  sanotaan yhtenäiseksi, jos mistä tahansa solmusta voi kulkea mihin tahansa solmuun verkon kaaria pitkin.

Alla oleva verkko ei ole yhtenäinen.



Epäyhtenäinen verkko.

Esimerkiksi sellainen verkko, jossa jokaisen solmuparin välillä on kaari, on yhtenäinen, koska ehto selvästi toteutuu. Määritelmän mukaista reittiä solmusta  $a$  solmuun

$b$  kutsutaan poluksi. (Polusta oletetaan yleensä, ettei se kulje saman solmun kautta useammin kuin kerran.)

Onko mitään kivaa kriteeriä sille, onko verkko yhtenäinen? Tutkimme tähän liittyen kahta kysymystä. Ensinnäkin: mikä on pienin määrä kaaria, jolla verkko voi olla yhtenäinen? Toiseksi: kuinka paljon kaaria vaaditaan, jotta verkko on varmasti yhtenäinen?

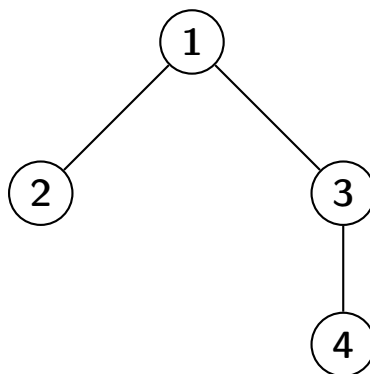
### Tehtävä

Olkoon  $G$  verkko, jossa on  $n$  ( $n \geq 2$ ) solmua. Todista, että mikäli  $G$ :n kaarien määrä on enintään  $n - 2$ , niin  $G$  ei ole yhtenäinen. Todista lisäksi, että jos verkon  $G$  kaarien määrä on  $n - 1$ , niin  $G$  voi olla yhtenäinen.

Ideana on tutkia, mitä kaarettomalle verkolle tapahtuu, kun siihen lisätään  $n - 2$  kaarta. Alkutilanteessa verkossa on  $n$  erillistä yhden solmun joukkoa. Verkossa on tällöin  $n$  komponenttia. (Komponentiksi kutsutaan sellaista solmujen joukkoa, jossa mistä tahansa solmusta pääsee mihin tahansa solmuun.)<sup>97</sup> Lisäämällä yhden kaaren joidenkin kahden solmun välille voidaan yhdistää kaksi erillistä komponenttia yhdeksi (mutta näin ei välttämättä käy). Yhdellä siirrolla saadaan siis vähennettyä komponenttien määrää (enintään) yhdellä. Jotta  $G$  olisi yhtenäinen  $n - 2$  siirron jälkeen, tulisi siinä olla vain yksi komponentti, mutta edellisen päättelyn nojalla siinä on vähintään kaksi komponenttia.

Väitteen toinen osa ratkeaa triviaalilla esimerkillä: jos verkon solmut on numeroitu  $1, 2, 3, \dots, n$ , niin voimme yhdistää kaarella solmut 1 ja 2, solmut 2 ja 3, solmut 3 ja 4 ja niin edelleen. On kuitenkin olemassa paljon muitakin esimerkkejä. Niitä voi luoda edellisen kohdan todistuksen avulla: valitaan ensin solmut 1 ja 2 ja yhdistetään ne kaarella. Komponenttien määrä pienenee yhdellä. Yhdistetään sitten solmu 3 solmuun 1 tai solmuun 2, jolloin komponenttien määrä pienenee yhdellä. Yhdistetään sitten solmu 4 johonkin solmuista 1, 2 ja 3, jolloin komponenttien määrä pienenee taas yhdellä. Jatketaan vastaavasti.

Sellaisia yhtenäisiä verkkoja, joissa kaarien määrä on yhden pienempi kuin solmujen määrä, kutsutaan puiksi.



Neljä solmua sisältävä puu.

<sup>97</sup>Lisäksi tietysti oletetaan, että mikäli komponentin solmusta  $a$  pääsee kaaria pitkin solmuun  $b$ , niin myös  $b$  kuuluu kyseiseen komponenttiin.

Jos verkko on puu, niin sille pätee muun muassa seuraavat ehdot:

- Verkossa ei ole syklejä. Sykliksi kutsutaan sellaista reittiä verkossa, jonka alku- ja loppusolmu ovat sama solmu ja jonka varrella missään muussa solmussa ei käydä useammin kuin kerran.
- Jos  $a$  ja  $b$  ovat mielivaltaisia verkon (eri) solmuja, niin on olemassa täsmälleen yksi polku solmusta  $a$  solmuun  $b$ . (Muista, että polku saa käydä yhdessä solmussa enintään kerran.)

Edelliset kohdat pätevät myös toiseen suuntaan: Jos verkko on yhtenäinen ja siinä ei ole syklejä, niin sen tulee olla puu. Vastaavasti jos minkä tahansa kahden solmun välillä on täsmälleen yksi polku, niin verkko on puu.

Puita käsitellessä puhutaan usein juurista, lapsista ja lehdistä. Puulla on yksi juuri, josta lähtee kaaria muihin solmuihin. (Juuren sijainnin saa käytännössä valita itse.) Näitä juuren naapureita kutsutaan juuren lapsiksi, ja juuri on näiden lapsien vanhempi. Näistä lapsisolmuista voi edelleen lähteä kaaria uusiin solmuihin, jotka muodostavat uusia lapsi-vanhempi -suhteita. Solmua, jolla ei ole yhtäkään lasta, kutsutaan puun lehdeksi.

Voidaan osoittaa, että edellisen tehtävän yhteydessä esitetty tapa luoda puu antaa (solmujen uudelleennumerointia vaille) kaikki mahdolliset puut. Voidaan ajatella, että solmu 1 on puun juuri ja solmulle 1 lisätään prosessin aikana joitain lapsia, kuten solmu 2. Puun hahmottaminen juuren näkökulmasta antaa helpon, konkreettisen tavan visualisoida puun.

Seuraavaksi esitetään vastaus aiemmin esitettyyn kysymykseen ”Kuinka paljon kaaria vaaditaan, jotta verkko on varmasti yhtenäinen?”

### Tehtävä

Olkoon  $G$  verkko, jossa on  $n$  ( $n \geq 2$ ) solmua. Todista, että mikäli  $G$ :n kaarien määrä on vähintään  $\frac{(n-1)(n-2)}{2} + 1$ , niin  $G$  on yhtenäinen. Todista lisäksi, että jos verkon  $G$  kaarien määrä on  $\frac{(n-1)(n-2)}{2}$ , niin se ei välttämättä ole yhtenäinen.

Toisessa osassa luonnollinen idea antaa ratkaisun. Jos solmut on numeroitu  $1, 2, \dots, n-1, n$ , niin muodostetaan sellainen verkko, jossa kaikki solmuista  $1, \dots, n-1$  on yhdistetty toisiinsa kaarilla, mutta solmua  $n$  ei ole yhdistetty yhteenkään toiseen solmuun. Nyt verkossa on kaksi komponenttia ja  $\binom{n-1}{2} = \frac{(n-1)(n-2)}{2}$  kaarta.

Ensimmäinen osa on vaikeampi. Ideana on, että jos verkon kaarien määrä on vähintään  $\frac{(n-1)(n-2)}{2} + 1$ , niin siitä ”puuttuu” enintään  $n - 2$  kaarta. Olkoon siis  $G'$  se verkko, jonka solmujen joukko on sama kuin verkolla  $G$  ja jossa solmujen  $a$  ja  $b$  välillä on kaari täsmälleen silloin, kun solmujen  $a$  ja  $b$  välillä ei ole kaarta verkossa  $G$ . Verkkoa  $G'$  kutsutaan verkon  $G$  komplementiksi. Verkossa  $G'$  on nyt enintään  $n - 2$  kaarta, joten se ei edellisen tehtävän nojalla voi olla yhtenäinen, eli siinä on vähintään kaksi komponenttia.

Olkoot nyt  $a$  ja  $b$  mielivaltaisia solmuja. On kaksi mahdollista tapausta:

- Solmut  $a$  ja  $b$  ovat verkon  $G'$  eri komponenteissa. Tällöin solmujen  $a$  ja  $b$  välillä ei määritelmän nojalla ole kaarta verkossa  $G'$ , joten verkossa  $G$  niiden välillä on kaari. Solmut  $a$  ja  $b$  kuuluvat siis samaan verkon  $G$  komponenttiin.
- Solmut  $a$  ja  $b$  ovat samassa verkon  $G'$  komponentissa. Koska  $G'$  ei ole yhtenäinen, on olemassa jokin toinen verkon  $G'$  (epätyhjä) komponentti, joka ei sisällä solmuja  $a$  ja  $b$ . Olkoon  $c$  jokin tämän toisen komponentin solmu. Nyt (kuten edellisessä tapauksessa) solmujen  $a$  ja  $c$  ja solmujen  $b$  ja  $c$  välillä on kaaret verkossa  $G$ , eli  $a$  ja  $b$  ovat samassa verkon  $G$  komponentissa.

Molemmissa tapauksissa mielivaltaiset solmut kuuluvat samaan komponenttiin, joten  $G$  on yhtenäinen.

Tehtävään on myös toisenlainen ratkaisu: Oletetaan, että  $G$  ei ole yhtenäinen. Tällöin verkon  $G$  solmut voidaan jakaa kahteen (epätyhjään) osaan  $V_1$  ja  $V_2$  niin, ettei näiden osien välillä ole kaaria. Nyt verkon  $G$  kaarien määrä on enintään osien  $V_1$  ja  $V_2$  sisältämien kaarien määrien summa. Olkoon  $n_1$  osan  $V_1$  solmujen määrä, jolloin  $V_1$ :n solmujen välillä voi olla enintään

$$\binom{n_1}{2}$$

solmua. Määritellään  $n_2$  vastaavasti, jolloin  $n_1 + n_2 = n$ . Ristiriidan saamiseksi riittää todistaa, että

$$\binom{n_1}{2} + \binom{n_2}{2} < \frac{(n-1)(n-2)}{2} + 1.$$

Loppu onkin hyvin rutiininomaista laskemista. Kirjoittamalla auki binomikertoimien määritelmän ja kertomalla puolittain kahdella saadaan

$$(n_1^2 - n_1) + (n_2^2 - n_2) < n^2 - 3n + 4.$$

Sijoitetaan yhtälön oikealle puolelle  $n = n_1 + n_2$ . Sievennysten jälkeen jäljelle jää

$$2n_1 + 2n_2 < 2n_1n_2 + 4$$

eli

$$0 < (n_1 - 1)(n_2 - 1) + 1,$$

mikä selvästi pätee.

Seuraava esimerkkitehtävä on Suomen IMO-joukkueen valintakokeesta vuodelta 2017.

### Tehtävä

Kesäleirille osallistuu koululaisia kolmesta eri kaupungista. Jokaisesta kaupungista osallistuu täsmälleen  $n \in \mathbb{Z}_+$  koululaista. Leirin päätyttyä jokainen koululainen tuntee täsmälleen  $n + 1$  leirille osallistunutta muualta kuin kotikaupungistaan tullutta koululaista. Osoita, että leirin päättyessä jotkut kolme koululaista sekä ovat kolmesta eri kaupungista että tuntevat kaikki toisensa.

Huomaa, että tehtävänannossa ei puhuta mitään verkoista. Kilpailutehtävissä onkin tyypillistä, että itse tehtävänannossa ei käytetä teknisiä termejä. Kilpailijan oletetaan ymmärtävän, että tehtävä koskee verkkoja.

On siis annettuna verkko, jonka solmut on jaettu joukkoihin  $A$ ,  $B$  ja  $C$ . Tiedetään, että jokaisen joukoista  $A$ ,  $B$ ,  $C$  koko on  $n$  ja solmusta  $a \in A$  on yhteensä  $n + 1$  kaarta joukkojen  $B$  ja  $C$  solmuihin (ja vastaavasti joukoista  $B$  ja  $C$  muihin joukkoihin). Huomataan, että esimerkiksi joukon  $A$  solmujen välisillä kaarilla ei ole tehtävän kannalta merkitystä, joten niitä ei tarvitse huomioida.

Huomataan, että jos on olemassa sellainen solmu  $a \in A$ , josta on kaari kaikkiin joukon  $B$  solmuihin, niin olemme valmiit. Tällöin on nimittäin vielä jokin solmu  $c \in C$ , joka on yhteydessä solmuun  $a$  ja jonka tulee olla yhteydessä johonkin solmuun  $b \in B$ . Nyt  $a$  on oletuksen nojalla yhteydessä solmuun  $b$ , joten solmut  $a$ ,  $b$  ja  $c$  ovat halutunlaiset.

Seuraava luonnollinen askel on tutkia tapausta, jossa  $a \in A$  on yhteydessä kaikkiin paitsi yhteen joukon  $B$  solmuista. Olkoon  $b \in B$  se solmu, johon  $a$  ei ole yhteydessä. On olemassa jokin solmu  $c_a \in C$ , joka on yhteydessä solmuun  $a$ . Jos  $c_a$  on yhteydessä johonkin joukon  $B$  solmuun  $b'$ , joka ei ole solmu  $b$ , niin kolmikko  $a, b', c_a$  on halutunlainen. Muussa tapauksessa  $c_a$  on yhteydessä enintään (ja täten tasan) yhteen solmuun joukossa  $B$ , eli  $c_a$  on yhteydessä kaikkiin joukon  $A$  solmuihin. Tällöin ongelma palautuu edellisen kappaleen tapaukseen.

Saimme siis palautettua ongelman jo käsiteltyyn tapaukseen. Näin tulee käymään myös siinä tapauksessa, että  $a \in A$  on yhdistetty kaarella  $n - 2$  kappaleeseen joukon  $B$  solmuja. Oikeastaan sama logiikka toimii myös yleisesti. Kokonaisen todistuksen saa kirjoitettua siististi seuraavasti.

Tehdään vastaoletus: Kolmea eri kaupungista tulevaa ja toistensa tuntevaa koululaista ei löydy. Olkoon  $a_{i,B}$  niiden joukon  $B$  solmujen määrä, joihin joukon  $A$  järjestykseltään  $i$ :nnes solmu on yhdistetty kaarella, kun  $1 \leq i \leq n$ . Määritellään vastaavasti luvut  $a_{i,C}$ ,  $b_{i,A}$ ,  $b_{i,C}$ ,  $c_{i,A}$  ja  $c_{i,B}$ . Valitaan suurin näistä luvuista; olkoon se  $k$ . Symmetrian nojalla voidaan olettaa, että  $k = a_{i,B}$  jollain  $i$ . Merkitään tätä joukon  $A$  järjestykseltään  $i$ :nnettä solmua kirjaimella  $a$ . Olkoot  $b_1, \dots, b_k$  ne joukon  $B$  solmut, jotka ovat yhteydessä solmuun  $a$ .

Valitaan jokin niistä  $n - k + 1$  solmusta  $c \in C$ , jotka ovat yhteydessä solmuun  $a$ . Vastaoletuksen nojalla  $c$  ei ole yhteydessä mihinkään solmuista  $b_1, \dots, b_k$ . Täten  $c$  on yhteydessä enintään  $n - k$  solmuun joukossa  $B$  ja siten  $k + 1$  solmuun joukossa  $A$ . Tämä on ristiriita luvun  $k$  maksimiominaisuuden kanssa, joten vastaoletus oli väärä ja todistettava väite pätee.

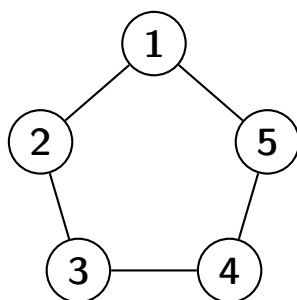
Seuraava tehtävä on vuoden 2018 ELMO-kilpailusta.

**Tehtävä**

Olkoon  $n$  positiivinen kokonaisluku. Kuningaskunnassa on  $2018n + 1$  kaupunkia. Kuningas haluaa rakentaa kaksisuuntaisia teitä eri kaupunkien välille niin, että kaikilla kaupungeilla  $C$  ja kokonaisluvuilla  $1 \leq i \leq 2018$  pätee, että täsmälleen  $n$  kaupunkia on etäisyydellä  $i$  kaupungista  $C$ . [Kahden kaupungin välinen etäisyys on pienin määrä teitä millään reitillä näiden kaupunkien välillä.] Millä luvun  $n$  arvoilla kuninkaan on mahdollista toteuttaa toiveensa?

Huomataan, että arvolla  $n = 1$  tavoite ei onnistu: Valitaan mikä tahansa kaupunki  $C$ . Nyt verkon tulisi olla 2019 solmua sisältävä polku, jonka yksi päätepiste on  $C$ . Tämä ei tietenkään onnistu kaikilla  $C$ .

Arvolla  $n = 2$  halutaan muun muassa, että jokaisella solmulla on kaksi naapuria. Huomataan, että  $2018 \cdot 2 + 1$  solmua sisältävä sykli toteuttaa halutut ehdot. (Ei ole vaikeaa todistaa, että ainoa yhtenäinen verkko, jossa jokaisella solmulla on 2 naapuria, on sykli.)



Viiden pituinen sykli.

Vastaavasti arvolla  $n = 3$  halutaan, että jokaisella solmulla on kolme naapuria. Seuraava hyvin tunnettu tulos auttaa ratkaisemaan tämän tapauksen.

**Lemma**

Olkoon  $G$  verkko. Olkoon  $k$  niiden verkon  $G$  solmujen määrä, joiden aste on pariton. Tällöin  $k$  on parillinen.

Solmun aste on yksinkertaisesti niiden solmujen määrä, joihin solmusta on kaari.

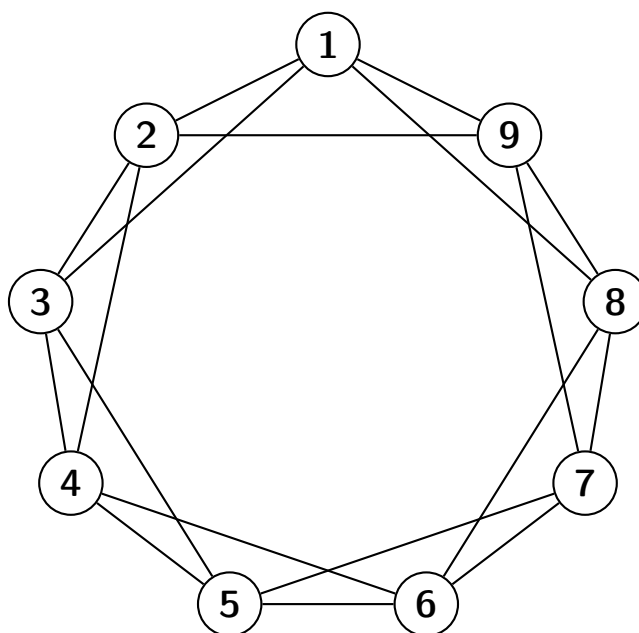
Tulos tunnetaan nimellä Handshaking lemma. Verkon voi nimittäin ajatella kuvaavan ihmisten välisiä kättelyitä. Jokainen uusi kättely lisää kahden ihmisen kättelyiden määriä yhdellä, eli verkon solmujen asteiden summa kasvaa kahdella. Siispä solmujen asteiden summan parillisuus pysyy aina samana, eli se on aina parillinen. Täten paritonasteisten solmujen määrä on parillinen.

Tämän vuoksi tehtävänannon tavoitetta ei voi saavuttaa, kun  $n = 3$ : haluaisimme, että verkon jokaisen  $2018 \cdot 3 + 1$  solmun aste on pariton, mutta tällöin paritonasteisia solmuja olisi pariton määrä. Vastaava päättely todistaa, että mikään pariton  $n$  ei kelpaa.

Siirrytään sitten tapaukseen  $n = 4$ . Tätä olisi mukavampaa käsitellä pienemmällä kuin  $2018 \cdot 4 + 1$  solmua sisältävällä verkolla, joten yritetään tutkia vastaavaa väitettä kokoa  $k \cdot 4 + 1$  olevalla verkolla. Parittomien  $n$  poissulkeminen perustuu luvun  $k$  parillisuuteen, joten varmuuden vuoksi kannattaa valita  $k$  parilliseksi. Tutkitaan siis tapausta  $n = 4$  ja  $k = 2$  eli yhdeksän solmun kokoista verkkoa.

Mistä tahansa solmusta  $C$  lähtee neljä kaarta, ja lisäksi loput neljä solmua ovat kahden etäisyydellä solmusta  $C$ . Tämä kertoo jo melko paljon verkon rakenteesta. Koska ehto on symmetrinen solmujen suhteen, on luontevaa yrittää löytää konstruktion, joka on symmetrinen jokaisen solmun suhteen. Vielä yksi ajatus on se, että mikäli kaikki solmut kuuluvat yhteen isoon sykliin (kuten tapauksessa  $n = 2$ ), niin etäisyyksiä on kohtalaisen helppo ”mitata”. Näillä ideoilla ja yritysten ja erehdysten kautta keksitään seuraava konstruktion.

Olkoot solmut  $C_1, C_2, \dots, C_9$ . Yhdistetään solmut  $C_i$  ja  $C_j$  jos ja vain jos  $i$  ja  $j$  ovat enintään kahden päässä toisistaan ”modulo 9”. Siis esimerkiksi solmu  $C_1$  on yhdistetty solmuihin  $C_2, C_3, C_8$  ja  $C_9$ . On selvää, että haluttu ehto pätee solmulle  $C_1$ , ja symmetrian vuoksi väite pätee tällöin kaikille solmuille  $C_i$ .



Ratkaisu alkuperäisen tehtävän  $2n + 1$ -varianttiin arvolla  $n = 4$ .

Nähdään, että tästä saadaan ratkaisu myös alkuperäisen tehtävän tapaukseen  $n = 4$ : Olkoot solmut  $C_1, C_2, \dots, C_{2018 \cdot 4 + 1}$ . Yhdistetään solmut  $C_i$  ja  $C_j$  kaarella jos ja vain jos  $i$  ja  $j$  ovat enintään kahden päässä toisistaan (modulo  $2018 \cdot 4 + 1$ ).

Enää ei ole vaikeaa yleistää tätä mielivaltaiselle parilliselle  $n$ : edellisen kohdan ehto ”enintään kahden päässä toisistaan” vain korvataan ehdolla ”enintään  $\frac{n}{2}$ :n päässä toisistaan”. Tämän konstruktion toimivuuden tarkistaminen jätetään lukijalle.

Kaiken kaikkiaan kuningas pystyy toteuttamaan ehdon jos ja vain jos  $n$  on parillinen.



Viimeinen tehtävä on IMO-lyhytlistalta vuodelta 2013.

### Tehtävä

Omalaatuinen fyysikko löysi uudenlaisen alkeishiukkasen, jolle hän antoi nimeksi imoni, kun joitakin sellaisia yllättäen ilmestyi hänen laboratorioonsa. Jotkin imonien parit ovat lomittuneita, ja jokainen imoni voi olla osallisena monessa eri lomittumisessa. Fyysikkomme on löytänyt tavan suorittaa seuraavanlaisia operaatioita näille hiukkasille, yhden operaation kerrallaan.

1. Jos jokin imoni on lomittunut parittoman monen muun laboratorion imonin kanssa, niin fyysikko voi tuhota sen.
2. Fyysikko voi kaksinkertaistaa laboratorionsa imonien määrän luomalla jokaiselle imonille  $I$  kopion  $I'$ . Tässä operaatiossa kaksi kopiota  $I'$  ja  $J'$  lomittuvat jos ja vain jos  $I$  ja  $J$  ovat lomittuneet ja jokainen kopio  $I'$  lomittuu alkuperäisen imonin  $I$  kanssa. Mitään muita lomittumisia ei synny tai häviä tämän operaation aikana.

Osoita, että fyysikko voi näitä operaatioita sopivasti toistaen tuottaa sellaisen kokoelman imoneita, jossa mitkään kaksi imonia eivät ole lomittuneet.

Toista operaatiotyyppiä voi havainnollistaa geometrisesti seuraavasti: Verkon  $G = (V, E)$  solmut on aseteltu levyille. Levystä luodaan kopio, joka asetetaan alkupe-  
räisten solmujen yläpuolelle, ja kohdakkain osuvat solmut yhdistetään kaarella. Jos tehdään vielä toinen uusi kopio, levyjä asettuu neljä päällekkäin, mutta niiden väliset kytkökset ovat monimutkaisempia kuin vain kohdakkain olevien solmujen yhdistäminen. Toinen tapa visualisoida asiaa on asetella levyjä myös muihin ulottuvuuksiin kuin päällekkäin. Yleisesti tilanne muuttuu  $n$ -ulotteisen hyperkuution tutkimiseksi. Katsomme tilannetta pääsääntöisesti ensimmäisestä näkökulmasta ja puhumme verkon ”pystyriveistä”, mutta myöhemmin käytämme myös hyperkuutioidea.

Symbolisemmin asian voi esittää näin: Ensimmäisellä kopioimiskerralla solmujen joukko  $V$  muuttuu pareiksi muotoa  $(v, x)$ , missä  $x \in \{0, 1\}$ . Tässä  $x$  vastaa sitä, monennessako levyssä solmu on. Toisella kopioimiskerralla solmut muuttuvat muotoon  $((v, x), y)$ ,  $x, y \in \{0, 1\}$ , mikä on käytännössä vain parit muotoa  $(v, z)$ , missä  $z \in \{0, 1, 2, 3\}$ . Yleisesti  $n$  operaation jälkeen parit ovat muotoa  $(v, z)$ , missä  $0 \leq z \leq 2^n - 1$ . Mikäli välissä ei tehdä poisto-operaatioita, niin solmut  $(v, x)$  ja  $(v, y)$  on yhdistetty kaarella jos ja vain jos lukujen  $x$  ja  $y$  binääriesitykset<sup>98</sup> poikkeavat tasan yhden numeron kohdalla.

Naiivi idea<sup>99</sup> tehtävän ratkaisemiseksi olisi vähentää verkossa olevia pystyrivejä eli yritetään poistaa kaikki solmut muotoa  $(w, i)$ ,  $i = 0, 1, \dots, 2^n - 1$ , missä  $w$  on jokin

<sup>98</sup>Normaalisti luvut esitetään kymmenkannassa:  $567 = 5 \cdot 10^2 + 6 \cdot 10^1 + 7 \cdot 10^0$ . Binääriesityksessä kannaksi valitaan 2. Luvut yhdestä viiteentoista ovat binääriesityksessä 1, 10, 11, 100, 101, 110, 111, 1000, 1001, 1010, 1011, 1100, 1101, 1110 ja 1111.

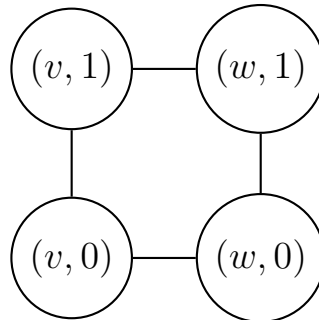
<sup>99</sup>Ehkä vielä naiivimpaa olisi yrittää todistaa väitettä induktiolla verkon solmujen määrän suhteen. Tämä ei kuitenkaan helposti johda ratkaisuun: jokainen tyypin 2 operaatio tuplaa verkon solmujen määrän, joten kopiointien väleissä tulisi saada tehtyä todella paljon tyypin 1 operaatioita.

verkon  $G$  solmu. Pystyrivien määrä ei muutu uusia kopioita tehdessä (vaikkakin verkon rakenne muuten muuttuu monimutkaisemmaksi), joten teoriassa tämä idea voisi toimia. Tämän strategian toteuttamisessa on kuitenkin elintärkeää muokata pystyrivin solmuja hallitusti eli kahden tyyppin 2 operaation välissä aina poistaa pystyriviltä joko kaikki solmut tai olla tekemättä mitään – muutenhan käsitteessä ”pystyrivi” ei olisi järkeä.

Esimerkkinä voidaan tutkia kolmen solmun  $V_1, V_2, V_3$  verkkoa, jossa kaikkien parien  $(V_1, V_2)$ ,  $(V_2, V_3)$  ja  $(V_3, V_1)$  välillä on kaaret. Tällöin kopion luomisen jälkeen voidaan poistaa seuraavat solmut tässä järjestyksessä:  $V_1, V_2', V_1', V_2$ . Tämä poistaa peräti kaksi pystyriviä. Jäljelle jäänyt pystyrivi on myös helppo poistaa. Tämä esimerkki osoittautui helpoksi.

Tutkitaan sitten yleistä tapausta. Olkoon annettuna verkko  $G_1 = (V_1, E_1)$ . Aivan aluksi poistetaan verkosta solmuja niin kauan, kunnes kaikkien solmujen asteet ovat parillisia. Olkoon syntynyt verkko  $G_2 = (V_2, E_2)$ .

Ei ole muuta vaihtoehtoa kuin tehdä kopio verkosta. Olkoon  $G_3$  syntynyt verkko, jonka solmut ovat muotoa  $(v_2, x)$ , jossa  $v_2 \in V_2$  ja  $x \in \{0, 1\}$ . Valitaan jokin solmu  $(v, 0)$ , jolla on naapuri  $(w, 0)$ . Poistetaan seuraavat solmut tässä järjestyksessä:  $(v, 0), (w, 1), (v, 1), (w, 0)$ . Tämä on sallittua, koska jokaisessa kohdassa poistetun solmun aste on pariton. Pystyrivien määrä pienenee kahdella.



Jos neliön solmujen asteet ovat parittomia, voidaan solmut poistaa.

Edellä oletettiin, että solmulla  $(v, 0)$  on muotoa  $(w, 0)$  oleva naapuri, jonka aste on pariton. Kun operaatioita tehdään toistuvasti, verkkoon voi muodostua myös sellaisia pystyrivejä, joiden solmujen asteet ovat parillisia. Lisäksi on mahdollista, että jossain vaiheessa jollain pystyrivillä ei ole yhtäkään naapuria.

Tässä on listattuna kaikki mahdolliset tapaukset, joita voi tulla vastaan, kun valitaan jokin paritonasteinen pystyrivi.

1. Paritonasteisella pystyrivillä on paritonasteinen naapuri.
2. Paritonasteisella pystyrivillä on vain parillisasteisia naapureita.
3. Paritonasteisella pystyrivillä ei ole naapureita.
4. Paritonasteisia pystyrivejä ei ole.

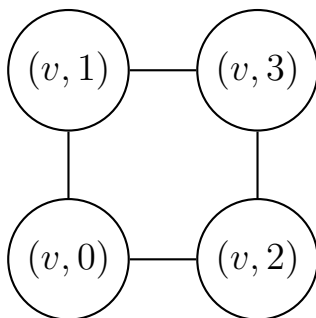
Tapaus 1 käsiteltiin jo: jos pystyrivit ovat  $(v, 0)$ ,  $(v, 1)$  ja  $(w, 0)$ ,  $(w, 1)$ , niin poistetaan solmut  $(v, 0)$ ,  $(w, 1)$ ,  $(v, 1)$  ja  $(w, 0)$  tässä järjestyksessä.

Tapaus 2 käsitellään vastaavasti poistamalla solmut järjestyksessä  $(v, 0)$ ,  $(w, 0)$ ,  $(w, 1)$ ,  $(v, 1)$ .

Tapauksessa 3 pystyrivin  $(v, 0)$ ,  $(v, 1)$  solmujen asteet ovat 1. Tällöin vain poistetaan solmu  $(v, 1)$ , jolloin solmun  $(v, 0)$  aste on 0. Tästä lähtien aina, kun teemme tyypin 2 operaation, tulee solmun  $(v, 0)$  naapuri poistaa. Tämä on hyvin pieni (ja helppo) yksityiskohta, mutta prosessin kannalta on tärkeää aina poistaa kaari, jos se yhdistää kaksi solmua, joiden asteet ovat 1.

Tapauksessa 4 verkon jokaisen solmun aste on parillinen ja ainoa mahdollisuus on luoda kopio verkosta.

Olemme nyt tilanteessa, jossa jokaisen pystyrivin solmujen määrä on 4 ja jossa jokaisen pystyrivin jokaisen solmun aste on pariton. (Pois lukien solmut, joiden aste on 1: näistä sovittiin, että aste tiputetaan aina nolnaan.) Huomataan, että paritonasteinen pystyrivi  $(v, 0)$ ,  $(v, 1)$ ,  $(v, 2)$ ,  $(v, 3)$  voidaan poistaa – tähän vastaa jo aiemmin käsiteltyä neliön poistamista.



Neliön poistaminen onnistuu nytkin.

Voimme siis jälleen vähentää pystyrivien määrää.

Kysymys kuuluu: voimmeko edetä näin niin kauan kuin pystyrivejä on jäljellä? Vastaus on myönteinen, mutta tämä ei ole aivan selvää. Tutkitaan yksityiskohtaisesti, mitä tapahtuu siinä kohdassa, kun pystyrivien koot ovat  $2^n$ .

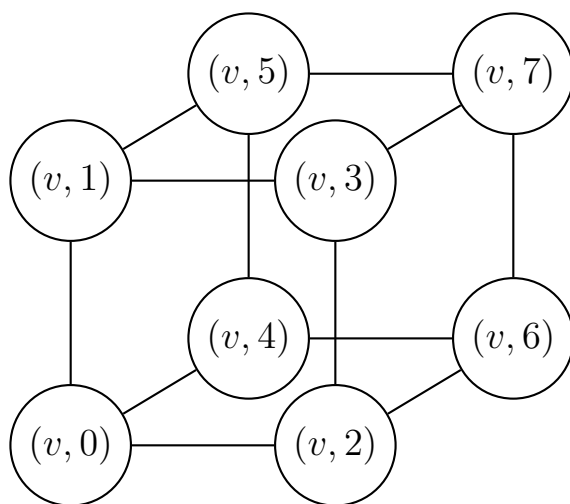
Tutkitaan jotain pystyriviä, jonka solmujen asteet ovat parittomia. Jos tällaista pystyriviä ei ole, niin teemme verkosta kopion, jolloin verkosta löytyy ainakin yksi paritonasteinen pystyrivi, joka voidaan valita. Olkoon tarkasteltava pystyrivi  $(v, 0)$ ,  $(v, 1)$ ,  $\dots$ ,  $(v, 2^n - 1)$ .

Haluaisimme poistaa tämän pystyrivin kokonaan. Pystyrivin rakenne muistuttaa todellisuudessa  $n$ -ulotteista hyperkuutiota. Jos  $n = 2$ , niin kyseessä on vain edellisessä kuvassa esitetty neliö.

Yleisellä  $n$  tilannetta voi olla vaikea hahmottaa geometrisesti, mutta symbolisesti tämä on kohtalaisen helppoa lukujen binääriesitysten kautta: solmut  $(v, x)$  ja  $(v, y)$  on yhdistetty kaarella jos ja vain jos lukujen  $x$  ja  $y$  binääriesityksissä on täsmälleen yksi kohta, jossa luvuilla on eri numero. (Yksi tapa motivoida tämä on ajatella

$n$ -ulotteista kuutiota, jonka kärkipisteet on  $n$ -ulotteisessa koordinaatistossa niin, että jokaisen pisteen jokainen  $n$ :stä koordinaatista on joko 0 tai 1. Nämä  $n$  koordinaattia vastaavat jotain binääriesityksessä annettua lukua, ja toisin päin. Kaaret vastaavat tällöin  $n$ -ulotteisen kuution särmiä.)

Miten sitten saamme poistettua kuution kärkipisteet annetuilla operaatioilla? Jo aiemmin käsitellyssä tapauksessa  $n = 2$  poistimme ensin lukuja 0 ja 3 (binääriesityksessä 00 ja 11) vastaavat solmut, ja sitten poistimme lukuja 1 ja 2 (binääriesityksessä 01 ja 10) vastaavat solmut. Tapauksessa  $n = 3$  ideana on aina poistaa ”vastakkaisia kulmia”: ensiksi voidaan poistaa luvut 0, 3, 5 ja 6 (binääriesityksessä 000, 011, 101 ja 110) ja sitten luvut 1, 2, 4 ja 7 (binääriesityksessä 001, 010, 100 ja 111). Tässä on kuitenkin pieni ongelma: solmujen 1, 2, 4 ja 7 asteet ovat solmujen 0, 3, 5 ja 6 poistamisen jälkeen parillisia. Emme kuitenkaan ole enää kaukana ratkaisusta.



Kuution poistaminen melkein onnistuu.

Huomataan, että mikäli  $n$  on parillinen, niin  $n$ -ulotteisen hyperkuution solmut voi poistaa poistamalla ensiksi ne solmut  $(v, x)$ , joissa luvun  $x$  binääriesityksessä on parillinen määrä ykkösiä, ja sitten ne solmut  $(v, y)$ , joissa luvun  $y$  binääriesityksessä on pariton määrä ykkösiä. Tällöin samassa vaiheessa poistettavien solmujen välillä ei ole kaaria ja toisessa vaiheessa solmuilta on poistettu parillinen määrä naapureita, koska kuution sisällä solmuilla on  $n$  naapuria. Siis ainoastaan parittomilla  $n$  muodostuu edellä kuvailtu ongelma. Tutkimme täten enää vain parittomia  $n$ .

Ongelman korjaamiseen voidaan ottaa hieman vinkkiä siitä, mitä teimme aiemmin. Tapauksessa  $n = 1$ , eli kahden kokoisilla pystyriveillä, tutkimme pystyrivin  $(v, 0)$ ,  $(v, 1)$  lisäksi jotain solmun  $(v, 0)$  naapuria  $(w, 0)$  ja sen pystyriviä  $(w, 0)$ ,  $(w, 1)$ . Teimme operaatiot kahdella tavalla riippuen siitä, oliko solmun  $(w, 0)$  aste parillinen vai pariton. Jos solmun  $(w, 0)$  aste oli pariton, niin poistimme neliöstä ensiksi vastakkaiset kulmat, ja jos solmun  $(w, 1)$  aste oli parillinen, niin poistimme ensiksi neliön alarivin solmut  $(v, 0)$  ja  $(w, 0)$  ja sitten ylärivin solmut  $(w, 1)$  ja  $(v, 1)$ . Lisäksi tuli erikseen tutkia tapaus, jossa parittomalla pystyrivillä ei ollut yhtään naapuria.

Toimimme siis vastaavasti yleisessä tapauksessa. Käsittelemme samat tapaukset kuin tapauksessa  $n = 1$ .

1. Paritonasteisella pystyrivillä on paritonasteinen naapuri.
2. Paritonasteisella pystyrivillä on vain parillisasteisia naapureita.
3. Paritonasteisella pystyrivillä ei ole naapureita.
4. Paritonasteisia pystyrivejä ei ole.

*Tapaus 1:* Idea on sama kuin tapauksessa  $n = 1$ . Sen sijaan, että yrittäisimme käsitellä pystyriiviä  $(v, 0), \dots, (v, 2^n - 1)$  yksinään  $n$ -ulotteisena kuutiona, käsittelemmekin pystyrivejä  $(v, 0), \dots, (v, 2^n - 1)$  ja  $(w, 0), \dots, (w, 2^n - 1)$  yhdessä  $n + 1$ -ulotteisena kuutiona (esimerkiksi tapauksessa  $n = 1$  siirryimmekin tutkimaan kahta kahden kokoista pystyriiviä, eli neliötä). Koska hyperkuutioiden käsittely onnistuu parillisilla ulottuvuuksilla ja  $n + 1$  on parillinen, voidaan molemmat pystyrit poistaa samanaikaisesti.

*Tapaus 2:* Tämä on vaikein tapaus. Tapauksessa  $n = 1$  toimimme niin, että poistimme solmut  $(v, 0), (w, 0), (w, 1)$  ja  $(v, 1)$  tässä järjestyksessä. Ei ole selvää, miten kannattaa toimia yleisesti. Tätä voidaan kuitenkin käsitellä toisen erikoistapauksen kautta.

Vaikka tutkimmekin enää parittomia  $n$ , niin intuition saamiseksi voimme hetkeksi tutkia erikoistapausta  $n = 2$ . Ongelman voi nyt halutessaan visualisoida  $n + 1 = 3$ -ulotteisena kuutiona. Ei ole kovin vaikeaa nähdä, että tällöin ongelma ratkeaa poistamalla ensin solmu  $(v, 0)$ , jonka jälkeen poistetaan solmu  $(w, 0)$ . Tämän jälkeen voidaan poistaa solmu  $(w, 1)$ , jonka perään poistetaan solmu  $(v, 1)$ . Vastaavasti poistetaan parit  $(w, 2), (v, 2)$  ja  $(v, 3), (w, 3)$ .

Huomionarvoista on, että voimme poistaa solmuja pareissa: poistamme ensin solmun  $(v, x)$  ja sen jälkeen solmun  $(w, x)$  tai toisin päin. Huomataan, että tämä toimii myös yleisellä  $n$ : kunhan säilytämme symmetrian, niin solmujen  $(v, x)$  ja  $(w, x)$  asteilla on eri parillisuus. Toisen aste on siis pariton, joten voimme poistaa sen, ja tämän jälkeen voimme poistaa myös toisen parin solmuista.

*Tapaus 3:* Tässä tapauksessa voimme yksinkertaisesti poistaa kaikki solmut  $(v, x)$ , joissa luvun  $x$  binääriesityksessä on parillinen määrä ykkösiä. Jäljelle jää kaikki ne  $2^{n-1}$  solmua muotoa  $(v, y)$ , missä  $y$ :llä on pariton määrä ykkösiä binääriesityksissään. Nämä solmut eivät ole yhteydessä toisiinsa, joten niiden aste on 0. Tämä on hyvä lopputulos.

*Tapaus 4:* Ei auta muuta kuin luoda kopio verkosta.

Olemme siis vihdoinkin valmiit: Jos verkossa on jäljellä jokin paritonasteinen pystyriivi, niin se voidaan poistaa. Jos jäljellä on vain parillisasteisia pystyrivejä, niin verkosta voidaan luoda kopio. Tällöin pystyrivien asteet muuttuvat parittomiksi ja niistä voidaan poistaa vähintään yksi.

Kommentti: Tehtävä on haastava. Henkilökohtaisesti eniten ongelmia ratkaisussa tuotti se, etten tiennyt, tulisiko ratkaisu toimimaan: ”Voiko niinkin yksinkertainen ratkaisu kuin pystyrivien poistaminen yksitellen toimia? Epätriviaaleja yksityiskohtia syntyy melko paljon: ehkä tämä idea onkin huono”. Pieni kriittisyys ratkaisua kohtaan

on tervettä, mutta toisaalta moni vaikea tehtävä vaatii sen, että sitä oikeasti alkaa tekemään ja tarvittaessa käsitellee yksityiskohtia matkan varrella.

Muuten ratkaisussa ei ole sen kummoisempia motivaatioita. Minulle luonnollinen ja helppo tapa ajatella kopiointia oli päällekkäin asettuvat levyt ja niiden pystyrivit. Pystyrivien määrä ei kasva kopioinnilla, joten luonteva idea on yrittää vähentää niiden määrää poisto-operaatioilla. Tutkimalla hieman pieniä tapauksia huomataan, että ongelma palautuu pystyrivien eli hyperkuutioiden kärkipisteiden poistamiseen. Tämä ongelma itsessään ei ole enää kovin vaikea. Ratkaisun suurin vaikeus onkin mielestäni käsitellä kaikki yksityiskohdat ja oletukset niin, ettei todistukseen jää aukkoja.

## 22 Lisätehtäviä (Kombinatoriikka)

Tässä luvussa esitetään kombinatoriikan lisätehtäviä, jotka ovat tärkeitä vaihtelevista syistä.

Ensimmäinen tehtävä on ongelmanratkaisun näkökulmasta kohtalaisen mielenkiintoinen, mutta esimerkillä on myös toinen tarkoitus. Kombinatoriikassa tulee välillä vastaan todistuksia, jotka tuntuvat päteviltä mutta joiden pätevyyden varmistaminen voi olla vaikeaa.<sup>100</sup> Tehtävän yhteydessä on esitetty tällainen todistus.

### Tehtävä

Tasossa on  $n$  ( $n \geq 3$ ) pistettä, jotka eivät kaikki ole samalla suoralla. Osoita, että pisteiden joukosta voidaan valita sellaiset kolme pistettä  $A$ ,  $B$  ja  $C$ , jotka eivät ole samalla suoralla, että kaikki loput pisteet ovat joko kolmion  $ABC$  ympärysympyrän sisällä tai sen kehällä.

Tässä on esitetty yksi ratkaisuhahmotelma, jonka askeleet on numeroitu myöhemmä käsittelyä varten.

1. Valitaan jokin (suuri) ympyrä niin, että kaikki annetut pisteet ovat sen sisällä.
2. Pienennetään tämän ympyrän sädettä, kunnes sen kehällä on vähintään yksi piste. Olkoon tämä piste  $A$ .
3. Liikutetaan tätä ympyrää niin, että sen kehä kulkee aina pisteen  $A$  kautta. Liikutetaan ympyrää kunnes sen kehällä on jokin toinen piste  $B$ .
4. Pienennetään tätä ympyrää niin, että pienennyksen aikana sen kehä kulkee pisteiden  $A$  ja  $B$  kautta. Pienennetään ympyrää, kunnes sen kehällä on jokin kolmas piste  $C$ .
5. Nyt ympyrä on kolmion  $ABC$  ympärysympyrä, ja täten pisteet  $A$ ,  $B$  ja  $C$  toteuttavat tehtävänannon ehdot.

Onko tämä pätevä todistus? Nopealla vilkaisulla voisi sanoa, että ratkaisu on toimiva: voimme tietysti valita askeleen 1 mukaisen ympyrän, ja sitä voidaan tietysti pienentää askeleen 2 mukaisesti ja niin edelleen. Ratkaisussa on kuitenkin virhe, ja se herättää muutenkin muutaman kysymyksen:

1. Onko kohdan 1 kuvailema ympyrä todella olemassa?
2. Miten ympyrää pienennetään kohdassa 2?
3. Miten ympyrää liikutetaan kohdassa 3?
4. Miten ympyrää pienennetään kohdassa 4?

<sup>100</sup>Kirjoittaessani ratkaisun ensimmäistä kertaa tein virheen, joka paljastui vasta Akseli Jussinmäen oikolukiessa tekstiä, vaikka yritin olla tarkka yksityiskohtien kanssa. Olin myös keksinyt vaihtoehtoisen ratkaisun tehtävään, jossa ollut kriittinen virhe paljastui vasta paljon myöhemmin.

5. Miksi ympyrän pienentäminen kohdassa 4 johtaa siihen, että sen kehältä löytyy kolmas piste  $C$ ?
6. Miksi kolmion  $ABC$  ympärysympyrä toteuttaa halutut ehdot kohdassa 5?

Kysymyksiä tulikin melko monta. Onko ratkaisu siis huono?

Puolustetaan ratkaisua hieman. Totta kai jokaisesta ratkaisusta voi kysyä vielä tarkentavia kysymyksiä ja vaatia lisää yksityiskohtia. Lisäksi osa kysymyksistä on melko keuhkoja: kysymyksen 6 vastaus on ”tulos seuraa siitä, miten ympyrä on valittu”, ja kysymyksen 1 vastaus on ilmiselvä.

Ongelmana on kuitenkin se, että ratkaisusta voidaan esittää useampi sellainenkin kysymys, johon vastaaminen ei ole aivan triviaalia. Lisäksi ratkaisussa on, kuten aiemmin mainittiin, virhe.

Käydään kysymykset yksitellen läpi. Olkoot annetut pisteet  $P_1, P_2, \dots, P_n$ .

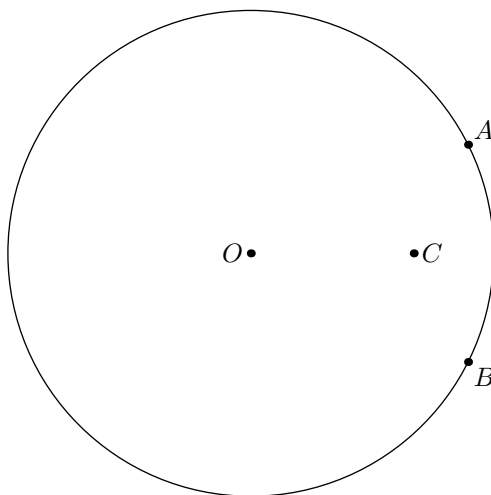
1. On. Tämän voi todistaa seuraavasti: Asetetaan pisteet  $xy$ -koordinaatistoon. Olkoon  $d_i$  pisteen  $P_i$  etäisyys origosta. Valitaan ympyrän keskipisteeksi origo ja säteeksi suurin luvuista  $d_1 + 1, d_2 + 2, \dots, d_n + 1$ . Tällöin kaikki pisteistä  $P_i$  ovat ympyrän sisällä.
2. Pidetään ympyrän keskipiste prosessin aikana origossa, ja pienennetään ympyrää.
3. Käännetään ympyrää niin, että sen säde pysyy vakiona ja että sen kehä kulkee koko ajan pisteen  $A$  kautta. Käännetään ympyrää, kunnes kehä osuu toiseen pisteeseen  $B$ .
4. Ympyrää voi pienentää liikuttamalla sen keskipistettä janan  $AB$  keskinormaalia pitkin.
5. Ei johdakaan – todistuksessa on tässä kohtaa virhe. Tätä käsitellään tarkemmin alla.
6. Tämä seuraa konstruktiosta: ympyrän ulkopuolella ei missään kohtaa ole mitään pisteistä  $P_1, \dots, P_n$ .

Huomataan, että suurella osalla kysymyksistä on kohtalaisen helpot vastaukset, ja niiden voi ajatella olevan vain helppoja yksityiskohtia. Kuinka paljon yksityiskohtia ratkaisussa voi sivuuttaa? Aiheesta (ja yleisesti ratkaisujen kirjoittamisesta) on kirjoittanut Evan Chen (<https://web.evanchen.cc/handouts/english/english.pdf>) vapaasti käännettynä näin: ”Tarkastajat ovat kiinnostuneita siitä, oletko ratkaissut tehtävän, eivätkä kyvystäsi täyttää vastauspapereitasi tekstillä” ja ”Menetät pisteitä jos kisaaja, joka ei ratkaissut tehtävää, olisi voinut kirjoittaa samat asiat kuin sinä. Esimerkiksi aina kun sanot jotain kuten ’Nähdään selvästi, että  $X$ ’, tarkastajan tulee miettiä, tiedätkö oikeasti miksi  $X$  pätee vai yritätkö bluffata”. Kisaajan tehtävä on siis vakuuttaa tarkastaja siitä, että osaa ratkaista tehtävän.



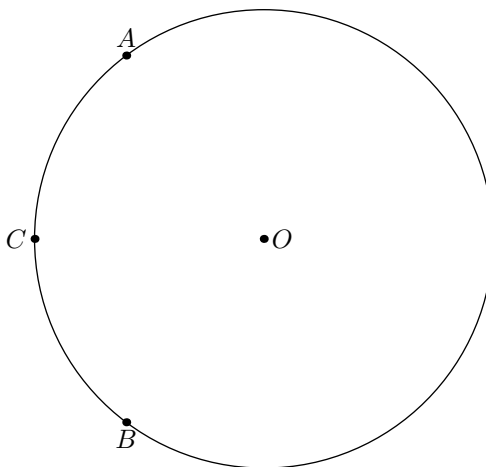
Mainittakoon vielä, että asioita kuten ”2017 on alkuluku” ja ” $2^{20} = 1048576$ ” ei tarvitse perustella sen tarkemmin. Myöskin tunnettuja tuloksia saa käyttää ratkaisuissa, kunhan käyttää maalaisjärkeä. (On epätodennäköistä, että pelkästään toteamalla ”Tämä tehtävä on erikoistapaus tunnetusta tuloksesta  $X$ ” saa täydet pisteet.) Näistä aiheista voi lukea lisää Evan Chenin tekstistä.

Käsitellään vielä kysymystä 5. Tutkimme siis tilannetta, jossa ympyrän kehällä on pisteet  $A$  ja  $B$ , ja kuljetamme ympyrän keskipistettä janan  $AB$  keskinormaalia pitkin janaa  $AB$  kohti. Tämän liikuttamisen seurauksena ympyrä ei välttämättä koskaan tule osumaan kolmanteen pisteeseen  $C$ , kuten seuraava kuva näyttää. Kuvassa  $O$  on ympyrän keskipiste.



Ongelmana on, että ympyrä on pienimmillään se ympyrä, jonka halkaisija on  $AB$ . Jos  $C$  ei ole tämän ympyrän kehällä tai sen ulkopuolella, ei ympyrän pienentäminen riitä.

Ratkaisu ongelmaan on tietysti jatkaa keskipisteen  $O$  siirtämistä janan  $AB$  toiselle puolelle.



Yleisesti menetellään siis niin, että keskipistettä  $O$  siirretään lähemmäs janaa  $AB$ , ja jos tämän aikana ympyrän kehä ei kulje muiden pisteiden kautta, jatketaan

keskipisteen siirtämistä eteenpäin. Ei ole vaikeaa nähdä, että kehä lopulta osuu johonkin muuhun pisteeseen. (Voidaan esimerkiksi valita jokin piste  $C$ , joka ei ole samalla suoralla pisteiden  $A$  ja  $B$  kanssa, ja todeta, että jossain vaiheessa  $O$  kulkeutuu kolmion  $ABC$  ympärysympyrän keskipisteeseen.)

Huomaa, että vasta edellisessä kappaleessa otamme huomioon sen ehdon, etteivät kaikki pisteet ole samalla suoralla. Tätä ei otettu huomioon alkuperäisessä ”ratkaisussa”, mikä myös herättää epäilyksiä sen toimivuudesta.

Olemme nyt korjanneet ratkaisun ja todistaneet, että se toimii.

Kommentti: Erityisesti kombinatoriikassa on melko yleistä, että kilpailijalla on todistukselle jokin epämääräinen hahmotelma, jota on vaikea pukea formaaliksi todistukseksi. Yllä on vain yksi esimerkki tällaisesta tilanteesta. Monesti (myös kombinatoriikan ulkopuolella) ratkaisun vaikeus piileekin siinä, miten heuristiset ajatukset ongelmasta saadaan muutettua eksakteiksi tuloksiksi.

Seuraava tehtävä on vuoden 2013 EGMOsta. Esimerkin tavoitteena on korostaa asioiden tulkitsemista oikeanlaisina matemaattisina objekteina.

### Tehtävä

Lumikki ja seitsemän kääpiötä asuvat talossaan metsän siimeksessä. Tiedämme kääpiöistä seuraavat asiat:

- Kuudestatoista peräkkäisestä päivästä jokaisena osa kääpiöistä työskenteli timanttikaivoksessa, kun taas loput kääpiöt keräsivät metsässä marjoja.
- Kukaan kääpiöistä ei tehnyt minkään päivän aikana molempia töitä.
- Minkä tahansa kahden eri (ei välttämättä peräkkäisen) päivän aikana kolme kääpiötä tekivät kukin molempia töitä.
- Ensimmäisenä päivänä kaikki seitsemän kääpiötä työskentelivät timanttikaivoksessa.

Osoita, että jonakin näistä 16 päivästä kaikki seitsemän kääpiötä keräsivät marjoja.

Huomataan, että jokaisen päivän tapahtumat voidaan kuvata seitsemällä numerolla, joista jokainen on joko nolla tai yksi. Nolla kuvaa sitä, että kääpiö työskenteli timanttikaivoksessa, ja ykkönen kuvaa sitä, että kääpiö keräsi marjoja. Jos esimerkiksi kääpiöt 1, 2 ja 4 ovat keränneet marjoja ja muut ovat työskennelleet timanttikaivoksessa, on päivän merkkijono 1101000.

Mitä näistä merkkijonoista tiedetään? Tiedetään, että niiden joukossa on merkkijono 0000000. Lisäksi tiedetään, että minkä tahansa kahden merkkijonon joukossa on vähintään kolme kohtaa, joissa ne eroavat. Näistä ehdoista pitäisi seurata, että merkkijonon joukossa on myös jono 1111111.

Mitä ehdot oikeastaan kertovat merkkijonoista? Merkkijonoja on 16 kappaletta, ja mahdollisia seitsemän merkin binäärijonoja on  $2^7 = 128$  kappaletta. Näillä 16

merkkijonolla ei siis ole kovin paljoa ”tilaa”, mutta ne ovat silti melko ”kaukana” toisistaan. Tämä vaikuttaa olevan syy sille, miksi tehtävänannon väite pätee. Ainoa tapa, jolla merkkijonot saadaan sommiteltua toisiinsa nähden on sellainen, jossa yksi merkkijonoista on ykkösistä koostuva jono 111111.

Enää tulee tarkentaa ajatusta siitä, kuinka merkkijonot on kaukana toisistaan. Tämän voi tehdä seuraavasti: Olkoot 16 päivän merkkijonot  $s_1, s_2, \dots, s_{16}$ . Jokaiselle merkkijonolle  $s_i$  tutkitaan niitä binäärimerkkijonoja, jotka eroavat merkkijonosta  $s_i$  enintään yhden merkin kohdalla. (Siis myös  $s_i$  lasketaan mukaan.) Näitä merkkijonoja on  $7 + 1$  kappaletta. Tämä antaa jokaiselle merkkijonolle  $s_i$  joukon merkkijonoja, jotka ovat sitä ”lähellä”. Merkitään tätä joukkoa merkinnällä  $A_i$ .

Pointtina on, että joukot  $A_1, A_2, \dots, A_{16}$  eivät sisällä mitään yhteisiä alkioita. Intuitiivisesti tämä johtuu siitä, että mikäli merkkijonoilla  $s_i$  ja  $s_j$  olisi jokin merkkijono, jonka lähellä ne molemmat ovat, niin  $s_i$  ja  $s_j$  olisivat myös kohtalaisen lähellä toisiaan. Tämä onkin jo melkein todistus väitteelle: Oletetaan, että  $A_i$  ja  $A_j$  sisältävät yhteisen merkkijonon  $s$ . Oletuksen nojalla  $s$  ja  $s_i$  eroavat enintään yhdessä kohdassa ja  $s$  ja  $s_j$  eroavat myös enintään yhdessä kohdassa. Nyt  $s_i$  ja  $s_j$  eroavat toisistaan enintään kahdessa kohdassa. Tämä on ristiriidassa sen oletuksen kanssa, että  $s_i$  ja  $s_j$  eroavat toisistaan vähintään kolmessa kohdassa.

Joukot  $A_1, \dots, A_{16}$  ovat siis erillisiä, ja jokainen niistä sisältää 8 merkkijonoa. Yhdessä ne sisältävät täten  $8 \cdot 16 = 128$  merkkijonoa. Tässä ovat siis kaikki seitsemän merkin binäärijonot. Tämä on selvästi edistystä. Merkkijonot  $s_1, \dots, s_{16}$  on siis valittu ”tasaisesti” niin, että jokainen seitsemän merkin merkkijono on lähellä jotain niistä. Nyt tulee todistaa, että tämä onnistuu vain silloin, kun jokin merkkijonoista  $s_i$  on ykkösjono.

Luonnollinen idea on vastaoletus. Oletetaan siis, että mikään jonoista  $s_i$  ei ole ykkösjono. Edellisen päättelyn nojalla jokin joukoista  $A_1, \dots, A_{16}$  kuitenkin sisältää ykkösjonon, joten jonkin jonoista  $s_i$  tulee koostua kuudesta ykkösestä ja yhdestä nolasta. Symmetrian vuoksi voidaan olettaa, että kyseinen nolla on jonon viimeinen merkki, jolloin siis jokin jonoista  $s_i$  on 111110.

Tiedämme siis, että 16 jonostamme löytyy ainakin jonot  $A = 0000000$  ja  $B = 1111110$ . Tutkitaan loppuja 14 jonoa. On luonnollista ja kätevää tutkia erikseen niitä, joiden viimeinen merkki on 0, ja niitä, joiden viimeinen merkki on 1.

Olkoon siis  $s$  jokin 14 jonosta. Oletetaan ensiksi, että sen viimeinen merkki on 0. Koska sen tulee erota jonosta  $A$  vähintään kolmessa kohdassa, tulee siinä olla vähintään kolme ykköstä. Toisaalta jonojen  $s$  ja  $B$  tulee myös erota vähintään kolmesta kohdasta, joten jonossa  $s$  tulee olla enintään kolme ykköstä. Siis  $s$  sisältää tasan kolme ykköstä. Vastaavalla logiikalla huomataan, että mikäli jonon  $s$  viimeinen merkki on 1, niin siinä on joko 2, 3 tai 4 ykköstä ensimmäisten kuuden merkin kohdalla (ja lisäksi viimeinen merkki on 1).

Vaihtoehtoja ei siis ole kovin montaa. Yritetään vielä laskea, kuinka paljon kussakin osakategoriassa voi olla jonoja (tavoitteena saada ristiriita). Tutkitaan ensiksi niitä jonoja  $s$ , joiden viimeinen merkki on 1 ja joissa on 2 ykköstä ensimmäisten kuuden merkin kohdalla. Olkoon näitä  $k$  kappaletta. Koska jokaisen näistä  $k$  jonosta tulee

erota toisistaan vähintään kolmessa kohdassa, ei millään kahdella niistä saa olla ykköstä samassa kohdassa kuuden ensimmäisen merkin kohdalla. Tästä seuraa, että  $k \leq 3$ . Vastaavalla logiikalla todistetaan, että niitä jonoja  $s$ , joiden viimeinen merkki on 1 ja joilla on ensimmäisten kuuden merkin kohdalla 4 ykköstä, on enintään kolme (koska niillä ei saa olla nollia samoissa kohdissa).

Jäljellä on vielä niiden merkkijonojen määrän laskeminen, joilla on täsmälleen kolme ykköstä ensimmäisten kuuden merkin joukossa (ja joilla joko on tai ei ole viimeisessä kohdassa ykköstä). Tutkitaan ensiksi vain niitä merkkijonoja, jotka päättyvät nollaan. Oletetaan, että näitä on vähintään yksi. Voidaan symmetrian nojalla olettaa, että yksi näistä jonoista on 1110000. Nyt muissa kolme ykköstä sisältävissä jonoissa on enintään yksi ykkönen ensimmäisten kolmen merkin joukossa. Tutkitaan kahta tapausta.

1. On olemassa jokin kolme ykköstä sisältävä jono, jolla ei ole yhtään ykköstä ensimmäisten kolmen merkin kohdalla (ja joka päättyy nollaan). Tämä jono on tällöin 0001110. Nähdään, että mikä tahansa (nollaan päättyvä) jono, jossa on kolme ykköstä, sisältää vähintään kaksi yhteistä ykköstä jommankumman jonoista 1110000 ja 0001110 kanssa. Täten muita jonoja, joiden etäisyys näihin on vähintään kolme, ei ole, eli tässä tapauksessa kolme ykköstä sisältäviä (nollaan päättyviä) jonoja on kaksi kappaletta.
2. Kaikissa (nollaan päättyvissä) jonoissa, joissa on kolme ykköstä (ja jotka eivät ole 1110000), on yksi ykkönen ensimmäisten kolmen merkin joukossa. Tutkitaan kahta tällaista jonoa. Oletetaan, että niiden ensimmäisten kolmen merkin joukossa oleva ykkönen on samassa kohdassa. Koska näiden jonojen loput kaksi ykköstä ovat paikoilla 4, 5 tai 6, on jokin kohta, jossa molemmilla jonoilla on ykkönen. Täten nämä jonot eroavat enintään kahdessa kohdassa, mikä on ristiriita. Tästä seuraa, että on olemassa enintään neljä (nollaan päättyvää) merkkijonoa, joissa on kolme ykköstä: niitä, joissa on yksi ykkönen ensimmäisten kolmen merkin kohdalla, on edellisen nojalla enintään kolme, ja lisäksi on merkkijono 1110000.

Huomataan siis, että pahimmassa tapauksessa kolme ykköstä sisältäviä (nollaan päättyviä) merkkijonoja on enintään neljä kappaletta.

Täysin vastaava päättely toimii tietysti myös niille ykköseen päättyville jonoille, joissa on kolme ykköstä ensimmäisten kuuden merkin kohdalla.

Olemmeko saaneet ristiriidan? Jonojen 0000000 ja 1111110 lisäksi nollaan päättyvissä jonoissa on aina kolme ykköstä, ja niitä on edellisen nojalla enintään neljä. Ykköseen päättyvissä jonoissa on 2, 3 tai 4 ykköstä, ja näitä on edellisen päättelyn nojalla enintään 3, 4 ja 3 kappaletta. Yhteensä jonoja on siis  $(1+1)+4+(3+4+3) = 16$ .

Emme siis saaneet ristiriitaa. Menikö kaikki työ hukkaan? Ei suinkaan: nyt tiedämme, että jokaisessa ylärajassa tulee päteä yhtäsuuruus. Siis esimerkiksi on olemassa täsmälleen kolme ykköseen päättyvää jonoa, joissa on kaksi ykköstä ensimmäisen kuuden merkin kohdalla. Tämä antaa huomattavasti lisätietoa.

Tutkitaan niitä jonoja, jotka päättyvät ykköseen. Näissä on edellisen nojalla

3 sellaista jonoa, joissa on kaksi ykköstä ensimmäisten kuuden merkin kohdalla. Oletetaan (symmetriaan pohjautuen), että nämä jonot ovat

1100001, 0011001 ja 0000111.

Tutkitaan nyt jotain sellaista (ykköseen päättyvää) jonoa, jossa on kolme ykköstä ensimmäisten kuuden merkin kohdalla. Näitä on edellisen nojalla olemassa peräti neljä kappaletta. Tällaisella jonolla ei voi olla kahta yhteistä ykköstä kuuden ensimmäisen merkin kohdalla minkään edellä mainitun kolmen jonon kanssa. Siispä tällaisella jonolla tulee olla yksi ykkönen jommassakummassa kohdista 1 ja 2, yksi ykkönen jommassakummassa kohdista 3 ja 4 ja yksi ykkönen jommassakummassa kohdista 5 ja 6. Yhteensä on siis  $2^3 = 8$  vaihtoehtoa näille neljälle jonolle. Lisäksi näissä neljässä jonossa ei saa olla kahta, joilla on kahdessa samassa kohdassa ykkönen ensimmäisten kuuden merkin kohdalla. (Siis esimerkiksi paria 1010101 ja 1010011 ei voi esiintyä.) Tästä oikeastaan seuraa, että voimme olettaa (symmetriaan pohjautuen),<sup>101</sup> että nämä neljä jonoa ovat

1010101, 1001011, 0110011 ja 0101101.

Seuraavaksi luonnollisesti tutkitaan niitä ykköseen päättyviä jonoja, joissa on neljä ykköstä ensimmäisten kuuden merkin kohdalla. Näitä jonoja on kolme kappaletta, ja niitä voidaan ajatella sitä kautta, missä niiden kaksi nollaa sijaitsevat. Minkään näistä jonoista nollat eivät voi olla kohdissa 1 ja 2: tällöin jono olisi 0011111, ja tämä eroaa vain kahdessa kohdassa jonosta 0011001, jonka todettiin aiemmin olevan jonojemme joukossa. Vastaavasti todetaan, että mikään jonoista ei voi olla 1100111 eikä 0000111.

Tutkitaan jotain näistä kolmesta jonosta. Ilman yleisyyden menettämistä voidaan olettaa, että sen ensimmäinen nolla on jommassakummassa kohdista 1 ja 2 ja toinen nolla on jommassakummassa kohdista 3 ja 4. Käydään tapaukset rohkeasti läpi. Jokaisessa tapauksessa ristiriita saavutetaan vertaamalla jonoa sellaiseen jonoon, jossa on kolme ykköstä ensimmäisten kuuden merkin joukossa ja jonka on jo todettu kuuluvan jonojemme joukkoon. (Nämä on listattu yllä.)

- Jono on 1010111. Aiemmin todettiin jonon 1010101 kuuluvan joukkoon. Tästä seuraa ristiriita.
- Jono on 1001111. Aiemmin todettiin jonon 1001011 kuuluvan joukkoon. Tästä seuraa ristiriita.
- Jono on 0110111. Aiemmin todettiin jonon 0110011 kuuluvan joukkoon. Tästä seuraa ristiriita.
- Jono on 0101111. Aiemmin todettiin jonon 0101101 kuuluvan joukkoon. Tästä seuraa ristiriita.

---

<sup>101</sup>Toinen vaihtoehto olisi vaihtaa jokaisen jonon nollat ykkösiksi ja toisin päin (paitsi tietysti pitää viimeinen merkki ykkösenä). Tilannetta voi visualisoida geometrisesti niin, että kuution kärjistä tulee valita neljä kärkeä niin, että mitkään kaksi kärkeä eivät ole vierekkäisiä.

Vihdoinkin: ristiriita. Täten ykkösjonon tulee kuulua jonojen joukkoon.

Kommentti: Ratkaisun alussa siirryttiin tutkimaan kääpiöiden, marjojen poiminnan ja timanttikaivoksen sijasta binäärijonoja. Monesti kombinatoriikassa on tärkeää muokata tehtävänanto oikeaan muotoon, koska tämä antaa oikean työskentely-ympäristön ongelmalle.<sup>102</sup> Tässä tehtävässä binäärijonot on helpompia hahmottaa ja käsitellä kuin kääpiöiden työtehtävät. Lisäksi ratkaisu on lyhyempi, kun notaatio ja termistö ovat kunnossa.

“Matemaattisen” termistön käyttämistä ei tule sekoittaa kankeaan tai formaaliin ajatteluun. Esimerkiksi tämän ratkaisun alussa mainittiin, kuinka merkkijonoilla on vain vähän tilaa, mutta ne ovat kaukana toisistaan – ei kovin formaalia, mutta tämä on ratkaisun vaikein ja tärkein idea. (Tämä ajatus on mielestäni vaikeampaa löytää, jos ajattelee kääpiöitä ja työpäiviä kuin jos ajattelee merkkijonoja.)

Loppuosa ratkaisusta onkin suhteellisen suoraviivaista arviointia ja tapauskäsittelyä, kun tiedetään, että jossain jonossa on kuusi ykköstä. Tämä tapauskäsittely on jälleen yksi esimerkki tilanteesta, jossa on aivan yhtä toimivaa vain tehdä jotain kuin suunnitella eleganttia argumenttia (ja ensimmäinen on ehkä varmempaa).<sup>103</sup> Erilaisia konfiguraatioita on oikeastaan niin vähän, että uskoisin, että järkevällä läpikäynnillä (eli ottamalla huomioon symmetriat ja käymällä sopivat tapaukset läpi<sup>104</sup>) voisi käydä suunnilleen kaikki tapaukset läpi ilman, että lähtisi sen tarkemmin analysoimaan erilaisten jonojen määriä. Monesti kuitenkin ennen huomattavaa manuaalista työtä vaativaa lähestymistapaa kannattaa katsoa, voisiko työn määrää vähentää hieman joillain havainnoilla. Tässä ratkaisussa tämä saavutettiin muodostamalla sopivat ylärajat, joilla saatiin tarkat määrät tietynlaisten jonojen määrille. Tämän jälkeen tapauksia oli jäljellä käytännössä katsoen yksi, kun läpikäynnin teki järkevästi.<sup>105</sup>

Tapauskäsittelyn lukeminen on mielestäni huomattavasti ikävämpää kuin sen tekeminen. Minulta kului ehkäpä noin puoli tuntia huomata, että tapauskäsittely voidaan tehdä ja sitten suorittaa se. Kyseinen tehtävä oli viimeinen (ja siten vaikein) EGMO-kilpailupäivän kolmesta tehtävästä, joten ratkaisu on ajallisesti varsin tehokas.

Viimeinen esimerkkitehtävä on vuoden 2018 IMO-lyhytlistalta. Tehtävä on otettu esimerkiksi erityisesti sen vaikeuden takia.

<sup>102</sup>Verkkoja käsittelevät tehtävät ovat tästä yksi esimerkki, ja binäärijonoja käsittelevät tehtävät eivät nekään ole kovin harvinaisia. Yleisesti voi olla hyödyllistä esittää tehtävät mahdollisimman ”puhtaassa” muodossa. Esimerkiksi modulotarkastelut tai erilaisten invarianttien muodostaminen ovat hieman helpompia keksiä ja hahmottaa, kun puhutaan  $n$  positiivisesta kokonaisluvusta eikä  $n$  kivikasasta, joissa on jokin positiivinen kokonaislukumäärä kiviä.

<sup>103</sup>Tehtävään on elegantimpiakin ratkaisuja, jotka jatkokehittävät ideaa joukoista  $A_i$ . En lähtenyt pohtimaan tällaista, koska huomasin, että vastaoletus ja sitä seuraavat ideat johtaisivat ratkaisuun (vaikkakin tämä vaatisi hieman työtä).

<sup>104</sup>Ongelman voi jakaa monella tavalla tapauksiin, ja jotkut tavat ovat parempia kuin toiset.

<sup>105</sup>Ratkaisussa otettiin huomioon symmetria, jolloin saatiin vain yksi vaihtoehto kaksi ykköstä ensimmäisten kuuden merkin joukossa sisältäville jonoille. Lisäksi oleellista oli lähteä nimenomaan kahdesta ykkösestä eikä kolmesta, koska tällöin tapauksia olisi tullut useampi.

**Tehtävä**

Olko  $a$  ja  $b$  erisuuria positiivisia kokonaislukuja. Liitutaululle, joka on aluksi tyhjä, kirjoitetaan loputtomasti lukuja seuraavien sääntöjen mukaisesti.

1. Jos liitutaululla on vähintään yksi lukupari, jonka luvut ovat keskenään yhtä suuria, niin (yhden tällaisen) parin ensimmäistä lukua kasvatetaan  $a$ :lla ja toista lukua  $b$ :llä.
2. Jos tällaista paria ei ole olemassa, taululle kirjoitetaan kaksi kappaletta lukua 0.

Osoita, että tehtiin operaation 1 valinnat miten tahansa, tehdään tyyppin 2 operaatioita vain äärellisen monta kappaletta.

Ratkaisu etenee pienin askelin: emme hyökkää suoraan tehtävän kimppuun, vaan ratkaisemme ensiksi helpompia ongelmia. Syynä tähän on, että tehtävä on vaikea eikä ole selvää, miten väitettä pystyisi todistamaan. Siksi pyrimme ensiksi saamaan käsitystä siitä, mitä prosessissa oikein tapahtuu.

Tutkitaan väitettä tapauksessa  $a = 1$  ja  $b = 2$ . Tällöin taulun sisältö näyttää eri vaiheissa seuraavalta.

- Tyhjä
- $(0, 0)$
- $(1, 2)$
- $(1, 2, 0, 0)$
- $(1, 2, 1, 2)$

Nyt edessä on valinta: voimme korvata joko liitutaulun ykköset luvuilla 2 ja 3 tai kakkoset luvuilla 3 ja 4. Tutkitaan, mitä ensin mainitussa tapauksessa tapahtuu.

- $(2, 2, 3, 2)$
- $(3, 4, 3, 2)$
- $(4, 4, 5, 2)$
- $(5, 6, 5, 2)$
- $(6, 6, 7, 2)$

Huomataan, että stabiili rakenne on syntynyt: taululla on yhdessä vaiheessa luvut  $2, n, n$  ja  $n + 1$ , ja operaation jälkeen taululla on luvut  $2, n + 1, n + 1$  ja  $n + 2$ . On helppoa tarkistaa, että mikäli aiemmin tehdyssä valintatilanteessa olisikin suorittanut operaation ykkösten sijasta kakkosille, oltaisiin päädytty vastaavaan tilanteeseen. Tämä ratkaisee tehtävän tapauksessa  $a = 1$  ja  $b = 2$ .

Luonnollinen jatkokysymys on, onko kaikilla  $a$  ja  $b$  olemassa tällainen stabiili rakenne. Tämä ei vielä ratkaise alkuperäistä ongelmaa, mutta vastauksen löytäminen kysymykseen on hyvä välietappi. (Lisäksi ei ole selvää, mitä muutakaan tässä vaiheessa voisi tehdä.)

Miltä stabiili rakenne näyttäisi tapauksessa  $a = 1$  ja  $b = 3$ ? Yksi tapa selvittää asia on suorittaa tehtävänannon prosessia näillä arvoilla ja katsoa, mitä tapahtuu. Alla on listattu, mitä prosessissa tapahtuu, kun tyypin 1 operaatioilla muutetaan aina taulun pienintä lukuparia. Luvut on selvyuden vuoksi kirjoitettu jokaisessa vaiheessa suuruusjärjestykseen.

- Tyhjä
- (0, 0)
- (1, 3)
- (0, 0, 1, 3)
- (1, 1, 3, 3)
- (2, 3, 3, 4)
- (2, 4, 4, 6)
- (2, 5, 6, 7)
- (0, 0, 2, 5, 6, 7)
- (1, 2, 3, 5, 6, 7)
- (0, 0, 1, 2, 3, 5, 6, 7)
- (1, 1, 2, 3, 3, 5, 6, 7)
- (2, 2, 3, 3, 4, 5, 6, 7)
- (3, 3, 3, 4, 5, 5, 6, 7)
- (3, 4, 4, 5, 5, 6, 6, 7)
- (3, 5, 5, 5, 6, 6, 7, 7)
- (3, 5, 6, 6, 6, 7, 7, 8)
- (3, 5, 6, 7, 7, 7, 8, 9)
- (3, 5, 6, 7, 8, 8, 9, 10)
- (3, 5, 6, 7, 9, 9, 10, 11)
- (3, 5, 6, 7, 10, 10, 11, 12)
- (3, 5, 6, 7, 11, 11, 12, 13)



Stabiili rakenne on syntynyt: taululla on aina lukunelikko muotoa  $(n, n, n+1, n+2)$ , ja jokaisella operaatiolla nelikkoo vastaava luku  $n$  kasvaa yhdellä.

Otetaan käyttöön luonteva notaatio stabiilien rakenteiden merkitsemiseksi. Merkitään edellä saatua stabiilia rakennetta merkinnällä  $[1, 1, 2, 3]$ . Aiemmin käsitellyssä tapauksessa  $a = 1$  ja  $b = 2$  saatu stabiili rakenne olisi samalla notaatiolla  $[1, 1, 2]$ .

Nyt ei ole vaikeaa keksiä stabiileja rakenteita myös muille lukujen  $a$  ja  $b$  arvoille. Ensinnäkin huomataan, että tapauksessa  $a = 1$  stabiilin rakenteen muodostaa  $[1, 1, 2, 3, \dots, b]$ . Tapauksessa  $a = 2$  ja  $b = 3$  huomataan rakenne  $[1, 1, 2, 2, 3]$  (käymällä tarvittaessa prosessia läpi). Tämä antaa vielä valinnanvaraa operaatioille: voisimme kasvattaa joko ykkösten paria tai kakkosten paria. Olemme kuitenkin tähän mennessä tutkineet vain sitä, voidaanko stabiilia rakennetta saada aikaan, emmekä sitä, päädytäänkö stabiiliin rakenteeseen varmasti. Tutkimme siis sitä, onko olemassa edes yhtä tapaa valita tyypin 1 operaatiot, jotta tyypin 2 operaatioita tehdään vain äärellisen monta, emmekä sitä, käykö näin varmasti. Täten voimme tässä vaiheessa tyytyä siihen, että rakenne  $[1, 1, 2, 2, 3]$  mahdollistaa äärettömän ketjun tyypin 1 operaatioita.<sup>106</sup>

Kokeilemalla tarvittaessa vielä lisää konkreettisia tapauksia huomataan seuraavalla tahansa luvuilla  $a$  ja  $b$  toimiva rakenne: Voimme symmetrian nojalla olettaa, että  $a < b$ . Nyt rakenne

$$[1, 1, 2, 2, 3, 3, \dots, a, a, a+1, a+2, \dots, b]$$

mahdollistaa äärettömän määrän tyypin 1 operaatioita putkeen, koska voimme aina kasvattaa ykkösparia, jolloin päädyimme samaan rakenteeseen.

Välietappi on nyt saavutettu. Seuraava luonnollinen kysymys: voimmeko todella saavuttaa stabiilin rakenteen? Voidaanko esimerkiksi tapauksessa  $a = 2$  ja  $b = 3$  taululle todella saada samanaikaisesti luvut muotoa  $n, n, n+1, n+1, n+2$ ?

Aivan kaikissa tapauksissa tämä ei onnistu: jos  $a = 2$  ja  $b = 4$ , niin kaikki taulun luvut ovat aina parillisia, ja emme voi saavuttaa löytämäämme rakennetta  $[1, 1, 2, 2, 3, 4]$ . Tapaus  $a = 2, b = 4$  on kuitenkin käytännössä sama kuin  $a = 1, b = 2$ , koska voimme vain supistaa luvun 2 pois. Yleisesti voidaan olettaa, että  $\text{sy}(a, b) = 1$ .

Mitä rakenteen saavuttaminen edellyttäisi? Haluaisimme siis saada taululle samanaikaisesti luvut  $n, n+1, n+2, \dots, n+(b-1)$ , ja lisäksi joitain näistä luvuista haluttaisiin taululle kaksi kappaletta. Tämä motivoi seuraavan, helpomman kysymyksen: mitkä luvut taululle voidaan ylipäättään saada muodostettua?

Ongelmassa on siis kyse siitä, että haluamme esittää jonkin kokonaisluvun  $N$  lukujen  $a$  ja  $b$  summana: luvusta 0 lukuun  $N$  pääseminen käy aina niin, että lukua kasvatetaan joko luvulla  $a$  tai luvulla  $b$ . Tutkimme siis yhtälöä  $N = ax + by$ , missä  $x$  ja  $y$  ovat epänegatiivisia kokonaislukuja. Tämä muistuttaa Bezout'n lemmaa, mutta oleellisena erona on, että luvut  $x$  ja  $y$  eivät saa olla negatiivisia. Tämän vuoksi emme voi esittää esimerkiksi lukuja  $1, 2, \dots, a-1$  tässä muodossa. Intuitio kuitenkin sanoo,

<sup>106</sup>Huomataan kylläkin, että myös kakkosten muuttaminen palautuu lopulta samaan rakenteeseen, koska ketju näyttäisi tältä:  $(1, 1, 2, 2, 3) \rightarrow (1, 1, 3, 4, 5) \rightarrow (3, 3, 4, 4, 5)$ . Mutta kuten mainittiin, on liian aikaista murehtia tällaisia asioita.

että mikäli  $\text{sy}(a, b) = 1$ , niin mikä tahansa riittävän suuri kokonaisluku voidaan esittää tässä muodossa.

### Lemma

Olkoot  $a$  ja  $b$  positiivisia kokonaislukuja, joilla  $\text{sy}(a, b) = 1$ . On olemassa sellainen luku  $C$ , että kaikilla positiivisilla kokonaisluvuilla  $N$ , joilla  $N > C$ , on olemassa epänegatiiviset kokonaisluvut  $x$  ja  $y$ , joilla

$$N = ax + by.$$

Lemman todistus on formalisointi intuitiivisesta lemman pätevyyttä koskevasta käsityksestä. Jos pystymme esittämään luvun  $N$  halutussa muodossa, niin voimme esittää myös luvun  $N + a$  halutussa muodossa kasvattamalla lukua  $x$  yhdellä. Tämän vuoksi kaikilla  $0 \leq r < a$  riittää pystyä esittämään jokin luku, joka on kongruenttia luvun  $r$  kanssa modulo  $a$ , halutussa muodossa. Tämä onnistuu seuraavasti.

Koska  $\text{sy}(a, b) = 1$ , luvulla  $b$  on olemassa käänteisalkio  $t$  modulo  $a$ , jolloin siis  $bt \equiv 1 \pmod{a}$ . Selvästi tämä  $t$  voidaan valita olemaan väliltä  $[0, a)$ . Olkoon  $y = rt$ . Nyt  $y \geq 0$  ja  $by = brt \equiv r \pmod{a}$ , mikä todistaa lemmän.

(Voidaan todistaa, että suurin luku, jota ei voi esittää muodossa  $ax + by$ , missä  $x, y \geq 0$ , on  $ab - a - b$ . Tätä ei kuitenkaan tarvita tässä.)

Voimme siis saada taululle näkyviin minkä tahansa riittävän suuren kokonaisluvun. Entä voimmeko saada aikaan rakenteen  $[1, 1, 2, 2, \dots, a, a, a + 1, \dots, b]$ , eli voimmeko saada nämä luvut samanaikaisesti taululle?

Jos saisimme päättää, milloin lisäämme taululle nollia, olisi vastaus kysymykseen helppo: voisimme vain yksitellen lisätä taululle haluamiamme lukuja haluamamme määrän. Emme kuitenkaan voi menetellä näin vaikkapa tapauksessa  $a = 2$  ja  $b = 3$ : siinä kohtaa, kun halutuista luvuista  $(n, n, n + 1, n + 1, n + 2)$  on lisätty joko kaksi kappaletta lukuja  $n$  tai kaksi kappaletta lukuja  $n + 1$ , tulee pelin sääntöjen mukaan pari hajottaa, ennen kuin taululle saa lisätä kaksi uutta nollaa. Lisäksi voisi olla, että rakennettaessa uutta haluttua lukua tulemme vahingossa osuneeksi jo luotuihin lukuihin, jolloin emme voikaan edetä kuten haluamme.

Pysähdytään hetkeksi. Edellä huomattiin ongelma: stabiilia rakennetta ei voida luoda. Meillä on kuitenkin vielä isompi ongelma: vaikka todistaisimme, että jollain tyyppin 1 operaatioiden valinnoilla väite pätee, niin tästä ei seuraa, että väite pätee kaikilla valinnoilla. Ensimmäisen ongelman ratkaiseminen on hyödytöntä, jos jälkimmäistä ei saada ratkaistua. Tutkitaan siis tässä kohtaa jälkimmäistä ongelmaa.

Miten siirtojärjestys vaikuttaa lopulliseen tilanteeseen? Tapauksessa  $a = 1, b = 2$  huomaisimme, että valinnoilla ei ollut väliä: tyyppin 2 operaatioita tuli joka tapauksessa tehtyä kaksi kappaletta. Tutkitaan sitten monimutkaisempaa tapausta  $a = 1, b = 3$ , jossa yksi mahdollinen prosessi listattiin aiemmin. Alkutilanteessa prosessia päädyimme tilanteeseen, jossa taululla olivat luvut  $1, 1, 3, 3$ . Päätimme kasvattaa ykkösiä, jolloin prosessi jatkui seuraavasti:

$$(1, 1, 3, 3) \rightarrow (2, 3, 3, 4) \rightarrow (2, 4, 4, 6) \rightarrow (2, 5, 6, 7).$$

Jos olisimmekin kasvattaneet kolmosia, niin prosessi olisi ollut

$$(1, 1, 3, 3) \rightarrow (1, 1, 4, 6) \rightarrow (2, 4, 4, 6) \rightarrow (2, 5, 6, 7).$$

Lopputulos ei siis muuttunut – tämä on tärkeä huomio.

Huomio herättää kaksi uutta, toisiinsa liittyvää kysymystä:<sup>107</sup>

- Miksi valinnat eivät vaikuttaneet lopputulokseen tapauksessa  $a = 1, b = 3$ ?
- Onko lopputulos yleisestikin valinnoista riippumaton?

Vastataan ensin mainittuun kysymykseen ensimmäisenä. Erikoistapauksessa  $a = 1, b = 3$  tulemme joka tapauksessa suorittamaan operaation ykkösparille ja kolmosparille. Lisäksi huomataan, että mikäli operaatio suoritetaan ensiksi ykkösille, tulee tämän jälkeen operaatio suorittaa heti kolmosille, ja päinvastoin. Tämän vuoksi molemmilla valinnoilla päädytään tilanteeseen  $(2, 4, 4, 6)$ .

Tästä pääsemmekin sujuvasti jälkimmäiseen kysymykseen. Vastaus on myönteinen, ja todistus on oikeastaan hyvin helppo, kun ongelmaa katsoo oikeasta näkökulmasta. Lähdetään jostain aloitustilanteesta, ja tutkitaan jotain ketjua tyyppin 1 operaatioita (eli emme lisää taululle lukuja ketjun aikana). Todistetaan, että kun nämä tyyppin 1 operaatiot ”tehdään loppuun”, eli kun taululla ei ole enää kahta kappaletta samaa lukua, niin syntynyt lopputila ei riipu valitusta operaatioketjusta (olettaen, että prosessi päättyy).

Kriittinen huomio on, että taululle syntyvien lukujen  $n$  määrään vaikuttaa vain lukujen  $n - a$  ja  $n - b$  esiintymisten määrä. Tämä on selvää: jotta taululle saadaan luotua uusi luku  $n$ , tulee suorittaa tyyppin 1 operaatio joko kahdelle kappaleelle lukua  $n - a$  tai kahdelle kappaleelle lukua  $n - b$ . Alla on perusteltu tarkemmin, miten väite seuraa tästä.

Lähdetään aloitustilanteesta, jossa lukua  $n$  on  $f(n)$  kappaletta. Tutkitaan kahta tyyppin 1 operaatioketjua. Olkoon  $g(n)$  ensimmäisen operaatioketjun niiden operaatioiden määrää, joilla taululle syntyy luku  $n$ . Määritellään  $h(n)$  vastaavasti toiselle operaatioketjulle. Riittää osoittaa, että  $g(n) = h(n)$  kaikilla  $n$ . Tehdään vastaoletus, ja valitaan pienin sellainen  $n$ , jolla pätee  $g(n) \neq h(n)$ . Edellisen kappaleen huomion avulla saadaan

$$g(n) = \left\lfloor \frac{f(n-a) + g(n-a)}{2} \right\rfloor + \left\lfloor \frac{f(n-b) + g(n-b)}{2} \right\rfloor,$$

ja vastaava yhtälö luvulle  $h(n)$ . Koska  $g(n-a) = h(n-a)$  ja  $g(n-b) = h(n-b)$ , pätee  $g(n) = h(n)$ , mikä on ristiriita.

<sup>107</sup>Jälkimmäinen kysymyksistä on tietysti se, joka on päällimmäisenä mielessä. Ensimmäinen kysymys on kuitenkin myös tärkeä. Tieto ”Tapauksessa  $a = 1, b = 3$  lopputilanne ei riipu tehdyistä valinnoista.” on toki hyödyllinen, koska se johdattaa oikeille jäljille. Tärkeä sana on kuitenkin ”miksi”: jos pystymme vastaamaan tähän kysymykseen, saamme ymmärrystä, joka ei koske enää pelkästään erikoistapausta  $a = 1, b = 3$ . Tästä syystä ensimmäisen kysymyksen vastaus johtaa toisen kysymyksen vastaukseen.

Huomaa, että käytännössä sama todistus osoittaa, että mikäli jostain aloitustilasta on mahdollista tehdä äärettömän monta tyypin 1 operaatiota ilman tyypin 2 operaatioita, niin tällöin mikä tahansa tyypin 1 operaatioiden ketju kestää äärettömän pitkään: Tehdään vastaoletus. Oletetaan, että äärellisen prosessin luvut ovat enintään  $M$  prosessin päätettyä. Tutkitaan ääretöntä prosessia jollain ajanhetkellä. Ilman yleisyyden menettämistä voidaan olettaa, että siinä tehdään nyt sellaiset operaatiot, jottei mikään luvuista  $0, 1, \dots, M$  esiinny taululla useammin kuin kerran. Nyt edellisen kappaleen ideoilla saadaan, että mikä tahansa luku väliltä  $[0, M]$  esiintyy yhtä monta kertaa äärellisessä ja äärettömässä prosessissa. Koska lukujen määrät ovat samat, ei äärettömässä prosessissa voi olla lukuja, jotka ovat yli  $M$ , eli ääretön prosessi onkin nyt päättynyt.

Missä vaiheessa ratkaisumme on? Tiedämme, että operaatioiden järjestyksellä ei ole väliä lopputuloksen kannalta. Tiedämme, että on olemassa stabiileja rakenteita, jotka mahdollistaisivat vain äärellisen monen tyypin 2 operaation käyttämisen. Tiedämme, että jokainen riittävän suuri kokonaisluku  $n$  pystytään luomaan (kun  $\text{synt}(a, b) = 1$ ). Ainoa ongelma on, ettemme tiedä, miten stabiilin rakenteen pystyisi muodostamaan.

Olemme kuitenkin käytännössä ratkaisseet tämän ongelman. Olkoon  $k$  positiivinen kokonaisluku. Tutkitaan prosessia, jossa tyypin 2 operaatioita tehdään täsmälleen  $k$  kappaletta mutta jossa tyypin 2 operaatioita saa tehdä myös silloin, kun taululla on yhtä suuria lukuja. Oletetaan, että tämä prosessi päättyy äärellisellä määrällä operaatioita tilanteeseen, jossa taululla ei ole yhtä suuria lukuja.

Väite on, että lopputulos ei tällöin riipu valitusta operaatiosarjasta. Todistus: Ilman yleisyyden menettämistä voidaan olettaa, että kaikki  $k$  tyypin 2 operaatiota tehdään heti aluksi. (On ihan se ja sama, ”varastoimmeko” taululla nollia, vai varastoimmeko tyypin 2 operaatioita, joilla myöhemmin lisäämme taululle nollia.) Nyt ongelma on palautettu aiemmin käsiteltyyn ongelmaan: tyypin 1 operaatioiden valinnat eivät vaikuta lopputulokseen (edellisessä todistuksessa valitaan  $f(0) = 2k$  ja  $f(n) = 0$  kaikilla  $n \neq 0$ .)

Todistuksen viimeinen silaus: Kuten aiemmin todettiin, olisi mahdollista muodostaa stabiili rakenne, jos tyypin 2 operaatioita saisi tehdä, vaikka taululla olisi monta kappaletta samaa lukua. On siis olemassa sellainen  $k$ , että lähdettäessä alkutilanteesta, jossa taululla on  $2k$  nollaa (eikä muuta), on mahdollista muodostaa ääretön tyypin 1 operaatioiden ketju. Tällöin kaikkien muidenkin tästä alkutilasta tehtyjen ketjujen tulee olla äärettömiä (kuten aiemmin pääteltiin, jos jokin ketju olisi äärellinen, tulisi kaikkien muidenkin ketjujen olla äärellisiä). Tämä ”kaikki muut” operaatioketjut kattava joukko sisältää muun muassa ne operaatiosarjat, joissa tyypin 1 operaatiossa valitaan nollapari vain silloin, kun muita pareja ei ole jäljellä. Nämä vastaavat tehtävänannon prosesseja. Jos niissä tehdään  $k$  kappaletta tyypin 2 operaatioita, ei niissä edellisen nojalla tulla tekemään enää lisää tyypin 2 operaatioita. Tämä päättää ratkaisun.

Kommentti: Tehtävä on hyvin vaikea. Tehtävä oli vuoden 2018 IMO-lyhytlistan kombinatoriikan osion kuudes tehtävä seitsemästä, ja listan tehtävät on pyritty laittamaan vaikeusjärjestykseen. Tehtävä onkin kirjan korkeimmalta kohdalta valittu

IMO-lyhytlistan tehtävä.<sup>108</sup> Henkilökohtaisesti miellän tehtävän toki vaikeana, mutten mitenkään huippuvaikeana. Tehtävän ratkaisuun kulunut aika ei ole pisin, mitä olen käyttänyt yksittäiseen tässä kirjassa esiintyvän tehtävän ratkaisemiseen.

Miksi tehtävä sitten on vaikea? Tässä tehtävässä korostuu se, että kokonainen ratkaisu vaatii järkyttävän määrän eri ideoita: stabiilit rakenteet, niiden saavuttaminen, lopputuloksen riippumattomuus järjestyksestä ja pelin sääntöjen muuttaminen eri ideoiden yhdistämiseksi. Ideoiden keksiminen ja niiden tärkeyden tunnistaminen ei ole helppoa, ja ideat pitää pystyä myös toteuttamaan (eli halutut väitteet tulee todistaa). Kokonaisuutena vaikeutta tuo se, miten tunnistaa oikeat lähestymistavat väärästä. Tässä tehtävässä yllättää hieman se, että järjestyksen vaikuttamattomuus lopputulokseen ja stabiilien rakenteiden saavuttaminen yhdistyvät lopussa niinkin näppärästi. Tätä on hyvin vaikeaa nähdä ratkaisun alussa.

Tässä on tarkemmin omasta ratkaisuprosessistani. Ajattelin aluksi, että tehtävänannon väite ei päde: Meidän tulisi äärellisellä määrällä lukuja saada suoritettua ääretön määrä tyyppin 1 operaatiota. Miksei joukon pienimmät luvut aina vähitellen tipu muiden lukujen tahdista? (Vastaus: pienimpiä lukuja kasvatetaan  $a$ :lla, jolloin ne eivät ole enää pienimpiä. Jos  $a$  olisi nolla, niin päättely olisi pätevä, mutta muuten ei.) Kokeilin erikoistapausta  $a = 1, b = 2$ , ja päädyin ratkaisun alussa esitettyihin ideoihin stabiileista rakenteista ja niiden saavuttamisesta: ”Pystynkö todistamaan, että on edes mahdollista pärjätä vain äärellisen monella tyyppin 2 operaatiolla?”

Tiesin, että tämä ei johda kokonaiseen ratkaisuun, ja ajattelin saavani tästä lähinnä ymmärrystä enkä lopulliseen ratkaisuun jääviä lemmoja (toisin kävi – minulla kävi tuuri), mutta halusin hakea tätä kautta intuitiota. Yksi syy tämän kysymyksen tarkasteluun oli, ettei minulla ollut ideoita siihen, miten alkuperäistä väitettä voisi todistaa, joten minun oli pakko tarttua oljenkorsiin. Minulla oli kuitenkin hyvä filis tästä lähestymistavasta.<sup>109</sup>

Alun perin tehtävää ratkoessani tein virheellisen päättelyn<sup>110</sup> stabiilien rakenteiden saavuttamiseen liittyen: unohdin, että tyyppin 2 operaatioita saa suorittaa vain, jos taululla ei ole yhtä suuria lukuja. Tämä ei ollut tappava virhe, mutta tämä johti ratkaisun lopussa nähtyyn pieneen sääntöjen muokkaukseen liittyvään teknisyyteen.

”Todistettuani”, että tehtävänannon mukainen prosessi on olemassa, oli luontevaa tutkia, miten kaukana tämä oli koko väitteen todistuksesta, eli kuinka paljon järjestyksen muuttaminen voi vaikuttaa lopputulokseen. Tätä kautta tein kriittisen huomion ratkaisussa esitetyllä tavalla erikoistapauksen  $a = 1, b = 3$  kautta. Kun

<sup>108</sup>Muut kirjan lyhytlistoilta otetut tehtävät ovat olleet useimmiten alkupään tehtäviä: ne ovat enimmäkseen paikoilta 1 ja 2, osa on kohdasta 3 ja myös pari neloskohdan tehtävää löytyy. Nämä vastaavat IMO:n kilpailupäivän ensimmäistä tai toista tehtävää. Tämä tehtävä on (sekä lyhytlistasijoituksen että minun mielipiteeni mukaan) hieman liian vaikea ollakseen IMO-päivän toinen tehtävä. (Jotkin kirjan tehtävät on valittu muualta kuin IMO-lyhytlistoilta, ja niiden vaikeustaso on vaikea asettaa lyhytlista-asteikolle.)

<sup>109</sup>Painotan vielä tämän kohdan tärkeyttä, koska tämä on hyvä, konkreettinen esimerkki intuitiosta. Tässä kohtaa ratkaisuprosessia minulla ei ollut paljoakaan käsitystä siitä, mitä ongelmassa tapahtuu. Tiesin, ettei tämän väliongelman ratkaisu riittäisi koko ongelman ratkaisemiseksi. Olin silti hyvin vakuuttunut siitä, että tämä lähestymistapa on hyödyllinen.

<sup>110</sup>Ajattelen hyvin suurpiirteisesti, ja se sopii minulle hyvin. Tämän haittana on kuitenkin se, että välillä tulee tehtyä virheitä, jotka huomaa vasta ratkaisua kirjoittaessa.

huomasin, miksi tapauksessa  $a = 1, b = 3$  operaatioiden järjestyksellä ei ole väliä, aloin todella luottamaan<sup>111</sup> siihen, että myös yleisessä tapauksessa järjestyksellä ei ole väliä. Minulla oli usko siihen, että tutkin ongelmaa oikealla tavalla ja että minulla käytännössä oli yleisen tapauksen todistus yksityiskohtia vaille. Todistus syntyikin nopeasti.

Tässä kohtaa ajattelin olevani valmis. Vasta ratkaisua kirjoittaessani huomasin, että stabiileja rakenteita ei voidakaan saavuttaa. En säikähtänyt tätä kovin paljoa: ajattelin (tiesin?), että ratkaisussa on oikeat elementit ja että jossain kohdassa tulisi vain vähän muokata yksityiskohtia ("ei tämä nyt oikeasti mikään iso ongelma ole"). Ratkaisun korjaaminen ei ollutkaan erityisen vaikeaa.

Yksi tärkeä ongelmanratkaisun aspekti on ajattelun selkeys. Ratkaisussa esitettiin lukuisia kysymyksiä, joihin lähdettiin etsimään vastausta. Näitä kysymyksiä olivat esimerkiksi "Päteekö tehtävän väite joillain valinnoilla?" ja "Miten siirtojärjestys vaikuttaa lopputulokseen?" Edistystä saadessa mietittiin, mitä oikeastaan ollaan todistettu ja mikä on vielä epäselvää. Kun on selkeä ajatus siitä, mitä osaa tehtävästä yritetään ratkoa, on myös sivuteille ajautumisen ja yksityiskohtiin juuttumisen riski pienempi.

Ajattelun selkeyden lisäksi ratkaisussa korostuu kyky keksiä monia ideoita sekä luottamus siihen, että siinä, mitä tekee, on järkeä. Näitä aiheita on käsitelty lisää Kevyempää luettavaa -luvusta löytyvästä tekstistä Mistä kehittyminen koostuu?

---

<sup>111</sup>Jälleen konkreettinen esimerkki intuitiosta.

## 23 Esitietoja

Tässä liitteessä esitetään joitain tietoja, jotka lukijan olisi hyvä tietää varsinaista tekstiä lukiessa. Luku on jaettu karkeasti yläkoulu- ja lukiotietoihin, joiden lisäksi mainitaan joitain sekalaisia asioita. Materiaalissa ei tietenkään ole mahdollista käydä oppimäärien sisältöjä kokonaan läpi, ja asioita ei pystytä esittämään kovin syvällisesti. Tämän vuoksi lukijan suositellaan etsivän netistä lisätietoja epäselvistä asioista. Esimerkiksi Avoin oppikirja on koonnut kattavasti yläkoulutietoja netissä saatavilla oleviin oppikirjoihin: <https://avoinoppikirja.fi/mat-ylakoulu>.

Nuorempien lukijoiden suositellaan myös tutustuvan valmennuksen sivuilta löytyviin nuoremmille suunnattuihin materiaaleihin: <https://matematiikkakilpailut.fi/aiheet/>.

### 23.1 Yläkoulutietoja

Tämän osion sisältö on seuraava:

- Muuttujan käsite
- Polynomit
- Yhtälönratkaisu
- Geometria
- Epäyhtälöt
- Funktiot

Aiheet on järjestetty suunnilleen tärkeysjärjestykseen varsinaisen tekstin kannalta.

#### **Muuttujat ja potenssiinkorotus**

Muuttuja tarkoittaa karkeasti symbolia, jolle voi antaa eri arvoja. Esimerkiksi muuttujan  $x$  arvon voidaan sanoa olevan 4, eli  $x = 4$ .

Muuttujia voidaan kertoa luvuilla ja saada lausekkeita. Esimerkiksi  $2 \cdot x + 3$  on lauseke, joka saadaan kertomalla tuntematon luku  $x$  luvulla 2 ja lisäämällä 3. Jos muuttujan  $x$  arvo on 4, niin lausekkeen arvo on  $2 \cdot 4 + 3 = 11$ .

On muutama yleisesti käytössä oleva lyhennysmerkintä. Esimerkiksi tuloa  $123 \cdot x$  merkitään vain lyhyesti  $123x$ . Tätä lyhennysmerkintää ei tietenkään käytetä luvuille, koska muuten 12 voisi tarkoittaa lukua kaksitoista tai lukua  $1 \cdot 2 = 2$ .

Tuloa  $x \cdot x$  merkitään  $x^2$ , tuloa  $x \cdot x \cdot x$  merkitään  $x^3$  ja yleisesti tuloa, jossa on  $n$  kappaletta muuttujaa  $x$ , merkitään  $x^n$ . Tätä voidaan käyttää myös luvuille: esimerkiksi  $3^4 = 3 \cdot 3 \cdot 3 \cdot 3 = 81$ . Tätä operaatiota kutsutaan potenssiinkorotukseksi:  $3^4$  luetaan ”kolme potenssiin neljä”.

Potensseilla on pari hyödyllistä laskusääntöä. Yksi on sääntö  $x^{m+n} = x^m \cdot x^n$ , missä  $m$  ja  $n$  ovat positiivisia kokonaislukuja.<sup>112</sup> Esimerkiksi jos  $m = 3$  ja  $n = 2$ , niin väite sanoo, että  $x^5 = x^3 \cdot x^2$ . Tämän yhtälön pätevyys seuraa potenssin määritelmästä: vasemmalla puolella on  $x \cdot x \cdot x \cdot x \cdot x$ , eli muuttujaa  $x$  on viisi kappaletta, ja oikean puolen tulo on  $(x \cdot x \cdot x) \cdot (x \cdot x)$ , eli myös oikealla puolella  $x$  esiintyy tulossa viisi kertaa. Vastaavasti huomataan, että pätee myös  $(x^m)^n = x^{m \cdot n}$ , eli esimerkiksi  $(x^3)^2 = x^6$ .

Lauseke  $x^0$  määritellään olemaan 1: ikään kuin kerromme nolla kappaletta termejä keskenään. Jos miettii tilannetta ”summaan  $1 + 2 + 3$  summataan lisäksi vielä nolla termiä”, niin lopputuloksena tulee vain  $1 + 2 + 3$ , koska nollan kappaleen summaaminen ei tee mitään. Siis nollan termin summa on 0. Vastaavasti tilanteessa ”tulo  $1 \cdot 2 \cdot 3$  kerrotaan vielä nollalla kappaleella termejä” vastaus on vain  $1 \cdot 2 \cdot 3$ , joten nollan kappaleen termejä tulo on 1. Tämän vuoksi  $x^0$  on luontevaa määritellä olemaan 1.

Lisäksi määritellään  $x^{-n} = \frac{1}{x^n}$ , eli esimerkiksi  $x^{-2} = \frac{1}{x^2}$ . Tämä on luontevaa, koska kehiteltyjen laskusääntöjen nojalla  $x^n \cdot x^{-n} = x^{n+(-n)} = x^{n-n} = x^0 = 1$ . Luvun  $x^{-n}$  tulee siis olla sellainen luku, jonka kertominen luvulla  $x^n$  antaa lopputulokseksi ykkösen. Tämä luku on tietysti  $\frac{1}{x^n}$ .

## Polynomit

Termi ”polynomi” on yhteisnimitys kaikille tietäntyyppisille lausekkeille. Polynomeja ovat esimerkiksi lausekkeet  $123x^3 - 456x^2 + 3$  ja 1, mutta  $\frac{1}{x}$  ei ole polynomi. Tarkka määritelmä on seuraava:

### Määritelmä

Polynomit (muuttujan  $x$  suhteen) ovat kaikki lausekkeet muotoa  $a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ , missä  $n \geq 0$  on kokonaisluku ja  $a_0, a_1, a_2, \dots, a_n$  ovat lukuja.

Polynomit saadaan siis kertomalla muuttujan  $x$  potensseja  $x^k$  joillain luvuilla ja summaamalla näitä termejä yhteen. Polynomin asteeksi kutsutaan lauseen mukaista lukua  $n$ , eli se on siis isoin eksponentti, mitä polynomissa esiintyy. Astetta merkitään kaavoissa termillä  $\deg$ .

Huomaa, että määritelmässä esiintyvä symboli  $a_0$  merkitsee vain jotain lukua, ja notaatiolla ei ole mitään tekemistä potenssiin korottamisen  $a^0$  kanssa. Jos haluaa merkitä vaikkapa tuhatta eri muuttujaa, on tällainen notaatio paljon kätevämpi kuin jokaisen muuttujan merkitseminen eri kirjaimella (tai kirjainyhdistelmällä).

Niin kuin luvuilla myös polynomeilla on omat laskutoimituksensa. Seuraava esimerkki näyttää, miten lasketaan yhteen kaksi polynomia.

<sup>112</sup>Väitteet pätevät oikeastaan millä tahansa reaalityyppisillä  $m$  ja  $n$  (reaalilukuja käsitellään myöhemmin). Tällöin pitää ajatella, että esimerkiksi  $x^{1/2}$  on luvun  $x$  neliöjuuri  $\sqrt{x}$ , koska laskusäännöillä  $(x^{1/2})^2 = x^{(1/2) \cdot 2} = x$ . (Luvun  $x$  neliöjuuri  $\sqrt{x}$  on se luku, jonka toinen potenssi eli neliö on  $x$ . Esim.  $\sqrt{25} = 5$ .) Vastaavasti voi määritellä, mitä on vaikkapa  $x^{\frac{2}{3}}$ : se on se luku, jonka kolmas potenssi eli kuutio on  $x^2$ . Ei ole kuitenkaan selvää, miten kuuluisi määritellä  $x^y$ , kun  $y$  ei ole rationaalinen. Lukijan ei tarvitse välittää tästä.



**Esimerkki**

Lasketaan yhteen polynomit  $100x^3 + 15x^2 - 3x + 7$  ja  $-2x^3 + 4x^2 - 7$ .

Tehdään tämä tutkimalla jokaisen muuttujan  $x$  potenssin  $x^k$  kertoimia yksitellen:

- Termin  $x^3$  kerroin on ensimmäisessä polynomissa 100 ja toisessa  $-2$ . Siispä lopputuloksessa se on  $100 + (-2) = 98$ .
- Termin  $x^2$  kerroin on ensimmäisessä polynomissa 15 ja toisessa 4. Siispä lopputuloksessa se on  $15 + 4 = 19$ .
- Termin  $x$  kerroin ensimmäisessä polynomissa on  $-3$ . Toisessa polynomissa kerrointa ei ole merkitty, mikä tarkoittaa kerrointa 0 (olisi turhaa työtä kirjoittaa termi  $0x$ ). Siispä lopputuloksessa kerroin on  $-3 + 0 = -3$ .
- Vakiotermi on ensimmäisessä polynomissa 7 ja toisessa  $-7$ . Siispä lopputuloksessa se on 0.

Täten summa on  $98x^3 + 19x^2 - 3x$ . Huomaa, että esimerkiksi termejä  $98x^3$  ja  $19x^2$  ei voi yhdistää mitenkään, joten vastausta ei voi enää sieventää.

Kahden polynomien kertominen keskenään ei ole aivan näin suoraviivaista. Ennen kuin edetään tähän, tutkitaan hetki allekkain kertolaskua. Kerrotaan allekkain luvut 123 ja 45.

$$\begin{array}{r} \times \quad 1 \ 2 \ 3 \\ \quad 4 \ 5 \\ \hline \quad 6 \ 1 \ 5 \\ 4 \ 9 \ 2 \\ \hline 5 \ 5 \ 3 \ 5 \end{array}$$

Miten kertolasku tarkalleen ottaen toimii? Allekkain kertolaskussa valitaan aina numeropareja: ensiksi 3 ja 5, sitten 2 ja 5, sitten 1 ja 5, minkä jälkeen toistetaan sama numeron 5 sijaan numerolla 4. Kun kerrotaan vaikkapa numerot 3 ja 4 keskenään, jätetään kertolaskuun yksi tyhjä ruutu (rivillä, jossa on 492): tämä johtuu siitä, että todellisuudessa numero 4 vastaa lukua 40.

Allekkain kertolaskussa siis kerrotaan luvut  $123 \cdot 45$  kirjoittamalla kertolasku muodossa  $(1 \cdot 100 + 2 \cdot 10 + 3 \cdot 1) \times (4 \cdot 10 + 5 \cdot 1)$ . Tämän jälkeen valitaan ensimmäisestä sulkulausekkeesta yksi yhteenlaskun termi ja toisesta toinen ja kerrotaan ne yhteen. Käymällä kaikki yhdistelmät läpi (kuusi kappaletta) ja laskemalla yhteen tulokset saadaan vastaus.

Polynomien kertolasku toimii samalla tavalla, ja allekkain kertolasku oikeastaan vastaa polynomien kertolaskua arvolla  $x = 10$ .

**Esimerkki**

Kerrotaan polynomit  $x^2 + 2x + 3$  ja  $4x + 5$  keskenään.

Haluamme siis laskea tulon

$$(x^2 + 2x + 3) \times (4x + 5).$$

Käydään läpi kaikki tavat valita ensimmäisestä sulkulausekkeesta yksi termi ja toisesta sulkulausekkeesta toinen termi. Tehdään tämä samassa järjestyksessä kuin allekkain kertolaskussa.

- Valitaan polynomista  $x^2 + 2x + 3$  termi 3 ja polynomista  $4x + 5$  termi 5. Saadaan  $3 \cdot 5 = 15$ .
- Valitaan polynomista  $x^2 + 2x + 3$  termi  $2x$  ja polynomista  $4x + 5$  termi 5. Saadaan  $2x \cdot 5 = 10x$ .
- Valitaan polynomista  $x^2 + 2x + 3$  termi  $x^2$  ja polynomista  $4x + 5$  termi 5. Saadaan  $x^2 \cdot 5 = 5x^2$ .
- Valitaan polynomista  $x^2 + 2x + 3$  termi 3 ja polynomista  $4x + 5$  termi  $4x$ . Saadaan  $3 \cdot 4x = 12x$ .
- Valitaan polynomista  $x^2 + 2x + 3$  termi  $2x$  ja polynomista  $4x + 5$  termi  $4x$ . Saadaan  $2x \cdot 4x = 8x^2$ . Huomaa, että lopputuloksessa kuuluu olla termi  $x^2$ , koska tulon  $2x \cdot 4x$  molemmissa termeissä on yksi kappale muuttujaa  $x$ , joten lopputulokseen tulee  $x \cdot x = x^2$ .
- Valitaan polynomista  $x^2 + 2x + 3$  termi  $x^2$  ja polynomista  $4x + 5$  termi  $4x$ . Saadaan  $x^2 \cdot 4x = 4x^3$ .

Summataan vastaukset yhteen polynomien yhteenlaskulla:

$$15 + 10x + 5x^2 + 12x + 8x^2 + 4x^3 = 4x^3 + 13x^2 + 22x + 15.$$

Arvolla  $x = 10$  tämä antaa

$$4 \cdot 10^3 + 13 \cdot 10^2 + 22 \cdot 10 + 15 = 4000 + 1300 + 220 + 15,$$

ja tämä on 5535, joka on sama tulos kuin allekkain kertolaskussa.

Polynomien kertolasku toimii muillakin polynomeilla vastaavalla tavalla. Laskeminen on melko työlästä, mutta rutiini tuo nopeutta laskuihin.

Käsitellyissä polynomeissa oli vain yhtä muuttujaa  $x$ . Vastaavasti voidaan kuitenkin käsitellä vaikkapa kahden muuttujan polynomeja (esimerkiksi  $x + 4y$  ja  $2xy + 3$  ovat kahden muuttujan polynomeja).

### Yhtälönratkaisu

Yhtälössä on annettuna jokin yhtäsuuruus, joka muuttujan tulisi toteuttaa. Esimerkiksi  $3x - 6 = 0$  on yhtälö. Yhtälöistä halutaan usein määrittää ratkaisut. Selvästikin jos  $3x - 6 = 0$ , niin tulee olla  $3x = 6$ . Tästä nähdään, että  $x = 2$ .

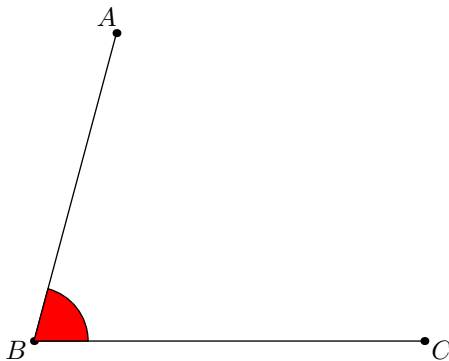
Yleisesti yhtälöiden molemmille puolille saa lisätä jonkin luvun ja molemmilta puolilta voi vähentää jonkin luvun. Molemmat puolet saa kertoa jollakin luvulla, ja molemmat puolet saa jakaa luvulla, joka ei ole nolla. Edellä yhtälöön lisättiin 6 molemmille puolille, ja sen jälkeen jaettiin puolittain kolmella.

Tutkitaan yhtälöä  $3x + 5 = -x - 7$ . Lisätään puolittain 7, jolloin saadaan yhtälö  $3x + 12 = -x$ . Lisätään puolittain vielä  $x$ , jolloin saadaan  $4x + 12 = 0$ . Tämä yhtälö on samankaltainen kuin aiemmin esitetty yhtälö  $3x - 6 = 0$ , ja se ratkeaa samalla tavalla. Saadaan  $x = -3$ . Yleisesti yhtälö kannattaa ensin sieventää muotoon ”jotain = 0”, koska yhtälön käsitteleminen on tällöin helpompaa.

Tässä on vielä toinen esimerkki. ”Kaupassa leivän hinta on 2 euroa. Hinta koostuu verottomasta hinnasta ja arvonlisäverosta, jonka suuruus on 24 prosenttia verottomasta hinnasta. Laske leivän veroton hinta.” Ratkaisua varten merkitään leivän verotonta hintaa muuttujalla  $x$ . Tiedämme, että kahden euron hinta koostuu verottomasta hinnasta  $x$  ja arvonlisäverosta, jonka suuruus on  $24\% \cdot x$  eli  $0.24x$ . Siis  $x + 0.24x = 2$ , eli  $1.24x = 2$ . Täten  $x = \frac{2}{1.24}$  (jolle voi vielä halutessaan laskea likiarvon laskimella).

## Geometria

Kuvissa esiintyviä kulmia merkitään muodossa  $\angle ABC$ . Alla olevassa kuvassa on merkitty punaisella kulma  $\angle ABC$ . Kulmassa kerrotaan siis ensiksi yhden sivun päätepiste  $A$ , sitten itse kulman kärjen piste  $B$  ja lopuksi toisen sivun päätepiste  $C$ . Ei ole väliä, kumman sivun päätepisteistä kirjoittaa ensimmäisenä, eli  $\angle ABC$  ja  $\angle CBA$  tarkoittavat samaa asiaa.<sup>113</sup>

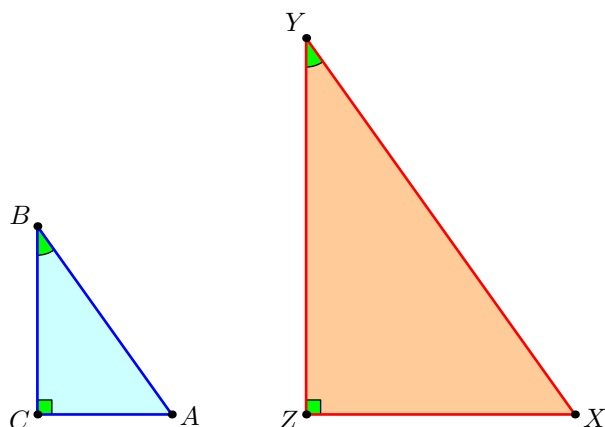


Yläkoulun geometriassa käsitellään paljolti suorakulmaisia kolmioita. Näihin liittyen esitetään trigonometriaa sekä Pythagoraan lause. Käydään ensiksi läpi trigonometriaa.

Ideana on, että suorakulmaisen kolmion muodon päättää yksi kulma (suoran kulman lisäksi). Jos siis tiedämme, että kolmiossa  $ABC$  kulma  $\angle ACB$  on 90 astetta ja kulma  $\angle ABC$  on vaikkapa 30 astetta, niin kolmion  $ABC$  muoto on selvillä. Kolmion

<sup>113</sup>Joskus käytetään myös ns. suunnattuja kulmia, jolloin  $\angle ABC$  ja  $\angle CBA$  eivät olekaan aivan sama asia, vaan  $\angle ABC$  saadaan kiertämällä vastapäivään pisteestä  $A$  pistettä  $C$  kohti, ja vastaavasti  $\angle CBA$  saadaan kiertämällä vastapäivään pisteestä  $C$  pistettä  $A$  kohti. Kuvassa olisi siis tällä määritelmällä merkittynä kulma  $\angle CBA$  eikä  $\angle ABC$ . Tässä kirjassa ei kuitenkaan käytetä suunnattuja kulmia.

koosta ei kuitenkaan ole tietoa: olisi mahdollista, että kolmio  $XYZ$  olisi samanmuotoinen kuin kolmio  $ABC$ , mutta jokainen kolmion  $XYZ$  sivu olisi kaksinkertainen kolmion  $ABC$  sivuihin verrattuna:



Mutta koska kolmioiden muodot ovat samat, niin sivujen suhteet<sup>114</sup>

$$\frac{AB}{BC} \text{ ja } \frac{XY}{YZ}$$

ovat samat. Voisimme siis periaatteessa selvittää, mikä tämä suhde on, käyttämällä tietoa  $\angle ABC = 30^\circ$ , koska suhdehan määräytyy yksikäsitteisesti, kun tiedetään kulma.

Asiasta puhumisen helpottamiseksi määritellään sini, kosini ja tangentti.

### Määritelmä

Olkoon  $ABC$  suorakulmainen kolmio, jossa kulma  $\angle ACB$  on 90 astetta ja jossa kulman  $\angle ABC$  koko on  $\alpha$ . Määritellään sini suhteena

$$\sin(\alpha) = \frac{AC}{AB},$$

kosini suhteena

$$\cos(\alpha) = \frac{BC}{AB}$$

ja tangentti suhteena

$$\tan(\alpha) = \frac{AC}{BC}.$$

Siniin, kosiniin ja tangenttiin viitataan yhteisnimityksellä trigonometrinen funktio.

Sini on siis vastakkaisen sivun ja hypotenuusan, eli suoraa kulmaa vastapäätä sijaitsevan sivun, suhde. Suoran kulman viereisiä sivuja kutsutaan kateeteiksi. Vastaavasti kosini on vierekkäisen kateetin suhde hypotenuusaan, ja tangentti on vastakkaisen kateetin suhde vierekkäiseen kateettiin.

<sup>114</sup>Tässä (ja muuallakin kirjassa) merkitsemme pisteiden  $A$  ja  $B$  välisen janan pituutta merkinnällä  $AB$ .

Trigonometrinen funktioiden arvojen laskeminen ei ole kovin helppoa (käsin), eikä siihen ole tarvettakaan. Käytännössä käytetään laskinta tai tietokonetta apuna. Kilpailuissa ei kuitenkaan useimmiten sallita laskimia, mutta kilpailutilanteessa ei usein myöskään tarvitse laskea konkreettisilla luvuilla mitään.

Viimeisenä esitetään Pythagoraan lause.

### Lause (Pythagoraan lause)

Olkoon  $ABC$  suorakulmainen kolmio, jonka kateettien pituudet ovat  $a$  ja  $b$  ja jonka hypotenuusan pituus on  $c$ . Tällöin  $a^2 + b^2 = c^2$ .

Lause käytännössä antaa tavan laskea suorakulmaisen kolmion kolmannen sivun pituuden, kun kahden sivun pituudet tunnetaan. Esimerkiksi jos kateettien  $a$  ja  $b$  pituudet ovat 3 ja 4, niin pätee  $c^2 = a^2 + b^2 = 9 + 16 = 25$ , eli  $c = 5$ .

Lausetta ei todisteta tässä, vaan sen todistus esitetään varsinaisessa geometriaosiossa.

### Epäyhtälöt

Epäyhtälöiden avulla puhutaan siitä, kumpi joistakin luvuista on suurempi. Esimerkiksi  $1 < 2$  tarkoittaa sitä, että 1 on pienempi kuin 2. Vastaavasti merkitään  $2 > 1$ . Epäyhtälöitä voi tietysti käyttää myös muuttujille, eli  $x < y$  tarkoittaa, että muuttujan  $x$  arvo on pienempi kuin muuttujan  $y$  arvo. Esimerkiksi väite  $x + 1 > x$  tarkoittaa sitä, että  $x + 1$  on suurempi kuin  $x$  (mikä tietysti pitää paikkaansa). Lisäksi epäyhtälöissä voidaan sallia yhtäsuuruus: merkintä  $x \leq y$  tarkoittaa, että  $y$  on joko suurempi kuin  $x$  tai yhtä suuri kuin  $x$  (eli  $y$  on vähintään  $x$ ).

Epäyhtälöitä voi käsitellä melko samalla tavalla kuin yhtälöitäkin.<sup>115</sup> Esimerkki: ”Määritä kaikki luvut  $x$ , joilla  $x + 5 < 2x + 2$ .” Tässä voidaan ensiksi vähentää puolittain 2, jolloin epäyhtälö muuttuu muotoon  $x + 3 < 2x$ . (Siis: väite  $x + 3 < 2x$  pätee täsmälleen silloin, kun  $x + 5 < 2x + 2$ .) Tästä voidaan vähentää puolittain  $x$ , jolloin jäljelle jää  $3 < x$ . Alkuperäinen epäyhtälö pätee siis täsmälleen silloin, kun  $x$  on suurempi kuin 3.

### Funktiot

Funktiot (merkitään usein kirjaimilla  $f, g$  ja  $h$ ) voidaan ajatella koneina, jotka ottavat sisään luvun ja jotka palauttavat jonkin luvun.<sup>116</sup> Esimerkki funktiosta: funktio  $f$  ottaa sisään luvun  $x$  ja palauttaa luvun  $x + 1$ . Toisin sanoen  $f$  aina kasvattaa annettua lukua yhdellä. Tätä merkitään kirjoittamalla  $f(x) = x + 1$ .

Funktioiden ei kuitenkaan tarvitse olla missään mielessä yksinkertaisia laskusääntöjä. Esimerkiksi aiemmin määritelty sinifunktio  $\sin(\alpha)$  ottaa sisään kulman  $\alpha$ , jonka

<sup>115</sup>Välillä tulee kuitenkin olla tarkkana. Jos epäyhtälön kertoo puolittain negatiivisella luvulla, niin epäyhtälön suunta muuttuu (jos  $1 < 2$ , niin  $1 \cdot (-3) > 2 \cdot (-3)$ ). Kahden samansuuntaisen epäyhtälön yhteenlasku toimii, eli jos  $a < b$  ja  $c < d$ , niin  $a + c < b + d$ . Näitä ei kuitenkaan saa vähentää toisistaan: pätee  $0 < 1$  ja  $2 < 100$ , mutta  $0 - 2 > 1 - 100$ . Eri suuntaan osoittavia epäyhtälöitä ei myöskään saa laskea yhteen.

<sup>116</sup>Yleisesti funktiot voivat ottaa sisään tai palauttaa mitä tahansa objekteja, vaikkapa kulmien suuruuksia tai lukupareja.

suuruus on nollan ja 90 asteen väliltä, ja palauttaa sopivan sivujen pituuksien suhteen. Sinifunktion toiminta ei ole yksinkertainen, mutta kuten jo aiemmin todettiin, se kuitenkin noudattaa selvää logiikkaa.

Tässä on funktiolle vielä hieman tarkempi ja formaalimpi määritelmä, johon voi tarvittaessa palata myöhemmin. Jos  $A$  ja  $B$  ovat mitä tahansa joukkoja,<sup>117</sup> niin funktio  $f$  joukolta  $A$  joukolle  $B$  (merkitään  $f : A \rightarrow B$ ) on sellainen objekti, joka ottaa syötteenä jonkin joukon  $A$  elementin ja palauttaa jonkin joukon  $B$  elementin. Ainoat rajoitukset ovat, että tämän funktion tulee ”toimia” kaikilla joukon  $A$  elementeillä, eli jokaista joukon  $A$  elementtiä  $a$  tulee vastata jokin joukon  $B$  alkio  $b$ , ja lisäksi tämän alkion tulee olla yksikäsitteinen. Esimerkiksi sinifunktio on funktio joukolta ”kulmat, joiden suuruus on nollan ja 90 asteen väliltä” joukolle ”positiiviset luvut”. Jokaista kulmaa vastaa yksikäsitteinen sinifunktion arvo.

Funktioihin liittyen mainitaan vielä nollakohdat. Tutkitaan yksinkertaisuuden vuoksi funktiota  $f$ , joka ottaa sisään kokonaisluvun ja palauttaa kokonaisluvun. Sanotaan, että kokonaisluku  $x$  on funktion  $f$  nollakohta, jos  $f(x) = 0$ . Funktion nollakohdat liittyvät siis vahvasti yhtälönratkaisuun. Esimerkiksi jos funktio  $f$  on määritelty kaavalla  $f(x) = 3x - 6$ , luku  $x$  on nollakohta jos  $3x - 6 = 0$ . Tällä yhtälöllä on yksi ratkaisu  $x = 2$ .

---

<sup>117</sup>Joukot käydään yksityiskohtaisemmin läpi myöhemmin.

## 23.2 Lukiotietoja

Kaikkea lukion oppimäärästä ei yritetä käsitellä tässä.<sup>118</sup> Tämän osion sisältö on seuraava:

- Induktio
- Lukujoukot ja joukot
- Binomikertoimet ja binomilause
- Lukujonot
- Trigonometria yksikköympyrässä
- Toisen asteen yhtälö
- Logaritmi

Aiheet on jälleen järjestetty suunnilleen tärkeysjärjestykseen.

### Induktio

Induktio esitetään ensimmäisenä, koska se on yksi yleisimmistä ja tärkeimmistä todistustekniikoista. Tämän luvun ulkopuolella induktiotodistuksia ei usein edes kirjoiteta näkyviin, vaan lukijan oletetaan osaavan täydentää yksityiskohdat itse. Kannattaa siis pyrkiä sisäistämään induktion idea.

Esitetään induktion periaate konkreettisella tilanteella.

Jaakko kiipeää äärettömän pitkiä tikapuita ylöspäin. Tiedämme seuraavat asiat Jaakosta:

1. Jaakko pääsee tikapuiden ensimmäiselle askelmalle.
2. Jaakko voi aina nousta vielä yhden askelman ylöspäin.

Tällöin tiedämme, että Jaakko pääsee mille tahansa tikapuiden askelmista.

Tutkitaan induktiota esimerkkitehtävän kautta.

#### Tehtävä

Todista, että luku  $n(n + 1)$  on parillinen kaikilla positiivisilla kokonaisluvuilla  $n$ .

Edetään kuten tikapuesimerkissä. Jokainen positiivinen kokonaisluku  $n$  vastaa tikapuiden askelmaa. Tulee varmistaa kaksi asiaa:

1. Pääsemme ensimmäiselle askelmalle, eli väite pätee arvolla  $n = 1$ .

<sup>118</sup>Esimerkiksi analyysiin ei kosketa tässä kappaleessa ollenkaan, vaikka algebran osioissa välillä käytetäänkin derivaattoja ja integraaleja.

2. Pääsemme aina vielä yhden askelman ylöspäin, eli jos väite pätee arvolla  $n = k$ , niin se pätee myös arvolla  $n = k + 1$ .

Ensimmäinen ehto on selvä: kun  $n = 1$ , niin  $n(n + 1) = 1 \cdot (1 + 1) = 2$ , joka on parillinen.

Toinen ehto on hieman vaikeampi. Oletamme siis, että  $k(k + 1)$  on parillinen. Haluamme todistaa, että  $(k + 1)(k + 2)$  on parillinen. Kertomalla auki saadaan  $(k + 1)(k + 2) = k^2 + 3k + 2 = k(k + 1) + 2k + 2$ . Summan ensimmäinen termi  $k(k + 1)$  on oletuksen nojalla parillinen, ja termit  $2k$  ja  $2$  ovat selvästi parillisia. Siis myös summa on parillinen, ja toinen ehto on todistettu.

Ensimmäinen ehto osoittaa, että väite pätee arvolla  $n = 1$ . Koska väite pätee arvolla  $n = 1$ , niin toisen ehdon nojalla väite pätee arvolla  $n = 2$ . Koska väite pätee arvolla  $n = 2$ , niin toisen ehdon nojalla väite pätee arvolla  $n = 3$ . Koska väite pätee arvolla  $n = 3$ , niin... Väite siis pätee kaikilla  $n$ .

Esitetty tehtävä on tietysti helppo ilman induktiotodistustakin,<sup>119</sup> mutta induktiota voidaan hyödyntää myös lukuisissa muissa tehtävissä. Tässä on esimerkkitehtävä, joka suositellaan todistettavaksi induktiolla. Tehtävä on klassinen esimerkki induktiosta ja esimerkiksi Wikipediasta löytää väitteelle todistuksen induktiotodistusta käsittelevältä sivulta.

### Tehtävä

Olkoon  $n$  positiivinen kokonaisluku. Todista, että

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

### Lukujoukot ja joukot

Kokonaisluvut ovat tietysti luvut  $0, 1, 2, 3, \dots$  ja  $-1, -2, -3, \dots$ , ja niiden joukkoa merkitään symbolilla  $\mathbb{Z}$ .<sup>120</sup> Positiivisia kokonaislukuja merkitään usein symbolilla  $\mathbb{Z}_+$ . Myös termiä ”luonnollinen luku” käytetään viittaamaan positiivisiin kokonaislukuihin, mutta ei ole vakiintunutta käytäntöä siitä, onko  $0$  luonnollinen luku.

Rationaaliluvut ovat muotoa  $\frac{m}{n}$  olevat luvut, missä  $m$  ja  $n$  ovat kokonaislukuja (voidaan merkitä  $m \in \mathbb{Z}$  ja  $n \in \mathbb{Z}$ , missä  $m \in \mathbb{Z}$  tarkoittaa ” $m$  on joukon  $\mathbb{Z}$  alkio”). Näiden joukkoa merkitään symbolilla  $\mathbb{Q}$ .<sup>121</sup> Tämä joukko on siitä mukava, että tulokseksi saadaan aina rationaaliluku, kun kaksi rationaalilukua lasketaan yhteen, vähennetään toisistaan, kerrotaan keskenään tai jaetaan toisillaan (paitsi nollalla ei saa jakaa). Myös seuraavaksi esitettävillä reaali- ja kompleksiluvuilla on nämä ominaisuudet.

Rationaaliluvuissa on tiettyjä ”puutteita”: rationaaliluvuissa ei esimerkiksi ole sellaista lukua  $q$ , jolla  $q^2 = 2$ , eli toisin sanoen  $\sqrt{2}$  ei ole rationaalilukujen joukon

<sup>119</sup>Kahdesta peräkkäisestä kokonaisluvusta aina toinen on parillinen, ja parillinen kertaa mikä tahansa kokonaisluku on edelleen parillinen.

<sup>120</sup>Miksi juuri kirjain  $Z$ ? Saksan sana ”Zahl” tarkoittaa lukua. Saksassa on elänyt monia kuuluisia ja tuotteliaita matemaatikkoja, joten saksankielinen alkuperä on luonnollinen.

<sup>121</sup>Kirjain  $Q$  tulee englannin sanasta ”quotient”, joka tarkoittaa osamäärää.



alkio (jos et ole nähnyt todistusta tälle, kannattaa katsoa se netistä). Tätä ongelmaa paikkaamaan on luotu reaalityluvut  $\mathbb{R}$ . Reaalitylukujen tarkka määrittelyminen on hankalaa, mutta ne voi vain ajatella olemaan ”kaikki luvut”. Esimerkiksi  $\sqrt{2}$  on reaalityluku. Kaikki reaalityluvut voidaan esittää desimaaliesityksessä kirjoittamalla numeroita peräkkäin. (Tämä esitys voi olla äärettömän pitkä, kuten tapauksessa  $1/3 = 0.3333\dots$ )

Reaalityluvuissakin on vielä pieni puute: ei ole olemassa reaalitylukua  $x$ , jolla  $x^2 = -1$ . Tätä puutetta paikkaamaan on luotu vielä kompleksilukujen joukko  $\mathbb{C}$ , joka sisältää luvut muotoa  $a + bi$ , missä  $a, b \in \mathbb{R}$  ja  $i$  on sellainen kompleksiluku, jolla  $i^2 = -1$ .<sup>122</sup> Kompleksilukuja ei kovin usein tarvita kilpailumatematiikassa, mutta niistä on hyvä olla tietoinen.<sup>123</sup> Lisäksi algebrassa kompleksiluvuilla on tärkeä rooli polynomien nollakohtien kannalta: esimerkiksi polynomilla  $x^2 + 1$  ei ole nollakohtia reaalitylukujen joukossa, mutta kompleksilukujen joukossa sillä on kaksi nollakohtaa:  $i$  ja  $-i$ .

Yleisesti joukolla viitataan johonkin kokoelmaan jotakin asioita. Esimerkiksi joukkoa, joka sisältää luvut 1 ja 2, merkitään  $\{1, 2\}$ . Joukon sisältämiin asioihin viitataan sanalla alkio. Joukon alkio voi olla mitä vain: esimerkiksi  $\{\text{kissa}\}$  on joukko, joka sisältää alkion kissa. Joukot voivat sisältää myös lisää joukkoja:  $\{\{1, 2\}, \{2, 3\}\}$  on joukko, joka sisältää kaksi kahden kokoista joukkoa.

Sopimuksen mukaan joukoissa saa olla sama alkio vain kerran. Esimerkiksi  $\{1, 1\}$  ei kelpaa joukoksi. Huomaa, että esimerkki  $\{\{1, 2\}, \{2, 3\}\}$  on joukko: alkio  $\{1, 2\}$  ja  $\{2, 3\}$  eivät ole samat. Myöskään joukon alkioiden järjestyksellä ei ole väliä, eli  $\{1, 2\}$  ja  $\{2, 1\}$  ovat sama joukko.

Joukon  $S$  kokoa merkitään  $|S|$ . Jos esimerkiksi  $S = \{7, 9, 10\}$ , niin  $|S| = 3$ .

### Binomikertoimet

Aloitetaan seuraavalla tehtävällä.

#### Tehtävä

Rivissä on  $n$  kappaletta kolikoita, ja niistä tulee valita kaksi. Kaikki kolikot ovat erilaisia, ja kolikoiden valitsemisjärjestyksellä ei ole väliä. Kuinka monella eri tavalla valinnan voi tehdä?

Numeroidaan kolikot luvuin  $1, 2, \dots, n$ . Jos  $n = 3$ , on kolme erilaista valintavaihtoehtoa:  $\{1, 2\}$ ,  $\{2, 3\}$  ja  $\{1, 3\}$ .

Ensimmäiselle kolikolle on  $n$  eri vaihtoehtoa. Tämän jälkeen toinen kolikko tulee valita jäljellä olevista  $n - 1$  kolikosta. Siispä tapoja on  $n(n - 1)$ , paitsi että tämä tulee vielä jakaa kahdella, jottei esimerkiksi valintoja  $\{1, 2\}$  ja  $\{2, 1\}$  lasketa eri valinnoiksi. Siis vastaus on  $\frac{n(n-1)}{2}$ .

<sup>122</sup>Kompleksilukujen yhteen- ja vähennyslasku määritellään aivan kuten voisi luullakin. Esimerkki:  $(1 + 2i) + (3 + 4i) = (1 + 3) + (2 + 4)i = 4 + 6i$ . (Vertaa polynomien  $1 + 2x$  ja  $3 + 4x$  yhteenlaskuun). Tulo lasketaan seuraavasti:  $(1 + 2i)(3 + 4i) = 1 \cdot 3 + 1 \cdot 4i + 2i \cdot 3 + 2i \cdot 4i = 3 + 4i + 6i + 8i^2$ . Käytetään tietoa  $i^2 = -1$ , jolloin edellinen sievenee muotoon  $3 + 4i + 6i - 8 = -5 + 10i$ . (Vertaa polynomien kertolaskuun, johon on lisätty tieto  $x^2 = -1$ .)

<sup>123</sup>Mielestäni on ihan hyödyllistä tietää esimerkiksi kompleksiluvuista perusteet, vaikka niitä ei käytetäkään erityisen usein, koska tämä antaa lisää ymmärrystä tietyistä aiheista.

Entä jos kolikoita olisi pitänyt valita 3? Tällöin vastaus olisi samanlaisella logiikalla

$$\frac{n(n-1)(n-2)}{3 \cdot 2}.$$

Jakaja  $3 \cdot 2$  tulee siitä, että sama kolmikko tulee aluksi laskettua 6 kertaa.

Kuinka monta kertaa sama 100 kolikon joukko tulee lasketuksi? Tutkitaan siis, kuinka monella tavalla voidaan valita vaikkapa kolikot  $1, 2, \dots, 100$ . Vastaus on  $100 \cdot 99 \cdot 98 \cdot \dots \cdot 2 \cdot 1$ : ensimmäiseksi kolikoksi voidaan valita jokin näistä sadasta kolikosta, toiseksi kolikoksi jokin 99 jäljelle jääneestä kolikosta ja niin edelleen. Tätä lukua merkitään yksinkertaisuuden vuoksi merkinnällä  $100!$ , ja yleisesti merkitään  $k! = k \cdot (k-1) \cdot \dots \cdot 2 \cdot 1$ . Lisäksi määritellään  $0! = 1$ .<sup>124</sup> Sanotaan, että  $100!$  on luvun 100 kertoma.

Mikä on vastaus alkuperäiseen tehtävään, jos tuleekin valita 100 kolikkoa? Vastauksella logiikalla kuin aiemmin

$$\frac{n(n-1)(n-2) \cdots (n-99)}{100!}.$$

Tämä voidaan merkitä nätimmin muodossa

$$\frac{n!}{100!(n-100)!}.$$

Tämä on ns. binomikerroin, ja sitä merkitään

$$\binom{n}{100}.$$

Yleisesti

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

kertoo, kuinka monella tavalla  $n$  kolikosta voidaan valita  $k$  kolikkoa, kun järjestyksellä ei ole väliä. Tässä oletetaan, että  $0 \leq k \leq n$ . Kun  $k = n$ , niin määritelmä  $0! = 1$  on hyödyllinen: vastauksen tuleekin olla 1.

Binomikertoimista mainitaan tässä pari ominaisuutta. Ensinnäkin huomataan, että

$$\binom{n}{k} = \binom{n}{n-k},$$

mikä on selvää binomikertoimien kaavasta, mutta myös niiden merkityksestä. Se, että valitsee  $k$  kappaletta kolikoita, on sama kuin valitsisi, mitkä  $n-k$  kolikkoa eivät tule valituksi.

Seuraavaksi osoitetaan väite

$$\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}.$$

<sup>124</sup>Kuten määriteltessä  $x^0 = 1$  todettiin, nollan luvun kertolaskun tulos on hyvä määritellä ykköseksi.

Yhtälön paikkansapitävyyden voi tarkistaa suoralla laskulla käyttäen binomikertoimien esitystä kertomien avulla. Tässä esitetään toisenlainen ratkaisu. Kuvitellaan tapoja valita  $n + 1$  kolikosta  $k + 1$  kolikkoa. Näitä tapoja on määritelmän mukaan  $\binom{n+1}{k+1}$ . Tapojen määrän voi laskea myös toisella tavalla. Jokainen valinta kuuluu yhteen seuraavista tapauksista:

1. Kolikko 1 tulee valituksi.
2. Kolikko 1 ei tule valituksi.

Ensimmäisessä tapauksessa jäljelle jää  $n$  kolikkoa, joista tulee valita  $k$  kappaletta, joten tapoja on  $\binom{n}{k}$ . Toisessa tapauksessa jäljelle jää  $n$  kolikkoa, joista tulee valita  $k + 1$  kappaletta, joten tapoja on  $\binom{n}{k+1}$ . Yhteensä eri tapoja on siis  $\binom{n}{k} + \binom{n}{k+1}$ . Väite seuraa tästä.

Tässä toinen kiinnostava väite: pätee

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n} = 2^n.$$

Tämä yhtälö perustuu siihen, että molemmilla puolilla lasketaan joukon  $\{1, 2, \dots, n\}$  osajoukkojen määrä: toisaalta näitä on  $2^n$  kappaletta<sup>125</sup> mutta toisaalta määrä saadaan laskemalla ensiksi nollan kokoisten osajoukkojen määrä, lisäämällä tähän yhden kokoisten osajoukkojen määrä ja niin edelleen.

Lopuksi mainitaan yhteys binomilauseeseen. Binomilause kertoo, miltä  $(x + y)^n$  näyttää auki kerrottuna, kun  $n$  on positiivinen kokonaisluku.

#### Lause (Binomilause)

Olkkoon  $n$  positiivinen kokonaisluku. Tällöin

$$(x + y)^n = \binom{n}{0}x^n + \binom{n}{1}x^{n-1}y + \binom{n}{2}x^{n-2}y^2 + \cdots + \binom{n}{n}y^n.$$

Tässä on todistus. Tutkitaan termille  $x^k y^{n-k}$  tulevaa kerrointa, kun  $(x + y)^n$  kerrotaan auki. Miten termi  $x^k y^{n-k}$  saadaan muodostettua tulosta

$$(x + y)^n = (x + y)(x + y)(x + y) \cdots (x + y)?$$

Joistain  $k$  kappaleesta termejä tulee valita muuttuja  $x$ , ja lopuista  $n - k$  kappaleesta termejä tulee valita muuttuja  $y$ . Koska polynomien kertolasku perustuu kaikkien kombinaatioiden läpikäymiseen, saadaan tästä haluttu tulos: kerroin on  $\binom{n}{k}$ .

Lukijaa suositellaan etsimään netistä Pascalin kolmio ja miettimään yhteyttä binomikertoimien ja Pascalin kolmion välillä.

<sup>125</sup>Jokainen osajoukko voidaan luoda seuraavasti: päätetään, valitaanko 1 osajoukkoon vai ei (kaksi eri vaihtoehtoa), päätetään, valitaanko 2 osajoukkoon vai ei (kaksi eri vaihtoehtoa) ja niin edelleen. Yhteensä tehdään  $n$  valintaa, ja mahdollisia lopputuloksia on  $2^n$  kappaletta.

## Lukujonot

Lukujonot ovat nimensä mukaisesti jonoja lukuja. Lukujonot voivat olla joko äärellisen tai äärettömän pituisia. Tässä luvussa tutkitaan enimmäkseen äärellisiä lukujonoja.

Tärkeimpiä lukujonoja ovat aritmeettiset ja geometriset lukujonot. Keskitytään ensiksi aritmeettisiin lukujonoihin.

### Määritelmä

Sanotaan, että luvut  $a_1, a_2, \dots, a_n$  muodostavat aritmeettisen lukujonon, jos erotus  $a_{i+1} - a_i$  on sama kaikilla  $i = 1, 2, \dots, n - 1$ .

Olkoon tämä kahden peräkkäisen alkion erotus  $d$ . Nyt lukujonon alkioit ovat  $a_1, a_1 + d, a_1 + 2d, \dots, a_1 + (n - 1)d$ . Esimerkiksi lukujono  $1, 2, 3, \dots, n$  on aritmeettinen lukujono.

Induktion yhteydessä mainittiin tehtävä  $1 + 2 + \dots + n = \frac{n(n+1)}{2}$ . Vastaavasti voisi kysyä, onko mahdollista laskea yleisen aritmeettisen lukujonon lukujen summa. Seuraavaksi esitetään ratkaisu tälle ongelmalle.

Lasketaan siis summa  $a, a + d, a + 2d, \dots, a + (n - 1)d$ . Tässä lukujonossa on  $n$  jäsentä, ja keskimääräisen luvun koko on  $a + \frac{n-1}{2}d$ . Summa on keskiarvo kerrottuna lukujen määrällä eli

$$na + \frac{n(n-1)}{2}d.$$

Arvoilla  $a = 1$  ja  $d = 1$  saadaan summa  $1 + 2 + \dots + n$ .

Seuraavaksi esitetään geometrinen lukujono.

### Määritelmä

Sanotaan, että luvut  $a_1, a_2, \dots, a_n$  muodostavat geometrisen lukujonon, jos on olemassa sellainen luku  $q$ , että  $a_{i+1} = qa_i$  kaikilla  $i = 1, 2, \dots, n - 1$ .

Toisin sanoen: jos lukujonon kaikki jäsenet ovat nolasta eroavia, niin se on geometrinen, jos  $\frac{a_{i+1}}{a_i}$  on sama kaikilla  $i = 1, 2, \dots, n - 1$ . Jos tätä suhdetta merkitään kirjaimella  $q$ , niin lukujonon jäsenet ovat  $a_1, a_1q, a_1q^2, \dots, a_1q^{n-1}$ . Esimerkiksi kakosen potenssit  $1, 2, 4, 8, \dots, 2^{n-1}$  muodostavat geometrisen lukujonon.

Kuten aritmeettiselle lukujonolle myös geometriselle lukujonolle on summakaava. Olkoon  $S = a_1 + a_2 + \dots + a_n$  haluttu summa. Edellä todettiin, että lukujonon jäsenet ovat muotoa  $a_1q^k$ , missä  $k = 0, 1, \dots, n - 1$ . Siis

$$S = a_1 + a_1q + a_1q^2 + \dots + a_1q^{n-1}.$$

Ideana on vähentää luvusta  $S$  luku  $qS$ , jolloin melkein kaikki termit supistuvat. Koska

$$qS = a_1q + a_1q^2 + \dots + a_1q^{n-1} + a_1q^n,$$

niin vähentämällä tämä aiemmasta yhtälöstä saadaan

$$S - qS = a_1 - a_1q^n.$$

Jakamalla puolittain luvulla  $1 - q$  saadaan

$$S = a_1 \frac{1 - q^n}{1 - q} = a_1 \frac{q^n - 1}{q - 1}.$$

Huomaa, että menetelmä ei toimi, jos  $q = 1$ . Tällöin summa on kuitenkin helppo laskea, koska lukujono on vain  $a_1, a_1, a_1, \dots, a_1$ .

Arvoilla  $q = 2$  ja  $a_1 = 1$  saadaan

$$1 + 2 + 4 + \dots + 2^{n-1} = 2^n - 1.$$

Induktioharjoituksena voi tämän yhtälön yrittää todistaa induktiolla muuttujan  $n$  suhteen.<sup>126</sup>

Joskus on tarvetta laskea myös äärettömien geometrinen lukujonojen summia. Lukujonon  $1 + 2 + 4 + 8 + \dots$  summa ei ole luku (sanotaan, että summa ei suppene), ja tällöin kysymyksessä ei ole järkeä. Tilanne on kuitenkin eri, kun halutaan laskea vaikkapa summa

$$1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \dots$$

Tämän summan arvo on 2. Summan saa laskettua tutkimalla saatua kaavaa

$$S = a_1 \frac{q^n - 1}{q - 1}$$

ja ”asettamalla luvun  $n$  arvoksi äärettömän”.<sup>127</sup> Jos  $-1 < q < 1$ , niin termi ” $q^\infty$ ” on 0. Tällöin summa on

$$S = a_1 \frac{-1}{q - 1} = a_1 \frac{1}{1 - q}.$$

Esimerkki  $1 + \frac{1}{2} + \frac{1}{4} + \dots$  vastaa arvoja  $a_1 = 1$  ja  $q = \frac{1}{2}$ .

Jos  $q \geq 1$  tai  $q \leq -1$ , niin ääretöntä summaa ei voi laskea.

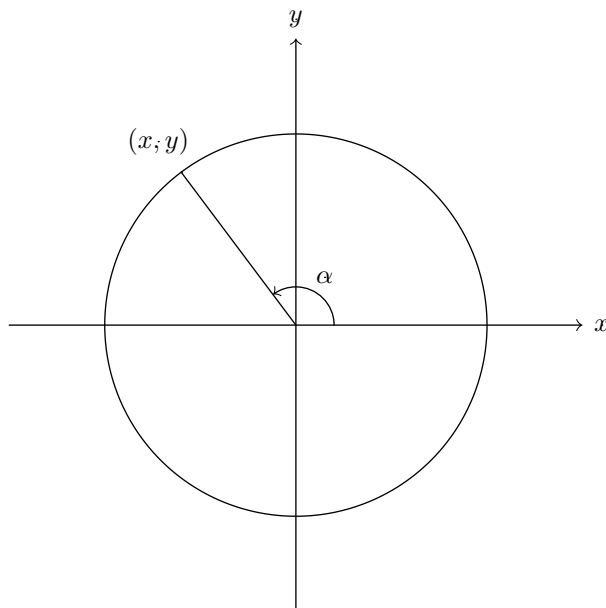
### Trigonometria

Yläkoulun osiossa esitettiin trigonometriset funktiot suorakulmaisen kolmion avulla. Tässä on se puute, että tällöin tutkittavat kulmat ovat välttämättä nollan ja 90 asteen väliltä. Trigonometria halutaan kuitenkin yleistää käsittelemään muitakin kolmioita kuin suorakulmaisia kolmioita, ja tällöin kolmion kulmat voivat hyvinkin olla yli 90 astetta.

Tämä puute korjataan määrittelemällä trigonometrinen funktioiden arvot yksikköympyrän avulla. Yksikköympyrä tarkoittaa yksinkertaisesti ympyrää, jonka säde on yksi ja jonka keskipiste on origo. Valitaan sitten jokin kulma  $0^\circ \leq \alpha < 360^\circ$ , ja piirretään ympyrän säde, joka on  $x$ -akselista nähden kulman  $\alpha$  verran vastapäivässä.

<sup>126</sup>Myös yleisen geometrisen lukujonon summakaavan voi todistaa induktiolla.

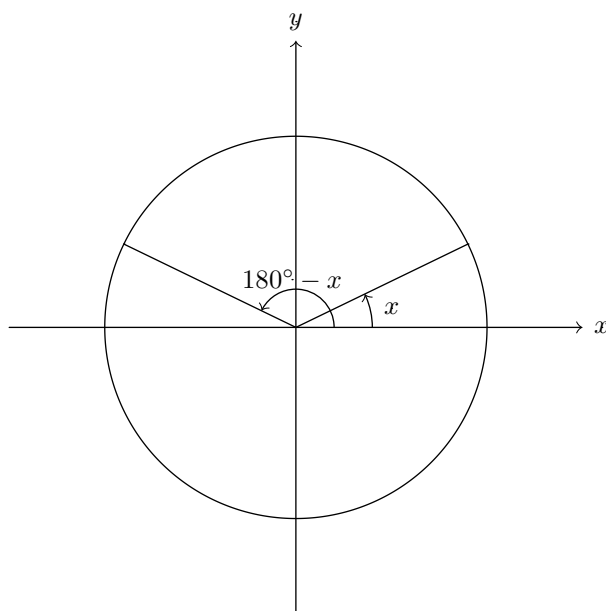
<sup>127</sup>Tämän voi muotoilla tarkemmin raja-arvojen avulla.



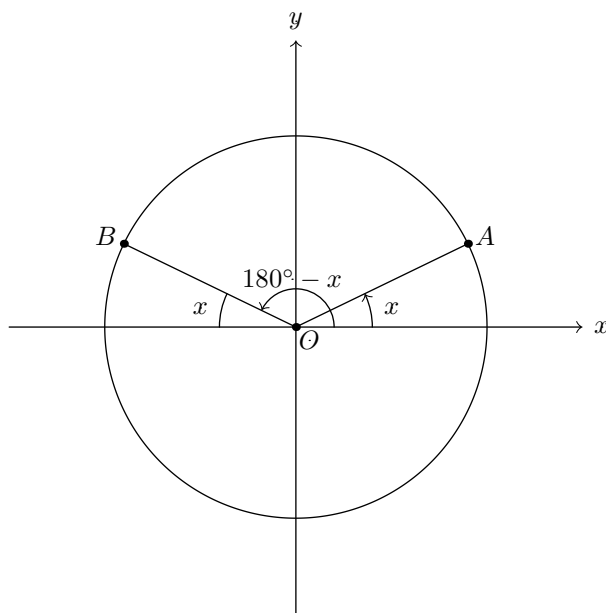
Tämä jana leikkaa ympyrän jossain pisteessä  $(x, y)$ . Määritellään nyt  $\sin(\alpha) = y$  ja  $\cos(\alpha) = x$  sekä  $\tan(\alpha) = \frac{y}{x}$ , kun  $x \neq 0$ . Sini ja kosini on nyt määritelty kaikille kulmille  $0^\circ \leq \alpha < 360^\circ$ . (Huomaa, että arvot voivat olla negatiivisia.) Lisäksi voidaan ajatella, että esimerkiksi kulma  $730^\circ$  eli  $10^\circ + 360^\circ + 360^\circ$  on vain sama asia kuin kulma  $10^\circ$ , koska täydet kierrokset eivät vaikuta valittuun säteeseen. Vastaavasti vaikkapa  $-330^\circ$  vastaa kulmaa  $30^\circ$ .

Tällä tavalla määritelty sini ja kosini antavat samat tulokset kuin suorakulmaisen kolmion antamat arvot kun  $0 < \alpha < 90^\circ$ , minkä voi nähdä piirtämällä sopivan kuvan ja tutkimalla sitä.

Yksikköympyrää tutkimalla voi todistaa erilaisia trigonometrinen funktioiden ominaisuuksia. Osoitetaan harjoituksen vuoksi, että kaikilla kulmilla  $x$  pätee  $\sin(x) = \sin(180^\circ - x)$ . Tutkitaan ensiksi tapausta  $0^\circ \leq x \leq 90^\circ$ . Tällöin tilanne näyttää tältä:



Nyt säteiden päätepisteiden  $y$ -koordinaatit ovat samat. Tämän voi todistaa seuraavasti: Olkoon  $O$  origo, ja olkoon kulmaa  $x$  vastaavan säteen päätepiste  $A$  ja kulmaa  $180^\circ - x$  vastaavan säteen päätepiste  $B$ . Koska oikokulma on  $180^\circ$ , säde  $OB$  ja negatiivinen osa  $x$ -akselista muodostavat kulman  $x$ . Tämä on sama kulma kuin säteen  $OA$  ja positiivisen  $x$ -akselin välinen kulma. Kuvio on siis symmetrinen  $y$ -akselin suhteen, eli pisteillä  $A$  ja  $B$  todella on samat  $y$ -koordinaatit. Koska sini vastaa  $y$ -koordinaattia, on yhtälö  $\sin(x) = \sin(180^\circ - x)$  todistettu.



Vastaavasti voidaan käsitellä tapaus  $90^\circ \leq x \leq 180^\circ$  (oikeastaan tämä seuraa jo edellisestä) ja niin ikään myös tapaus  $180^\circ \leq x < 360^\circ$ .

Trigonometrian tuloksia ja sovelluksia kilpailumatematiikkaan käsitellään tarkemmin varsinaisen tekstin puolella.

### Toisen asteen yhtälö

Toisen asteen yhtälöt ovat muotoa  $ax^2 + bx + c = 0$ , missä  $a, b$  ja  $c$  ovat vakioita (ja  $a \neq 0$ ). Usein halutaan selvittää yhtälön toteuttavat luvut  $x$ . Ideana on yrittää palauttaa yhtälö muotoon  $y^2 = d$ , mistä  $y$  osataan ratkaista ottamalla neliöjuuri. Tämä onnistuu yhtälössä  $ax^2 + bx + c = 0$  silloin, kun  $b = 0$ : tällöin vähentämällä  $c$  ja jakamalla  $a$ :lla saadaan  $x^2 = -\frac{c}{a}$ . Yleinen tapaus voidaan redusoida tähän tapaukseen ”siirtämällä” muuttujaa  $x$  sopivasti, eli toisin sanoen kirjoittamalla yhtälö esimerkiksi muuttujan  $x + 1$  avulla muuttujan  $x$  sijasta. Muuttujan  $x$  siirtäminen valitaan niin, että ensimmäisen asteen termi  $bx$  saadaan katoamaan.

Tuumasta toimeen. Jaetaan yhtälö  $ax^2 + bx + c = 0$  luvulla  $a$  (joka ei ole 0), jolloin yhtälö on

$$x^2 + \frac{b}{a}x + \frac{c}{a} = 0.$$

Toteutetaan siirtämisidea: vasen puoli on suunnilleen  $(x + \frac{b}{2a})^2$ : ainoastaan vakio

menee pieleen. Pätee siis

$$0 = x^2 + \frac{b}{a}x + \frac{c}{a} = \left(x + \frac{b}{2a}\right)^2 - \left(\frac{b}{2a}\right)^2 + \frac{c}{a}.$$

Kirjoitetaan yhtälö uudelleen muotoon

$$\left(\frac{b}{2a}\right)^2 - \frac{c}{a} = \left(x + \frac{b}{2a}\right)^2.$$

Tämä yhtälö on juurikin aiemmin kuvailtua muotoa  $y^2 = d$ . Otetaan puolittain neliöjuuri. Huomaa, että  $y^2 = d$  tarkoittaa, että  $y$  on joko  $\sqrt{d}$  tai  $-\sqrt{d}$ , ja molemmat tapaukset tulee huomioida.<sup>128</sup> Saadaan siis

$$x + \frac{b}{2a} = \pm \sqrt{\left(\frac{b}{2a}\right)^2 - \frac{c}{a}}.$$

Tässä  $\pm$ -merkki tarkoittaa, että  $x + \frac{b}{2a}$  on joko  $\sqrt{\left(\frac{b}{2a}\right)^2 - \frac{c}{a}}$  tai  $-\sqrt{\left(\frac{b}{2a}\right)^2 - \frac{c}{a}}$ .

Loppu onkin rutiininomaista lausekkeiden sieventelyä. Vähennetään puolittain  $\frac{b}{2a}$ :

$$x = -\frac{b}{2a} \pm \sqrt{\frac{b^2}{4a^2} - \frac{c}{a}}.$$

Tämän voi kirjoittaa vielä (neliöjuurien laskusääntöjä käyttämällä) muodossa

$$x = -\frac{b}{2a} \pm \frac{\sqrt{b^2 - 4ac}}{\sqrt{4a^2}} = -\frac{b}{2a} \pm \frac{\sqrt{b^2 - 4ac}}{2a}$$

eli

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

## Logaritmi

Yhtälöstä  $x^3 = 125$  saa ratkaistua  $x$ :n ottamalla puolittain kolmannen juuren: koska  $x^3 = 125$ , niin  $\sqrt[3]{x^3} = \sqrt[3]{125}$ . Vasen puoli on  $x$  ja oikea puoli on 5, koska  $5^3 = 125$ . Täten yhtälöllä on ratkaisu  $x = 5$ .

Tutkitaan sitten yhtälöä muotoa  $3^x = 81$ . Kokeilemalla eri vaihtoehtoja voidaan löytää ratkaisu  $x = 4$ . Olisi kuitenkin hyvä olla jokin systemaattinen tapa ratkaista tämäntyyppisiä yhtälöitä. Apuun tulevat logaritmit.

Olkoot  $a$  ja  $b$  positiivisia reaalilukuja ( $a \neq 1$ ). Tutkitaan yhtälöä muotoa  $a^x = b$ . Tällä yhtälöllä on olemassa täsmälleen yksi ratkaisu. Tässä on väitteelle perustelu, jonka lukija voi halutessaan sivuuttaa. Perustelussa oletetaan  $a > 1$ , mutta tapaus  $a < 1$  voidaan käsitellä vastaavasti.

Kun  $x$  on ”hyvin negatiivinen”, niin  $a^x$  on suunnilleen nolla. Kun  $x$  on hyvin suuri, niin myös  $a^x$  on hyvin suuri. Koska  $b$  on nollan ja äärettömän välissä, on olemassa

<sup>128</sup>Toisen asteen yhtälöllähän on useimmiten kaksi erisuurta ratkaisua.



jokin luvun  $x$  arvo, jolla  $a^x$  on täsmälleen luku  $b$ . Olemme nyt perustelleet,<sup>129</sup> että ratkaisuja on ainakin yksi. Ratkaisuja on myös enintään yksi, koska jos  $a^x = b$  ja  $a^y = b$ , niin  $a^x = a^y$  eli  $a^{x-y} = 1$ . Tästä seuraa,<sup>130</sup> että  $x - y = 0$  eli  $x = y$ .

Merkitsemme tätä yhtälön  $a^x = b$  ratkaisua merkinnällä  $\log_a(b)$ , jolloin siis  $a^{\log_a(b)} = b$ . Tämä luku on nimeltään ” $a$ -kantainen logaritmi luvusta  $b$ ”.

Esimerkiksi  $\log_2(64) = 6$ , koska  $2^6 = 64$ , ja  $\log_2(4096) = 12$ , koska  $2^{12} = 4096$ . Määritelmään totuttelu vaatii jonkin verran aikaa.

Huomataan, että logaritmi kasvaa hitaasti: niinkin isolla luvulla kuin 4096 logaritmin arvo (kannalla 2) on vain 12. Luvun  $2^{100}$  kaksikantainen logaritmi  $\log_2(2^{100})$  on hyvin pieni (100), vaikka  $2^{100}$  on luku, jossa on 31 numeroa.

Mitä hyötyä logaritmin määritelmästä on? Logaritmeilla on paljon käteviä ominaisuuksia. Yksi on seuraava: pätee  $\log_a(xy) = \log_a(x) + \log_a(y)$  (missä  $a, x$  ja  $y$  ovat mielivaltaisia positiivisia reaalilukuja ja  $a \neq 1$ ). Logaritmi siis muuttaa tulon summaksi. Tämä muistuttaa hieman potenssiinkorotuksen sääntöä  $a^{x+y} = a^x \cdot a^y$ , jossa summa muuttui tuloksi, ja laskusäännön todistus logaritmeille perustuikin vastaavaan potenssien sääntöön.<sup>131</sup> Logaritmilla on siis päinvastainen vaikutus kuin potenssiinkorotuksella (mikä on luonnollista, koska logaritmi on määritelty potenssiinkorotuksen käänteisoperaatioksi).

Myös yhtälö  $\log_a(x^y) = y \cdot \log_a(x)$  pätee. Tässä on perustelu: Mihin potenssiin luku  $a$  pitää korottaa, jotta saadaan luku  $x^y$ ? Määritelmän nojalla vastaus on  $\log_a(x^y)$ . Toisaalta jotta luvusta  $a$  saadaan  $x^y$ , riittää ensin korottaa lukua  $a$  niin, että saadaan luku  $x$ , ja korottaa saatu luku potenssiin  $y$ . Tämä saavutetaan korottamalla  $a$  ensin potenssiin  $\log_a(x)$  ja sitten potenssiin  $y$ , eli yhteensä potenssiin  $y \cdot \log_a(x)$ . (Pätee siis  $a^{y \cdot \log_a(x)} = (a^{\log_a(x)})^y = x^y$ , joka saadaan käyttämällä potenssien laskusääntöjä ja logaritmin määritelmää.)

<sup>129</sup>Perustelu toivottavasti selittää intuitiivisesti, miksi yhtälöllä on ratkaisu. Kokeneemmat lukijat kuitenkin huomaavat, että formaali todistus vaatisi tiedon funktion  $a^x$  jatkuvudesta (mikä perustuu potenssiinkorotuksen määritelmään) ja väliarvolauseeseen. Emme kuitenkaan syvenny yksityiskohtiin.

<sup>130</sup>Tarkka perustelu sivuutetaan jälleen.

<sup>131</sup>Perustelu yhtälölle  $\log_a(xy) = \log_a(x) + \log_a(y)$ : Luku  $\log_a(x)$  on se luku  $s$ , jolla  $a^s = x$ . Luku  $\log_a(y)$  on se luku  $t$ , jolla  $a^t = y$ . Nyt potenssien laskusäännöillä saadaan, että  $a^{s+t} = a^s \cdot a^t = x \cdot y = xy$ . Täten  $s + t$  on se luku, johon korottamalla luvusta  $a$  saadaan  $xy$ . Mutta tämä luku on määritelmän nojalla  $\log_a(xy)$ , joten  $\log_a(xy) = s + t$ . Tämä todistaa halutun väitteen.

### 23.3 Sekalaisia asioita

Tähän osioon on koottu asioita, jotka eivät ole osa selkeämpää kokonaisuutta.

Yleensä matematiikassa muuttujalla  $n$  viitataan johonkin kokonaislukuun, joka on useimmiten positiivinen. Yleensä kontekstista voi päätellä, mitä arvoja mikään muuttuja voi saada (tai sillä ei ole juurikaan väliä), ja valitut kirjaimet auttavat tässä päättelyssä. Esimerkiksi virkkeestä ”Osoitetaan, että kaikilla  $n$  luku  $n(n+1)$  on parillinen” voidaan päätellä, että  $n$  on kokonaisluku, koska  $n$  usein viittaa kokonaislukuun ja koska ei ole järkeä puhua epäkokonaisluvun parillisuudesta.

Matemaattisissa teksteissä käytetään välillä sanoja, joita harvemmin näkee muissa teksteissä. Tähän on koottu muutama näistä. Sanat *lause* ja *lemma* viittaavat matemaattisiin väitteisiin. Lause viittaa johonkin isoon ja tärkeää tulokseen. Lemma puolestaan on apulause tai aputulos. Sanayhdistelmä ”jos ja vain jos” tarkoittaa, että jokin asia tapahtuu täsmälleen silloin, kuin jokin toinen asia tapahtuu. Siis ” $A$  pätee jos ja vain jos  $B$  pätee” tarkoittaa, että ”jos  $B$  pätee, niin  $A$  pätee, ja jos  $A$  pätee, niin  $B$  pätee”. Esimerkiksi voidaan sanoa ” $n$  on parillinen jos ja vain jos  $n+1$  on pariton”. *Triviaali* tarkoittaa, että jokin asia on ilmiselvä (mutta joillain ihmisillä on tapana käyttää sanaa myös vähemmän selvien asioiden yhteydessä).

Kilpailutehtävissä saa käyttää vapaasti yleisesti tunnettuja tuloksia. (Poikkeustapauksena on tietysti, jos jostain syystä kilpailussa pyydetäisiin todistamaan jokin tällainen yleisesti tunnettu tulos tai jokin sen erikoistapaus.) Tällaisia ovat muun muassa kaikki lauseet, jotka on todistettu tässä kirjassa (mutta yksittäisten tehtävien ratkaisuihin ei ole soveliaista viitata).

Intuitiivisesti on selvää, mitä kokonaislukujen jaollisuudella tarkoitetaan: luku 10 on jaollinen luvulla 2, muttei luvulla 3. Tässä on tarkka määritelmä:

#### Määritelmä

Sanotaan, että kokonaisluku  $a$  on jaollinen kokonaisluvulla  $b$ , jos  $\frac{a}{b}$  on kokonaisluku.

Jaollisuutta merkitään  $b|a$ , eli  $b$  jakaa  $a$ :n. Jos  $b$  ei jaa lukua  $a$ , niin merkitään  $b \nmid a$  (samoin kuin jos  $x$  ja  $y$  eivät ole yhtä suuria, niin merkitään  $x \neq y$ ). Jaollisuudella on muun muassa seuraavat luonnolliset ominaisuudet:

- Jos  $a | b$  ja  $a | c$ , niin  $a | b + c$  ja  $a | b - c$  (koska jos  $\frac{b}{a}$  ja  $\frac{c}{a}$  ovat kokonaislukuja, niin myös  $\frac{b+c}{a}$  ja  $\frac{b-c}{a}$  ovat)
- Jos  $a | b$ , niin  $a | bc$  millä tahansa kokonaisluvulla  $c$  (koska jos  $\frac{b}{a}$  on kokonaisluku, niin myös  $\frac{bc}{a}$  on kokonaisluku).

Alkuluvulla tarkoitetaan ykköstä suurempaa kokonaislukua, joka on jaollinen vain itsellään ja ykkösellä. Ensimmäiset alkuluvut ovat siis 2, 3, 5, 7, 11 ja 13. Alkulukuun viitataan usein kirjaimella  $p$ .<sup>132</sup>

<sup>132</sup>Kirjaimen  $p$  käyttö tulee siitä, että englanniksi alkuluku on ”prime number”.

Merkintä  $|x|$  tarkoittaa luvun  $x$  itseisarvoa. Jos  $x \geq 0$ , niin itseisarvo on  $x$ , ja jos  $x < 0$ , niin itseisarvo on  $-x$ . Itseisarvo siis kertoo luvun etäisyyden nolasta ja on siksi hyvä tapa mitata luvun suuruutta. (Kompleksiluvun  $a + bi$  etäisyys nolasta saadaan Pythagoraan lauseella tutkimalla pisteitä kompleksitasossa:  $|a + bi| = \sqrt{a^2 + b^2}$ .)

Merkintä  $\lfloor x \rfloor$  kuvastaa ns. lattiafunktioita, joka on luvun  $x$  pyöristys alaspäin kokonaislukuun. Esimerkiksi  $\lfloor 3.9 \rfloor = 3$  ja  $\lfloor \sqrt{2} \rfloor = 1$ . Negatiivisten lukujen kanssa on hyvä olla tarkkana:  $\lfloor -0.5 \rfloor = -1$ . Vastaavasti kattofunktio  $\lceil x \rceil$  on luvun  $x$  pyöristys ylöspäin. Luvun  $x$  murto-osalle on merkintä  $\{x\}$ , jonka määritellään olevan  $\{x\} = x - \lfloor x \rfloor$ . Esimerkiksi  $\{1.2345\} = 0.2345$ .<sup>133</sup>

Jos  $a$  ja  $b$  ovat reaalilukuja, niin välillä  $[a, b]$  tarkoitetaan niiden lukujen  $x$  joukkoa, jotka toteuttavat ehdot  $a \leq x$  ja  $x \leq b$ . Siispä  $a$  ja  $b$  ovat mukana tässä välissä. Merkintä  $(a, b)$  tarkoittaa väliä, jossa on kaikki luvut  $x$ , joilla  $a < x$  ja  $x < b$ . Tässä  $a$  ja  $b$  eivät siis ole mukana. Joissain lähteissä käytetään merkintää  $]a, b[$  tarkoittamaan samaa asiaa. Vastaavasti voidaan määritellä vielä  $[a, b)$  ja  $(a, b]$ .

Summamerkintöjä voidaan lyhentää. Summa  $1 + 2 + \dots + 100$  voidaan kirjoittaa tiivistä muotoon

$$\sum_{i=1}^{100} i.$$

(Summamerkki  $\Sigma$  on kreikan kielen kirjain iso sigma.) Tässä  $i$  on siis muuttuja, joka käy läpi arvot  $1, 2, \dots, 100$ . Otamme summan näistä muuttujan  $i$  arvoista. Toinen esimerkki: Summa  $7^2 + 8^2 + 9^2 + 10^2 + \dots + 35^2$  on

$$\sum_{i=7}^{35} i^2.$$

Tässä  $i$  käy läpi kokonaislukuarvot väliltä  $[7, 35]$ , ja summaamme näillä  $i$  luvut  $i^2$ .

Vastaavasti voidaan merkitä tiiviisti tuloa. Aiemmin määriteltiin  $n! = 1 \cdot 2 \cdot \dots \cdot (n-1) \cdot n$ . Tätä merkitään

$$n! = \prod_{i=1}^n i.$$

Tulomerkki on kreikan kirjain iso pii. Logiikka on siis sama kuin aiemmin, mutta summa on korvattu tulolla.

Lukujen  $1, 2, \dots, n$  permutaatiolla tarkoitetaan jotain uudelleenjärjestystä näille luvuille. Esimerkiksi lukujen  $1, 2, 3$  permutaatioita ovat seuraavat jonot:

- $(1, 2, 3)$
- $(1, 3, 2)$
- $(2, 1, 3)$
- $(2, 3, 1)$

<sup>133</sup>Tämä notaatio on, ikävä kyllä, sama kuin joukkojen merkitsemiseen käytetty notaatio. Kontekstista voidaan kuitenkin päätellä, mitä tarkoitetaan.

- $(3, 1, 2)$
- $(3, 2, 1)$

Lukujen  $1, 2, \dots, n$  permutaatioiden määrä on  $n!$  (miksi?).

Aiemmin esiteltiin induktiotodistus. Toinen yleinen todistustekniikka on vastaoletustodistus. Haluamme todistaa väitteen  $X$ . Todistamme väitteen olettamalla, että  $X$  ei päde, ja saamalla aikaan ristiriidan. Siis ei voi olla mahdollista, että  $X$  ei päde, joten  $X$  pätee. Klassinen esimerkki vastaoletustodistuksesta on alkulukujen äärettömyyden todistaminen.

### Lause (Alkulukujen äärettömyys)

On olemassa äärettömän monta alkulukua.

Ennen lauseen todistusta todetaan ilmiselvä fakta: jokainen ykköstä suurempi kokonaisluku  $n$  on jaollinen jollain alkuluvulla. Jos nimittäin  $n$  ei ole jaollinen millään itseään pienemmällä alkuluvulla, niin sen tulee itse olla alkuluku.

Sitten lauseen todistukseen. Oletetaan, että on olemassa vain äärellisen monta alkulukua. Olkoot ne  $p_1, p_2, \dots, p_n$ . Tutkitaan lukua

$$P = p_1 p_2 \cdots p_n + 1.$$

Mitä luvusta  $P$  tiedetään? Se on ykköstä suurempi kokonaisluku, joten edellä esitetyn faktan nojalla  $P$  on jaollinen jollain alkuluvulla. Koska kaikki alkuluvut ovat  $p_1, p_2, \dots, p_n$ , niin pätee  $p_i \mid P$  jollain indeksillä  $i$ . Siispä  $p_i \mid p_1 p_2 \cdots p_n + 1$ , mutta koska  $p_i \mid p_1 p_2 \cdots p_n$ , niin tulisi päteä  $p_i \mid 1$ , mikä ei ole mahdollista. Tämä on ristiriita.

Oletimme, että on olemassa vain äärellisen monta alkulukua, ja päädyimme mahdottomuuteen. Täten alkulukuja täytyy olla äärettömän monta.

## 24 Lisämateriaaleja

Tähän lukuun on koottu kilpailumatematiikkaan liittyvää lisämateriaalia.

### Tehtävät

Kuten jo kirjan alussa mainittiin, tehtävien ratkomisen tärkeyttä ei voi liioitella. Tässä on lyhyesti siitä, miten itse olen harjoitellut. (Kevyempää luettavaa -osiosta löytyy tarkempi kuvaus itse kilpailu-urastani.) Muiden ei tietenkään kannata harjoitella täsmälleen samalla tavalla kuin minun, vaan tarkoituksena on lähinnä antaa esimerkkejä kilpailuista ja tehtäväkokoelmista, joiden avulla voi harjoitella.

Tutustuin matematiikkakilpailuihin peruskoulun kilpailun tehtävillä. Näitä on koottu kattavasti MAOLin sivuilla: <https://maol.fi/neljan-tieteen-kisat/vanhat-kilpailutehtavat/>. En juurikaan tehnyt kilpailuja ”vakavasti” ajan kanssa, vain ainoastaan katselin ja mietiskelin tehtäviä. Taisin kuitenkin käydä läpi suunnilleen kaikki kilpailut, mitä MAOLin sivuilta löytyi.

Minulla oli myös mielessä Viron kansallinen kilpailu, johon kutsuttiin peruskoulun loppukilpailussa kaksi parhaiten menestynyttä, joten siirryin jossain kohtaa tekemään virolaisten kilpailujen tehtävillä. Suomen kilpailu on verrattain nopeatempoinen, kun taas Viron kilpailussa on 5 tuntia aikaa ratkaista viisi tehtävää.

Löysin tehtävät vain viroksi, mutta viro on sen verran lähellä suomea, että kääntäjän avulla ymmärsin suurimman osan tehtävänannoista ilman ongelmia. Tehtävät löytyvät Viron valmennuksen sivuilta: esimerkiksi vuoden 2020 loppukilpailun tehtävät löytyvät osoitteesta [http://www.math.olympiadid.ut.ee/html/index.php?id=2019\\_20](http://www.math.olympiadid.ut.ee/html/index.php?id=2019_20) kohdasta ”Olympiaadi loppvoor”. Sivuilta löytyy 9. luokkalaisten sarjan lisäksi myös 10., 11. ja 12. luokkalaisten sarjat.

Tein kisoja (jälkeenpäin miettien yllättävänkin) systemaattisesti: kävin kilpailuja vuosi vuodelta läpi, ja olin varannut jokaista kilpailua varten itselleni vapaan illan, jonka aikana tein tehtäviä kuten oikeassa kilpailussa. Istumalihaksia minulla ei kuitenkaan ollut riittävästi, että olisin aina jaksanut käyttää täydet viisi tuntia.

Harjoitteluksi voi nähdä myös sen, että olin Päivölän matematiikkalinjan kesäviikoilla. Vaikka kesäviikoilla keskityttiinkin lukiomatematiikkaan ja erityisesti analyysiin, uudenlaisen matematiikan näkeminen ja oppiminen ei todellakaan ollut pahitteeksi.

Syksyllä aloin käymään aktiivisesti valmennuksessa ja keskityinkin lukiotason kilpailumatematiikkaan. Tein vanhoja MAOLin alku- ja loppukilpailuja. Näitä löytyy MAOLin sivuilta (linkki ylempänä) ja valmennuksen sivuilta (<https://matematiikkakilpailut.fi/MAOL/>). Alkukilpailuja en muistaakseni tehnyt kovin järjestelmällisesti; loppukilpailut puolestaan kävin läpi systemaattisesti kuten Viron kilpailuun harjoitellessani.

Luonnollinen seuraava vaihe oli Pohjoismaisen matematiikkakilpailun tehtävien ratkominen. Vanhat kisat löytyvät valmennuksen sivuilta: <https://matematiikkakilpailut.fi/PM/>. Nämä kävin niin ikään järjestelmällisesti läpi. En tietenkään saanut kaikkia tehtäviä tehtyä, mutta opin paljon niin onnistumisistani kuin epäon-

nistumisistani.

Näihin aikoihin minut valittiin ensimmäistä kertaa IMO-joukkueeseen. Ajattelin, että IMO-tehtävät ovat hyvin vaikeita (mikä on ihan perusteltua). Tästä syystä en käynyt vanhoja kisoja erityisemmin läpi, mutta ratkoin kylläkin IMO-lyhytlistojen helpoimpia tehtäviä. Nämä löytää AoPSin kisatehtäväkokoelmasta: [https://artofproblemsolving.com/community/c3223\\_imo\\_shortlist](https://artofproblemsolving.com/community/c3223_imo_shortlist).

Tarinan opetus on, että on olemassa hyvin vaihtelevantasoisia kilpailuja. Aloitin peruskoulun alkukilpailun tehtävistä ja päädyin IMO-tason tehtäviin, mutta minun ei tarvinnut missään vaiheessa tehdä suurta hyppäystä, vaan pystyin aina valitsemaan hieman vaikeampia tehtäviä.

Edellä ei myöskään ole todellakaan listattu kaikkia maailman kilpailuja. Esimerkiksi seiskaluokkalaisten matematiikkakilpailut (<https://matematiikkakilpailut.fi/seiskat/>) ovat ehkäpä vielä aloittelijaystävällisempiä kuin MAOLin peruskoulun kilpailu. Toisessa ääripäässä IMO ei ole ainoa kovatasoinen kilpailu: on lukuisia kansainvälisiä kilpailuja, ja myös monet kansalliset kilpailut ovat hyvin vaativia.<sup>134</sup> AoPSin kilpailukokoelma ([https://artofproblemsolving.com/community/c13\\_contests](https://artofproblemsolving.com/community/c13_contests)) sisältää tehtäviä enemmän kuin tarpeeksi.

Harjoitteluun sopivia tehtäviä on siis enemmän kuin mitä yksi ihminen ehtii tekemään. Koin itse runsaudenpulaa nähdessäni AoPSin tehtäväkokoelman ja miettiessäni mitä teen seuraavaksi. Ei kuitenkaan kannata etsiä juuri ”oikeita” tehtäviä: kunhan tehtävien vaikeustaso on kohdillaan (eli tehtävät tuntuvat hieman liian vaikeilta), ei sillä ole väliä, mistä kilpailusta tehtävät tarkalleen ovat.

Evan Chen on kirjoittanut tätä aihetta käsittelevän tekstin, jonka suosittelen lukemaan: <https://usamo.wordpress.com/2019/01/31/math-contest-platitudes-v3/>. Nostan tekstistä tähän esiin sen, että jokaisella on oma tapansa tehdä (kilpailu)matematiikkaa. Muilta saa toki ottaa inspiraatiota ja vinkkejä, mutta ei kannata väkisin tehdä jotain, minkä on kuullut toimivan jollakulla toisella. Ei esimerkiksi kannata välttämättä tehdä juuri samoja kilpailuja kuin mitä minä olen listannut edellä, jos se ei tunnu kehittävältä (ja ennen kaikkea hauskalta).

Alla on vielä aihealuekohtaisesti joitain materiaaleja, joita voisin suositella niille, jotka kaipaavat lisäluettavaa. Nämä ovat jälleen henkilökohtaisia suosituksia, eli jos materiaalit eivät tunnu itselle sopivilta, kannattaa etsiä jotakin sopivampaa.

## Geometria

Ylivoimaisesti paras näkemäni geometrian materiaali on Evan Chenin kirjoittama kirja *Euclidean Geometry in Mathematical Olympiads* (EGMO). Tämä on myös ylipäättään paras kilpailumatematiikkaan liittyvä materiaali, jonka olen löytänyt.

## Kombinatoriikka

<sup>134</sup>Ei ole perusteetonta väittää, että esimerkiksi Kiinan tai Yhdysvaltojen IMO-joukkueen valintakokeet ovat (ainakin välillä) haastavampia kuin varsinaiset IMO-kisapäivät. (Kansallisen kilpailun ja valintakokeiden tehtävien vaativuutta voi arvioida melko hyvin maan menestyksellä IMOssa.) Lisäksi kutsuun perustuvaa kansainvälistä Romanian Master of Mathematics -kilpailua pidetään vaikeampana kuin Kansainvälisiä matematiikkaolympialaisia.

Kombinatoriikka on mielestäni ehkäpä vähiten teoriaa vaativa kilpailumatematiikan osa-alue (eli kannattaa siis ratkoa tehtäviä). Joitain yleisiä periaatteita kuitenkin on. Hyvä materiaali löytyy täältä postauksista 1, 11 ja 49: [https://artofproblemsolving.com/community/c365902h601134\\_olympiad\\_combinatorics\\_book](https://artofproblemsolving.com/community/c365902h601134_olympiad_combinatorics_book). Materiaalit muodostavat siis yhdessä kokonaisen kirjan. (Ilmeisesti materiaalin lukemista varten täytyy kirjautua sisään AoPSiin.)

### Algebra

Hyvä funktionaaliyhtälöihin liittyvä materiaali löytyy täältä postauksesta numero 29: [https://artofproblemsolving.com/community/c365902h1592427\\_my\\_fe\\_ha\\_ndout](https://artofproblemsolving.com/community/c365902h1592427_my_fe_ha_ndout). (Myös tämän lukemiseksi täytyy kirjautua sisään.)

Paul Vaderlindin kirjoittama kattava esitys klassisista epäyhtälöistä löytyy puolestaan täältä: <https://matematiikkakilpailut.fi/kirjallisuus/vaderlind.pdf>

### Lukuteoria

Lukuteorian suhteen kirjassa ei ole merkittäviä puutteita. Lukijan suositellaan siis lähinnä tekevän lukuteorian tehtäviä.

Tämän kirjan lukuteoriaosio käsittelee paljolti samoja aiheita kuin Esa Vesalaisen lukuteoriamateriaali. Voi silti olla hyödyllistä lukea Vesalaisen tekstiä: <https://matematiikkakilpailut.fi/kirjallisuus/laajalukuteoriamoniste.pdf>.<sup>135</sup>

Lisäksi mainitaan pari pientä juttua. Yksi kohtalaisen tunnetuksi muodostunut tulos on Lifting the Exponent (LTE): [https://artofproblemsolving.com/community/c6t108f6h393335\\_lifting\\_the\\_exponent\\_lemma\\_containing\\_pdf\\_file](https://artofproblemsolving.com/community/c6t108f6h393335_lifting_the_exponent_lemma_containing_pdf_file). Matti Lehtisen teksti Pellin yhtälöistä löytyy täältä: <https://matematiikkakilpailut.fi/kirjallisuus/pell.pdf>.

### Muuta

EGMOn yhteydessä mainittiin Evan Chen. Nykyään Chen toimii Yhdysvaltojen IMO-joukkueen valmennus- ja valintatoiminnassa. Hänellä on paljon laadukasta materiaalia:

- Olympiamateriaaleja sisältävät sivut: <https://web.evanchen.cc/olympiad.html>
- Blogi: <https://usamo.wordpress.com/>
- ”Napkin”. Materiaalin sisältö on kuvattu linkin sivustolla, mutta tiivistetysti materiaalissa on esitelty ”korkeamman matematiikan” eri osa-alueita. Sisältö ei siis varsinaisesti ole kilpailumatematiikkaa, mutta se on mahdollisesti mielenkiintoista luettavaa. <https://web.evanchen.cc/napkin.html>

Suosittelen vahvasti Chenin blogipostauksien lukemista: niissä on erinomaisia ajatuksia ongelmanratkaisuun ja yleisesti kilpailumatematiikkaan liittyen. Ylhäällä on poimittu jo yksi harjoitteluun liittyvä kirjoitus, ja tässä on kaksi lisäpoimintaa:

<sup>135</sup>Vesalainen on lisäksi käsitellyt joitain aiheita, jotka olen itse sivuuttanut (esimerkiksi täydelliset luvut, Wilsonin lause, neliöiden summat, Gaussin kokonaisluvut ja Pythagoraan kolmikot).

- <https://usamo.wordpress.com/2017/03/06/on-reading-solutions/>
- <https://usamo.wordpress.com/2019/10/26/understanding-with-system-1/>



## 25 Kevyempää luettavaa

Olen kirjoittanut erilaisia epämatemaattisia tekstejä, joiden uskon kiinnostavan lukijoita. Kerron lähinnä omia ajatuksiani ja mielipiteitäni (aikana, jona opiskelin ensimmäistä lukukautta yliopistossa), enkä juurikaan koeta vetää mitään yleisiä johtopäätöksiä. Olen lisäksi linkannut muita tekstien aiheisiin liittyviä materiaaleja, joiden uskon niin ikään olevan kiinnostavia.

Ensimmäinen teksti käsittelee kilpailu-uraani, ja tekstin pääpaino on kilpailu-urani alkupuolella. Toisessa kirjoituksessa käsittelem ajatuksiani lahjakkuudesta itseni kohdalla. Kolmannessa tekstissä pohdin, mistä kehittyminen koostuu eli mitä asioita opin harjoittelemalla. Neljäntenä on teksti koskien kilpailumatematiikan hyötyjä.

### 25.1 Kilpailu-urani

Kuulin ensimmäistä kertaa matematiikkakilpailuista ala-asteella – kuulemma tulevala yläkoulullani järjestettäisiin matematiikkakilpailu joka syksy. Kilpailu kiinnosti minua, koska jo tuolloin pidin matematiikasta, mutten ajatellut asiaa sen enempää. Yläkoulun seitsemännellä luokalla sain kuulla, että kilpailuun saavat osallistua vain kahdeksannen ja yhdeksannen luokan oppilaat.

Kahdeksannen luokan syksyllä alkoi taas puhe kilpailusta, ja innostuin asiasta toden teolla. Tutkin edellisten vuosien tehtäviä ja pisterajoja loppukilpailuun pääsemiseksi, laskin kilpailuun jäljellä olevia päiviä ja luin lisää muista matematiikkakilpailuista. Erityisesti minua houkutti lukemani tieto siitä, että loppukilpailuun päässeet kutsuttaisiin jatkovalmennukseen: ”Tätä minä haluan.”<sup>136</sup>

Itse kilpailupäivänä olin melko jännittynyt. Kilpailu sujui tästä huolimatta melko hyvin, vaikkakin aika tuntui loppuvan kesken enkä ymmärtänyt yhden alkupään tehtävän kysymystä. Kilpailun jälkeisinä päivinä tarkistin monta kertaa päivässä MAOLin nettisivut tulosten toivossa. Viikkojen odottaminen palkittiin: eräänä päivänä tulokset löytyivät sivuilta, ja sain tietää päässeeni loppukilpailuun rimaa hipoen.

Valmistauduin tammikuussa pidettävään loppukilpailuun kuten alkukilpailuunkin eli ratkomalla vanhoja kilpailutehtäviä. Totesin yllätyksekseni, etteivät aiempien vuosien voittajien pistemäärät tuntuneet mahdottomilta saavuttaa. Hakemalla netistä peruskoulun kilpailussa pärjänneiden nimiä huomasin, että jotkut heistä olivat pärjänneet myös lukion kilpailuissa ja jopa kansainvälisesti. Löysin Kansainvälisten matematiikkaolympialaisten sivut, ja haaveilin pääseväni Suomen joukkueeseen jonain päivänä.

Loppukilpailu järjestettiin Helsingissä. Perjantaina oli luvassa kolmiosainen kilpailu, ja lauantaina olisi palkintojenjako. Kisapäivänä olin hyvissä ajoin tapahtumapaikalla, ja odotellessani katselin muita kisaajia. He näyttivät hyvin pelottavilta ja valmistautuneilta voittamaan minut.

<sup>136</sup>En vielä tiennyt, että valmennukseen saavat tulla kaikki halukkaat.

Kilpailu meni omalta osaltani erittäin hyvin: jokainen kilpailun kolmesta osiosta sujui ilman suurempia ongelmia. Olin tästä huolimatta yllättynyt kuullessani palinkintojenjaossa, että olin ollut kilpailun paras suomalainen! Tämän seurauksena sain edustuspaikan Viron kansalliseen kilpailuun.

Loppuosa kahdeksannen luokkani keväästä kului Viron kilpailuun valmistautuessa sekä yleisesti matematiikan parissa. Harjoitteluun käytin pääasiassa Viron kilpailun vanhoja tehtäviä (kilpailu meni ihan hyvin: voitin noin puolet virolaisista). Suuntasin myös katsettani kohti lukion kilpailuja ja tutkin valmennuksen sivuilta löytyvää materiaalia.

Olin keväällä myös ensimmäistä kertaa valmennusviikonlopussa. Ennen viikonloppua olin käyttänyt huomattavan määrän aikaa valmennustehtävien miettimiseen, ja olin tyytyväinen saadessani ratkaistua niistä yhden tai kaksi.

Itse viikonloppuna olin aika hukassa. Tehtävät tuntuivat vaikeilta ja minulta puuttui esitietoja (kuten logaritmit). Minua kuitenkin rohkaisi se, etteivät muutkaan tajunneet kaikesta kaikkea. Olin myös hyvin hämmästynyt, kun muut eivät saaneetkaan heti ratkaistua uusia valmennustehtäviä.

Kesällä osallistuin Päivölän matematiikkalinjan kesäviikoille, joiden avulla sain paikattua matemaattisen yleissivistykseni aukkoja. Lisäksi kuulin paljon tarinoita vanhoista opiskelijoista, jotka olivat menestyneet lukemattomissa eri kilpailuissa. Heistä tuli minun esikuviani, ja toivoin pääseväni joskus pääseväni heidän joukkoonsa.

Yhdeksannen luokan syksyllä tapahtui paljon. Mieleenpainuvin, yllättävin ja tärkein hetki tapahtui ensimmäisellä valmennusviikonlopulla, kun kuulin pääseväni Suomen joukkueeseen Baltian tiehen. Samoihin aikoihin oli peruskoulun ja lukion matematiikkakilpailuiden alkukilpailut, joista molemmista pääsin jatkuun.

Vuoden 2016 Baltian tie järjestettiin marraskuussa Oulussa. Minulla oli matkalla todella mukavaa: tutustuin muuhun joukkueeseen, vitsailimme paljon, majoituimme kotoisissa mökeissä, järjestelyt sujuivat hyvin, kävimme hienoissa paikoissa ja niin edelleen. Kävin myös uimassa hyytävässä Itämeressä erään joukkueen jäsenen houkuteltua minut suklaalevyllä. Matkassa minua jäi harmittamaan ainoastaan oma suoritukseni joukkuekilpailussa: en kokenut saaneeni tehtyä juuri mitään. Eräs joukkueestamme kuitenkin kommentoi, että vuoden päästä voisin olla parempi kuin kukaan tämänhetkisestä joukkueesta. Pidin tätä enemmänkin lohduttavana kommenttina kuin realistisena arviona.

Käytin seuraavan joululomani suurelta osin harjoitteluun. Tein suunnilleen joka päivä yhden MAOLin lukion loppukilpailun, ja aina kilpailun tehtyäni tutkin sen malliratkaisuja. Jälkeenpäin ajateltuna tämä oli minulle selvästi käännekohta: opin hurjasti ongelmanratkaisua, ja aloin vihdoinkin saamaan valmennus- ja kisatehtäviä tehtyä.

Vuoden 2017 MAOLin loppukilpailussa osallistuin sekä peruskoulun että lukion sarjaan, ja tein kilpailut perätysten iltapäivän ja illan aikana. Peruskoulun kilpailu meni muuten loistavasti, mutta menetin askarteluosiossa paljon pisteitä. Lukion kilpailu meni niin ikään erinomaisesti. Vietin myöhäisillasta monta tuntia ystäväni kanssa tuloksia spekuloiden – arvaukset menivät aivan päin mäntyä, mutta hauskaa

oli.

Tulokset olivat kannaltani erinomaiset, ja erityisesti lukion kilpailun tulos tuli suurena yllätyksenä. Olin peruskoulun kisassa jälleen paras suomalainen, ja lukion kilpailussa pääsin toiselle sijalle. Palkintojenjakotilaisuuden jälkeen yksi Viron valmentajista kyseli minulta tunnelmaa, enkä oikein saanut sanaa suustani.

Keväällä oli vielä Viron kansallinen kilpailu, Pohjoismaiden (lukion) kilpailu sekä Suomen IMO-joukkueen valintaleiri. Olin harjoitellut tekemällä vanhojen Pohjoismaisten tehtävät ja kehityin lujaa tahtia. Voitin Viron kilpailun, mutta Pohjoismaiden kilpailu meni kehnosti. Olin kuitenkin kehittynyt sen verran, että IMOon pääseminen ei tullut yllätyksenä, ja nälkäni kasvoi. Tavoittelin pronssia.<sup>137</sup>

IMO-matka oli mahtava kokemus. Matka koostuu kahdesta osasta: viikon pituisesta pohjoismaiden joukkueiden valmennusleiristä Tanskassa, sekä viikosta itse IMOn järjestäjämaassa. Tanskassa oli opetusta samaan tyyliin kuin valmennusviikonlopuissa, ja lisäksi oli pari harjoituskilpailua. Vapaa-ajallamme pelasimme pöytäjalkapalloa ja ultimatea sekä kiipeilimme puissa. Kävin myös kaupassa ostamassa itselleni suuren laatikollisen kaurakeksejä.

Vuoden 2017 IMO järjestettiin Brasiliassa. Käytännössä kaikki toiminta ekskursion lukuun ottamatta tapahtui erinomaisella hotellillamme, ja käytännön järjestelyt toimivat sujuvasti. Ruoka oli herkullista (erityisesti appelsiinimehu oli suomalaisten mieleen), ekskursion viihdyttäviä ja vapaa-ajan huone hoiti tehtävänsä loistavasti.

Jännitin kilpailupäiviä paljon, ja ensimmäisenä päivänä kilpailun ensimmäiset parikymmentä minuuttia kuluivat paljolti rauhoittumiseen. Kilpailu meni kuitenkin suunnilleen toivotusti. Ainoa ongelma oli se, että tein kahden pisteen arvoisen hutiloinnin ensimmäisessä tehtävässä, minkä seurauksena menetin pronssin. Otin tämän melko raskaasti, ja olin hieman tympääntyneellä mielellä suuren osan loppumatkasta.

Mennessäni lukioon tilanne matematiikkapiireissä muuttui rajusti: IMO-joukkueen kuudesta jäsenestä neljälle IMO oli viimeinen kilpailu, joten kilpailujoukkueissa oli paljon tilaa uusille tulokkaille. Esimerkiksi syksyn Baltian tie -joukkueesta en tuntenut kahta henkilöä entuudestaan ollenkaan.

Konkareiden poistuttua kilpailupiireistä tulin hieman liiankin itsevarmaksi omista kyvyistäni, mikä näkyi muun muassa harjoittelumotivaation laskuna. Ylimielisyys tuli vastaan Baltian tiessä: kilpailutilanteessa en pärjännytkään niin hyvin kuin mitä olisin halunnut tai uskonut. Havahduin tämän kautta raakaan todellisuuteen ja lisäksi tajusin, että muut joukkueen jäsenet eivät olleetkaan hassumpia.

Muuten syksy ja kevät etenivät kohtalaisen samoja ratoja kuin edellisenä vuonna. MAOLin lukion loppukilpailussa ennen kilpailua muut kisajat näyttivät yhtä pelottavilta kuin aiemminkin, mutta onnistuin kuitenkin voittamaan kilpailun. Osallistuin myös tietotekniikan Datatähti-kilpailuun, jonka tuloksesta yllätyin positiivisesti sijoittuessani neljänneksi (en ollut aivan yhtä innokas kisakoodauksesta kuin matematiikkakilpailuista, minkä vuoksi menestyminen tuli yllätyksenä). Keväällä oli

<sup>137</sup>IMOssa (ja monissa muissakin tiedeolympialaisissa) jaetaan mitaleja niin, että noin puolet saa mitalin, ja mitalien määrien suhde on 1 : 2 : 3. Täten kultaa saavien kilpailijoiden osuus on  $\frac{1}{12}$  kaikista kilpailijoista ja vähintään hopeaa saavia on yksi neljäsosa.

vielä Pohjoismainen kilpailu ja IMO-valintaleiri. Pohjoismainen meni edellistä vuotta mukaillen kehnosti.

Vuoden 2018 IMO järjestettiin Romaniassa. Matka oli jälleen kerran mahtava. Matkustin Tanskaan jo viikkoa ennen varsinaista harjoitusleiriä ja osallistuin epäviralliselle leirille, jossa harjoittelin yhdessä muiden paikalle päässeiden pohjoismaalaisten kanssa. Kaksi viikkoa intensiivistä mutta miellyttävää leireilyä ennen olympialaisia sopi minulle hyvin. Leireiltä löytyi pöytäjalkapallopöydät, jotka auttoivat rentoutumaan harjoittelun lomassa.

Oma kilpailuni meni hyvin, mutta kuten edellisenäkin vuonna tein kahden pisteen arvoisen hutiloinnin ensimmäisessä tehtävässä, minkä seurauksena menetin tällä kertaa hopean. En kuitenkaan ottanut tappiota niin raskaasti tällä kertaa, koska sain kuitenkin mitalin. Lisäksi olin alkanut näkemään, että kilpailuista saa muutakin kuin mainetta ja kunniaa, joten en pitänyt IMOa enää kysymyksenä elämästä ja kuolemasta.

Viimeisenä kilpailuvuotenani en keskittynyt enää niin pääasiallisesti kilpailemiseen, vaan tein ensimmäisen kosketukseni ”oikeaan” matematiikkaan. Löysin ongelman,<sup>138</sup> joka kiinnosti minua valtavasti ja jonka parissa vietin paljon aikaa. Osallistuin kuitenkin kilpailuihin normaalisti ja välillä harjoittelin kilpailumatematiikkaa, koska tavoittelin viimeisestä IMOstani hopeaa.

Pietarin Baltian tie oli varsin mukava kilpailumatka. Kiertelimme paljon kaupungilla, ja kauniita maisemia ja rakennuksia oli kaikkialla. Erityisesti kirkot olivat vertaansa vailla. Kilpailu itsessään meni mielestäni mukiinmenevästi, vaikkakaan Suomen sijoitus ei ollut kummoinen.

Viimeisessä MAOLin loppukilpailussani osallistuin matematiikkaan, tietotekniikkaan ja fysiikkaan. Jotkin asiat eivät muutu: edelleen muut ihmiset näyttivät pelottavilta ja valmiilta voittamaan minut. Matematiikassa suoritukseni ei ollut parasta tasoani, mutta voitin onneksi kuitenkin kilpailun. Datatähdessä pääsin kolmannelle sijalle, ja fysiikassa olin yllättäen viides.

Toinen asia, mikä ei kohdallani muuttunut, oli Pohjoismaisessa kilpailussa kehnosti suoriutuminen. Kolmas muuttumaton asia: IMO-matka oli mahtava. Iso-Britannian vuoden 2019 IMOssa oli hauskaa, kuten aina muutenkin muiden matematiikkavalmennuksessa olevien kanssa. Lisäksi pärjäsin oikein hyvin, ja sain tavoittelemani hopean.

---

Selim Virtanen on kirjoittanut vuoden 2018 IMO-matkasta sarjan blogipostauksia: <https://selimvirtanen.blogspot.com/2018/>

---

<sup>138</sup>Olkkoon  $P$  kokonaislukukertoiminen polynomi. Sanotaan, että alkuluku  $p$  on  $P$ :n alkutekijä, jos  $p$  jakaa jonkin luvun muotoa  $P(n)$ , missä  $n$  on kokonaisluku. Mitä voidaan sanoa polynomien alkutekijöistä? Ongelman pintaa on raapaistu Lukuteorian lisätehtävät -luvun toisen tehtävän kommentissa.

## 25.2 Miksi juuri minä?

Olen menestynyt lukiolaisten tiedekilpailuissa mainiosti – suhteellinen sijoitukseni vuoden 2019 IMOssa oli paras Suomen IMOon osallistumisen historiassa. Minun näkökulmastani tämä tuntuu hassulta: neljä vuotta sitten olin verrattain tavallinen kahdeksannetta luokkaa käyvä poika, ja yhtäkkiä olinkin yksi Suomen parhaista lukiolaisista matematiikassa. En koe, että olisin tehnyt mitään, mihin viiden miljoonan väestöstä kukaan muu ei pystyisi. Miksi siis juuri minä olen pärjännyt näin hyvin muihin verrattuna?

Jos minulta olisi neljä vuotta sitten kysytty, mikä on tärkeintä huipulle pääsemisessä, olisin ehdottomasti maininnut luonnonlahjakkuuden. Olen kuitenkin alkanut kyseenalaistamaan tätä ajatusta (vaikkakin uskon kyllä, että joillakin on hieman parempi mututuntuma vaikkapa matemaattisten ongelmien ratkaisemiseen kuin joillain toisilla). Koen, että ennen kaikkea tärkeintä on puhdas ja rehellinen kiinnostus sitä kohtaan, mitä tekee.<sup>139</sup>

Vahva kiinnostus jotakin kohtaan ei ole itsestäänselvyys. Moni varmaankin vastaisi myöntävästi, jos heiltä kysyttäisiin ”Haluaisitko olla jonkin lajin olympiakultamitalisti?”, mutta tämä ei tarkoita, että he todella haluaisivat sitä. Jos edes promillea Suomen väestöstä kiinnostaisi todella paljon olla Suomen paras matematiikassa, olisi kilpailu paljon kovempaa. Sen pohjalta, mitä olen nähnyt muiden ihmisten suhtautumisesta matematiikkaan, olen sitä mieltä, että minut erottaa muista kiinnostuksen määrä: minä todella haluan oppia matematiikkaa. Lisäksi kilpailuja ajatellen minun kilpailuhenkisestä luonteestani ei varsinaisesti ole haittaa: minä myös todella halusin olla paras.

Pelkkä kiinnostus ei varmasti riitä huipulle pääsemisessä, koska monessa lajissa huipulle tähtää useampi henkilö, jotka kaikki haluavat huipulle todella paljon. Esimerkiksi maailman parhaista tennispelaajista varmasti kaikilla tai melkein kaikilla on motivaatio aivan huipussaan, mutta jotkut heistä ovat silti parempia kuin toiset. Tästä huolimatta kiinnostus on mielestäni Suomen kilpailumatematiikkapiirejä ajatellen tärkein mittari.

Jos oletetaan, että syynä menestykseeni on kiinnostuksen määrä, niin miksi minua sitten kiinnostaa enemmän kuin muita?<sup>140</sup> Pystyn tietysti puhumaan vain omista kokemuksistani ja siitä, minkä koen vaikuttaneeni kiinnostukseeni ja mikä mielestäni erottaa minut muista.

Tuttavani on kuvaillut minua sanalla ”worrywart”, joka tarkoittaa karkeasti henkilöä, joka tuppaa murehtimaan erilaisia asioita. Jo pienestä pitäen minulla on ollut tämä luonteenpiirre, ja, ehkä yllättäen, se on ajanut minua eteenpäin. Ajattelin, että jokaisella luokalla on oma matikkaneronsa, enkä kokenut olevani mitenkään erityinen. Kuitenkin aina ala- ja yläkoulussa kuullessani kysymyksen ”Mitä haluatte olla isona?” vastasin haluavani olla matemaatikko. Yhdistelmä ”matematiikassa pärjäävät vain

<sup>139</sup>Kiinnostus tietysti vaikuttaa harjoittelun määrään.

<sup>140</sup>Tajusin vasta hiljattain, että on myös toiseen suuntaan vetävä voima: monia muita kiinnostaa myös muut asiat kuin matematiikka. Minulla ei ole muita aikaavieviä harrastuksia, joten olen pystynyt keskittymään matematiikkaan.

ne, jotka ovat luonnostaan huippuja” ja ”haluan olla isona matemaatikko” selvästi vaati, että minä olisin luonnostaan hyvä matematiikassa. Minusta ei tuntunut tältä, ja kuvittelin, että isona joko pääsisin matemaatikoksi tai jäisin työttömäksi, kerjäisin kadulla rahaa ja näkisin nälkää.<sup>141</sup>

Kilpailu-urani alkaessa kahdeksannella luokalla aloin huomaamaan, että saatan olla kansallisella tasolla kilpailukykyinen. Huomasin tämän tutkiessani peruskoulun matematiikkakilpailun tuloksia: vaikutti siltä, että voisin ihan hyvin saada samantaisia tuloksia kuin Suomen parhaat. Aluksi olin hieman epäuskoinen ja ajattelin vain olevani ylimielinen. Myöhemmin kilpailuissa osoittautui, että ajatukseni olivat realistisia.

Ajattelin, että tämä ei kuitenkaan riitä: lukiokilpailujen tehtävät ovat paljon vaativampia kuin peruskoulun kisan tehtävät, ja jos en halua kuolla nälkään, niin minun tulee pärjätä vielä paremmin. Tämä tilanne toistui moneen kertaan: ”pärjäsin ihan hyvin edellisessä kilpailussa, mutta jos oikeasti haluan olla riittävän hyvä tehdäkseni matematiikkaa työkseni, niin minun pitää tulla paremmaksi, tai muuten jään työttömäksi ja kuolen nälkään.” En voi väittää, että ajatusmaailmani olisi nykyään kovinkaan erilainen.

Edelliset kappaleet luovat melko synkän kuvan; ikään kuin tekisin matematiikkaa vain, jotten kuolisi nälkään. Ensinnäkin ymmärsin kyllä, että ainakaan peruskoulussa tai lukiossakaan kukaan ei kuole nälkään, vaan yksi mahdollisuus on vain käydä koulua. En siis olisi aivan heti asumassa kadulla, vaikka epäonnistuisin jossain kilpailussa. Toiseksi minä tähtäsin matemaatikoksi tulemiseen ihan hyvästä syystä: minä tykkäsin matematiikasta.

Konkreettinen esimerkki ajatusmaailmastani liittyy lukion toisena vuonna tekemääni tutkielmaan.<sup>142</sup> Minulle oli ollut jo jonkin aikaa selvää, että haluaisin tehdä työni teoreettisesta matematiikasta. Minulla oli kuitenkin jonkinlaiset standardit työni laadun suhteen: en haluaisi tehdä mitään tylsää työtä, vaan siinä tulisi olla jotain uutta ja mielenkiintoista. Tästä syystä aloitin työn aiheen pohtimisen ja projektin työstämisen suhteellisen aikaisin. Osittain standardieni, työn vaativuuden ja kiinnostukseni takia projektiin kului todella paljon aikaa. Lopputuloksena työ menestyi loistavasti tutkielmakilpailuissa. Tämä on malliesimerkki negatiivisen ja positiivisen motivaattorin yhdistelmän tehokkuudesta minun kohdallani.

Ymmärsin vasta lukiossa, että työpaikan saaminen ei välttämättä vaadi huippuosaamista jollain alalla ja että muut eivät oikeastaan ajattele samalla tavalla kuin minä. Muita ihmisiä ei pelottanut nälkään kuoleminen, ja monet eivät halunneet mitään yhtä paljon kuin minä matematiikan osaamista.

Osittain ajatusmaailmaani sekoittivat tunnetut lausahdukset ”verta, hikeä ja kyyneliä” ja ”tuhansia tunteja töitä”. Kun aloitin matematiikkakilpailujen tekemisen, minusta ei tuntunut, että tekisin työtä<sup>143</sup> – työhän on määritelmän mukaan (silloisen

<sup>141</sup>Nälkäkuolema voi kuulostaa tässä vitsiltä, mutta minulla oli oikeasti aika lailla tällainen ajatusmaailma. Tietenkään en aktiivisesti pelännyt nälkään nääntymistä, mutta ajatus oli mielessäni.

<sup>142</sup>Tutkielmakilpailun sivut: <https://tukoke.tek.fi/>.

<sup>143</sup>Matematiikka eroaa hieman monista urheilulajeista: esimerkiksi tenniksessä kaikki harjoittelu ei tapahdu tenniskentällä. Vahvasti kärjistäen tenniksessä joutuu siis tekemään ikäviä, tennik-

minäni mielestä) tylsää ja ikävää. Ajattelin, että muut tekivät paljon enemmän työtä, ja minä tein tätä vain ohimennen huvikseni. Jälkeenpäin olen todennut, että lainaukset antavat virheellisen kuvan harjoittelusta. On totta, että olen viettänyt tuhansia tunteja matematiikan parissa, mutta en missään nimessä käyttäisi sanaa ”työ” aktiviteettien kuvailemiseen. Minä todellakin nautin siitä, mitä teen! Ja vaikka joskus tulee vaikeita hetkiä ja turhautumista, niin ”työni” ei silti tunnu vastenmieliseltä.

---

Lisätty myöhemmin: Yllä keskityin (ehkä hieman yksipuolisesti) omiin mielenmaisemiini, mutta on paikallaan mainita myös ulkoisten tekijöiden tärkeys. Äitini oli hyvinkin kannustava, ja hänen on kiittäminen monista enemmän tai vähemmän matematiikkaan liittyvistä virikkeistä, joita minulla on ollut nuoresta lähtien, kuten pulmakirjat ja pitkään kestänyt shakkiharrastus. Lisäksi ala-asteen opettajani tarjosi minulle kiinnostavia lisätehtäviä saatuaani kirjan tehtävät tehtyä.

Eli vaikka minulla oli jo pienestä pitäen synnynnäistä kiinnostusta matematiikkaa kohtaan, on itsestäni riippumattomilla tekijöillä ollut valtava vaikutus kiinnostukseni jatkumiseen ja kasvamiseen. Ikävää on tietysti se, että kaikilla ei ole läheskään samankaltaisia mahdollisuuksia. Valoinen puoli on se, että vanhemmat ja opettajat pystyvät itse vaikuttamaan asiaan.

Maunulan yhteiskoulun sivuilla on kerrottu matematiikkaharrastajan polusta, joka osuu mielestäni naulan kantaan: <https://www.mayk.fi/matematiikkalukio/kehitys/matematiikkaharrastajan-polku/>

## 25.3 Mistä kehittyminen koostuu?

Sain hopeaa vuoden 2019 Kansainvälisissä matematiikkaolympialaisissa. Miksen kyennyt samaan suoritukseen jo vuoden 2017 olympialaisissa? Lyhyt ja sisällötön vastaus: olin kehittynyt näiden kahden vuoden aikana. Oleellista on tietysti se, miten olin kehittynyt. Mitä sellaisia asioita vuoden 2019 Olli osasi, joita vuoden 2017 Olli ei osannut?

Yksi tärkeimmistä taidoista, mielestäni jopa tärkein, on kyky keksiä monenlaisia eri ideoita. Vuonna 2017 ollessani IMOssa sain ratkaistua tehtävät 1 ja 4,<sup>144</sup> mutta tämäkään ei tullut helposti: tehtävää 4 ratkoessani juutuin pitkäksi aikaa, koska en keksinyt juurikaan ideoita, joilla tehtävän saisi ratkaistua. Tehtävään 2 minulla oli yksi järkevä idea, josta sainkin pisteitä, mutta tie päättyi tähän. Tehtävään 5 minulla ei ollut mitään ideoita.

Vuonna 2019 tehtävän 2 ratkaisemiseen minulta kului pari tuntia. Tämän parin

---

seen liittymättömiä asioita, kun taas matematiikassa voi keskittyä aina olennaiseen. Tämä voi lisätä tenniksessä huipulle pääsemiseen vaadittavaa kiinnostuksen määrää. Toisaalta tenniksestä huippukiinnostuneelle harjoittelu, joka ei ole puhtaasti tenniksen peluuta, lienee vähintäänkin siedettävää.

<sup>144</sup>Lukijan ei tarvitse tietää tekstiä lukiessaan, mistä tehtävistä tarkalleen on kyse. Tehtävien numeroiden on tarkoitus kertoa, kuinka mones (ja kuinka vaikea) tehtävä kyseessä on. Tehtävät 1 ja 4 ovat kahden kilpailupäivän ensimmäiset ja helpoimmat tehtävät, tehtävät 2 ja 5 ovat keskivaikeita ja tehtävät 3 ja 6 ovat vaikeita.

tunnin aikana keksin ja kokeilin lukuisia eri ideoita tehtävän ratkaisemiseksi, ja lopulta löysin jotain, jolla tehtävä ratkesi. Idea ei ollut niin vaikea, etteikö vuoden 2017 Olli olisi mitenkään voinut keksiä sitä, mutta vuoden 2017 Olli olisi varmaankin jumittunut yhteen toimimattomaan ideaan, eikä siksi olisi saanut tehtävää ratkaistua.

Toinen tärkeä taito, joka liittyy edelliseen kohtaan, on kyky arvioida idean toimivuutta. Vuonna 2017 yritin pitkän aikaa ratkaista tehtävää 2 lähestymistavalla, joka ei yksinkertaisesti toiminut. Vuonna 2018 minulla oli tehtävään 2 toimiva idea, mutten syystä tai toisesta uskonut siihen riittävästi ja alkanut oikeasti ratkomaan tehtävää. Vuonna 2019 minulla oli tehtävään 5 idea, jonka tiesin toimivan. Lähestymistapa vaati paljon laskemista ja uskoa siihen, että idea toimii, mutta sain vietyä ratkaisun loppuun.

Kolmas tekijä on nopeus. Vuonna 2017 minulta kului yli puolet toisesta kilpailupäivästä tehtävän 4 ratkaisemiseen, kun taas vuonna 2019 sain tehtävän 1 tehtyä ensimmäisten kymmenen minuuttin aikana. (Olin melko nopea muihinkin kilpailijoihin verrattuna.) Olenkin kuullut sanottavan, että parhaat IMO-kilpailijat käyttävät viisi minuuttia päivän ensimmäiseen tehtävään, vartin toiseen tehtävään ja loppuajan viimeiseen tehtävään. Tässä on ehkä hieman liioittelua, muttei niin paljon kuin voisi kuvitella.

Vahvat kisaajat ovat nopeita monestakin syystä, mutta ehkäpä merkittävimmät ovat rutiini ja intuitio. Monet helpot tehtävät ovat rutiininomaisia siinä mielessä, että ne ratkeavat yhdellä yleisimmistä ideoista tai ratkaisumenetelmistä, jotka tulevat hyvältä kisaajalta selkäytimestä. Toisaalta taas jos tarvitsee keksiä jotakin vaikeampaa, niin paljon harjoitelleen kilpailijan kehittynyt intuitio kertoo, mistä suunnasta kannattaa lähteä liikkeelle.

Vielä yksi tekijä on itseluottamus. Aloittaessani kilpailujen parissa ajattelin liian usein, etten voisi saada jotain tehtävää ratkaistua, koska en tiedä riittävästi matematiikasta. Hämmästyin toistuvasti huomattessani, että minähän tiesin kaikki tarvittavat asiat, mutta vika olikin ongelmanratkaisutaidoissani. Itseluottamus on tärkeää: monesti tehtäviä ratkoessa tilanne voi hetkellisesti näyttää pahalta (erityisesti laskennallisissa tehtävissä), ja vaatii itseluottamusta olla välittämättä tästä ja viedä ratkaisu maaliin.

---

Loppukommentti: Yksi tapa kuvailla kehittyntä ongelmanratkaisutaitoani on, että osaan katsoa ongelmaa kauempaa, tunnustella sitä ja miettiä rauhassa lähestymistapaa. Aiemmin ehkäpä vain kokeilin sokeasti jotain satunnaista, ja jos idea ei toiminut, niin en miettinyt sen tarkemmin syytä idean toimimattomuudelle, vaan yritin vain jotain muuta. Kriittistä on ”kovien” taktiikoiden lisäksi soveltaa ”pehmeitä” ongelmanratkaisumenetelmiä: lue <https://usamo.wordpress.com/2019/05/03/hard-and-soft-techniques/>.

## 25.4 Kilpailumatematiikan hyöty

”Kilpailumatematiikasta ei ole hyötyä.”



Olen kuullut monenkin ihmisen sanovan näin. Aloittaessani kilpailumatematiikan parissa ajattelin ”ei se mitään, tämä on hauskaa”. Nykyään ajattelen ”kylläpä on, mutta ennen kaikkea tämä on hauskaa”.

Vähiten yllättävä hyöty kilpailumatematiikasta on se, että olen oppinut matematiikkaa. Vastaukseksi tähän olen kuullut ”en näe, miten klassisen geometrian oppiminen olisi hyödyllistä”.<sup>145</sup> Toki olen oppinut klassista geometriaa, mutta kilpailumatematiikassa on muutakin. Lempiosa-alueeni matematiikasta on lukuteoria, joten voisin nähdä itseni lukuteoreetikkona tulevaisuudessa. En siis sanoisi kilpailujen kautta oppimani lukuteorian olevan hyödytöntä.

Toisaalta kilpailuissa ei tarvitse kovin laajasti lukuteoriaa: lukuteoriaa on tutkittu pari vuosituhatta, ja kilpailuissa tarvittavan lukuteorian pystyy tiivistämään muutamaan kymmeneen sivuun. Kilpailumatematiikasta ei siis opi kovin syvällisesti teoriaa, eikä se ole kilpailujen tarkoituksaan (pikemminkin päinvastoin). Mielestäni kilpailumatematiikan paras anti on kehittyneet ongelmanratkaisutaidot.

Tilanne on siis tämä: Matematiikassa on (joltain osin) kyse ongelmien ratkaisemisesta. Tavoitteenani on ryhtyä isona matemaatikoksi. Auttaisi, jos kehittäisin ongelmanratkaisutaitojani. Kilpailumatematiikassa keskitytään ongelmanratkaisuun.<sup>146</sup> Minulle sanotaan, ettei kilpailumatematiikasta ole hyötyä.

Tuntuu naurettavalta, että joskus uskoin, ettei kilpailumatematiikasta olisi hyötyä.

Sen lisäksi, että kilpailumatematiikka motivoi matematiikan opiskelun ja ongelmanratkaisutaitojen kehittämisen, se on harrastus. Pidin matematiikasta ja sain kilpailupiirien kautta ympäristön, joka mahdollisti ja motivoi matematiikan harjoittelemisen. Tapasin muita kiinnostuneita, joilta opin ja joille opetin. Verkostoiduin ja tätä kautta hyödyin muutenkin kuin matemaattisesti.

Yksi esimerkki näistä hyödyistä on tutustuminen Päivölään, jossa myöhemmin suoritin lukion. Toinen esimerkki: sain kuulla tutkielmakilpailuista ja pääsin ympäristöön, joka mahdollisti ja motivoi matematiikan tutkimuksen tekemisen. Pääsin lähemmäksi haavettani matemaatikon urasta.

Edellä mainitut kilpailumatematiikan hyödyt koskevat enemmän tai vähemmän kaikki sen harrastajia: vaikkei tavoitteena olisikaan tutkijan ura, on ongelmanratkaisutaitojen kehittäminen silti hyvästä, ja harrastuksesta saa silti tuttuja.

Yksi henkilökohtaisempi ja vähemmän ilmeinen hyöty kilpailumatematiikasta minulle on motivaatio työntekoon. Pienenä minulle opetettiin, että koulut tulee käydä hyvin, koska hyvä koulutus johtaa hyvään elämään. Minä keskityin kyllä koulunkäyntiini, mutta kasvaessani takaraivossani alkoi itämään ajatus ”milloin näen työni hedelmät?” Jälkiviisaana voin todeta, ettei elämäni ole paljoakaan vaikuttanut se, että sain seitsemännellä luokalla puukäsitöistä arvosanan 8 tehtyäni ylitöitä koulun jälkeen.

Kilpailumatematiikan kautta olen päässyt tilanteeseen, jossa työntekoni laadulla

<sup>145</sup>Olen kuullut näitä kilpailumatematiikan vastaisia kommentteja harvakseltaan, mutta olen silti hieman hämilläni siitä, miksi jollakulla olisi jotakin kilpailumatematiikkaa vastaan.

<sup>146</sup>Vielä vahvemmin: IMO-kilpailijat ovat maailman parhaita ongelmanratkaisijoita ikäisistään.

ja määrällä on suora korrelaatio pärjäämiseeni ja saamiini palkkioihin. Näin oli kilpailuihin harjoitellessa ja tutkimuskilpailun projektia tehdessä, ja niin on nyt myös opiskellessani yliopistossa. Hyödyn työnteostani, ja työnteko tuntuu mielekkäältä, koska hyödyn siitä (ja tietysti koska työt koskevat matematiikkaa).

”Kilpailumatematiikasta ei ole hyötyä.” Entä jos olisin vastannut ”olet oikeassa, lopetan kilpailumatematiikan”? Mitä olisin tehnyt ylimääräisellä ajallani? Harrastanut jotain ”hyödyllistä”? Kuten mitä?

Yksi minulle kohdennettu kommentti kuului ”opiskele oikeaa matematiikkaa” (viitaten yliopistoissa opiskeltavaan matematiikkaan). Tämä ei oikeastaan ole kovin huono idea. Olen toisaalta saanut kilpailumatematiikan kautta matemaattista kypsyystta ja ongelmanratkaisutaitoja, jotka puolestaan auttavat merkittävästi yliopisto-opinnoissa. Siis myös tästä näkökulmasta kilpailumatematiikan harjoittelu oli varsin hyvä valinta.

---

Toisenlaisesta aiheeseen liittyvästä näkökulmasta voi lukea täältä: <https://usamo.wordpress.com/2018/01/05/lessons-from-math-olympiads/>. Myös seuraavan linkin takaa löytyy aiheita sivuavia ajatuksia: <https://usamo.wordpress.com/2016/08/13/against-the-research-vs-olympiads-mantra/>.

## 26 Kiitokset

Valmennustapahtumat ja niissä järjestettävän opetuksen tarjoaa Suomen matemaattisen yhdistyksen valmennusjaosto. Kiitokset tästä kuuluvat koko valmennusjaostolle ja heidän panokselleen valmennustoiminnan mahdollistamiseksi sekä Opetushallitukselle toiminnan tukemisesta taloudellisesti. Kirjoittaja on kiitollinen Opetushallitukselle myös tämän kirjan kirjoittamisen tukemisesta.

En tietenkään olisi voinut kirjoittaa kirjaa, ellen olisi oppinut kilpailumatematiikkaa. Henkilökohtaiset kiitokset kuuluvat kaikille valmentajille, joiden opetuksessa olen vuosien mittaan ollut. Erityisesti haluan kiittää Otte Heinävaaraa, joka toimi minulle esikuvana ja jolta opin valtavasti ongelmanratkaisua.

Inspiraation lähteenä kirjalle toimi kisakoodauksen puolella vaikuttava Antti Laaksonen ja hänen materiaalinsa Kisakoodarin käsikirja. Kisakoodarin käsikirja tietysti auttoi minua harjoitellessani ohjelmointikilpailuihin, mutta se toimi myös esimerkkinä tälle kirjalle.

Monet valmennuksessa tutustumiini henkilöistä ovat tulleet minulle hyväksi ystäviksi. He ovat omalta osin motivoineet minua harjoittelemaan ja kilpailu-urani päätyttyä ryhtymään valmentajaksi. Lisäksi olen käynyt hyödyllisiä keskusteluja heidän kanssaan ja saanut opettamista ja kirjantekoa koskevaa palautetta.

Viimeisenä haluan kiittää Akseli Jussinmäkeä, johon myös tutustuin valmennuksen kautta. Hänen valtavan työpanoksensa, tuhansien kommenttien ja huolellisten korjausten myötä kirjasta kehittyi lukukelpoinen versio.