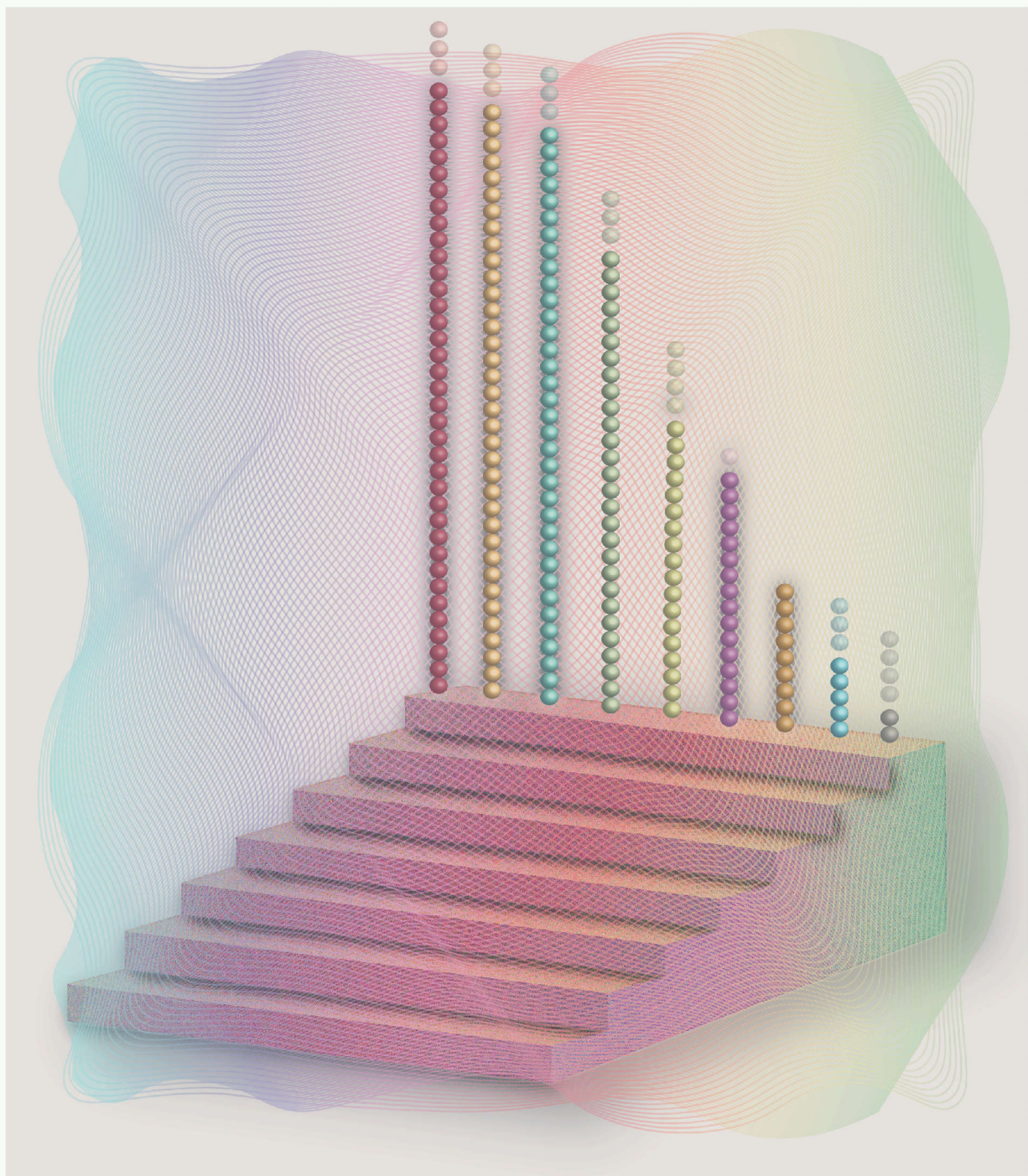


# S&LMU

MATEMATIIKKALEHTI 1/2022

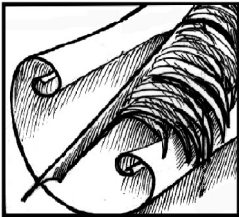
---

[matematiikkalehtisolmu.fi](http://matematiikkalehtisolmu.fi)



## Sisällys

|                                                                                                             |    |
|-------------------------------------------------------------------------------------------------------------|----|
| Pääkirjoitus: Kaavoja, laskemista, matematiikkaa ja munkinpaistoa (Anne-Maria Ernvall-Hytönen) .....        | 3  |
| Päättelyä ja laskemista (Juha-Matti Huusko) .....                                                           | 5  |
| Eduskuntavaalien suhteellisuusteoriaa – paikkajaosta ja sitä säätelevistä normeista (Jukka Liukkonen) ..... | 7  |
| Matematiikkaan innostaminen – inspiraatiota Integraalipäiviltä (Otso Huuska) .....                          | 15 |
| Keplerin naimahuolet – optimaalinen pysäyttäminen (Markku Halmetoja) .....                                  | 17 |
| George Malaty 1944–2022 (Marjatta Näätänen) .....                                                           | 19 |
| Näennäisen triviaalit temput matematiikassa (Anne-Maria Ernvall-Hytönen) .....                              | 23 |



## Kaavoja, laskemista, matematiikkaa ja munkinpaistoa

### *Pääkirjoitus*

Penkkarien aikaan somessa herätti hämmästyystä penkkarivalokuva, jossa autoon ripustetussa lakanassa luki ”Man behöver int matematik för att räkna”, eli ”Matematiikkaa ei tarvita laskemiseen”. Hämmästyks liittyi siihen, että eikö tosiaankaan matematiikkaa tarvita laskemiseen. Toki tiedossa oli, että virke oli penkkarilakanasta, joissa vuosien varrella on ollut erilaisia provosioivia ja raflaavia toteamuksia, joita ei ehkä ole tarkoitettu otettavan kovin vakavasti.

Hufvudstadsbladetista kuitenkin selvisi, että kyseessä ei ollutkaan kokonainen virke, vaan osa lausetta, jonka loppuosa oli rajautunut valokuvasta pois: ”Man behöver int matematik för att räkna promille.” Kyseessä ei ollutkaan kokonaisvaltainen matematiikan ja laskemisen yhteyden kyseenalaistaminen vaan vain sen kyseenalaistaminen, tarvitaanko matematiikkaa promillen laskemiseen. Veikkaisin tekstin viittaavan alkoholi-liittännäisen promillen laskemiseen, eikä esimerkiksi sen selvittämiseen, mikä on promille Suomen bruttokansantuotteesta. Viittaus on siis itse asiassa laskuun, jossa usein vain sijoitetaan kaavaan ilman suurempaa pohdintaa. Moni matematiikkaan intohimoisesti suhtautuvakin voisi olla ihan samaa mieltä siitä, että kyseessä ei todellakaan ole kunnollinen matematiikka, vaan mahdollisesti esimerkiksi laskento, mitä toki sitäkin matematiikassa tarvitaan.

Matematiikkaa on paljon muutakin kuin vain laskemista, ja ennen kaikkea muuta kuin laskemista. Matematiikkaan liittyy myös esimerkiksi vastauksen mielekkyyden tarkastelu. Yksinkertaisimmillaan se voisi tarkoittaa tätä: jos laskee Suomen bkt:sta promillen kokoisen osuuden ja päätyy siihen tulokseen, että saman ver-

ran rahaa löytyy omalta pankkitililtä, niin joko on yksi poikkeuksellisen rikkaista ihmisistä tai sitten on tehnyt laskuvirheen.

Omiin vapputraditioihini liittyy munkkien paistaminen ja ylioppilaskokeiden sensorointi. Sensoroin myös sinä aikana, kun munkit porisevat padassa. Oleellista on valita tehtävä, johon on lyhyitä ratkaisuja niin, että aina muutaman ratkaisun luettuaan vilkaisee kattilaan, kääntää munkit, muutaman ratkaisun jälkeen ottaa munkit kattilasta ja pistää uudet neljä munkkia tilalle ja jatkaa samoin. Asiat etenevät ja kaikki sujuu. Ainakin ideaalimaailmassa. Totuus nimittäin helposti on se, että sensori on vähän liian innoissaan ratkaisuisista ja unohtaa muutaman ratkaisun välein vilkaista kattilaan. Tällöin munkit saattavat muuttua jonkin verran tummemmiksi kuin oli tarkoitus. Ryhdyinkin ker- ran miettimään, mikä on realistinen todennäköisyysjakauma sille, millä hetkellä muistan ottaa munkit kattilasta. Ensimmäinen veikkaukseni oli, että kyseessä on jonkinlainen normaalijakauma, jossa on mahdollisesti katkaistut hännät tai vähintään hyvin nopeasti kape- nevat hännät, eli pieni keskihajonta. Tämän voi selittää sillä, että tuntuu sitä epätodennäköisemmältä hetkel- tä kääntää munkkeja mitä kauempana optimaalisesta hetkestä ollaan, erityisesti tuntuu varsin epätodennä- köiseltä, että edes hajamielinen sensori jättäisi munkit pataan tunniksi ja onnellisena sensoroisi vieressä. Ide- aalimaailmassa tästä varmasti saisi hyvän jakauman, jolla voisi laskea vaikka mitä. Täysin toinen asia onkin se, olisiko laskuissa mitään järkeä.

Kuten yleensäkin ongelmanratkaisussa, ideaalimallia kannattaa tarkastella kriittisesti. Ensimmäinen kysy-

mys on tämä: onko oikeasti realistista, että munkinpais-topadan vieressä sensoroiva sensori käretyttäisi munkit, eikä esimerkiksi sensorin nenä sanoisi kattilassa tapahtuvan jotain outoa jo siinä vaiheessa, kun munkit olisivat vasta tummanruskeita, eivät mustia?

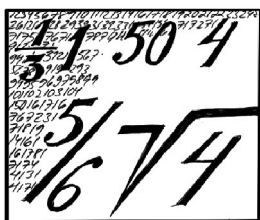
Jos oletettaisiin, että sensori todella olisi niin todellisuudesta vieraantunut, että normaalijakauma itse asiassa olisi tilannetta hyvin kuvaava jakauma, niin mielenkiintoista olisi pohtia, millä todennäköisyydellä esimerkiksi 32 munkin taikinasta kärehtää tasan yksi tai esimerkiksi korkeintaan kymmenen munkkia.

Tässä vaiheessa vain laskemalla ja vain kaavoja soveltamalla menisi helposti metsään. Oleellista on muistaa se, että padassa on kerrallaan neljä munkkia. Jos siis käy niin onnettomasti, että sensori unohtuu lukemaan ratkaisuja ja munkit mustuvat, niin munkkeja menee pilalle neljä kappaletta kerrallaan. Tässä tapauksessa ei siis todellakaan voi laskea niin, että jos neljän munkin kärehtämistodennäköisyys on  $q$ , niin yhden munkin kärehtämistodennäköisyys on  $\sqrt[4]{q}$ . Tasan yhden munkin kärehtämistodennäköisyys onkin (suurin piirtein) nolla. Jos taas halutaan tietää, millä todennäköisyydellä kärehtää korkeintaan kymmenen munkkia, on laskettava todennäköisyys sille, että kärehtää 0, 4 tai 8 munkkia. Muut vaihtoehdot ovat mahdottomia.

Yllä oleva esimerkki voi olla absurdi tai naiivi, mutta siinä kuvastuu yksinkertaisella tavalla osa siitä, mikä minusta matematiikassa on oleellista: pohdinta ja järjestyys. Ei vain lasketa, vaan mietitään millainen asetelma on, mitä oikeasti tiedetään, ja pohditaan lisäksi onko lopputulos mielekäs. Kun esimerkiksi yllä olevien tietojen lisäksi hyödynnetään lisätietoa, että allekirjoittanut ei ole koskaan polttanut yhtään munkkia, voi hyvällä syyllä todeta, että alkuperäinen todennäköisyysjakauma luultavasti oli virheellinen. Toinen asia on tietysti se, oliko koko pohdinnassa yhtään mitään järkeä.

Anne-Maria Ernvall-Hytönen





## Päättelyä ja laskemista

**Juha-Matti Huusko**

Itä-Suomen yliopisto

juha-matti.huusko@uef.fi

Matematiikan ongelmia ratkottaessa tarvitaan usein sekä päättelyä että laskemista. Työvaiheet ovat siinä mielessä toisiaan täydentäviä, että jos päättelee enemmän, jää laskettavaa vähemmän.

Tarkoitan päättelyllä tässä yhteydessä sitä, että ongelmasta tunnustetaan ominaisuuksia, joilla ongelmaa voidaan yksinkertaistaa. Tällaisten ominaisuuksien tunnustaminen ei aina onnistu. Päättely vaatii siis mielikuvitusta ja kekseliäisyyttä.

Suoraviivaiset laskut ovat usein pitkiä, mutta niissä pärjää vähemmällä mielikuvituksella. Kunhan ratkaisutapa on tuttu, niin tietää, että pitkän laskeskelun lopuksi saa palkinnoksi ratkaisun selville.

Tarkastellaan esimerkkinä polynomitehtävää, jonka esitin ensimmäisen vuoden opiskelijoille syksyllä 2021.

**Tehtävä.** Etsi toisen asteen polynomi  $p$ , jonka kuvaaja  $p(x) = y$  kulkee pisteiden  $(1, 4)$ ,  $(3, 4)$  ja  $(4, 7)$  kautta.

Jotta ratkaisussa pääsee alkuun, täytyy palauttaa mieleen, millainen toisen asteen polynomin lauseke on. Lausekkeenhan tosin pystyi kirjoittamaan muutamassa eri muodossa: aukikirjoitettuna, tekijöiden tulona tai neliöön täydennettynä. Muitakin muotoja taisi olla.

Annetuissa lähtötiedoissa pistävät silmään pisteet  $(1, 4)$  ja  $(3, 4)$ . Näillähän on sama  $y$ -koordinaatti! Voisiko tätä käyttää jotenkin hyväksi?

Aloitetaan yksinkertaisimmasta ratkaisutavasta.

**Ratkaisu 1.** Siis  $p(x) = ax^2 + bx + c$ . Saadaan yhtälöryhmä

$$\begin{cases} p(1) = a + b + c = 4 & | & R_1 \\ p(3) = 9a + 3b + c = 4 & | & R_2 \\ p(4) = 16a + 4b + c = 7 & | & R_3 \end{cases},$$

josta voidaan ratkaista **kolme** tuntematonta  $a$ ,  $b$  ja  $c$ .

Lasketaan. Gaussin eliminoinnilla saadaan

$$\begin{cases} a + b + c = 4 & | & R_1 \\ -6b - 8c = -32 & | & R'_2 \leftarrow R_2 - 9R_1 \\ -12b - 15c = -57 & | & R'_3 \leftarrow R_3 - 16R_1 \end{cases}$$

ja edelleen

$$\begin{cases} a + b + c = 4 & | & R_1 \\ 3b + 4c = 16 & | & R''_2 \leftarrow -\frac{1}{2}R'_2 \\ c = 7 & | & R'_3 \leftarrow R'_3 - 2R'_2 \end{cases}.$$

Siis  $c = 7$  ja

$$b = \frac{16 - 4c}{3} = -4$$

ja  $a = 4 - b - c = 1$ .

Toisessa ratkaisutavassa voidaan käyttää hyödyksi pisteitä  $(1, 4)$  ja  $(3, 4)$ , jotka sattuvat tässä tehtävässä olemaan erikoisia.

**Ratkaisu 2.** Polynomin  $p$  kuvaaja  $p(x) = y$  on ylöspäin tai alaspäin avautuva paraabeli. Tällainen paraabeli on symmetrinen jonkin pystysuoran suhteen.

Pisteillä  $(1, 4)$  ja  $(3, 4)$  on yhtä suuri  $y$ -koordinaatti, joten näiden pisteiden keskinormaali  $x = 2$  on mainittu paraabelin symmetria-akseli. Siis polynomin kuvaaja on paraabeli, jonka huippu on suoralla  $x = 2$ , joten  $p(x) = A(x - 2)^2 + B$ . Pisteiden  $(1, 4)$  ja  $(4, 7)$  avulla saadaan määrättyä **kaksi** tuntematonta  $A$  ja  $B$ .

Sijoitetaan annettuja pisteitä kaavaan  $p(x) = y$ , saadaan

$$\begin{cases} p(1) = A + B = 4 \\ p(3) = A + B = 4 \\ p(4) = 4A + B = 7 \end{cases}.$$

Lasketaan. Nähdään, että ensimmäinen ja toinen yhtälö ovat samoja. Tämä johtuu siitä, että pisteitä  $(1, 4)$  ja  $(3, 4)$  käytettiin jo hyväksi huipun paikkaa määrätessä. Vähentämällä kolmannesta yhtälöstä ensimmäinen saadaan  $3A = 3$  eli  $A = 1$ . Nyt ensimmäisen yhtälön perusteella  $B = 4 - A = 3$ . Siis

$$p(x) = (x - 2)^2 + 3 = x^2 - 4x + 7.$$

Kolmannessa ratkaisutavassa pisteitä  $(1, 4)$  ja  $(3, 4)$  voidaan käyttää hyväksi vielä vähän nokkelammin.

**Ratkaisu 3.** Polynomi on  $p(x) = 4 + q(x)$ , missä  $q(1) = q(3) = 0$ . Siis  $p(x) = 4 + K(x - 1)(x - 3)$ . Tuntematon **yksi** vakio  $K$  saadaan selville pisteen  $(4, 7)$  avulla.

Pisteistä  $(1, 4)$  ja  $(3, 4)$  ei ole nyt hyötyä: kaava  $p(x) = 4 + K(x - 1)(x - 3)$  tuottaa arvoilla  $p(1) = p(3) = 4$ , mikä jo tiedetään.

Lasketaan. Käyttämällä pistettä  $(4, 7)$  hyödyksi saadaan

$$p(4) = 4 + K \cdot 3 \cdot 1 = 7,$$

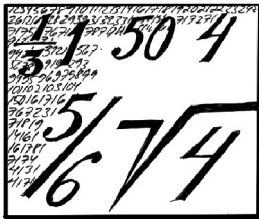
joten  $K = 1$ . Siis  $p(x) = x^2 - 4x + 7$ .

**Johtopäätös.** Mitä enemmän päättelee, sitä vähemmän laskemista jää. Ratkaisussa 1 täytyi selvittää kolme tuntematonta. Ratkaisussa 3 tuntemattomia oli enää vain yksi.

Mainittakoon, että voidaan myös löytää kaava, joka antaa suoraan polynomin lausekkeen, kun siihen sijoitetaan annettujen pisteiden  $x$ - ja  $y$ -koordinaatit. Tällainen kaava voidaan antaa useassa eri muodossa, kuitenkin sen löytäminen ei ole aivan helppoa.

Päätely vaatii mielikuvitusta ja keksimistä. Oikean niksien keksiminen on hyvin palkitsevaa. Samoin, jos voi ajatella ongelmaa "laatikon ulkopuolelta". Jätetään pohdittavaksi toinen tehtävä.

**Tehtävä 2.** Etsi toisen asteen polynomi  $p$ , jonka kuvaaja kulkee pisteiden  $(1, 4)$ ,  $(3, 3)$  ja  $(4, 7)$  kautta. Voitko löytää useamman kuin yhden tällaisen polynomin?



# Eduskuntavaalien suhteellisuusteoriaa – paikkajaosta ja sitä säätelevistä normeista

**Jukka Liukkonen**

Mat. yo. evp.

## Johdanto

Suomessa järjestettiin ensimmäiset eduskuntavaalit vuonna 1907. Suomi oli tuolloin vielä Venäjän keisarikunnan autonominen suuriruhtinaskunta, joka vasta kymmenen vuotta myöhemmin, vuonna 1917, muuttui itsenäiseksi valtioksi. Eduskuntavaalit ovat alusta lähtien noudattaneet *suhteellista vaalitapaa*, so. edustajapaikat jakautuvat, tai niiden ainakin periaatteessa pitäisi jakautua, puolueille samalla tavalla kuin vaaleissa saadut äänet. Paikkojen jakaminen maantieteellisten vaalipiirien kesken tehdään sekin suhteellisuusperiaatetta noudattaen. Jaon perusteena on vaalipiirin alueella asuvien Suomen kansalaisten lukumäärä. Vaalien suhteellisuudesta ja vaalipiirijaosta on säädetty Suomen perustuslaissa ([2], 25 §).

Laskennallisesta näkökulmasta eduskuntavaalien toteutus perustuu kahteen johtavaan menetelmään. Eduskuntapaikkojen jaossa vaalipiireille käytetään *Hare-Niemeyerin menetelmää*. Kansanedustajien paikat vaalipiirin sisällä jaetaan puolueille<sup>1</sup> ja ehdokkaille *D'Hondtin*<sup>2</sup> *menetelmällä*.<sup>3</sup>

Varsinkin jälkimmäistä on kritisoitu sen takia, että pienissä vaalipiireissä pienten puolueiden on vaikeaa saada

ehdokkaitaan eduskuntaan. Kritiikki on osittain perusteltua, mutta itse vaalipiirijako on ylivoimaisesti suurin syyllinen. Tämä on helppoa ymmärtää äärimmäisen esimerkin kautta: jos vaalipiirejä pienennettäisiin niin, että kustakin piiristä valittaisiin vain yksi kansanedustaja, ainoastaan suurin puolue saisi edustajanpaikan.

Äänten muuntaminen paikoiksi tarjoaa monenlaisia yllätyksiä. Pomminvarmaksi kuviteltu menetelmä saat-  
taa joissain tilanteissa antaa järjen tai oikeustajun vastaisia tuloksia. Pekka Alestalo käsittelee erään tapauksen hausassa Solmu-artikkelissaan [1].

## Äänet, kvootit ja paikat

Artikkelin loppuosassa tarkastellaan yleistä tilannetta, jossa  $\Sigma$  paikkaa jaetaan  $P$  puolueen kesken äänimäärien  $V_1, \dots, V_P$  perusteella. Kaikki tässä mainitut luvut ovat positiivisia kokonaislukuja. Puolueiden  $1, \dots, P$  paikkamäärät  $S_1, \dots, S_P$  ovat ei-negatiivisia kokonaislukuja. Paikkojen ja äänien kokonaismäärät ovat

$$S = S_1 + \dots + S_P, \quad V = V_1 + \dots + V_P.$$

Lopullisen paikkajaon on toteutettava ehto  $S = \Sigma$ . Vaatimus vaalien suhteellisuudesta tarkoittaisi ihanne-

<sup>1</sup>Yksinkertaisuuden vuoksi tässä artikkelissa kutsutaan *puolueiksi* vaaliliittoja, vaaliliittojen ulkopuolisia puolueita, yhteislistoja ja yhteislistoihin kuulumattomia valitsijayhdistyksiä.

<sup>2</sup>D'Hondt-sukunimen kirjoitusasu on varmistettu Kotimaisten kielten keskukselta.

<sup>3</sup>Aluevaaleissa kunkin hyvinvointialueen aluevaltuustopaikat jaetaan D'Hondtin menetelmällä (vaalilaki [3], 143 l §, 88–91 §). Menetelmä on käytössä niin ikään kunta- ja europarlamenttivaaleissa (vaalilaki [3], 91 §, 179 §).

tilanteessa yhtälöiden

$$\frac{S_p}{\Sigma} = \frac{V_p}{V}, \quad p = 1, \dots, P$$

voimassaoloa. Kuitenkin kysymys on kokonaislukujen osamäärien yhtäsuuruudesta, ja sellainen toteutuu vain harvoissa poikkeustapauksissa. Puolueelle  $p$  suhteellisuusperiaatteen mukaan siunaantuva täsmällinen paikkamäärä eli **kvootti**<sup>4</sup> (engl. *quota*)

$$Q_p = \frac{V_p}{V} \Sigma$$

ei yleensä olekaan kokonaisluku. Periaatteen toteuttamisyrittäminen merkitsee sellaisen paikkajaon etsimistä, että lukujonot

$$\mathbf{S} = (S_1, \dots, S_P) \quad \text{ja} \quad \mathbf{Q} = (Q_1, \dots, Q_P)$$

muistuttavat toisiaan mahdollisimman paljon. Ennen paikkojen laskemista on sovittava siitä, mitä tuo toisaan muistuttaminen tarkoittaa.

Lukujonoja kutsutaan vastedes **vektoreiksi**. Kvoottivektorin  $\mathbf{Q}$  ja paikkajaon  $\mathbf{S}$  laskenta edellyttää **äänisaalisvektorin**

$$\mathbf{V} = (V_1, \dots, V_P)$$

tuntemista. Varsinkin numeerisia vektoreita merkitään myös toisella tavalla, esimerkiksi

$$[2,5 \quad 4,1 \quad -1,7 \quad 12,0 \quad 7,9 \quad 1,1].$$

Vektorien nimet kirjoitetaan lihavoituina:  $\mathbf{V}$ . Niiden komponentit kuten myös muut skalaarit (so. luvut) kirjoitetaan lihavoimattomina:  $V_p$ . Vektorin nimi ilman lihavointia tarkoittaa vektorin komponenttien summaa, ellei asiayhteydestä ilmene muuta:

$$\mathbf{W} = (W_1, \dots, W_P), \quad W = W_1 + \dots + W_P.$$

## Hare-Niemeyerin menetelmä

Kvoottien summa on paikkojen kokonaismäärä:

$$Q_1 + \dots + Q_P = \Sigma.$$

Hare-Niemeyerin menetelmässä jokaiselle puolueelle  $p$  annetaan aluksi kvootin  $Q_p$  kokonaisosan ilmoittama määrä paikkoja. Tällöin yleensä muutama paikka jää jakamatta. Ne jaetaan murto-osien suuruuden perusteella. Puolueet asetetaan jonoon niin, että vastaavat murto-osat ovat laskevassa järjestyksessä, siis suurin ensin. Jonon alkupäästä lukien kullekin puolueelle annetaan yksi lisäpaikka, kunnes kaikki  $\Sigma$  paikkaa on jaettu. Jonon häntäpään puolueet eivät saa lisäpaikkoja. Periaate on selitetty ilman matemaattisia symboleja vaalilain [3] 6 §:ssä.

Menetelmässä yksi paikka vastaa äänimäärää  $V/\Sigma$ , jota sanotaan *Haren kvootiksi*. Koko äänisaalis tulee käytetyksi, mutta ei välttämättä sillä tavalla kuin yksittäinen äänestäjä on halunnut: loppuvaiheessa ääniä siirrellään puolueilta toisille suhteellisuuden nimissä. Vähän ääniä saanut puolue saattaa jäädä ilman paikkaa. Tällöin tehdään suuri suhteellinen virhe, itse asiassa äärettömän suuri.

## D'Hondtin menetelmä

Äänet voidaan käsittää valuutaksi, jolla puolueet ostavat paikkoja valtiolta. Paikkoja on myynnissä tasan  $\Sigma$  kappaletta, ja valtio haluaa myydä ne kaikki mahdollisimman suurella kappalehinnalla, joka on sama kaikille puolueille. Kaupan jälkeen yhdelläkään puolueella ei ole tarpeeksi valuuttaa yhdenkään lisäpaikan ostamiseen. Paikan kappalehinta saadaan selville asettamalla kussakin puolueessa ehdokkaat heidän saamansa äänimäärän mukaiseen laskevaan järjestykseen. Jokaiselle ehdokkaalle annetaan *vertausluku*. Eniten ääniä saaneen vertausluku on koko puolueen  $p$  äänimäärä  $V_p$  eli  $V_p/1$ , toiseksi eniten ääniä saaneen vertausluku on  $V_p/2$ , kolmannen vertausluku on  $V_p/3$  ja niin edelleen. Nimittäjät muodostavat lukujonon  $(1, 2, 3, \dots)$ . Kun jokaisen puolueen jokaisella ehdokkaalla on vertausluku, heidät voidaan laittaa pitkään jonoon vertausluvun mukaiseen laskevaan järjestykseen. Kansanedustajiksi otetaan jonon alkupäästä  $\Sigma$  ehdokasta. Edustajapaikan hinta on pienin vertausluku valituiksi tulneiden joukossa. Jos idea ei heti kirkastunut lukijalle, sitä kannattaa miettiä tovi. Periaate on selitetty vaalilain [3] 89 §:ssä.

Ehdokkaiden keskinäinen järjestys ratkaistaan arpomalla niissä tapauksissa, joissa kahdella saman puolueen ehdokkaalla on sama äänimäärä tai eri puolueiden ehdokkailla on sama vertausluku. Tästä on säädetty vaalilain [3] 90 §:ssä.

D'Hondtin menetelmässä kvootteja ei lasketa, eikä ääniä siirrellä puolueilta toisille. Ääniä jää tyypillisesti paljon käyttämättä. Paikan hinta voi tällöin olla selvästi pienempi kuin  $V/\Sigma$ . Puolue jää ilman edustajapaikkaa, jos sen kokonaisäänimäärä jää esimerkiksi yhden äänen vajaan paikan hinnasta.

## Suhteellisuuden mittareita

### Additiivisesta multiplikatiiviseen

Luvut 1 ja 2 ovat yhtä kaukana toisistaan absoluutisessa mielessä kuin luvut 1000 ja 1001, mutta suhteellisessa mielessä 1 ja 2 ovat huomattavasti kauempana toisistaan kuin 1000 ja 1001. Luvun 1 pitää kasvaa 100 % muuntuakseen luvuksi 2, mutta siirtymisen luvusta 1000 lukuun 1001 merkitsee vain 0,1 %:n

<sup>4</sup>Oikeusministeriön julkaisuissa käytetään tätä määritelmää kvootille. Termin merkityssisältö vaihtelee kirjallisuudessa.



muutosta. Perinteisesti suhteelliset erot on muutettu absoluuttisiksi eroiksi logaritmifunktiolla: luvun  $b$ -kertaistuminen merkitsee sen  $b$ -kantaisen logaritmin lisäystä vakiolla 1:

$$\log_b(bx) = \log_b(b) + \log_b(x) = 1 + \log_b(x)$$

riippumatta muuttujan  $x > 0$  arvosta. Samassa tilanteessa  $a$ -kantainen logaritmi kasvaisi vakiotermillä  $\log_a(b)$ .

Additiivisen maailman  $(\mathbb{R}, +, 0)$  olioilla ja operaatioilla on vastine multiplikatiivisessa suhdemaailmassa  $(]0, \infty[, \cdot, 1)$ . Siirtymän välittää eksponenttifunktio  $u \mapsto e^u = \exp(u)$ , ja siinä summa vaihtuu tuloksi, erotus osamääräksi, nolla ykköseksi, vastaluku käänteisluvuksi, vakiolla kertominen potenssiinkorotukseksi, aritmeettinen keskiarvo geometriseksi keskiarvoksi ja niin edelleen. Muunnoksen

$$\mathcal{M} : (\mathbb{R}, +, 0) \rightarrow (]0, \infty[, \cdot, 1)$$

toimintaperiaate ilmenee seuraavista esimerkeistä:

$$\begin{aligned}\mathcal{M}(u) &= e^u =: x, & \mathcal{M}(v) &= e^v =: y, \\ \mathcal{M}(0) &= e^0 = 1, & \mathcal{M}(u+v) &= e^{u+v} = e^u e^v = xy, \\ \mathcal{M}(u-v) &= e^{u-v} = \frac{e^u}{e^v} = \frac{x}{y}, \\ \mathcal{M}(au) &= e^{au} = (e^u)^a = x^a.\end{aligned}$$

### Skalaarin m-itseisarvo

Suhdemaailman lukujen vertaaminen keskenään aloitetaan määrittelemällä **multiplikatiivinen itseisarvo** eli **m-itseisarvo**  $\{x\}$  luvulle  $x > 0$ :

$$\{x\} = \begin{cases} x, & x \geq 1 \\ \frac{1}{x}, & 0 < x < 1. \end{cases}$$

M-itseisarvolla on useita esityksiä; esimerkiksi

$$\{x\} = \max\left(x, \frac{1}{x}\right) = e^{|\ln x|} = a^{|\log_a(x)|},$$

kun  $0 < x$  ja  $0 < a \neq 1$ . Havaitaan, että additiivisen maailman tutun identiteetin  $|u - v| = |v - u|$  tapaan m-maailmassa pätee

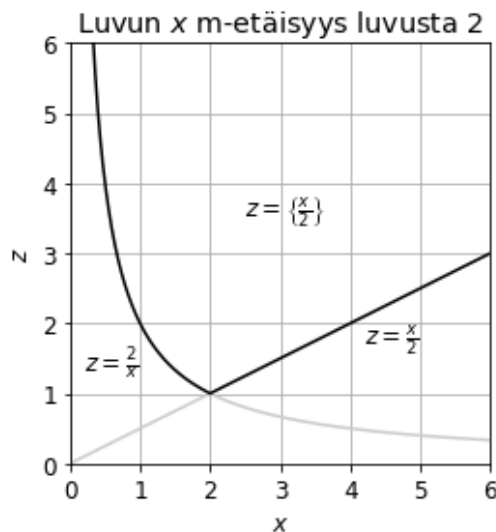
$$\left\{\frac{x}{y}\right\} = \left\{\frac{y}{x}\right\}.$$

Suhdemaailmassa kahden (positiivisen) luvun “etäisyys” toisistaan on isomman suhde pienempään. Tällöin etäisyys kasvaa, kun isompi isonee tai pienempi pienenee. Oheisessa kuvassa  $y = 2$ . Kun  $x$  on hyvin pieni positiivinen luku, m-itseisarvo  $\{x\}$  on hyvin suuri; itse asiassa

$$\{x\} = \frac{1}{x} \xrightarrow{x \rightarrow 0+} \infty,$$

kun  $0 < x < 1$ . Vaaleissa jotkut puolueet saattavat jäädä ilman paikkaa. Tätä tilannetta varten on kätevää sopia, että

$$\{0\} = \infty.$$



### Vektorin normi ja m-normi

Itseisarvo voidaan yleistää vektoreille  $\mathbf{u} = (u_1, \dots, u_n)$  monilla eri tavoilla. Tällöin puhutaan *vektorinormeista*. Ne kuvaavat vektorisuureen suuruutta. Additiivisessa maailmassa eniten käytetty normi on *kakkosnormi*

$$\|\mathbf{u}\|_2 = \sqrt{u_1^2 + \dots + u_n^2},$$

joka ilmoittaa vektorin Pythagoraan lauseen mukaisen pituuden  $n$ -ulotteisessa euklidisessa avaruudessa  $\mathbb{R}^n$ . Kakkosnormi, kuten kaikki normit, soveltuu myös vektorien eron mittaamiseen: vektorit  $\mathbf{u}$  ja  $\mathbf{v}$  muistuttavat toisiaan sitä enemmän, mitä lähempänä nollaa normin

$$\|\mathbf{u} - \mathbf{v}\|_2 = \sqrt{(u_1 - v_1)^2 + \dots + (u_n - v_n)^2}$$

arvo on. Tässä  $\mathbf{u} - \mathbf{v} = (u_1 - v_1, \dots, u_n - v_n)$ .

Additiiviset normit muunnetaan muunnoksella  $\mathcal{M}$  multiplikatiivisiksi **m-normeiksi**. Kun suhdemaailman vektori  $\mathbf{x}$  viedään käänteismuunnoksella  $\mathcal{M}^{-1}$  additiiviseen maailmaan vektoriksi  $\ln \mathbf{x} := (\ln x_1, \dots, \ln x_n)$ , lasketaan sen additiivinen kakkosnormi  $\|\ln \mathbf{x}\|_2$  ja palataan muunnoksella  $\mathcal{M}$  takaisin suhdemaailmaan, päädytään multiplikatiiviseen kakkosnormiin

$$\begin{aligned}\|\mathbf{x}\|_2 &= \exp(\|\ln \mathbf{x}\|_2) \\ &= \exp\left(\sqrt{(\ln x_1)^2 + \dots + (\ln x_n)^2}\right).\end{aligned}$$

Vektorin m-normi on mitta sille, kuinka paljon vektori suhdemielessä poikkeaa ykkösvektorista

$$\mathbf{1} = (1, \dots, 1).$$

M-kakkosnormin mukainen vektoreiden  $\mathbf{x}$  ja  $\mathbf{y}$  multiplikaatiivinen ero on

$$\left\{ \left\{ \frac{\mathbf{x}}{\mathbf{y}} \right\} \right\}_2 = \exp \left( \|\ln(\mathbf{x}/\mathbf{y})\|_2 \right) \\ = \exp \left( \sqrt{(\ln x_1 - \ln y_1)^2 + \dots + (\ln x_n - \ln y_n)^2} \right).$$

Vektoreiden osamäärä tulkitaan seuraavasti:

$$\frac{\mathbf{x}}{\mathbf{y}} = \left( \frac{x_1}{y_1}, \dots, \frac{x_n}{y_n} \right).$$

Laskutoimitukset tehdään vektoreille muutenkin komponentteittain, ellei toisin ilmoiteta. Myös tavanomaisten alkeisfunktioiden ( $\ln$  ym.) arvot vektoreille lasketaan komponentteittain.

### Normi- ja m-normiperheet

Additiivinen kakkosnormi on poiminta normiperheestä

$$\|\mathbf{u}\|_\kappa = (|u_1|^\kappa + \dots + |u_n|^\kappa)^{1/\kappa}, \quad \kappa \geq 1, \\ \|\mathbf{u}\|_\infty = \max(|u_1|, \dots, |u_n|).$$

Vastaavat multiplikaatiiviset normit ovat

$$\{\|\mathbf{x}\|_\kappa = \exp(\|\ln \mathbf{x}\|_\kappa) \\ = \exp\left((|\ln x_1|^\kappa + \dots + |\ln x_n|^\kappa)^{1/\kappa}\right), \\ \kappa \geq 1, \\ \{\|\mathbf{x}\|_\infty = \exp(\|\ln \mathbf{x}\|_\infty) \\ = \exp\left(\max(|\ln x_1|, \dots, |\ln x_n|)\right) \\ = \max(\{x_1\}, \dots, \{x_n\}).$$

Parametrilla  $\kappa \in [1, \infty]$  säädellään vektorin komponenttien keskimääräisen arvon ja huippuarvon painotusta. Esimerkiksi siirtyminen vektorista  $[1 \ 1 \ 7]$  vektoriin  $[3 \ 3 \ 3]$  ei vaikuta normin  $\|\cdot\|_1$  arvoon lainkaan (keskiarvo ei muutu), mutta  $\|\cdot\|_\infty$  pienenee arvosta 7 arvoon 3 (huippuarvo muuttuu). Mitä suurempi  $\kappa$ , sitä enemmän normi mittaa pelkästään vektorin suurimpia komponentteja. Rajanormi  $\|\cdot\|_\infty$  "näkee" ainoastaan suurimman komponentin.

Normia minimoitaessa on hyvä huomata, että additiivisen perheen normeista jokainen on itseisarvon  $|u_i| \geq 0$  kasvava funktio,  $i = 1, \dots, n$ . Vastaavasti m-normeista jokainen on m-itseisarvon  $\{x_i\} \geq 1$  kasvava funktio, sillä  $|\ln x_i| = \ln \{x_i\}$ .

Additiivisessa maailmassa erotuksen normi kuvastaa kahden vektorin, esimerkiksi paikkajako- ja kvoottivektorin, välisen eron suuruutta. Suhdemaailmassa eroa mitataan osamäärän m-normin avulla. Edustajapaikat jaetaan minimoimalla *tavoitefunktiota*

$$f_{\text{mul}}(\mathbf{S}) = \{\{\mathbf{S}/\mathbf{Q}\}\}_\kappa \quad \text{tai} \quad f_{\text{add}}(\mathbf{S}) = \|\mathbf{S} - \mathbf{Q}\|_\kappa$$

sen mukaan, halutaanko korostaa suhteellisuutta vai ei.

Multiplikaatiivisen tavoitefunktion lausekkeessa nähdään heti vaalien suhteellisuuden suurin ongelma: jokaisen puolueen pitää saada vähintään yksi paikka, muussa tapauksessa  $f_{\text{mul}}(\mathbf{S}) = \infty$ . Yksi paikka on tultava, vaikka puolue olisi saanut vain yhden äänen. Ongelmaan ei ole siistiä ratkaisua. On pakko sopia periaatteesta, jolla vähiten ääniä saaneita puolueita jätetään ilman paikkaa. Samalla suhteelliselle vaalitavalle heitetään hyvästit näiden puolueiden osalta. Äänikynnysten kehittämiseen ei puututa tässä artikkelissa.

### Paikkojen jakaminen puolueille

Muodollisesti kelvollisen paikkajaon  $\mathbf{S} = (S_1, \dots, S_P)$  on toteutettava seuraavat kriteerit:

- 1)  $0 \leq S_p \in \mathbb{Z}$  kaikilla  $p = 1, \dots, P$ ;
- 2)  $S_1 + \dots + S_P = \Sigma$ .

Tällaisten paikkajakojen joukossa  $\mathbb{S}$  on

$$\binom{\Sigma + P - 1}{\Sigma}$$

alkiota, sillä näin monella tavalla voidaan laittaa jonoon  $\Sigma$  kpl paikkoja ja  $P - 1$  kpl puoluerajoja. Äänestyksen jälkeen, kun äänisaalisvektori  $\mathbf{V}$  on selvillä, paikat jaetaan puolueille etsimällä joukosta  $\mathbb{S}$  alkio, joka parhaiten toteuttaa optimaaliselle paikkajaolle ennalta asetetut ehdot. Jos vaalipiirijako unohdetaan ja koko Suomi käsitetään yhdeksi vaalipiiriksi<sup>5</sup>, eduskuntavaaleissa  $P = 10$  ja  $\Sigma = 200$  ainakin suurin piirtein. Silloin mahdollisia paikkajakoja on noin  $1,76 \cdot 10^{15}$ . Niiden läpikäyminen yksi kerrallaan on liian suuri työ. Tarvitaan tehokkaampi algoritmi paikkajaon optimoimiseksi.

### Yleinen normiin perustuva paikkajakomenetelmä

Siirtyminen kvooteista paikkoihin merkitsee reaalityökalujen korvaamista kokonaisluvulla. Pyöristys alaspäin kokonaisluvuksi tehdään *lattiafunktion* (engl. *floor*) avulla. Lukujen kerrostalossa reaalityökalun  $x$  lattia  $\lfloor x \rfloor$  määritellään seuraavasti:

$$\lfloor x \rfloor = \max\{k \in \mathbb{Z} \mid k \leq x\}.$$

<sup>5</sup> Valtakunnan jakoa maantieteellisiin vaalipiireihin eduskuntavaaleissa voidaan kritisoida. Eduskunta on pääasiassa valtakunnallisia lakeja säätävä ja eräitä muita valtakunnallisia ja kansainvälisiä tehtäviä hoitava elin. Alue- ja kuntavaaleilla valitaan henkilöitä paikallisiin luottamustoimiin. Ahvenanmaalla on eduskuntavaaleissa erityisasema. Tässä artikkelissa tuota erityisasemaa ei oteta huomioon.

Vektorille lattia muodostetaan komponenteittain. Samoin vektorien suuruusvertailut tehdään komponenteittain. Esimerkiksi

$$\lfloor \mathbf{x} \rfloor = (\lfloor x_1 \rfloor, \dots, \lfloor x_n \rfloor),$$

$$\mathbf{x} < \mathbf{y} \Leftrightarrow x_i < y_i \text{ kaikilla } i = 1, \dots, n.$$

Jos paikkamäärien ei tarvitsisi olla kokonaislukuja, kvoottivektori olisi optimaalinen paikkajako. On melko yksinkertainen ja nopea tehtävä etsiä sellainen kokonaislukujono  $\tilde{\mathbf{S}}$ , joka käytetyn normin tai  $m$ -normin mielessä vähiten eroaa jonosta  $\mathbf{Q}$ . Tutkittavia vaihtoehtoja on vähän, sillä väistämättä

$$\lfloor \mathbf{Q} \rfloor \leq \tilde{\mathbf{S}} \leq \lfloor \mathbf{Q} + 1 \rfloor.$$

Vektori  $\tilde{\mathbf{S}}$ , jota jatkossa kutsutaan **näennäisratkaisuksi**, ei vielä välttämättä kelpaa paikkajaksi, sillä usein

$$\tilde{\mathbf{S}} = \tilde{S}_1 + \dots + \tilde{S}_P \neq \Sigma.$$

Siksi näennäisratkaisua on muutettava hieman. Muutetun vektorin  $\mathbf{S}$  ja kvoottivektorin  $\mathbf{Q}$  ero käytetyn normin tai  $m$ -normin mielessä on oltava minimaalinen ehdolla  $\mathbf{S} \in \mathbb{S}$ . Muutos tehdään lisäämällä näennäisratkaisuun keskenään samanmerkkisistä<sup>6</sup> kokonaisluvuita koostuva, ehdon

$$\mathbf{W} = \mathbf{W}_1 + \dots + \mathbf{W}_P = \Sigma - \tilde{\mathbf{S}}$$

toteuttava vektori  $\mathbf{W}$ . Optimaalisen vektorin  $\mathbf{W}$ , ja samalla optimaalisen paikkajaon

$$\mathbf{S} = \tilde{\mathbf{S}} + \mathbf{W},$$

löytäminen *brute force* -menetelmällä, so. tutkimalla kaikki vaihtoehdot, ei normaalisti ole liian raskas tehtävä, sillä  $|\mathbf{W}|$  on pahimmillaan luokkaa ”muutama”. Jos puolueita on kymmenen ja  $|\mathbf{W}| = 4$ , erilaisia vaihtoehtoja vektoriksi  $\mathbf{W}$  on 715 kpl. Eduskuntavaaleja muistuttavissa tuhansissa testiajoissa  $|\mathbf{W}|$  ei ylittänyt arvoa 3. Raakaa laskentavoimaa vieroksuva lukija suunnitteleen itse älykkään optimointialgoritmin.

Käytäessä läpi eri vaihtoehtoja saattaa paljastua, että optimaalisia paikkajakoja on useita. Optimointimenetelmää tai tavoitefunktiota voidaan pitää riittävän tarkkana, jos seuraava ehto on voimassa (*transpositio* tarkoittaa vektorin kahden komponentin vaihtamista keskenään):

**Optimoinnin tarkkuusehto:** jos  $\mathbf{S}$  ja  $\mathbf{S}'$  ratkaisevat optimointitehtävän, vektori  $\mathbf{S}'$  saadaan vektorista  $\mathbf{S}$  transpositioilla  $S_r \leftrightarrow S_t$ , missä  $Q_r = Q_t$ .

Ehdon tarkoittama tilanne syntyy, jos useampi puolue sattuu saamaan saman äänimäärän. Jotta paikkojen kokonaismääräksi saataisiin tasan  $\Sigma$ , jollekin näistä

puolueista saatetaan joutua esimerkiksi antamaan yksi ylimääräinen paikka, jota se ei äänimäärällään ansaitsisi. Kyseiset puolueet ovat symmetrisessä asemassa keskenään niin, että on laskennan ja tavoitefunktion arvon kannalta yhdenkertainen, mikä puolueista paikan saa. Käytännössä tällaiset tilanteet ratkaistaan arpomalla.

## Hare-Niemeyer, D'Hondt ja normit

Edellisessä kappaleessa esitetty paikkajakomenetelmä lähtee liikkeelle näennäisratkaisun  $\tilde{\mathbf{S}}$  määrittämisestä. Näennäisratkaisu sijaitsee aina joukossa

$$\{\mathbf{S} \mid \lfloor \mathbf{Q} \rfloor \leq \mathbf{S} \leq \lfloor \mathbf{Q} + 1 \rfloor\},$$

josta käytetään tässä työnimeä **kvoottivyö**<sup>7</sup>. On ilmeistä, että normin  $\|\mathbf{S} - \mathbf{Q}\|_\kappa$  minimointi kelvollisten paikkajakojen joukossa  $\mathbb{S}$  johtaa kvoottivyössä sijaitsevaan ratkaisuun. Lukija voi tämän tarkistaa. Myös Hare-Niemeyerin tuottama ratkaisu sijaitsee kvoottivyössä. Niin ikään on ilmeistä, että nämä ratkaisut yhtyvät, vieläpä parametrissa  $\kappa$  riippumatta. Täten Hare-Niemeyerilla aikaansaatu paikkajako on samalla optimointitehtävän

$$\min_{\mathbf{S} \in \mathbb{S}} \|\mathbf{S} - \mathbf{Q}\|_\kappa$$

ratkaisu.

D'Hondtin menetelmän huolellinen analyysi paljastaa, että se ratkaisee optimointitehtävän

$$\min_{\mathbf{S} \in \mathbb{S}} \|\mathbf{S}/\mathbf{Q}\|_\infty$$

siitäkin huolimatta, että menetelmässä kvootit eivät eksplisiittisesti ole käytössä. Huomaa, että yleensä

$$\|\mathbf{S} - \mathbf{Q}\|_\infty \neq \|\mathbf{S}/\mathbf{Q}\|_\infty \neq \|\{\mathbf{S}/\mathbf{Q}\}\|_\infty.$$

Täten D'Hondtin menetelmän tavoitefunktio poikkeaa muista tässä artikkelissa käsitellyistä tavoitefunktioista.

## Geometrinen menetelmä

Mikäli suhteellisuus on paikkajaon tärkein tavoite, paikkamäärien  $S_p$  ja kvoottien  $Q_p$  tulee olla mahdollisimman lähellä toisiaan  $m$ -normin mielessä. Makkosnormia käytettäessä tavoitefunktion

$$f(\mathbf{S}) = \left\{ \left\{ \frac{\mathbf{S}}{\mathbf{Q}} \right\} \right\}_2 = \exp(\|\ln(\mathbf{S}/\mathbf{Q})\|_2)$$

$$= \exp\left(\sqrt{(\ln S_1 - \ln Q_1)^2 + \dots + (\ln S_P - \ln Q_P)^2}\right)$$

<sup>6</sup>Nolla ajatellaan tässä samanmerkkiseksi kaikkien lukujen kanssa.

<sup>7</sup>Kvoottivyöksi kutsuttu joukko on itse asiassa  $P$ -ulotteisen avaruuden  $\mathbb{R}^P$  yksikkökuutio, joten yhtä hyvin voitaisiin puhua *kvoottikuutiosta*.

arvon tulee olla mahdollisimman pieni, mahdollisimman lähellä ykköstä. Paremman puutteesta tästä menetelmästä käytetään nimitystä **geometrinen menetelmä**.

### ▼ Esimerkki

Suomen eduskuntavaaleissa vuonna 2019 puolueet saivat ääniä ja paikkoja seuraavasti [5]:

| Puolue | SDP    | PS     | Kok    | Kesk   |
|--------|--------|--------|--------|--------|
| Äänet  | 546471 | 538805 | 523957 | 423920 |
| Osuus  | 18,3 % | 18,0 % | 17,5 % | 14,2 % |
| Paikat | 40     | 39     | 38     | 31     |
| Osuus  | 20,0 % | 19,5 % | 19,0 % | 15,5 % |

---

| Puolue | Vihr   | Vas    | RKP    | KD     | Muut  |
|--------|--------|--------|--------|--------|-------|
| Äänet  | 354194 | 251808 | 139640 | 120144 | 89582 |
| Osuus  | 11,9 % | 8,4 %  | 4,7 %  | 4,0 %  | 3,0 % |
| Paikat | 20     | 16     | 9      | 5      | 2     |
| Osuus  | 10,0 % | 8,0 %  | 4,5 %  | 2,5 %  | 1,0 % |

Jos koko valtakunta käsitettäisiin yhdeksi vaalipiiriksi, D'Hondtin, Hare-Niemeyerin ja geometrinen menetelmä antaisivat jokainen paikkajakoiksi

|        |        |        |        |
|--------|--------|--------|--------|
| SDP    | PS     | Kok    | Kesk   |
| 37     | 36     | 35     | 28     |
| 18,5 % | 18,0 % | 17,5 % | 14,0 % |

---

|        |       |       |       |       |
|--------|-------|-------|-------|-------|
| Vihr   | Vas   | RKP   | KD    | Muut  |
| 24     | 17    | 9     | 8     | 6     |
| 12,0 % | 8,5 % | 4,5 % | 4,0 % | 3,0 % |

Myös optimoinnin välivaiheena syntyvä näennäisratkaisu  $\hat{S}$  yhtyisi tähän. Nykyinen vaalipiirijako hyödyttää puolueita seuraavasti (negatiivinen hyöty on haitta):

|     |    |     |      |
|-----|----|-----|------|
| SDP | PS | Kok | Kesk |
| 3   | 3  | 3   | 3    |

---

|      |     |     |    |      |
|------|-----|-----|----|------|
| Vihr | Vas | RKP | KD | Muut |
| -4   | -1  | 0   | -3 | -4   |

Esimerkiksi Kristillisdemokraateilla siirtyminen nykyisestä paikallisesti (suhteellisen) suhteellisesta vaalitavasta valtakunnallisesti suhteelliseen vaalitapaan olisi viime vaaleissa merkinnyt paikkamäärän muutosta 5:stä 8:aan eli 60 %:n kasvua.

Lienee selvää, että vaalipiireistä ei luovuta. Arvatenkin ehkä  $40+39+38+31 = 148$  kansanedustajaa vastustaisi luopumista, ja korkeintaan  $20+16+9+5+2 = 52$  kansanedustajaa poistaisi vaalipiirijaon. Pelin säännöistä päätetään pelin säännöillä! Tarkkaavainen lukija saat-  
taa miettiä, onko tässä jokin periaatteellinen, looginen ristiriita. Ei siinä voi olla, sillä näin homma toimii käytännössä.

Kvoottivektorin

$$Q \approx [36,57 \ 36,06 \ 35,06 \ 28,37 \ 23,70 \ 16,85 \\ 9,35 \ 8,04 \ 6,00]$$

avulla saadaan laskettua valtakunnallinen mitta vuoden 2019 eduskuntavaalien suhteellisuudelle:

$$\left\{ \left\{ \frac{S_{2019}}{Q} \right\} \right\}_2 \approx 3,3926.$$

Ilman vaalipiirijakoa suhteellisuus olisi ollut

$$\left\{ \left\{ \frac{S}{Q} \right\} \right\}_2 \approx 1,0456.$$

Herää kysymys, onko perustuslakimme [2] kirjoitettu pilke silmäkulmassa vaalien suhteellisuusvaatimuksen osalta. ▲

## Suosiiko D'Hondtin menetelmä suuria puolueita?

Hare-Niemeyerin menetelmä on additiivinen, geometrinen menetelmä on multiplikatiivinen ja D'Hondtin menetelmä additiivisen ja multiplikatiivisen sekoitus. Näitä kolmea verrattiin keskenään simuloimalla eduskuntavaaleja. Testiaineisto käsitti 100 000 satunnaisesti generoitua vaalitulosta. Generoinnin lähtökohtana oli vuoden 2019 eduskuntavaalien tulos

$$\hat{V} = (\hat{V}_1, \dots, \hat{V}_9) \\ = (546471, 538805, 523957, 423920, 354194, \\ 251808, 139640, 120144, 89582), \\ \Sigma = 200.$$

Jokaiselle puolueelle  $p = 1, \dots, P = 9$  erikseen generoitiin uusi äänisaalis

$$V_p = \left\lfloor \text{rnd} \left( \frac{1}{2}, 2 \right) \hat{V}_p \right\rfloor,$$

missä  $\text{rnd}(1/2, 2)$  on puoliavoinnille välille  $[1/2, 2[$  tasaisesti jakautunut satunnaisluku. Tämä tehtiin 100 000 kertaa, ja jokaisella kierroksella laskettiin paikat kaikilla kolmella menetelmällä.

Kierroksien joukossa oli 8885 sellaista, joissa kaikki kolme menetelmää antoivat saman paikkajaon. Muiden vastaavien kokeiden perusteella näyttää siltä, että menetelmien konsensus saavutetaan yleensäkin noin kymmenessä prosentissa vaaleista edellyttäen, että äänestystulokset on säädetty jokseenkin eduskuntavaalien äänisaalista  $\hat{V}$  muistuttaviksi.

Paikkajakoja  $S \in \{S_{H-N}, S_{\text{geo}}, S_{D'H}\}$  verrattiin kvootteihin  $Q$  laskemalla erotukset

$$S - Q.$$

Geometrisella keskiarvolla

$$\text{GM}(V) := (V_1 \dots V_P)^{1/P}$$

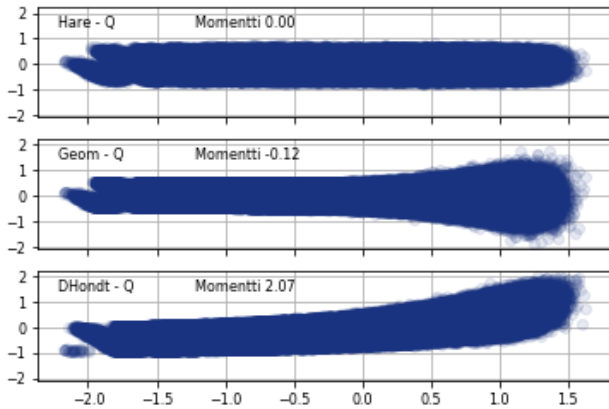
keskitetyn äänisaalisvektorin luonnollisesta logaritmisesta

$$\ln \frac{\mathbf{V}}{\text{GM}(\mathbf{V})}$$

ja erotuksista  $\mathbf{S} - \mathbf{Q}$  saatiin joka kierroksella pisteet

$$\left( \ln \frac{V_p}{\text{GM}(\mathbf{V})}, S_p - Q_p \right), \quad p = 1, \dots, P.$$

Nämä 100 000  $P = 900\,000$  pistettä piirrettiin koordinaatistoon läpikuultavalla värillä, vaalien läpinäkyvyyttä korostaen. Vaaka-akselilla vasemmalla ovat pienet, nollan kohdalla keskikokoiset ja oikealla suuret puolueet. Pystyakselilla on puolueen saaman paikkamäärän ja kvootin erotus.



Ylimpänä Hare-Niemeyer pysyttelee tiukasti alle yhden äänen päässä kvootista, kuten teorian mukaan kuuluu. Keskellä geometrinen menetelmä, suhteellisuuden pakottamana, levittäytyy suurten puolueiden päässä laajemmalle hoikentuen vastaavasti pienten puolueiden kohdalla. D'Hondtin menetelmän tuottama epäsymmetrinen "vihannes" käyristyy UNECE FFV-15-luokitusrajoja [4] koetellen.

Kuvasta selvästi havaitaan, että D'Hondtin menetelmä suosii suuria puolueita pienten kustannuksella. Havainto voidaan vahvistaa laskennallisesti työkalulla, joka saa ideansa fysiikasta. Kysymyksessä on **momentti**, kaikkien vipuvaikutusten äiti:

$$\begin{aligned} \text{Mom}(\Delta \mathbf{S}; \mathbf{V}) &:= \Delta \mathbf{S} \cdot \ln \frac{\mathbf{V}}{\text{GM}(\mathbf{V})} \\ &= \sum_{p=1}^P (\Delta S)_p \ln \frac{V_p}{\text{GM}(\mathbf{V})} \\ &= \sum_{p=1}^P (\Delta S)_p \ln V_p = \Delta \mathbf{S} \cdot \ln \mathbf{V}. \end{aligned}$$

Tässä  $\Delta \mathbf{S} = \mathbf{S} - \mathbf{Q}$ . Toisessa ja viimeisessä lausekkeessa piste  $\cdot$  tarkoittaa vektorien pistetuloa<sup>8</sup>:

$$\mathbf{u} \cdot \mathbf{v} = u_1 v_1 + \dots + u_n v_n = \sum_{k=1}^n u_k v_k.$$

<sup>8</sup>Kaavassa esiintyvä pistetulo saattaa hämätä fyysikoita. Kysymyksessä on itse asiassa momenttien summa samalla tavalla kuin jäykän kappaleen tasapainoehdossa.

Toiseksi viimeinen yhtälö johtuu logaritmien laskusäännöistä ja siitä, että kelvollisille paikkajaoille

$$(\Delta S)_1 + \dots + (\Delta S)_P = 0.$$

Kun kaikille kolmelle momentille, joista kustakin on 100 000 toteutumaa, lasketaan aritmeettinen keskiarvo AM, saadaan seuraava taulukko:

| $\mathbf{S}$              | AM(Mom( $\mathbf{S} - \mathbf{Q}$ ; $\mathbf{V}$ )) |
|---------------------------|-----------------------------------------------------|
| $\mathbf{S}_{\text{H-N}}$ | 0,00                                                |
| $\mathbf{S}_{\text{geo}}$ | -0,12                                               |
| $\mathbf{S}_{\text{D'H}}$ | 2,07                                                |

Taulukon perusteella D'Hondtin menetelmä pyrkii "kiertämään" suhteellisuusperiaatteen mukaista paikkajakoa positiiviseen kiertosuuntaan niin, että suurten puolueiden paikkamäärät kasvavat pienten kustannuksella. Sama ilmiö toistuu lähes samoilla momenteilla, kun äänisaalisvektori  $\hat{\mathbf{V}}$  peilataan päinvastaiseen järjestykseen (engl. *flip*) ja arvotaan uudet äänestystulokset, ihan vaan tarkistuksen vuoksi.

Mistähän D'Hondtin puoluetuki suurille puolueille johtuu? Vastauksen miettiminen jätetään lukijalle. Vihjeenä muistutetaan, että äänissä mitattu D'Hondtin hinta paikalle on yleensä pienempi kuin  $V/\Sigma$ , äänen kokonaismäärä jaettuna paikkojen kokonaismäärällä.

## Yhteenveto

Vaalien suhteellisuudella tarkoitetaan sitä, että edustajapaikat jakaantuvat puolueille samoin kuin vaaleissa saadut äänet. Suomen eduskuntavaaleissa suhteellisuus toteutuu heikosti: eräät pienet puolueet menettävät jopa useita paikkoja suurille puolueille vaalijärjestelmän takia. Perustuslain edellyttämälle suhteelliselle vaalitavalle pahin este on perustuslain niin ikään edellyttämä vaalipiirijako. Suhteellisuuden vinoumaa suurten puolueiden eduksi kärjistää vaalipiirien paikkajaoissa käytetty D'Hondtin menetelmä.

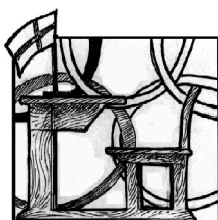
Eduskuntavaaleja simuloitiin ilman vaalipiirijakoa. Simulaatiossa tutkittiin suhteellisen vaalitavan toteutumista vertaamalla keskenään kolmea laskentamenetelmää: Hare-Niemeyerin menetelmä, geometrinen menetelmä ja D'Hondtin menetelmä. Näistä keskimmaisessä minimoidaan suoraan suhteellisuuden virhettä. Siksi ei ole yllättävää, että geometrinen menetelmä osoittautui suhteellisuusmielessä parhaimmaksi. D'Hondt selvästi suosi suuria puolueita, monesti jopa kahdella ylimääräisellä paikalla.

Artikkelissa tarkasteltiin vaaleja puhtaasti matemaattiselta kannalta — muutamia sivuhuomautuksia ehkä lukuunottamatta. Matematiikan ohella vaaleihin liittyy lukuisia puolue- ja yhteiskuntapoliittisia näkökohtia ja muita aspektoja.



## Viitteet

- [1] Alestalo, Pekka: *Alabaman paradoksi*.  
<https://matematiikkalehtisolmu.fi/2007/2/alestalo.pdf>
- [2] Finlex: *Suomen perustuslaki*.  
<https://www.finlex.fi/fi/laki/ajantasa/1999/19990731>
- [3] Finlex: *Vaalilaki*.  
<https://www.finlex.fi/fi/laki/ajantasa/1998/19980714>
- [4] United Nations Economic Commission for Europe: *Fresh Fruit and Vegetables - Standards. FFV-15, Cucumbers*.  
<https://unece.org/trade/wp7/FFV-Standards>
- [5] Yle: *Eduskuntavaalit 2019. Tulospalvelu. Puolueet*.  
<https://vaalit.yle.fi/ev2019/fi/parties>



## Matematiikkaan innostaminen – inspiraatiota Integraalipäiviltä

*Otso Huuska*

Lehtori (FY+MA), Rauman Lyseon lukio

Matematiikan kauneus ja kiehtovuus aukeni itselleni joskus yläasteaikana, suunnilleen samalla hetkellä, kun numeroiden sekaan alkoi ilmestyä muuttujia oppituneilla. Mahdollisuus kuvata abstrakteja asioita ja niiden välisiä suhteita tuntui välittömästi kiehtovalta, ja sanalliset käytännön tehtävät olivat itselleni useimmiten niitä tylsempiä. Opettajana ja muutenkin ihmisiä kohdatessa saan yhä uudelleen hämmästyä, kuinka tämä sama kauneus ei puhuttele suinkaan kaikkia. Moni kaipaa tietoa siitä, mihin matematiikkaa voi hyödyntää.

Vaikka sovelluskohteita matematiikalla on joka saralla, on mielestäni väärä tie kulkea, jos kouluissa matematiikan opetusta ja opiskelun motivointia rakennetaan matematiikan hyödyn varaan. Silloin menetetään matematiikan ydin, joka ei ole sovelluksissa, vaan kokeellisesti tutkittavissa olevasta maailmasta riippumattomassa abstraktissa rakenteessa. Mielikuvituksen leikkiä ei voi korvata insinööripuuhastelulla.

Oppimiseen innostaminen matematiikan kauneuden kautta on tietysti helpommin sanottu kuin tehty. Kauneuden ja abstraktin rakenteen lisäksi keskiössä voisi olla matematiikan elämyksellisyys. Tältä osalta Integraalipäivät ovat tarjonneet jonkinlaisia uusia eväitä itselleni opettajana ja matematiikasta kertojana.

### Taustaa

Integraalipäivät kokoavat yhteen eri asteiden opettajia sekä matematiikan yliopistotutkijoita, opiskelijoita ja matematiikan opettajaksi opiskelevia. Tutkijat esittelevät oman alansa sovelluskohteita tai ajankohtaista tutkimusta, ja heterogeenisissä pienryhmissä ideoidaan esitelmien pohjalta opetustuokioita eri luokka-asteille. Tavoitteena on luoda valmiita oppituntipohjia jonkin opetussuunnitelman aiheen käsittelyyn ajankohtaisen tutkimuksen kontekstissa. Samalla keskustellaan muiden matematiikan opetuksesta kiinnostuneiden ja eri taustoista tulevien kanssa matematiikasta ja sen opetuksesta. Kehiteltäviä oppitunteja testataan kouluissa tai matematiikkakerhoissa ja tämän jälkeen ne julkaistaan tapahtuman kotisivuilla<sup>1</sup>.

Kehiteltujen oppituntisuunnitelmien lisäksi osan esitelmien tallenteet ovat katsottavissa kotisivuilla<sup>2</sup>. Esimerkiksi myöhemmin tekstissä mainittaviin tapettiryhmiin pääsee tutustumaan Jarkko Karin esitelmän avulla.

Tapahtumaan on otettu mallia Ruotsin Kleindagarneista<sup>3</sup>.

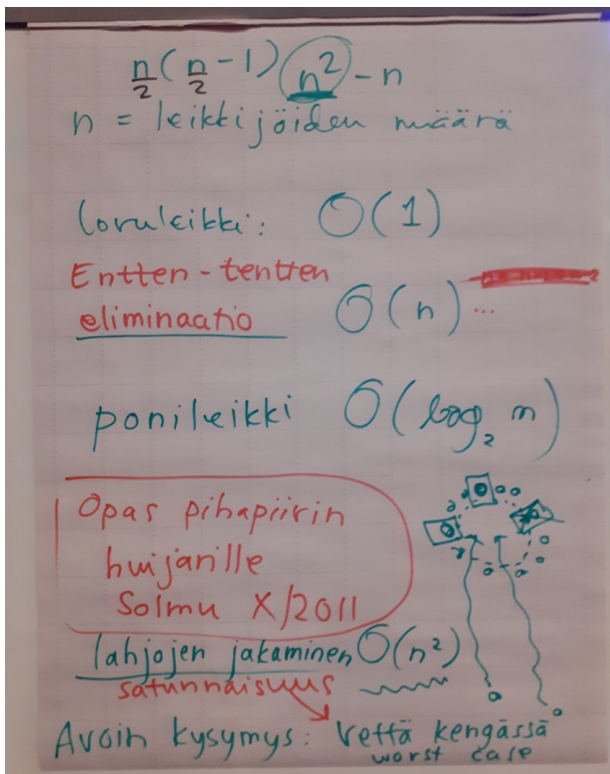
<sup>1</sup><https://blogs.helsinki.fi/integraalipaivat/>

<sup>2</sup><https://blogs.helsinki.fi/integraalipaivat/materiaali/esitelmat/>

<sup>3</sup><https://www.kleindagarna.se>

## Kokemuksia tapahtumasta

Olen päässyt mukaan molemmille toistaiseksi järjestetyille Integraalipäiville. Keväällä 2021 tapahtuma järjestettiin etänä, ja siitä muotoutui parhaiten organisoitu etätapahtuma, jossa olen ollut mukana. Tapahtuman päätarkoitus onnistui etänäkin hyvin, mutta epämuodolliset juttutuokiot jäivät varsin vähiin. Syksyllä 2021 Integraalipäivät järjestettiin Turussa, ja verkostoituminen onnistui tapahtuman sivutuotteena paljon paremmin. Korona toki varjosti myös näitä Integraalipäiviä, mikä näkyi joidenkin osallistujien peruutuksina.



Syksyn Integraalipäivillä puntaroitiin ongelmien työläyteen perehtymistä tuttujen leikkien avulla.

Integraalipäivien inspiroivat aiheet ovat vaihdelleet kuvankäsittelystä kvanttilaskentaan ja tason symmetrioista taudinleviämisen mallintamiseen. Näistä kaikista on laadittu oppituntipohjia, joistain yläkouluun, toisista lukion peruskursseille ja muutamista esimerkiksi matematiikkakerhossa hyödynnettäviksi. Viime aikoina olen opettanut yksinomaan fysiikkaa, enkä ole siksi päässyt testaamaan laadittuja pohjia vielä itse. Uskon kuitenkin niiden mahdollisuuksiin toimia innostavina elementteinä.

## Miten olen hyödyntänyt oppimaani?

Päivillä esillä olleista aiheista itse innostuneena olen jutellut niistä niin satunnaisten opiskelijoiden kuin opettajanhuoneen kollegoiden ja koulumaailman ulkopuo-

listenkin kanssa. Yleensä on päästy helposti sekä juttukumppanin kenties ahdistavana pitämän algebran sekä itselleni masentavan hyötynäkökulman ohitse keskustelemaan matematiikan kauneudesta. Usein olen myös saanut kommentin ”Onko tämäkin matematiikkaa”, kuten markkinoidessani mahdollisia tapetteja (eli tason symmetriaryhmiä) koulumme kuvataiteen opettajille.

Erinomainen esimerkki on ollut myös kuvankäsittely. Aiheena se on kaikille jollain tavoin tuttu ja arkinen. Lisäksi kuvankäsittelyssä päästään helposti leikkimään erilaisilla efekteillä, joiden mahdollisesta hyötykäytöstä ei yleensä kysellä. Liki jokainen innostuu kokeilemaan, mitä erilaisia väri-ilmiöitä tai geometrisia väännöksiä saa aikaan. Kun tähän lähtökohtaiseen, orastavaan innostukseen kytkee sitten mukaan matematiikkaa, keskustelukumppani onkin yhtäkkiä vastaanottavainen. On syntynyt iloinen elämys jostain hauskaasta ja kauniista, jolla voi tehdä jotain, ja sitten sen(kin) paljastetaan olevan matematiikkaa.

## Innostusta Integraalipäiviltä

Yhtä tärkeää kuin itse keskustelunaihe saattaa olla opettajan tai matematiikasta kertojan oma innostus. Ei ole poissuljettua, että rationaalifunktioiden esittelyyn liittyvä oma tunteen paloni vuosi vuodelta hieman hiipuu ja lähestyy aiheen rutiininomaista toistoa. Aina tulisi muistaa, että opiskelijoille elämys on ensimmäinen, vaikka minulle jo ties kuinka mones. Ylioppilaskirjoitusten ja opetussuunnitelman tiukassa paineessa ei kuitenkaan ole helppoa innostua täysillä joka oppitunnilla ja uppoutua vapaasti matematiikan vietäväksi.

Integraalipäivät ja muut vastaavat tapahtumat tarjoavatkin opettajalle paitsi konkreettista sisältöä, myös innostusta jaettavaksi muille. Ainakin itselleni on äärimmäisen virkistävää päästä koskettelemaan matematiikkaa joiltain muilta osin kuin tiukasti opetettavan asiassällön tai ylioppilaskokeiden tehtävien rajoissa. Tuskinpa kieltenopettajatkaan viettävät aikaa ja inspiroituvat lukemalla uudelleen ja uudelleen oppikirjojen tekstejä. Matematiikanopettajilla saattaa olla suurempi kynnys lähteä liikkeelle kohti uutta. Eivät matematiikan opettajat ole ollenkaan kaikki olleet aikanaan itse koulussa kymppin oppilaita matematiikassa, ja virheiden ja osamattomuuden pelko on valitettavan syvään rakennettu matematiikan opiskeluun suomalaisessa koulumaa-ilmassa – tai ainakin on ollut.

Mistä kynnys itse kullakin sitten koostuu, se kannattaa ylittää ja lähteä iloisesti mukaan inspiroitumaan seuraaville Integraalipäiville, kuten myös muihin opettajia yhteen kerääviin tapahtumiin. Uusien ajatusten virkistävä ja innostava voima on arvaamattoman suuri. Suosittelen lämpimästi hakemista Integraalipäiville, kun kevään 2022 päivien haku aukeaa. Kenties näemme siellä!



## Keplerin naimahuolet – optimaalinen pysäyttäminen

*Markku Halmetoja*

Johannes Keplerille<sup>1</sup> tuli tarve löytää uusi vaimo, kun hänen ensimmäinen vaimonsa Barbara Muehleck kuoli vuonna 1611 ([1]). Jotakin naisen asemasta 1600-luvun Euroopassa kertoo se, että Kepler saattoi ilman yleistä paheksuntaa kokeilla useaa eri puolisoehdokasta ennen ratkaisuun päättymistään. Luonnollisesti koeteltavat olivat hänen taloudessaan yksi kerrallaan. Itsenäisyyden ja oman tahdon osoittaminen oli naisille vaarallista, sillä sellaisista elkeistä saattoi helposti joutua syytteeseen noituudesta. Syyte johti useimmiten kidutuksen kautta kuolemaan. Mika Waltari kuvaa tätä teoksessaan Mikael Karvajalka [2]. Se ei ole heikkohermoisen luettavaa.

Kaikessa omituisuudessaan Keplerin menettely johtaa mielenkiintoiseen matemaattiseen ongelmaan: kun ehdokkaita koetellaan yksi kerrallaan eikä hylättyyn luultavasti voi jälkikäteen palata, niin milloin kannattaa lopettaa ja tyytyä käsillä olevaan ehdokkaaseen? Kepler ei voinut pohtia asiaa todennäköisyyslaskennan kannalta, sillä tämältyypisiä ongelmia ratkova päätöksentekoteoria ja optimaalisen pysäyttämisen teoria kehittyi vasta 1900-luvulla. Kepler-historiasta johdun pysäyttämisiongelmaa kutsutaan kirjallisuudessa usein *avioliitto-ongelmaksi* ja yleisesti myös *sihteeriongelmaksiksi*. Ennen me-too-aikaa julkaistussa teoksessa [3, s.15] kysymys on puettu tuskin toteutettavissa olevaksi kauneuskilpailuksi, jossa neidot saapuvat yksitellen tuomariston eteen. Se joko hylkää neitosen tai valitsee hänet kauneimmaksi loppuja näkemättä. Millaisella strategialla päätös tulisi tehdä, jotta joltisellakin

todennäköisyydellä kaunein tulisi valituksi? Menettely tuntuu perin epäoikeudenmukaiselta. Esimerkki on kertakaikkisen huono.

Yritämme seuraavassa kehittää ongelmalle uskottavamman kehyskertomuksen. Oletetaan, että television visailuohjelman palkintona henkilö saa osallistua leikkiin, jossa hän saa valita numerojärjestyksessä tuntemattomia rahasummia sisältäviä kirjekuoria. Kuoret on numeroitu 1:stä  $n$ :ään, missä  $n$  on vähintään kaksinumeroinen luku. Jokaisessa kuoressa on eri rahamäärä. Niiden suuruusluokasta osallistujalla ei ole tietoa. Hän valitsee ja avaa kuoria seuraavasti: avattuaan ensimmäisen kuoren hän joko hyväksyy siinä olevan rahamäärän palkinnokseen ja leikki päättyy tai hylkää sen ja ottaa käsittelynsä seuraavan kuoren. Näin peli jatkuu, kunnes hän hyväksyy jonkin kuoren sisällön. Hylättyihin kuoriin ja rahasummiin ei ole paluuta. Jos hän päättää ennalta pysähtyä vaikkapa horoskooppimerkkinsä mukaisen onnennumeron kohdalle, hän saa suurimman summan todennäköisyydellä  $1/n$ . Osoitamme seuraavassa, että parempikin strategia on olemassa.

Tutkitaan aluksi ensimmäiset  $a$  kuorta ja laitetaan muistiin niistä löytynyt suurin rahasumma. Tämän jälkeen avataan kuoria, kunnes löytyy suurempi summa kuin alussa muistiin laitettu. Tähän kuoreen ja summaan tyydytään ja peli päättyy. Jos muistissa olevaa summaa suurempaa ei löydy, kaikki kuoret tulevat avatuiksi ja viimeisen kuoren sisältöön on tyytyminen.

Lasketaan nyt todennäköisyys sille, että jaossa oleva suurin rahasumma löytyy kuoresta  $n$ :o  $x$  ( $> a$ ). Jot-

<sup>1</sup>Johannes Kepler (1571–1630), saksalainen astronomi ja matemaatikko.

ta näin kävisi, täytyy seuraavien asioiden toteutua: 1° kuorien  $1, 2, \dots, (x-1)$  suurin summa on jossakin kuorista  $1, 2, \dots, a$ , ja 2° suurin rahasumma todellakin on kuoreissa  $n$ :o  $x$ . Tapauksessa 1° suotuisia alkeistapauksia on  $a$  kappaletta ja alkeistapauksia kaikkiaan  $x-1$  kappaletta. Tapauksen 2° todennäköisyys on sama kuin jos horoskooppimenetelmää käytettäisiin. Täten

$$P(1^\circ) = \frac{a}{x-1} \quad \text{ja} \quad P(2^\circ) = \frac{1}{n}.$$

Tieto kuorien  $1, 2, \dots, (x-1)$  sisältöjen järjestyksestä ei vaikuta kuoren  $x$  sisältöön, joten tapaukset 1° ja 2° ovat toisistaan riippumattomat. Niinpä kertolaskusäännön mukaan todennäköisyys saada maksimivoitto pysähtymällä kuoreen  $n$ :o  $x$

$$P(1^\circ \wedge 2^\circ) = \frac{a}{x-1} \cdot \frac{1}{n}.$$

Tämä pätee erikseen jokaiselle  $a$ :n jälkeiselle kuorelle, joten laskemalla yhteen kyseiset todennäköisyydet saadaan

$$P(\text{max voitto}) = \frac{1}{n} \sum_{x=a+1}^n \frac{a}{x-1} = \frac{a}{n} \sum_{x=a}^{n-1} \frac{1}{x}.$$

Strategian loppuunsaattamiseksi tutkitaan vielä, millä  $a$ :n arvolla saatu todennäköisyys on suurimmillaan. Merkitään

$$P(\text{max voitto}) = f(a) = \frac{a}{n} \sum_{x=a}^{n-1} \frac{1}{x}.$$

Koska  $a$  on diskreetti muuttuja, derivaatasta ei näyttäisi olevan hyötyä. Vai onko sittenkin? Summa

$$\sum_{x=a}^{n-1} \frac{1}{x}$$

on likimäärin jakoväliä  $\Delta x = 1$  käyttäen puolisuunnikassäännöllä laskettu integraalin

$$\int_a^n \frac{1}{x} dx$$

liikiarvo. Siis

$$f(a) \approx \frac{a}{n} \int_a^n \frac{1}{x} dx = \frac{a}{n} \ln \frac{n}{a}.$$

Suurin arvo saavutetaan, kun  $a \approx n/e \approx 0,368n$ , ja se toteutuu todennäköisyydellä  $1/e \approx 0,368$ . Päävoiton todennäköisyys on siis huomattavasti suurempi kuin jos pelkällä onnennumerolla yritettäisiin. Esitetty strategia on puhdasta arvausta parempi, mutta tämän kirjoittajalla ei ole edellytyksiä pohtia ja ratkaista, onko se paras mahdollinen.

Optimaalisen pysäyttämisen teoria sai alkunsa 1940-luvulla USAssa, kun kehitettiin tilastollisia testejä, missä otannan koko ei ole kiinteä vaan aina kun tehdään uusi havainto, päätetään hyväksytäänkö tilastollinen hypoteesi tai hylätäänkö se tai jatketaanko havainnointia. Tärkeä sovellusalue on myös optioiden hinnoittelu finanssi- ja talousmatematiikassa. Tämän aihepiirin tutkijat Robert C. Merton ([4]) ja Myron Scholes ([5]) saivat taloustieteen Nobelin palkinnon vuonna 1997. Monet pysäytysteorian yleistykset ovat edelleen aktiivisen tutkimuksen kohteina.

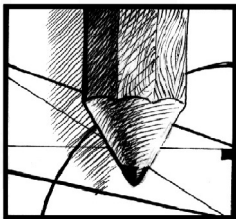
Keplerin ongelma ei ollut aivan tarkkaan tässä käsitelty, sillä hän ei esimerkiksi voinut aloittaessaan tietää, montako naista hän onnistuu saamaan koeajalle. Hän poikkesi ratkaisusta sikäläkin, että yritettyään kahden vuoden aikana yhteiselämää yhdentoista naisen kanssa hän onnistui luomaan uudestaan suhteen Susanna Reuttingeriin, jonka hän oli hylännyt viidentenä ehdokkaana. He solmivat avioliiton ja elivät onnellisina elämänsä loppuun asti.

*Kiitokset emer. prof. Paavo Salmiselle muutamista kirjoitustani täsmentäneistä kommentteista.*

## Viitteet

- [1] [https://en.wikipedia.org/wiki/Johannes\\_Keppler](https://en.wikipedia.org/wiki/Johannes_Keppler)
- [2] Mika Waltari: Mikael Karvajalka, WSOY 1948.
- [3] H. Stark, J.W. Woods: Probability, Random Processes, and Estimation Theory for Engineers, 2. edition, Prentice-Hall 1994.
- [4] [https://en.wikipedia.org/wiki/Robert\\_C.\\_Merton](https://en.wikipedia.org/wiki/Robert_C._Merton)
- [5] [https://en.wikipedia.org/wiki/Myron\\_Scholes](https://en.wikipedia.org/wiki/Myron_Scholes)





## George Malaty 1944–2022

*Marjatta Näätänen*

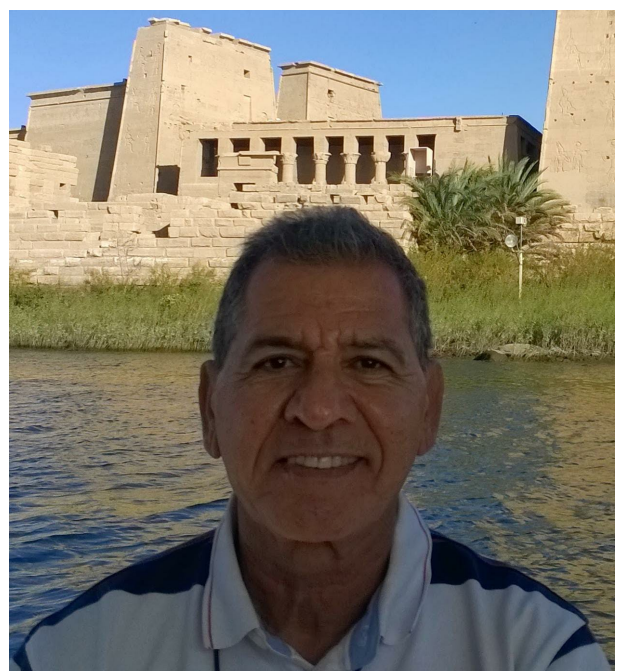
George Malaty syntyi El-Bahiran pienessä kaupungissa Egyptissä Niilin Deltassa 29.9.1944. Hänen isänsä oli asianaaja, äiti kotiäiti. George valmistui matematiikan opettajaksi (University of Ein-Shams, Cairo) vuonna 1966, toimi opettajana neljä vuotta, sitten assistenttina (Tanta University) 1970–1978, väitteli Moskovassa (Academy of Pedagogical Sciences) aiheena Uuden matematiikan käsitteiden omaksumisen erityispiirteitä lukioasteella Egyptin arabitasavallassa. Hän avioitui Irma Koposen kanssa, opetti Libyan Tripolissa ja muutti perheineen Suomeen 1984. Suomessa todettiin, että ”Ph.D Malatyn suoritukset ja julkaisut epäilyksittä täyttävät suomalaisen tohtorin arvonn edellytykset” (Helsingin yliopiston konsistorin lausunto, allekirjoittajana rehtori Olli Lehto). George toimi Joensuussa Itä-Suomen yliopiston lehtorina ja dosenttina 1986–2012. Hän toimi erittäin aktiivisesti luokanopettajien matematiikan taitojen kehittämiseksi. Suomen Kesäyliopistot ry valitsi hänet vuoden opettajaksi 1994. George kuoli Joensuussa 21.1.2022.

Artikkelit, tieteelliset julkaisut, kongressiesitelmät ja muut tehtävät löytyvät osoitteesta [https://wiivi.uef.fi/crisyp disp/\\_/fi/cr\\_redir\\_all/fet/fet/sea?direction=3&id=2700962](https://wiivi.uef.fi/crisyp disp/_/fi/cr_redir_all/fet/fet/sea?direction=3&id=2700962).

### Muistelmia yhteistyöstä George Malatyn kanssa

George teki suomalaisessa ympäristössä varsin omaleimaisen vaikutuksen. Jo hänen kielitaitonsa (arabia, venäjä, suomi, englantia, ranska ja viimeisten yhdeksän

Kanarialla vietetyn talven tuloksena arkipäivän espanja) kertoi, että kyse oli poikkeuksellisen lahjakkaasta ja työkykyisestä henkilöstä. George toi Egyptin aurinkoa ympäristöönsä ja teki työtään intohimoisesti matematiikan opetuksen hyväksi, hyödynsi kansainvälistä yhteistyötä ja sitkeästi voitti vaikeuksia. Kerron tässä lyhyesti yhteistyöstäni Georgen kanssa aiheina matematiikan opetuskokeilu ja Suomen Pisa-menestykseen liittynyt Pariisin matka.



## Matematiikan opetuskokeilu

Georgen tausta opinnoista Venäjällä johti mielenkiintoon eri maiden matematiikan opetusmenetelmiin. Vuonna 1999 teimme kokeilun, jonka tulokset on raportoitu matematiikkalehti Solmun erikoisnumerossa vuonna 2000<sup>1</sup>. Käytimme kahta monistetta, toinen venäläisen, toinen ranskalaisen tyylin mukaan. Opettajat eivät tienneet alkuperiä. Osa kokeiluun osallistuneista opettajista kertoi, että he olivat saaneet uutta näkökulmaa pitkäjänteisempään opetustapaan. Tällöin pidetään mielessä varsinkin tehtäviä valittaessa, että matematiikka on kokonaisuus, jota alemmalla tasolla opetettaessa rakennetaan samalla perustaa myöhemmin vastaan tulevalle. Tämä on perustava ajatus myös Unkarissa käytetylle, Vargan nimellä kulkevalle menetelmälle. Kokeilun lopputulos oli, että venäläisestä monisteesta pidettiin enemmän, esitystapa oli hyvä, tehtävät monipuolisia, mutta eivät liian helppoja – vastausta ei heti hoksannut. Oppilaatkin innostuivat ja huomasivat oppineensa jotain aivan uutta.

Lopputestit pidettiin toukokuun 1999 alussa. Syynä tähän oli, että kaikkien tulisi tehdä testi suunnilleen yhtä aikaa ja että vertailutesti on tapana tehdä toukokuun lopussa. Algebran testi oli standardi Kasselin testi, jonka tuloksista on vertailuaineistoa eri maista eri ikäisiltä oppilailta. Testikysymysten näkeminen oli oppilaille ja opettajille järkytys, kysymyksethän kattavat koko koulualgebran. Tarkoitus oli kuitenkin ainoastaan saada taso selvitettyä, tehdä vain ne tehtävät, jotka osasi ja olla kiinnittämättä muihin tehtäviin huomiota, mutta ilman eri kannustusta oppilaat luovuttivat kauhistuneina. Testi pidettiin monilla luokilla niin myöhään, että oppilaat päättelivät, ettei se vaikuttaisi enää arvosaan. Näin opettajan tehtäväksi jäi keksiä, miten motivoida vain arvosanastaan kiinnostuneet oppilaat tekemään parhaansa.

Keskiarvot kokeiluryhmissä olivat yleensä lievästi korkeammat kuin vertailuryhmissä, mutta ero ei ollut tilastollisesti merkitsevä. On mahdollista, etteivät käyetyt koko koulualgebran kattavat Kasselin testit ja niiden suoritusajankohta olleet optimaalisia näin lyhyen kokeilun tulosten esiin saamisessa. Tärkein selittävä tekijä ryhmän oppimismenestyksessä oli opettajan osuus. Lisäksi näyttää siltä, että mitä suurempi oli opettajan selittävä osuus, sitä suurempi oli myös ryhmän hajonta. Tämä voitaisiin tulkita niin, että opettaja, jonka selittävä osuus oli suuri, paneutui tosissaan kokeiluun, ja uuden materiaalin antamat haasteet sallivat suuren hajonnan.

Ryhmässä, jossa oli pitkä tauko matematiikan oppitunneissa, testitulokset huononivat selvästi, vaikka kyseessä oli siis saman testin uusinta. Tämä viittaa siihen,

että oppitunnit olisi oppimistulosten kannalta edullista sijoittaa kouluvuodelle tasaisesti ilman katkoja.

Ongelmana oli myös se, ettei oppitunteja pystytty resurssien puutteen takia seuraamaan, joten ei tiedetty, missä suhteessa kukin opettaja lopulta käytti kokeilumateriaalia ja tavallista oppikirjaa.

Suomalaiset koululaiset pitivät kokeilumateriaalia varsin vaativana, vaikka se oli Venäjällä tarkoitettu 1-2 vuotta nuoremmille.

Opetusmenetelmien muuttaminen on pitkäjänteistä työtä ja perusta pitäisi aloittaa jo ala-asteelta. Algebran kokeilussamme opettivat kokeilumateriaalilla suomalaisen opettajankoulutuksen saaneet opettajat, joille pystyttiin järjestämään vain kahden illan lisäkoulutus. Tässä tilanteessa siis Kasselin testiä käyttämällä ei tullut esille tilastollisesti merkitseviä eroja. Sen sijaan kokeiluun liittyneessä Olga Wolkoffin tutkimuksessa tehtiin kokeilussamme mukana olleelle ryhmälle ja kontrolliryhmälle Wolkoffin kehittämä yksityiskohtainen testi. Kokeilumateriaalia käyttävä opettaja ei käyttänyt lisänä suomalaista kirjaa ja opettajan selitykset venäläisen monisteen teoriaselvityksiin olivat välttämättömiä, vaikka ryhmän taso oli melko hyvä. Wolkoffin testi toi esille selvät erot oppimistuloksissa verrattuna suomalaista materiaalia käyttäneeseen kontrolliryhmään. Tulokset löytyvät Solmusta.

## Pisa-tutkimus

Suomen Pisa-menestys 2000-luvun alussa aiheutti suurta mielenkiintoa kansainvälisesti. Vaihtakseen kokeimuksia ja tietoja Suomen ja Ranskan matemaattiset yhdistykset järjestivät kokouksen Pariisissa. Suomen ryhmään valittiin itseoikeutetusti myös Pisaan tarkasti perehtynyt George. Hänen esitelmänsä aihe oli Mitkä ovat Suomen PISA-menestyksen taustalla olevat syyt? Koko kirjoituksen ja paljon muutakin asiaan liittyvää voi lukea Matematiikkalehti Solmun erikoisnumeroista vuodelta 2005–2006<sup>2</sup>. Tässä lyhyesti pari pääkohtaa Georgen asiaan hyvin monipuolisesti paneutuneesta kirjoituksesta. Hän aloitti tavoilleen uskollisena selkeällä ryhmittelyllä ja toi sitten myös kansainvälistä kokemustaan sekä historiallista näkökulmaa asiaan:

”Suomen PISA-menestys on yllättänyt matemaatikot ja matematiikan opetuksen asiantuntijat niin Suomesa kuin sen ulkopuolellakin, itseni mukaan lukien. Taus-tani ja kokemukseni vuoksi minun oli kuitenkin helppo ymmärtää menestyksen taustalla olevat syyt.

Viisi tärkeintä syytä Suomen PISA-menestykseen ovat:

- (1) onnistuminen opettajankoulutuksessa,
- (2) ammatillinen opetuskulttuuri,

<sup>1</sup><https://matematiikkalehtisolmu.fi/2000/4/>

<sup>2</sup><https://matematiikkalehtisolmu.fi/2005/erik1/>  
<https://matematiikkalehtisolmu.fi/2006/erik2/>

- (3) onnistuminen opettajien täydennyskoulutuksessa,
- (4) matematiikan opetuksen kehittämisen eteen tehdyt erilaiset panostukset,
- (5) koulunkäynnin traditiot Suomessa.

Ainakin osittain nämä syyt voivat näyttää suomalaisesta lukijasta itsestään selviltä, kuitenkin ne ovat vahvuutemme, jotka erottavat meitä muista maista. Toisaalta pitäisi korostaa, että onnistuminen opettajan koulutuksessa on suhteellista verrattuna muihin maihin, eikä opettajankoulutus meillä ole ongelmatonta.”

George toteaa:

”Opettajankoulutuksen onnistumisessa Suomessa on kaksi tärkeää näkökohtaa: opettajankoulutuksen tukintovaatimusten säilyminen korkeana ja motivoituneiden opiskelijoiden rekrytoimisen onnistuminen.”

Rekrytoinnista George jatkaa:

”Aineenopettajien rekrytointi onnistuu tyydyttävällä tavalla, sen sijaan luokanopettajan opinnot ovat yksi suosituimmista korkeakoulutuksen aloista Suomessa.”

George jatkaa tuomalla mukaan hyvin hallitsemansa historiallisen näkökulman: hän mainitsee luokanopettajien erityisaseman suomalaisessa yhteiskunnassa: he opettivat lukemista ja kirjoittamista noin 150 vuoden ajan, kirkon jälkeen. Vuoden 1921 kansakouluasetuksen jälkeen jokaisen kylään pyrittiin perustamaan kansakoulu, jolloin opettajasta tuli ”kansankynttilä”, Kirkkokadun viereen tuli Koulukatu.

Täydennyskoulutus oli erityisen lähellä Georgen sydäntä ja siihen hän panosti paljon työtään ja sai erinomaisia, Suomessa aivan poikkeuksellisia tuloksia:

”Yksi merkittävä ongelma matematiikan opetuksessa oli puute luokanopettajista, jotka olivat erikoistuneet matematiikkaan. Vaikka puolet luokanopettajakoulutuksen opinnoista on varattu kasvatustieteelle, niin matematiikalla ja matematiikan opetuksella on vaatimaton pakollinen osuus.”

Matematiikkaan erikoistuminen olikin perin harvinaista. Mutta tilanne muuttui Georgen aikana, aikaisemman alle 2 %:n sijaan jopa yli 80 % erikoistui matematiikkaan ja puolet heistä alkoi jatkaa opintoja aineenopettajan pätevyYTEEN asti. George teki innolla työtä opettajien täydennyskoulutuksen hyväksi ja sai myös opettajat innostumaan. Hän kirjoitti oppikirjoja algebrallisesta ja geometrisesta ajattelusta ja teki kansainvälistä yhteistyötä erityisesti tuodakseen Unkarin hyviä kokemuksia suomalaisten käyttöön. Hänen ponnistuksensa Joensuussa alkoivat matematiikan opetuksen ohjauksen parantamisesta normaalikoulussa. George pyysi opiskelijoitaan opettamaan matematiikkaa systemaattisemmin kuin oppikirjoissa, panostamaan matematiikan ymmärtämiseen ja käyttämään erilaisia keksimisstrategioita. Avustaakseen opiskelijoitaan oppituntien suunnittelussa George osallistui itse oppitunneille. Menestys syntyi tästä työstä, joka

johti ehdotukseen normaalikoulun matematiikkakerhojen perustamisesta, ensimmäinen perustettiin syksyllä 1988. Vastauksena opiskelijoiden pyyntöön George perusti vuonna 1989 heille iltamatematiikkakerhon. Seuraavana vuonna 1990 kerho muutettiin valinnaiseksi kurssiksi Matemaattinen ajattelu. Vuodesta 1993 lähtien kurssi on jaettu kahteen osaan, Geometrisen ajattelu ja Algebrallinen ajattelu. Vuonna 1993 yli 50 opiskelijaa valitsi erikoistumisaineekseen matematiikan, siis yli puolet luokanopettajaopiskelijoiden vuosittaisesta määrästä ja yli kolminkertainen määrä verrattuna kaikkiin muihin Suomen 10 opettajankoulutuslaitokseen. Georgen työn tuloksena menestys jatkui ja matematiikkaan erikoistuneiden osuus opiskelijoista nousi jopa yli 80 prosenttiin.

## Georgen menestyksellinen työ sai tunnustusta

Vuonna 1994 Korkeakoulujen arviointineuvosto nimitti Joensuun yliopiston matematiikan opettajankoulutuksen huippuyksiköksi. Samana vuonna Helsingin, Joensuun ja Oulun yliopistojen kasvatustieteelliset tiedekunnat arvioinut kansainvälinen komitea kirjoitti raportissaan:

”Joensuun yliopisto on menestyksellisesti kehittänyt matematiikan opetukseen erikoistuvien opettajien koulutusohjelmaa, joka voi toimia mallina muille tiedekunnille ja sisältöalueille... Ohjelma näyttää vähentävän tulevilla opettajilla yleiseksi havaittua matematiikan (opetuksen) aiheuttamaa ahdistusta”.

Vuosien 1990–95 aikana matematiikkakerhot levisivät koko maahan opettajien täydennyskoulutuksen kautta. 1990-luvun aikana George oli mukana yli 300 täydennyskoulutusohjelmassa yli 75 kunnassa mukaan lukien kaikki suurimmat kaupungit saavuttaen näin yli 12 000 opettajaa päiväkodeista lukioihin. Poliitikot ja median edustajat huomasivat tämän. Matematiikkakerhoista kerrottiin sanoma- ja viikkolehdistä. Myös televisiokanavilla esitettiin uutisia ja ohjelmia matematiikkakerhojen toiminnasta. Tämä julkisuus tuki muita virallisia toimenpiteitä, mukaan lukien LUMA-talkoot (opetusministeriö 1999).

Georgen työn ansiosta Itä-Suomen alueella on nyt entistä parempia matematiikan opettajia, eikä tämä rajoitu ainoastaan luokanopettajien koulutukseen, vaan myös erityisopettajien koulutukseen. Joensuun yliopistossa on erityiskasvatuksen laitos, jossa matematiikan ja sen opetuksen sisältö on sama kuin luokanopettajien koulutuksessa.

George analysoi ja luettelee koulujemme hyviä puolia, jotka ovat vaikuttaneet Pisa-menestykseen. Hän toteaa lopuksi:

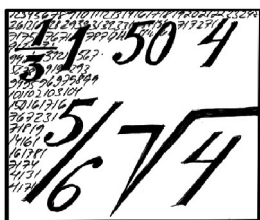
”Tämän vuoksi suomalaisten oppilaiden erot oppimistuloksissa ovat pienempiä kuin muissa maissa. Toisaal-

ta tämä osoittaa yhden suuren ongelman matematiikan opetuksessa, tarpeen huolehtia enemmän myös lahjakkaista oppilaistamme.”

Kuultuaan prof. Malatyn esityksen Suomen (silloisesta, siis vuoden 2005) tilanteesta kouluissa ranskalaiset kyselivät, miten tähän ihmeelliseen maahan voi muuttaa – mutta kokouksen seuraavissa esityksissä tuli jo selville, että Suomessakin ongelmat ovat alkaneet ka-

saantua.

Valitettavasti täytyy todeta, että melkein 20 vuodessa tilanteen selvä huonontuminen on jatkunut. George Malatyn tarkoitus olikin, että suomalaiset osaisivat arvostaa sitä, mikä heillä on ollut hyvää, eivätkä luopuisi siitä. Tämä olisi paras tapa kunnioittaa Georgen työtä ja muistoa.



## Näennäisen triviaalit temput matematiikassa

*Anne-Maria Ernvall-Hytönen*

Helsingin yliopisto

Tässä tekstissä on tarkoitus käsitellä kahta harvinaisen triviaalilta tuntuvaa ajatusta:

1. Jos summaan lisätään nolla, ei summan arvo muutu.
2. Ykkönen on pienin positiivinen kokonaisluku. (Toisinaan tämä on myös hyödyllistä muotoilla muotoon ”Kahden peräkkäisen kokonaisluvun erotus on yksi.”)

Kumpikin väite on täysin triviaali. Niillä voi kuitenkin saada yllättävän paljon aikaiseksi. En pysty kirjoittamaan yleistä teoriaa siitä, miten näitä tulisi käyttää – lähinnä ideana on ensimmäisen kohdan kanssa se, että yritetään muokata lauseketta sellaiseen muotoon, jota on helpompi käsitellä esimerkiksi vähentämällä siitä joku luku ja lisäämällä sama luku toiseen kohtaan lauseketta. Toinen kohta taas usein soveltuu esimerkiksi kokonaislukujen joukossa arviointiin. Näitä ideoita onkin helpoin valottaa esimerkein.

### Summan arvo ei muutu, jos lisätään nolla

#### Polynomien arviointi

Halutaan selvittää, mikä on polynomin  $p(x) = x^2 + 6x$  pienin mahdollinen arvo reaalilukujen joukossa. Tämän voisi tehdä derivoimalla, mutta ei tehdä nyt sitä, vaan täydennetään neliöksi:

$$p(x) = x^2 + 6x = x^2 + 6x + 9 - 9 = (x - 3)^2 + 9.$$

Nollan lisääminen tehtiin lisäämällä ja vähentämällä yhdeksän. Tämä tehtiin, koska siten saatiin polynomiin siisti neliölauseke ja lisäksi vakio. Nyt on helppo nähdä, että  $p(x) \geq 9$  ja lisäksi 9 todella on sen pienin arvo, sillä  $p(3) = 9$ .

#### Kongruenssin laskusäännön todistaminen

Todistetaan seuraavaksi, että jos  $a \equiv b \pmod{n}$  ja  $c \equiv d \pmod{n}$ , niin  $ac \equiv bd \pmod{n}$ . Kirjoitetaan kongruenssi ensin jaollisuuden avulla. Oletukset ovat  $n \mid a - b$  ja  $n \mid c - d$ . Väitetään, että  $n \mid ac - bd$ . Nyt on hyödyllistä vähentää ja lisätä termi  $ad$ , jolloin saadaan

$$ac - bd = ac - ad + ad - bd = a(c - d) + d(a - b).$$

Koska  $c - d$  ja  $a - b$  ovat oletusten nojalla jaollisia luvulla  $n$ , on erotus  $ac - bd$  jaollinen luvulla  $n$ .

Yllä oleva olisi yhtä hyvin voitu tehdä myös vähentämällä ja lisäämällä termi  $bc$ :

$$ac - bd = ac - bc + bc - bd = c(a - b) + b(c - d).$$

Oleellista on lisätä ja vähentää jokin sellainen termi, jonka avulla erotus saadaan esitettyä muodossa, jossa on selkeästi luvulla  $n$  jaollisia termejä.

#### Jaollisuus ja induktio

Osoitetaan induktiolla, että  $6^n - 1$  on jaollinen viidellä, kun  $n \geq 0$ . Tämän pystyisi helposti tekemään



kongruenssien avulla, mutta tehdään todistus nyt induktiolla niin, että saadaan jälleen yksi esimerkki siitä, miten nollan lisääminen voi olla hyödyllistä.

Induktion alkuaskel: Kun  $n = 0$ , saadaan  $6^0 - 1 = 0$ , joka on jaollinen viidellä. Alkuaskel on siis kunnossa.

Induktio-oletus: Oletetaan, että väite pätee, kun  $n = k$ , eli luku  $6^k - 1$  on jaollinen viidellä.

Induktioväite: Väitetään, että  $6^{k+1} - 1$  on jaollinen viidellä.

Todistetaan nyt induktioväite. Tärkeää on päästä käyttämään induktio-oletusta. Tämä voidaan tehdä monella eri tavalla. Otetaan nyt yksi esimerkki:

$$6^{k+1} - 1 = 6^{k+1} - 6^k + 6^k - 1.$$

Lisäämällä ja vähentämällä termi  $6^k$  saadaan lausekkeeseen osa, joka on suoraan induktio-oletuksesta. Lisäksi pitää vielä käsitellä lausekkeen alkuosa. Kirjoitetaan

$$6^{k+1} - 6^k = 6^k(6 - 1) = 5 \cdot 6^k,$$

joka on triviaalisti jaollinen viidellä. On siis saatu

$$6^{k+1} - 1 = 5 \cdot 6^k + 6^k - 1,$$

missä ensimmäinen termi oikealla on triviaalisti viidellä jaollinen ja loppuosa on induktio-oletuksen nojalla viidellä jaollinen. Väite on todistettu.

## Wienerin hyökkäys RSA-kryptojärjestelmään

RSA-kryptojärjestelmästä olen kirjoittanut aiemmin. Eräs hyökkäys järjestelmää kohtaan tunnetaan Wienerin hyökkäyksenä. Sen matemaattinen pohja on itse asiassa ketjumurtolukujen teoriassa. Luvun ketjumurtokehittelystä katkaisemalla saatavia lukuja kutsutaan konvergenteiksi. Esimerkiksi siis luvun

$$3 + \frac{1}{2 + \frac{1}{4}}$$

konvergenteja ovat luvun itsensä lisäksi myös luvut 3 ja  $3 + \frac{1}{2}$ . Näille pätee erilaisia hyviä ominaisuuksia. Eri-tyisesti niillä voidaan approksimoida lukuja poikkeuksellisen hyvin. Eräs hyödyllinen tulos on seuraavanlainen: Jos

$$\left| \xi - \frac{r}{s} \right| \leq \frac{1}{2s^2},$$

niin  $\frac{r}{s}$  on luvun  $\xi$  konvergentti. Luvun konvergentit on laskettavissa tehokkaasti. Käytännössä RSA:ssa on kyse siitä, että on julkinen eksponentti  $e$ , salainen eksponentti  $d$  ja modulo  $n$ . Salaus onnistuu, jos tiedetään  $e$  ja  $n$ , ja salauksen purkaminen puolestaan, jos tiedetään  $d$  ja  $n$ . Julkinen eksponentti ja modulo ovat julkisia. Modulo  $n$  jakautuu kahden keskenään erisuuren alkuluvun tuloksi  $n = pq$ , ja nämä alkutekijät ovat salaisia. Salaisen eksponentin  $d$  saa laskettua, jos tietää nämä

tekijät. Toisaalta, jos saa selvitettyä salaisen eksponentin, niin myös luvun  $n$  saa jaettua tekijöihin. Lukujen välinen yhteys on tämä:

$$ed \equiv 1 \pmod{\varphi(n)},$$

missä  $\varphi(n) = (p-1)(q-1)$  on Eulerin  $\varphi$ -funktion arvo. Yllä oleva yhtälö voidaan siis kirjoittaa muodossa

$$ed - k\varphi(n) = 1$$

jollain  $k$ . Kyseessä on Diofantoksen yhtälö, jossa on käytännössä kolme tuntematonta. Jos saadaan selville  $\varphi(n)$ , saadaan selville myös  $p$  ja  $q$  ja voidaan ratkaista  $d$ . Jos saadaan selville  $d$ , tiedetään salainen eksponentti, jolloin salatut viestit voidaan purkaa. Kolmen tuntemattoman Diofantoksen yhtälölle on liikaa ratkaisuja, eli pelkän yhtälön tuijottelu ei ole hyvä idea. Jos tehdään oletus, että luvun  $n$  alkutekijät eivät ole keskenään kovin erisuuria, eli  $p < q < 2p$ , niin voidaan arvioida

$$\begin{aligned} n - \varphi(n) &= pq - (p-1)(q-1) \\ &= p + q - 1 \leq p + q < 3p < 3\sqrt{n}, \end{aligned}$$

jolloin luvut  $n$  ja  $\varphi(n)$  ovatkin hyvin lähellä toisiaan. Oletetaan lisäksi, että  $1 < e < \varphi(n)$ , jolloin  $k < d$ . Lisäksi oletetaan  $d \leq \frac{1}{3}n^{1/4}$  (eli tämä hyökkäys toimii, jos  $d$  on verrattain pieni). Tarkastellaan nyt erotusta

$$\left| \frac{e}{n} - \frac{k}{d} \right|.$$

Tämä on läheistä sukua sille, että yhtälö

$$ed \equiv 1 \pmod{\varphi(n)}$$

jaettaisiin puolittain luvuilla  $d$  ja  $\varphi(n)$ , jolloin saataisiin yhtälö

$$\frac{e}{\varphi(n)} - \frac{k}{d} = \frac{1}{d\varphi(n)}.$$

Helpointa on kuitenkin käyttää muotoa  $ed - k\varphi(n) = 1$  ja sitä kautta hyödyntää lausekkeen ja yhtälön läheistä yhteyttä. Nyt voidaankin kirjoittaa

$$\left| \frac{e}{n} - \frac{k}{d} \right| = \left| \frac{ed - nk}{dn} \right| = \left| \frac{ed - k\varphi(n) + k\varphi(n) - nk}{dn} \right|.$$

Olemme jälleen lisänneet termiin keskelle nollan lisäämällä ja vähentämällä saman termin. Tavoite oli yllä mainittua yhtälöä hyödyntämällä saada osa lausekkeesta arvioitua pieneksi ja sen jälkeen jatkaa loppuosan kanssa:

$$\begin{aligned} \left| \frac{ed - k\varphi(n) + k\varphi(n) - nk}{dn} \right| &= \left| \frac{1 + k\varphi(n) - nk}{dn} \right| \\ &\leq \left| \frac{k\varphi(n) - nk}{dn} \right|. \end{aligned}$$

Epäyhtälö perustuu siihen, että osoittajassa oli suuri negatiivinen osa ja pieni positiivinen, jolloin positiivinen voitiin arvioida pois. Koska  $k < d$ , voidaan arvioida

$$\left| \frac{k\varphi(n) - nk}{dn} \right| \leq \left| \frac{\varphi(n) - n}{n} \right| \leq \frac{3\sqrt{n}}{n} = \frac{3}{\sqrt{n}} \leq \frac{1}{2d^2},$$

jolloin  $\frac{k}{d}$  saadaan laskemalla luvun  $\frac{e}{n}$  konvergentit.

Tässä tilanteessa nollan lisäämisen voi nähdä kahdella (yhteenkietoutuvalla) tavalla: sen avulla saatiin osoittajaan kaksi erotusta, joista kumpikin osattiin käsitellä. Näin myös saatiin erotus yhdistettyä tunnettuun yhtälöön.

## Ykkönen on pienin positiivinen kokonaisluku: kuinka tätä käytetään

### Polynomit rationaalipisteissä

Tiedämme, että polynomilla  $p(x) = x^2 - 2$  ei ole rationaalisia nollakohtia, vaan nollakohdat ovat  $x = \pm\sqrt{2}$ . Omalla laillaan luonnollinen kysymys onkin, miten lähelle nollaa päästään, jos lasketaan polynomin arvo jossain rationaalilukupisteessä. Selvää on, että ilman tarkempia rajoituksia voi todeta olevan mahdollista päästä mielivaltaisen lähelle nollaa. Jos nimittäin otetaan rationaaliluku  $u$ , jolla pätee  $\sqrt{2} < u < \sqrt{2} + 10^n$ , eli voidaan kirjoittaa  $u = \sqrt{2} + \varepsilon$ , niin

$$\begin{aligned} p(u) &= p(\sqrt{2} + \varepsilon) = (\sqrt{2} + \varepsilon)^2 - 2 \\ &= 2 + 2\sqrt{2}\varepsilon + \varepsilon^2 - 2 = 2\sqrt{2}\varepsilon + \varepsilon^2. \end{aligned}$$

Kun  $\varepsilon$  on hyvin pieni, saadaan polynomin arvo hyvin pieneksi. Lasketaan seuraavaksi raja, joka riippuu vain rationaaliluvun nimittäjästä. Olkoon  $\frac{r}{s}$  rationaaliluku, joka on sievennetyssä muodossa. Nyt

$$\left| p\left(\frac{r}{s}\right) \right| = \left| \left(\frac{r}{s}\right)^2 - 2 \right| = \left| \frac{r^2 - 2s^2}{s^2} \right|.$$

Tiedetään, että arvo ei voi olla nolla. Osoittajassa on kokonaislukujen tuloja ja erotuksia. Siispä osoittaja on kokonaisluku. Koska se ei ole nolla, on sen pakko olla itseisarvoltaan vähintään yksi. Siispä

$$\left| p\left(\frac{r}{s}\right) \right| = \left| \frac{r^2 - 2s^2}{s^2} \right| \geq \frac{1}{s^2}.$$

Lukijalle jätetään harjoitustehtäväksi osoittaa, että jos  $p$  on  $n$ . asteen polynomi, jolla ei ole rationaalisia nollakohtia, niin

$$\left| p\left(\frac{r}{s}\right) \right| \geq \frac{1}{s^n},$$

kun  $r$  ja  $s$  ovat kokonaislukuja ja  $s \neq 0$ .

### Jaollisuustehtävä matematiikkaolympialaisista

Vuonna 1992 kansainvälisissä matematiikkaolympialaisissa oli seuraava tehtävä:

*Määritä kaikki kokonaisluvut  $a$ ,  $b$  ja  $c$ ,  $1 < a < b < c$ , joille  $(a-1)(b-1)(c-1)$  on luvun  $abc-1$  tekijä.*

Jos  $(a-1)(b-1)(c-1)$  on luvun  $abc-1$  tekijä, niin

$$\frac{abc-1}{(a-1)(b-1)(c-1)}$$

on kokonaisluku. Arvioidaan

$$1 < \frac{abc-1}{(a-1)(b-1)(c-1)} < \frac{a}{a-1} \cdot \frac{b}{b-1} \cdot \frac{c}{c-1}.$$

Funktio  $f(x) = \frac{x}{x-1} = 1 + \frac{1}{x-1}$  on laskeva ykköistä suurempien lukujen joukossa, joten lauseke  $\frac{a}{a-1} \cdot \frac{b}{b-1} \cdot \frac{c}{c-1}$  on mahdollisimman suuri, kun luvut  $a$ ,  $b$  ja  $c$  ovat mahdollisimman pieniä. Tämä toteutuu, kun  $a = 2$ ,  $b = 3$  ja  $c = 4$ . Tässä on huomionarvoista, että tällaista arviota ei voitaisi tehdä, jos emme tietäisi lukujen olevan kokonaislukuja. Nyt

$$\frac{abc-1}{(a-1)(b-1)(c-1)} < \frac{2}{2-1} \cdot \frac{3}{3-1} \cdot \frac{4}{4-1} = 4.$$

Täytyy siis olla

$$\frac{abc-1}{(a-1)(b-1)(c-1)} = 2$$

tai

$$\frac{abc-1}{(a-1)(b-1)(c-1)} = 3.$$

Aloitetaan jälkimmäisestä tapauksesta. Huomaamme nimittäin, että osamäärä pienenee aika nopeasti, kun luvut kasvavat, jolloin intuitiivisesti tuntuu uskottavalta, että tämä tapaus on helpompi.

Jos  $a \geq 3$ , niin  $b \geq 4$  ja  $c \geq 5$ , jolloin

$$\frac{abc-1}{(a-1)(b-1)(c-1)} < \frac{3}{3-1} \cdot \frac{4}{4-1} \cdot \frac{5}{5-1} = \frac{5}{2} < 3.$$

Tämä ei siis ole mahdollista. On oltava  $a = 2$ . Nyt siis

$$2bc - 1 = 3(2-1)(b-1)(c-1) = 3(b-1)(c-1).$$

Koska vasen puoli on pariton, on oikeankin puolen oltava pariton. Siispä  $b$  ja  $c$  ovat parillisia. Testataan pienimmällä mahdollisella luvun  $b$  arvolla:  $b = 4$ . Nyt

$$2 \cdot 4c - 1 = 3(4-1)(c-1),$$

eli

$$8c - 1 = 9(c-1),$$

josta ratkaistaan  $c = 8$ . Nyt on löydetty yksi ratkaisu. Osoitetaan seuraavaksi, että ei voi olla  $b > 4$ . Jos näin olisi, niin olisi vähintään  $b = 6$  ja  $c = 8$ , jolloin olisi

$$\frac{abc-1}{(a-1)(b-1)(c-1)} < \frac{2}{2-1} \cdot \frac{6}{6-1} \cdot \frac{8}{8-1} = \frac{96}{35} < 3.$$

Jos siis osamäärä on kolme, on ainoa ratkaisu  $a = 2$ ,  $b = 4$  ja  $c = 8$ .

Siirrytään nyt toiseen tapaukseen, eli siihen, että osamäärä on kaksi. Nyt

$$abc - 1 = 2(a-1)(b-1)(c-1),$$

jolloin oikea puoli on parillinen. Jotta vasen puoli on myös parillinen, ovat  $a$ ,  $b$  ja  $c$  parittomia. On siis  $a \geq 3$ ,  $b \geq 5$  ja  $c \geq 7$ .

Osoitetaan ensimmäiseksi, että ei voi olla  $a > 3$ . Jos näin olisi, niin olisi  $a \geq 5$ ,  $b \geq 7$  ja  $c \geq 9$ , ja tällöin

$$\frac{abc - 1}{(a-1)(b-1)(c-1)} < \frac{5}{4} \cdot \frac{7}{6} \cdot \frac{9}{8} = \frac{105}{64} < 2.$$

Siis on oltava  $a = 3$ . Testataan tapaus  $b = 5$ :

$$3 \cdot 5 \cdot c - 1 = 2(3-1)(5-1)(c-1),$$

eli

$$15c - 1 = 16(c-1),$$

jolloin  $c = 15$  ja yksi ratkaisu on löytynyt. Osoitetaan vielä, että muita ratkaisuja ei ole. Riittää osoittaa, että ei voi olla  $b > 5$ . Jos näin olisi, olisi  $b \geq 7$  ja  $c \geq 9$ , jolloin voisimme arvioida

$$\frac{abc - 1}{(a-1)(b-1)(c-1)} < \frac{3}{2} \cdot \frac{7}{6} \cdot \frac{9}{8} = \frac{63}{32} < 2,$$

eli ratkaisuja ei löydy. Ainoat ratkaisut ovat siis jo aiemmin löydetty  $a = 2$ ,  $b = 4$  ja  $c = 8$  sekä  $a = 3$ ,  $b = 5$  ja  $c = 15$ .

Tässä tehtävässä oleellista oli vedota kahteen itsestään-selvyyteen:

- Jos osamäärä on kahden peräkkäisen kokonaisluvun välissä, ei se voi olla kokonaisluku.
- Koska  $a$ ,  $b$  ja  $c$  olivat kokonaislukuja ja keskenään erisuuria, kasvatti pienimmän luvun kasvattaminen usein myös kahta seuraavaa.

## Luvun $e$ irrationaalisuus

Osoitetaan Neperin luku  $e$  irrationaaliseksi. Olen kirjoittanut tästä aiemminkin, mutta aiemmin lähinnä irrationaalisuuden näkökulmasta, enkä niinkään todistuksen ideoita ajatellen. Tehdään vastaoletus:  $e$  on rationaalinen. Nyt siis  $e = \frac{a}{b}$  joillakin positiivisilla kokonaisluvuilla  $a$  ja  $b$ . Tiedämme, että

$$e = \sum_{k=0}^{\infty} \frac{1}{k!}.$$

Sijoitetaan luvun  $e$  paikalle  $e = \frac{a}{b}$  ja kerrotaan yhtälö puolittain jonkin sopivan positiivisen kokonaisluvun kertomalla  $n!$ . Nyt siis

$$an! = bn! \sum_{k=0}^{\infty} \frac{1}{k!}.$$

Oikean puolen summa voidaan jakaa kahteen osaan:

$$bn! \sum_{k=0}^{\infty} \frac{1}{k!} = bn! \sum_{k=0}^n \frac{1}{k!} + bn! \sum_{k=n+1}^{\infty} \frac{1}{k!}.$$

Koska

$$bn! \sum_{k=0}^n \frac{1}{k!} = b \sum_{k=0}^n \frac{n!}{k!}$$

on varmasti kokonaisluku, on luvun

$$bn! \sum_{k=n+1}^{\infty} \frac{1}{k!} = an! - bn! \sum_{k=0}^n \frac{1}{k!}$$

oltava kahden kokonaisluvun erotuksena myös kokonaisluku. Lähdetään arvioimaan:

$$\begin{aligned} 0 < bn! \sum_{k=n+1}^{\infty} \frac{1}{k!} &= b \sum_{k=n+1}^{\infty} \frac{n!}{k!} \\ &= b \left( \frac{1}{n+1} + \frac{1}{(n+1)(n+2)} + \cdots \right) \\ &\leq b \sum_{k=1}^{\infty} \frac{1}{(n+1)^k} \\ &= \frac{b}{(n+1)} \cdot \frac{1}{1 - \frac{1}{n+1}} = \frac{b}{n} < 1, \end{aligned}$$

kun valitaan  $n > b$ . Koska nollan ja ykkösen välissä ei ole kokonaislukuja, ei tämän lausekkeen arvo voi olla kokonaisluku. Väite on todistettu.

## Loppusanat

Näillä ideoilla on varsin paljon käyttöä erilaisten matemaattisten ongelmien ratkaisussa. Esimerkiksi luvun  $e$  transkendenttimitä arvioitaessa arvioidaan lineaarimuotoja, joille lähinnä saadaan ala-arvioksi, että ne varmasti ovat nolasta poikkeavia ja kokonaislukuarvoisia.

## Solmu 1/2022

ISSN-L 1458-8048

ISSN 1459-0395 (Painettu)

ISSN 1458-8048 (Verkkolehti)

Matematiikan ja tilastotieteen osasto

PL 68 (Pietari Kalmin katu 5)

00014 Helsingin yliopisto

*matematiikkalehtisolmu.fi*

Päätoimittaja:

*Anne-Maria Ernvall-Hytönen*, apulaisprofessori, Matematiikan ja tilastotieteen osasto, Helsingin yliopisto

Toimitussihteeri:

*Juha Ruokolainen*, FT

Sähköposti:

*toimitus@matematiikkalehtisolmu.fi*

Toimittajat:

*Pekka Alestalo*, dosentti, Matematiikan ja systeemianalyysin laitos, Aalto-yliopisto

*Sirkka-Liisa Eriksson*, dosentti, Matematiikan ja tilastotieteen osasto, Helsingin yliopisto

*Aapo Halko*, FT, Matematiikan ja tilastotieteen osasto, Helsingin yliopisto

*Olli Järvinen*, opiskelija, Matematiikan ja tilastotieteen osasto, Helsingin yliopisto

*Jyrki Lahtonen*, yliopistonlehtori, Matematiikan ja tilastotieteen laitos, Turun yliopisto

*Heikki Pokela*, tuntiopettaja, Tapiolan lukio

*Antti Rasila*, Associate Professor, Guangdong Technion - Israel Institute of Technology

*Mikko Sillanpää*, professori, Matemaattisten tieteiden laitos ja Biologian laitos, Oulun yliopisto

*Samuli Silta*, professori, Matematiikan ja tilastotieteen osasto, Helsingin yliopisto

*Kimmo Vehkalahti*, vanhempi yliopistonlehtori, Yhteiskuntatieteiden keskus, Helsingin yliopisto

*Esa Vesalainen*, tutkijatohtori, Matematiikan ja tilastotieteen osasto, Helsingin yliopisto

Tieteelliset asiantuntijat:

*Heikki Apiola*, dosentti, Matematiikan ja systeemianalyysin laitos, Aalto-yliopisto

*Mika Koskenoja*, dosentti, Matematiikan ja tilastotieteen osasto, Helsingin yliopisto

*Liisa Näveri*, FT, Opettajankoulutuslaitos, Helsingin yliopisto

Matematiikkadiplomit:

*Juha Ruokolainen*, juha piste ruokolainen 'at' yahoo piste com

*Marjatta Näätänen*, dosentti, Matematiikan ja tilastotieteen osasto, Helsingin yliopisto

Yliopistojen ja korkeakoulujen yhteyshenkilöt:

*Ari Koistinen*, FM, Metropolia Ammattikorkeakoulu

*Juha Lehtinen*, yliopistonlehtori, Matematiikan ja tilastotieteen laitos, Jyväskylän yliopisto

*Jorma K. Mattila*, professori, Sovelletun matematiikan laitos, Lappeenranta teknillinen yliopisto

*Jorma Merikoski*, emeritusprofessori, Informaatitieteiden yksikkö, Tampereen yliopisto

*Antti Viholainen*, tutkijatohtori, Fysiikan ja matematiikan laitos, Itä-Suomen yliopisto

Kansikuva:

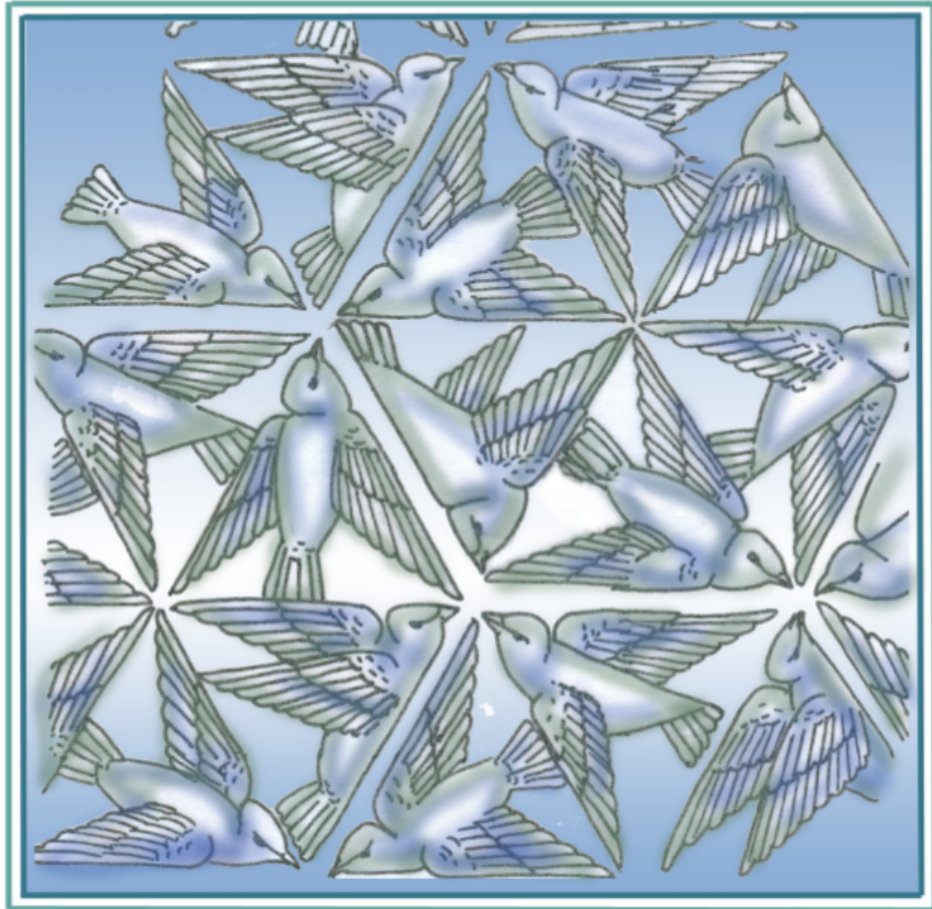
*Noora Isoeskelä*

Painopaikka:

*Painosalama Oy*

Numeroon 2/2022 tarkoitetut kirjoitukset pyydämme lähettämään 21.8.2022 mennessä.

Kiitämme taloudellisesta tuesta Jenny ja Antti Wihurin rahastoa.



 SOLMU  
MATEMATIIKKALEHTI

[matematiikkalehtisolmu.fi](http://matematiikkalehtisolmu.fi)