

Solmu

Matematiikkalehti
3/2012

<http://solmu.math.helsinki.fi>



Solmu 3/2012

ISSN-L 1458-8048

ISSN 1459-0395 (Painettu)

ISSN 1458-8048 (Verkkolehti)

Matematiikan ja tilastotieteen laitos

PL 68 (Gustaf Hällströmin katu 2b)

00014 Helsingin yliopisto

<http://solmu.math.helsinki.fi>

Päätoimittaja:

Markku Halmetoja, lehtori, Mäntän lukio

Toimitussihteeri:

Juha Ruokolainen, FT, Matematiikan ja tilastotieteen laitos, Helsingin yliopisto

Sähköposti:

toimitus@solmu.math.helsinki.fi

Toimituskunta:

Pekka Alestalo, dosentti, Matematiikan ja systeemianalyysin laitos, Aalto-yliopiston perustieteiden korkeakoulu

Heikki Apiola, dosentti, Matematiikan ja systeemianalyysin laitos, Aalto-yliopiston perustieteiden korkeakoulu

Sirkka-Liisa Eriksson, professori, Matematiikan laitos, Tampereen teknillinen yliopisto

Aapo Halko, FT, Matematiikan ja tilastotieteen laitos, Helsingin yliopisto

Ari Koistinen, FM, Metropolia Ammattikorkeakoulu

Mika Koskenoja, yliopistonlehtori, Matematiikan ja tilastotieteen laitos, Helsingin yliopisto

Matti Lehtinen, dosentti, Helsingin yliopisto

Liisa Näveri, tutkijatohtori, Opettajankoulutuslaitos, Helsingin yliopisto

Marjatta Näätänen, dosentti, Matematiikan ja tilastotieteen laitos, Helsingin yliopisto

Heikki Pokela, tuntiopettaja, Tapiolan lukio

Antti Rasila, tutkija, Matematiikan ja systeemianalyysin laitos, Aalto-yliopiston perustieteiden korkeakoulu

Hilkka Taavitsainen, lehtori, Ressun lukio

Graafinen avustaja:

Marjaana McBreen

Yliopistojen ja korkeakoulujen yhteyshenkilöt:

Virpi Kauko, FT, matemaatikko, virpi@kauko.org, Jyväskylä

Jorma K. Mattila, professori, jorma.mattila@lut.fi

Sovelletun matematiikan laitos, Lappeenrannan teknillinen yliopisto

Jorma Merikoski, dosentti, jorma.merikoski@uta.fi

Informaatiotieteiden yksikkö, Tampereen yliopisto

Petri Rosendahl, assistentti, petri.rosendahl@utu.fi

Matematiikan laitos, Turun yliopisto

Matti Nuortio, tutkijatohtori, matti.nuortio@oulu.fi

Matemaattisten tieteiden laitos, Oulun yliopisto

Timo Tossavainen, yliopistonlehtori, timo.tossavainen@uef.fi

Soveltavan kasvatustieteen ja opettajankoulutuksen osasto, Itä-Suomen yliopisto

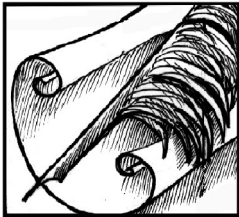
Numeroon 1/2013 tarkoitetut kirjoitukset pyydämme lähettämään 7.1.2013 mennessä.

Kiitämme taloudellisesta tuesta Jenny ja Antti Wihurin rahastoa.

Huom! Solmun paperiversio postitetaan vain niihin kouluihin, jotka ovat sitä erikseen pyytäneet. Toivomme, että lehteä kopioidaan kouluissa kaikille halukkaille.

Sisällys

Pääkirjoitus: Pitkän matematiikan alkajaisiksi (Markku Halmetoja)	4
Korean tasavalta – Daehan Minguk (Heikki Pokela)	6
Kiinalainen jäännöslause ripauksella kryptografiaa (Anne-Maria Ernvall-Hytönen)	8
Perinnöllisyyttä ja tilastotiedettä (Mikko J. Sillanpää)	11
Eksponenttijakaumasta (Jorma Merikoski)	13
Jännenelikulmioiden juhlaa – Tyttöjen matematiikkaolympialaisten tehtäväsatoa (Anne-Maria Ernvall-Hytönen)	15
Yksi helppo, viisi vaikeaa? – Kansainväliset matematiikkaolympialaiset 2012 (Matti Lehtinen)	19
Määrätyn integraalin opettamisesta differentiaalisesti (Kyösti Tarvainen)	23
Induktio, ympyrä, kartio ja pallo (Markku Halmetoja)	26
Pari vanhaa ylioppilastehtävää (Lehtori K.)	30



Pitkän matematiikan alkajaisiksi

Pääkirjoitus

Monet lukionsa juuri aloittaneista pitkän matematiikan opiskelijoista miettinevät parast'aikaa omia mahdollisuuksiaan menestyä valintansa kanssa. Tosiasia nimittäin on, että kaikki pitkällä matematiikalla aloittavat eivät suorita sitä loppuun. Syitä keskeyttämiseen voi olla monia. Jos matematiikka ei kertakaikkiaan kiinnosta ja valinta on suoritettu jonkinasteisen painostuksen alaisena, niin vaihto saattaa olla perusteltua. Liian heppoisin perustein sitä ei kuitenkaan pidä tehdä. Lukion alku on kevyehkön peruskoulun jälkeen monelle aikamoinen shokki. Vaatimukset ovat kovempia ja arvostelu ankarampaa, joten numerot pyrkivät alussa tippumaan lähes kaikissa aineissa. Tätä ei kuitenkaan pidä liikaa säikähtää vaan työhön on asennoiduttava uudella tavalla. Tärkeää on oppia kullekin aineelle ominaiset tehokkaat opiskelutavat. Matematiikassa se onneksi on helppoa, sillä aina voi tukeutua opiaineen omaan loogiseen rakenteeseen. Matematiikka nimittäin rakentuu hyvin yksinkertaisille perusperiaatteille, joista lähtien johdetaan uusia tuloksia niin, että kaikki osavaiheet ovat ymmärrettäviä. Valitettavasti tämä on nykyisien muotivirtauksien mukaan rakennetuissa oppimateriaaleissa osin onnistuttu häivyttämään ns. "käytännön sovellusten" alle. Tällöin varsinkin peruskoulussa matematiikka näyttäytyy oppilaalle sekavana kikka- ja kaavakokoelmana, josta poimitaan aina kulloisessakin sovelluksessa mahdollisesti tarvittava työkalu. Jos sama käytäntö jatkuu vielä lukiossakin, niin matematiikan opiskelu muuttuu kaavakirjan selämiseksi ja oma ajattelu jää kehittymättä.

Loogisesti etenevässä matematiikan oppimisessa lähde-

tään perusteista ja kulloinkin valmiiksi saatu kokonaisuus toimii samalla tavalla kuin vuorikiipeilijän rinneestä löytämä tasanne: sille voi pysähtyä lepäämään ja pohtimaan korkeammalle johtavia reittejä. Matematiikassa pysähdytään harjoittelemaan opittuun asiaan liittyvää laskutekniikkaa ja miettimään mahdollisia sovelluksia. Tärkeimmät löytyvät useimmiten matematiikan sisältä, sillä kunnolla opitun asian voi miltei poikkeuksetta aina laajentaa jollakin tavalla yleisemmäksi. Samalla opitun matematiikan määrä kasvaa ja laatu paranee, ja mitä suurempia kokonaisuuksia hallitsee, sitä parempia arkielämän sovelluksiakin pystyy käsittelemään.

Edellä sanotun havainnollistamiseksi katsotaan esimerkki oppimäärän alkupäästä. Pitkä matematiikka alkaa yleensä kahdella algebrallisella kurssilla, joilla opitaan jatkossa tarvittava lausekkeiden, yhtälöiden ja epäyhtälöiden käsittely. Lähtökohtana ovat peruskoulussa opitut reaalityökalujen järjestykseen ja laskutoimituksiin liittyvät laskulait, kuten yhteen- ja kertolaskun vaihdanta- ja liitälait, osittelulaki, kertolaskun merkkisäännöt ja tulon nollasääntö. Binomikaavojaakin

$$(a+b)(a-b) = a^2 - b^2$$

$$(a \pm b)^2 = a^2 \pm 2ab + b^2$$

tarvitaan, ja ne todistuvat osittelulain ja tulon vaihdantalain avulla. Toivottavasti ne ja neliöjuuri ovat jo peruskoulusta tuttuja. Siellä lienee myös opittu, että jos $a \geq 0$, niin yhtälön $x^2 = a$ ratkaisut ovat $x = \pm\sqrt{a}$. Mutta miksi tällä yhtälöllä ei ole muita ratkaisuja? Perusteluksi ei riitä opettajan antama ilmoitus. Asia on

selvitettävä yllämainittuihin laskulakeihin tukeutuen. Tiedetään, että $a = \sqrt{a^2}$, joten tarkasteltava yhtälö voidaan kirjoittaa muotoon

$$x^2 - \sqrt{a^2} = 0,$$

ja edelleen

$$(x + \sqrt{a})(x - \sqrt{a}) = 0. \quad (1)$$

Tulon nollasääntöä soveltaen (1) hajoaa kahdeksi ensimmäisen asteen yhtälöksi, joilla kummallakin on yksikäsitteisesti määrätty ratkaisu. Kovin merkillisiin arkipäivän sovelluksiin ei tällä tuloksella päästä, mutta samaa ajatusta voidaan soveltaa yleisempään yhtälöön

$$ax^2 + bx + c = 0, \quad (a \neq 0). \quad (2)$$

Hieman manipuloidulla, mm. $4a$:lla kertomalla, saadaan (2):n kanssa yhtäpitävästi

$$(2ax)^2 + 2(2ax)b + b^2 = b^2 - 4ac.$$

Jos $d = b^2 - 4ac \geq 0$, niin viimeksi saatu yhtälö voidaan binomikaavoja soveltaen kirjoittaa muotoon

$$(2ax + b)^2 - \sqrt{d}^2 = 0,$$

ja edelleen

$$(2ax + b + \sqrt{d})(2ax + b - \sqrt{d}) = 0.$$

Alkuperäinen yhtälö hajoaa tässäkin tapauksessa kahdeksi ensimmäisen asteen yhtälöksi, joiden perusteella saadaan toisen asteen yhtälön yleinen ratkaisukaava. Se on luonnollisesti osattava ulkoa ja sen johtaminen on käytävä läpi vaihe vaiheelta itsenäisesti, sillä muuten ei hallitse pitkän matematiikan kahden ensimmäisen kurssin olennaisinta sisältöä. Myöhemmin vastaan tulevia yhtälöitä voi ratkaista laskimellakin, mutta sen käyttö ilman että käsittää mitä on tekemässä näivettää aivotoiminnot ainakin matematiikan osalta.

Muinaisen Mesopotamian matemaatikot keksivät toisen asteen yhtälön ratkaisun noin 4000 vuotta sitten. Heidän mielenkiintonsa rajoittui vain yhtälön positiivisiin ratkaisuihin. Heillä ei ollut käytössään meidän helppoa algebrallista merkintätapaamme, vaan he ratkaisivat ongelman melkoista neroutta osoittaen geometrisen päättelyn kautta kirjaten tuloksensa verbaalisesti nuolenpääkirjoituksella savitauluihin. Matemaatikassa jos missä on kunnioitettava menneiden sukupolvien saavutuksia sillä ne ovat ikuisesti kestäviä. Ja niitähän ei voi kunnioittaa ellei niitä ymmärrä!

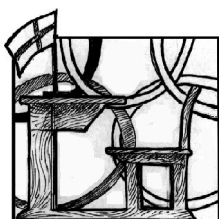
Tehtävien ratkaiseminen on olennainen osa koulumatematiikkaa. Ylioppilaskokeessakin osaaminen mitataan tehtäväsarjan avulla. Sillä on oma arvonsa valtakunnallisena mittarina, mutta opiskeluvaiheessa siihen ei kannata liikaa tuijottaa. Opiskelu saattaa vinoutua, jos tähtäimessä on yksinomaan siinä menestyminen. Lukion kurssit on syytä opiskella mahdollisimman perusteellisesti päättökoetta miettimättä; kun osaa asiat, on

menestys kaikenlaisissa kokeissa taattu. Tavanomaisen kotitehtävien kautta on tarkoitus saavuttaa välttämättömän laskemisen ja todistamisen rutiini. Siihen vaa-dittava tehtävämäärä lienee yksilöllinen, mutta jokaisen, joka aikoo oppimäärän suorittaa kunnolla, on se hankittava. Pelkillä rutiinitehtävillä ei kuitenkaan tavoiteta sellaista kypsyttää, jota yliopistossa opiskelun aloittaminen edellyttää. Siksi olisi käytettävä aikaa myös omatoimiseen harjoitteluun ja pohtimiseen. Tällöin tehtävät kannattaa valita huolella oman tasonsa mukaisiksi. Liian helpoista ei ole hyötyä ja liian vaikeista tulee stressi. Täytyy muistaa, että tehtävän vaikeus on suhteellinen käsite. Sama kysymys avautuu toiselle helposti ja toiselle ei ehkä koskaan. On myös olemassa satojakin vuosia tunnettuja matemaattisia ongelmia, joita kukaan ei toistaiseksi ole kyennyt ratkaisemaan. Ei siis kannata pahoittaa mieltään, jos tehtävä ei ratkea parin tunnin ankaran miettimisen jälkeen. Kokemus osoittaa, että ongelma, jota on keskittyneesti mietitty tunteja, joskus jopa päiviä, saattaa ratketa yllättäen jossakin aivan odottamattomassa yhteydessä. Jos siis tehtävä ei ratkea kohtuullisessa ajassa, niin unohda se toistaiseksi ja suorita helpompia tehtäviä. Ratkaisemattomaan kysymykseen voi aina palata myöhemmin.

Miten lähestytään tehtävää, joka aluksi vaikuttaa vaikealta tai jopa mahdottomalta? Tämäkin on varsin yksilökohtaista, mutta muutamia yleisiä strategioita kannattaa pitää mielessä. Aluksi voi muistella, onko aikaisemmin ratkaissut samantyyppisen helpomman kysymyksen, tai voisiko ratkaisua yrittää jossakin erikoistapauksessa. Kokemukset vastaavista tilanteista saattavat johtaa yleisen ratkaisun jäljille. Voi myös miettiä, missä yhteyksissä tehtävässä käytetyt käsitteet ovat muulloin esiintyneet. Voisiko annetuista tiedoista jonkin kiertotien kautta päästä ratkaisuun. Jos tehtävän lähtötiedoilla ei näyttäisi olevan juuri mitään tekemistä maalina olevan tuloksen kanssa, niin kannattaa ehkä ajatella takaperin: mitä olisi tunnettava, jotta kysytyn asian voisi ratkaista? Riittävätkö tehtävässä annetut tiedot näiden tarpeellisten esitietojen selville saamiseen. Kun yleinen ratkaisu on löydetty, kannattaa varmistaa, että se toimii myös erikoistapauksissa; tämä tavallaan takaa ratkaisun oikeellisuuden. Ratkaisu kannattaa myös analysoida kohta kohdalta kriittisesti ja miettiä, voisiko jonkin osan tehdä yksinkertaisemmin. Hyvästä tehtävästä kannattaa lopuksi myös laatia uusia muunnelmia ystäviensä iloksi!

Mistä löytää hyviä tehtäviä? Oppikirjoissa yleensä on vaativiaakin kysymyksiä, eikä niitä kaikkia ehditä käsitellä oppitunneilla. Jos niistä ei löydy riittävästi haastetta, niin esimerkiksi Solmun alisivulla <http://solmu.math.helsinki.fi/olympia/> on hyviä teoriapaketteja sekä valmennustehtäväsarjoja. Niihin up-poutumalla matematiikka muuttuu huomaamatta harrastukseksi, mistä on suuri etu kaikissa matemaattis-luonnontieteellisissä ja teknillisissä jatko-opinnoissa sekä myöhemmin työelämässä.

Markku Halmetoja



Korean tasavalta – Daehan Minguk

Heikki Pokela

Tapiolan lukio

PISA-menestys on houkuttellut ulkomaisia delegaatioita tutustumaan suomalaiseen koulujärjestelmään. Useammassa koulussa on jo totuttu vieraileviin ryhmiin. Omassa työpaikassani ovat korealaiset vierailleet kahteenkin otteeseen melko suurella ryhmällä. Mukana heillä on ollut niin ”rivi”opettajia kuin kasvatustieteen tutkijoita ja opetushallinnon virkamieskuntaakin.

Toisiin kulttuureihin tutustuminen avartaa, ja varsinkin vieraan kulttuurin koululaitoksen näkeminen antaa läpivalaisun yhteiskuntaan kenties jopa syvemmin kuin käynti museossa, turistiryistä puhumattakaan. Lähdin vastavierailulle Etelä-Koreaan tavoitteenani päästä keskustelemaan mahdollisimman monen koululaitoksen parissa toimivan henkilön kanssa. Näin välttäisin kokemasta nk. Potemkinin kullissia. Toki tämä kertomus tietenkin on subjektiivinen kuvaus eikä edes yritä esittää olevansa objektiivinen koko totuus Koreasta – tuosta koulutuksen suurvallasta.

Korealaisen Opetusministeriön alaisena toimii tutkimuskeskus KERIS (Korea education and research information centre), jonka erikoisalaa ovat interaktiiviset oppimisympäristöt. Pääsin vierailemaan heillä. Suomalainen peruskoulu oli heille miltei ikonin asemassa; he toivoisivat saavansa korealaista oppimiskäsitystä ajan myötä kammettua samaan suuntaan.

Heidän koelaboratorioissaan eli luokkahuoneissa oli jos jonkinlaista esitystekniikkaa. Jopa potkupalloa saatettiin pelata lattialle heijastetun interaktiivisen kentän avulla. Tämä oli kuulemma hyvä juttu, koska koulu-

jen ulkopuolella kaupungeissa harvemmin on edes tilaa pelikentille.

Korealaisen koulujärjestelmän epävirallisen rungon muodostavat yksityiset firmat, jotka antavat lisäopetusta koulutuntien jälkeen iltapäivällä. Esimerkiksi Daegun kaupungin varakkaimmilla alueilla on jopa kokonaisia katuja, joiden varsilla ei näy juuri muita kuin yksityisten koulutusfirmojen kylttejä. Seiskaluokasta lähtien kouluissa valtakunnallisten kokeiden pisteet lasketaan kaikki yhteen lukion päättyessä. Tämä ja pääsykokeet ratkaisevat, mihin yliopistoon pääsee, ja se puolestaan vaikuttaa, mihin sijoittuu yhteiskunnassa. Tuloksena on jonkinmoinen ylilyönti vanhempien suunnalta: lapsia opetetaan niin paljon kuin mahdollista kovalla hinnalla, jotta heidän tulevaisuutensa olisi turvattu. Onhan se inhimillisesti ymmärrettävää. Hivenen hillitäkseen menoa Korean hallitus on määrännyt kello kymmenen illalla takarajaksi. Sen jälkeen ei enää saa pitää yksityistunteja, mutta kieltoa rikotaan melko paljon.

Käynti korealaisessa koululuokassa antoi hyvin tutun vaikutelman. Miksipä luokkahuone olisi erilainen toisella puolella maapalloa, jos homma toimii. Opettajat valittelivat 50-luvulla rakennetun koulun epäsiisteyttä, homeongelmia ja huonoa ilmanvaihtoa. He arvelivat, että rikkaassa Suomessa ei enää kärsitä tällaisesta.

Opettajat tiedustelivat, kuinka oppilaita rangaistaan Suomessa. Jos Koreassa koulu käyttää ankaria rangaistuksia, siitä tulee usein suosittu vanhempien keskuu-

dessä. Korealainen oppimiskäsitys on tyypillisen aasialainen. Asioita treenataan (myös ulkomuistiin) riittävästi, jotta niiden välille on mahdollista muodostaa riittävästi yhtymäkohtia. Vasta tästä voi alkaa todellinen päättelyyn pohjaava oppiminen. Mielestäni meillä yritetään edetä ylemmille oppimistasoille ilman riittävää (ulko)muistia vahvistavaa harjoitusta.

Eräs matkan kohokohdista oli professori Yongjin Songin tapaaminen. Hän on Etelä-Korean olympiajoukkueen päävalmentaja. Etelä-Korea voitti vuoden 2012 matematiikkaolympialaiset Argentiinassa. Song oli onnesta soikeana, sillä kerrankin he voittivat sekä Kiinan että Japanin. Varsinkin Kiinaa Song pitää miltei mahdottomana ohittaa pistetaulukossa. Hänen mielestään olympiamitalit eivät tietenkään ole itsetarkoitus, vaan koulujärjestelmän kokonaiskehitys on tärkeätä. Mitalit ovat eräänlainen indikaatio onnistumisesta kokonaisuutena.

Professori Song kuuluu komiteaan, joka laatii Etelä-Korean kouluille matematiikan opetussuunnitelmat. Ymmärsin, että olympiajoukkueen päävalmentajana hänen osallistumisestaan kyseiseen komiteaan pidetään selviönä. Hän kuitenkin valitteli, että läheskään aina hänen mielipiteitään ei kuunnella, kun hän haluaisi kohentaa koulumatematiikan osaamistasoa. ”Ei tuota voida toteuttaa – sinä et tunne koulumaailman realiteetteja.”, hän saa usein vastaukseksi, koska hänellä ei ole pedagogian opintoja suoritettuina kuten muilla komitean jäsenillä. Hänen mielestään se, mitä matematiikasta opetetaan, pitäisi tulla matematiikan asiantuntijoilta ja pedagogian asiantuntijoiden huoleksi jäisi pikemminkin se, miten opetetaan.

Kilpailumatematiikan osa-alueita Song pitää edelleen olennaisina matematiikan opinnoissa. Viime aikoina hän on yrittänyt saada kombinatoriikan alkeita paremmin esille yläkouluun: jono, jossa on järjestys tai ei ole, voitaisiin hyvin opettaa jo yläkoulussa. Viimekesäistä

olympiavoittoa hän pitää hieman myös sen ansiona, että kombinatoriikan osuutta painotettiin valmennuksessa hieman aiempaa enemmän. Kysyin Songilta, onko kombinatoriikka sellainen osa-alue, jonka kouluopetukseen hän mahdollisesti luottaa vähiten. Hän vastasi, ettei luota täysin minkään osa-alueen kouluopetukseen, mutta kombinatoriikka on ollut huonoimmassa asemassa.

Koulujen lisäksi toki myös muuhun kulttuuritarjontaan kannattaa tutustua. Kävimme Sillan (ikivanha korealainen kuningaskunta) pääkaupungissa raunioilla ja museoissa. Korean historiaa leimaa pitkälti elämä kahden suurvallan, Kiinan ja Japanin, välissä. Tässä on monta yhtymäkohtaa meikäläiseen menneisyyteen. Eri-tyisesti Japani on miehittänyt Koreaa traumatisoiden maiden välisiä suhteita. Korean omaa kirjoitettua kieltä ei oppinut ylimystö suvainnut käyttää vielä reilu sata vuotta sitten. Virallisia dokumentteja kirjoitettiin kiinalaisin merkein. (Jokin yhtymäkohta tässäkin?)

Aseman hyväksikäyttö vaikuttaa olevan yleistä vielä nykyäänkin. Urallaan etenevän työntekijän on yleensä tarjottava rahaa ja/tai muita palveluksia suosittelijoilleen – muuten eteneminen voi tyssätä. Kysäisin, kuinka normaali ihminen kestää tämän. Ajattelen koko asia osaksi yhteiskuntaa, sain vastaukseksi. Jouduin tietty vastaamaan, kuinka Suomessa nämä asiat sujuvat. Vastasin, että täysin ilman korruptiota emme elä mekään, mutta käsittääkseni lieveilmiöt jäävät yksittäistapauksiksi.

Korealaisten (koulu)systeemeissä on epäilemättä hyviä puolia kuten koulutuksen vahva arvostus, mutta on myös vakavia ongelmakohtia. Ehkä puutteistaan huolimatta suomalainen koulujärjestelmä on paras kehitysalusta meidän tulevaisuuden koulullemme, vaikka paljon tehtävää onkin. Jokainen valtakunta valitsee itsenäisesti oman suuntansa, mutta onko silti itämailla jotain? Edes jotain tavoittelemisen arvoista?

Tulosta koulusi ilmoitustaululle Solmun etusivulta <http://solmu.math.helsinki.fi>

- Solmun juliste
- Monikielisen matematiikkaverkkosanakirjan juliste



Kiinalainen jäännöslause ripauksella kryptografiaa

Anne-Maria Ernvall-Hytönen

Matematiikan ja tilastotieteen laitos, Helsingin yliopisto

Johdanto

Kiinalaisen jäännöslauseen nimi vaatii ehkä hieman selvennystä. Lauseen alkuperäinen muotoilu löytyy Sun Zin kirjasta, johon englanniksi viitataan nimellä *The Mathematical Classic of Sun Zi*. Lauseen tarkka ajankohta lienee hieman hämärän peitossa: Wikipedia kertoo tämän kirjan olevan 300-luvulta. Toisaalta kirjoittajan elinajasta todetaan vain hänen eläneen 300–500-luvulla. Kenneth Rosenin lukuteorian kirjassa [1] (*Elementary number theory and its applications*) annetaan ymmärtää, että lause on ehkäpä 100-luvulta. Tarkalla ajankohdalla ei varmasti ole väliä, oleellisempaa on tietää, että kyseessä on vanha ja kiinalainen lause. Yleistetty muotoilu puolestaan löytyy Qin Jiushaon kirjasta *Da yan shu*, joka on kirjoitettu 1247.

Lauseen muotoilu ja todistus

Lyhyesti sanottuna kiinalainen jäännöslause kertoo kongruenssiyhtälöryhmälle tietyn ehdoin löytyvän ratkaisun:

Kiinalainen jäännöslause. Olkoot $m_1, m_2, \dots, m_r$ pareittain yhteistekijättömiä kokonaislukuja. Tällöin

kongruenssiyhtälöryhmällä

$$x \equiv a_1 \pmod{m_1}$$

$$x \equiv a_2 \pmod{m_2}$$

$$\vdots$$

$$x \equiv a_r \pmod{m_r}$$

on yksikäsitteinen ratkaisu modulossa

$$M = m_1 m_2 \cdots m_r.$$

Ennen kuin siirrytään todistukseen, todetaan, että ehto lukujen $m_1, m_2, \dots, m_r$ pareittaisesta yhteistekijättömyydestä on paikallaan: Mikäli tätä ehtoa ei olisi, ei välttämättä olisi yhtään ratkaisua, kuten jos $x \equiv 1 \pmod{2}$ ja $x \equiv 2 \pmod{6}$, jolloin ensimmäinen ehto kertoo luvun x olevan pariton, ja toinen ehto kertoo luvun x olevan parillinen ja hieman muuta vielä lisäksi. Toisaalta ratkaisuja voisi olla useita. Esimerkkinä tarkastellaan vaikkapa tilannetta, jossa $x \equiv 3 \pmod{6}$ ja $x \equiv 6 \pmod{9}$, jolloin luvut $x \equiv 15 \pmod{18}$ toteuttavat ehdot, eli modulossa $54 = 9 \cdot 6$ on useita ratkaisuja.

Nyt voimme siirtyä todistukseen.

Todistus. Merkitään $M_k = \frac{M}{m_k}$ kaikilla $1 \leq k \leq r$. Nyt $\text{syty}(m_k, M_k) = 1$, jolloin luvulla M_k on olemassa käänteisluku modulossa m_k (tämän löytää vaikkapa Diofantoksen yhtälön ratkaisemalla Eukleideksen algoritmia käyttäen), eli on olemassa sellainen s_k , että

$M_k s_k \equiv 1 \pmod{m_k}$. Muodostetaan luku

$$x_0 = a_1 M_1 s_1 + a_2 M_2 s_2 + \cdots + a_r M_r s_r.$$

Huomataan, että

$$x_0 = a_1 M_1 s_1 + \cdots + a_r M_r s_r \equiv a_k \pmod{m_k},$$

sillä $m_k \mid M_j$, jos $j \neq k$. (Muista, miten luku M_j on muodostettu!) Lisäksi $a_k M_k s_k \equiv a_k \pmod{m_k}$, koska luku s_k on luvun M_k käänteisluku modulossa m_k . Selvästi siis x_0 on ratkaisu.

Osoitetaan nyt, että muita ratkaisuja ei modulossa M ole. Tarkastellaan lukuja x_0 ja x_1 , jotka ovat yhtälöryhmän ratkaisuja. Tällöin

$$x_1 - x_0 \equiv a_k - a_k = 0 \pmod{m_k}$$

kaikilla $1 \leq k \leq r$, eli $m_k \mid (x_1 - x_0)$. Koska luvut m_k ovat yhteistekijättömiä, seuraa tästä $M \mid (x_1 - x_0)$, eli ratkaisu on yksikäsitteinen modulossa M . Todistus on valmis.

Katsotaanpa nyt esimerkkiä kiinalaisen jäännöslauseen käytöstä, eli ratkaistaan yhtälöryhmä

$$\begin{aligned} x &\equiv 2 \pmod{5} \\ x &\equiv 3 \pmod{7}. \end{aligned}$$

Koska $x \equiv 2 \pmod{5}$, voidaan kirjoittaa $x = 5k + 2$. Sijoitetaan tämä jälkimmäiseen yhtälöön:

$$5k + 2 \equiv 3 \pmod{7},$$

eli $5k \equiv 1 \pmod{7}$. Nyt voi tietenkin repiä hatusta luvun 5 käänteisluvun modulossa 7, tai sen voi selvittää yksinkertaisesti ratkaisemalla Diofantoksen yhtälön $5k - \ell 7 = 1$. Käytetään Eukleideksen algoritmia:

$$\begin{aligned} 7 &= 5 + 2 \\ 5 &= 2 \cdot 2 + 1 \end{aligned}$$

eli $1 = 5 - 2 \cdot 2$, josta sijoittaen ensimmäisestä yhtälöstä ratkaistun kakkosen jälkimmäiseen:

$$1 = 5 - 2 \cdot (7 - 5) = 3 \cdot 5 - 2 \cdot 7.$$

Luvun 5 käänteisluku modulossa 7 on siis luku 3, eli voidaan valita $k = 7h + 3$. Sijoitetaan tämä lausekkeeseen $x = 5k + 2$:

$$\begin{aligned} x &= 5k + 2 = 5(7h + 3) + 2 \\ &= 35h + 15 + 2 = 35h + 17 \equiv 17 \pmod{35}. \end{aligned}$$

Yhtälöryhmän ratkaisu modulossa 35 on siis $x \equiv 17$. Halutessaan tämän voi myös helposti tarkistaa.

Yllä olevan yhtälöryhmän ratkaisun olisi toki voinut hakea kiinalaisen jäännöslauseen todistusta jäljitellen.

Luvun loppuun pohdintatehtävä: Mikäli yhtälöryhmässä

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \end{aligned}$$

eivät luvut m_1 ja m_2 ole yhteistekijättömiä, niin milloin yhtälöryhmällä on kuitenkin ratkaisu? Missä modulossa se on yksikäsitteinen? Rosenin kirjan tehtävistä ([1], sivu 142) voi tässä olla apua, mutta tehtävä on kyllä ratkeava ilmankin sitä.

Hyödyllinen lukukokemus kiinalaisen jäännöslauseen käytöstä voi myös olla [2].

Hyödyt RSA:n käytössä

Jotta voimme järkevästi pohtia kiinalaisen jäännöslauseen hyödyistä RSA-kryptosysteemin käytössä, on syytä ensin käydä läpi RSA:n toimintaperiaate.

RSA on siis kryptosysteemi, eli salausjärjestelmä paremmalla suomella sanottuna. Sitä käytetään tiedon salaamiseen. Kriittistä on, että lähettäjä pystyy tiedon salaamaan, vastaanottaja puolestaan salauksen purkamaan, ja että ulkopuoliset eivät salausta voi purkaa. Käytännössä on lisäksi toivottavaa, että mikään operaatio ei kestä tuhattomien kauan.

RSA:ssa on julkinen avain (n, e) ja salainen avain $(\varphi(n), d)$, missä $\varphi(n)$ on Eulerin funktio (eli jos

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

on luvun n alkutekijähajotelma, niin

$$\varphi(n) = p_1^{\alpha_1-1} (p_1 - 1) p_2^{\alpha_2-1} (p_2 - 1) \cdots p_k^{\alpha_k-1} (p_k - 1).$$

Tiedetään myös, että n on muotoa pq , missä p ja q ovat kaksi eri alkulukua. On syytä huomata, että vaikka luku n tunnetaan, ei lukua $\varphi(n)$ ole helppo laskea, koska se edellyttää luvun n alkutekijöiden tuntemista, ja tämä taas on yleisessä tilanteessa hyvin hankalaa.

Käytännössä luvun $\varphi(n)$ pystyy laskemaan, mikäli luvut p ja q on tiedossa. Homma toimii myös toisin päin: jos luvun $\varphi(n)$ tietää, niin luvut p ja q on helppo selvittää. Jätetään tämän toteaminen aktiivisille lukijoille harjoitustehtäväksi.

Lisäksi luvut e ja d on valittu niin, että $ed \equiv 1 \pmod{\varphi(n)}$. Tämä valinta on helppo tehdä, mikäli $\varphi(n)$ on tiedossa, valitsemalla ensin e tai d ja ratkaisemalla sitten Diofantoksen yhtälö $ed - \ell \varphi(n) = 1$.

RSA toimii seuraavasti:

1. Alice saa päähänsä, että hän haluaa ottaa vastaan viestejä salattuna. Hän valitsee alkuluvut p ja q , laskee luvut $n = pq$ ja $\varphi(n) = (p-1)(q-1)$. Hän valitsee vielä luvun e ja laskee luvun d ratkaisemalla Diofantoksen yhtälön $ed - \ell \varphi(n) = 1$.

2. Hän julistaa lukuparin (n, e) kaikelle kansalle.
3. Bob päättää lähettää salaisen viestin Alicelle. Viesti on luku w .
4. Bob laskee luvun w^e modulossa n ja lähettää lopputuloksen Alicelle.
5. Alice ottaa vastaan Bobin lähettämän luvun, jota merkitään tässä kirjaimella v ja laskee:

$$v^d \equiv w^{ed} = w^{1+\ell\varphi(n)} \equiv w \pmod{n},$$

eli hän saa modulossa n Bobin lähettämän luvun w . Kunhan n on riittävän suuri (käytännössä se valitaan olemaan joitakin tuhansia bittejä, jotta systeemi on turvallinen), voi Bob lähettää varsin isojakin lukuja tietäen, että Alice saa ne oikein.

Salaus perustuu siis sille, että luvun d selvittäminen on hirvittävän hankalaa, ja brute force -ratkaisu kestäisi liian pitkään.

Yleisesti ottaen RSA on hyvin turvallinen: Mikäli RSA murtuu, niin myös lukujen tekijöihinjako-ongelma on ratkeava, ainakin kahden alkutekijän tapauksessa. Tämä ongelma taas on hyvin vanha, ja hyvin hankalaksi todettu. Kuitenkin joitakin rajoituksia on: luku d ei saa olla kovin pieni, eikä myöskään liian lähellä lukua $\varphi(n)$. Ei myöskään ole turvallista, jos luvut p ja q ovat liian lähellä toisiaan. Turvallisuuden nojalla toisaalta yleensä vaaditaan, että $p < q < 2p$. Nämä rajoitukset ovat melko kosmeettisia, vaikka toisinaan joitakin niistä kovin mielellään rikkoisikin nopeuden nimissä.

Jotain kuitenkin nopeudenkin kanssa on tehtävissä. Sen sijaan, että Alice laskisi luvun v^d suoraan modulossa n , voi hän laskea sen moduloissa p ja q , mikä on nopeampaa, sillä hän voi redusoida paitsi välituloksia moduloissa p ja q , voi hän redusoida eksponentin moduloissa p ja q , jolloin potenssiinkorotuksia täytyy tehdä paljon vähemmän. Laskettuaan luvut $w_p \equiv v^d \pmod{p}$ ja $w_q \equiv v^d \pmod{q}$, laskee hän luvun w käyttäen kiinalaista jäännöslauseetta, sillä $w \equiv w_p \pmod{p}$ ja $w \equiv w_q \pmod{q}$.

Laitetaan loppuun pohdiskelutehtävä (jolla ei ole mitään tekemistä kiinalaisen jäännöslauseen kanssa): Määritä mahdollisimman suuri h (riippuen luonnollisestikin luvusta n) niin, että tietäen vain luvun n pystyt löytämään sen alkutekijät p ja q , jos $n = pq$ ja $|p - q| < h$. (Vihje: neliöiden jakauma on mielenkiintoinen asia.)

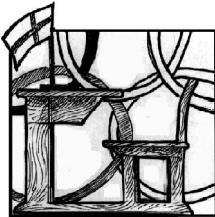
Viitteet

- [1] K. H. Rosen, *Elementary number theory and its applications*. Addison Wesley, 3rd Edition, 1993.
- [2] J. Herman, R. Kučera and J. Šimša, *Equations and Inequalities: Elementary Problems and Theorems in Algebra and Number Theory*, Canadian Mathematical Society Books in Mathematics 1, Springer-Verlag, New York, 2000.

Uutta Verkko-Solmun matematiikkadiplomisivulla

Diplomi VII tehtävineen sekä diplomin VIII tehtävät ovat ilmestyneet osoitteessa

<http://solmu.math.helsinki.fi/2008/diplomi/diplomi.html>



Perinnöllisyyttä ja tilastotiedettä

Mikko J. Sillanpää

Matemaattisten tieteiden laitos, Biologian laitos ja Biocenter Oulu
Oulun yliopisto
mikko.sillanpaa@oulu.fi

Modernin molekyylibiologian laboriotekniikat tuottavat suuria määriä geneettisiä mittaussaineistoja. Tilastomatematiikan lineaarisia regressiomalleja voidaan käyttää kytkemään tutkittavan perinnöllisen ominaisuuden (kuten esimerkiksi ihmisen pituuteen, verenpaineeseen tai johonkin sairauteen liittyvät mittaukset) ihmisen DNA:sta tehtyihin mittauksiin. Tällöin voidaan saada tietoa, missä kohdassa genomia (i. kromosomistoa) olevat mittaukset sopivat parhaiten yhteen tutkittavan perinnöllisen ominaisuuden mittausten kanssa. Tällaista toimenpidettä eli näkyvän tason havaintojen ”sovittamista” geneettisen tason mittauksiin (i. genotyyppeihin) kutsutaan yleisesti geenien kartoitustehtäväksi (ks. Esimerkki). Vaihtoehtoisesti samanlaista tilastomatematiikan mallia voidaan käyttää vaihtelevalla menestyksellä ennustamaan tutkittavaa perinnöllisen ominaisuuden arvoa tai sairastumisalttiutta/riskiä henkilöillä DNA:sta tehtyjen mittausten perusteella. Vastaavien tilastollisten mallien tutkimus ja käyttö modernissa kasvi- ja eläinjalostuksessa ennustamaan kyseisen lajikkeen tai eläimen perinnölliseen ominaisuuteen liittyvää jalostuksellista arvoa on yksi tämän hetken ajankohtaisimpia maatalouteen liittyviä tutkimuskysymyksiä (ks. Juga et al., 2012).

Koska useat perinnölliset ominaisuudet näyttäisivät olevan tämänhetkisen tutkimuksen valossa sellaisia, että niihin samanaikaisesti vaikuttaa suuri joukko gee-

nejä ja ympäristöllisiä tekijöitä, on niiden paikantaminen ja käyttö ennustetarkoituksiin tehokkaampaa malleilla, jotka tarkastelevat useampaa mittaushetkeä samanaikaisesti. Toisaalta koska yksilöiden määrä, joilta DNA-mittaukset otetaan, on tyypillisesti paljon pienempi kuin mittauspisteiden määrä, ei jokaisen mittauspisteiden vaikutusta voida samanaikaisesti arvioida (koska mahdollisten ratkaisujen määrä on suuri) ilman, että käytetään niin sanottua tilastollista muuttujanvalintaa tai *a priori* -informaatiota (esimerkiksi pakottamalla suuri joukko mittauspisteiden vaikutuksista nol- laan).

Tällainen suurien mittaussaineistojen tyypillinen ongelma tunnetaan nimellä ”small n , large p ”, ja sen arviointiin käytettävät muuttujanvalinnan tilastolliset menetelmät ovat tällä hetkellä monessa perinnöllisyyteen liittyvässä tutkimuskysymyksessä keskeisessä asemassa. Tutkimusaineistoissa voi tyypillisesti olla satoja tuhansia tai jopa miljoonia mittauspisteitä pitkin DNA:ta, jotka on mitattu tyypillisesti sadoilta tai tuhansilta tutkimusyksilöiltä.

Tällaisten ongelmien tilastollisten ratkaisumenetelmien suunnittelu ja jatkokehitys on geneettisten aineistojen käsittelyyn erikoistuneiden tilastotieteen tutkijoiden arkipäivää. Tällaisia henkilöitä koulutettaessa on tilastotieteen, matematiikan ja sovelletun matematiikan opintojen luoma luja pohja sellainen kivijalka, jota on mahdoton muilla opinnoilla korvata. Toisaalta

myös perinnöllisyystiedettä pitää jaksaa opiskella niin paljon, että sen käsitteillä voi vaivatta operoida. Siksi aito monitieteisyys ei mainosarvostaan huolimatta ole laji, jossa saadaan nopeita voittoja ja huikeita valmistusaikoja.

Henkilöitä, jotka käyttävät, ymmärtävät tai kehittävät yllä kuvatun kaltaisia tilastomatematiikan menetelmiä, on työmarkkinoilla jatkuvasti liian vähän kysyntään nähden. Tässä joukossa erityisesti ”hyvin biologiaa puhuvia” matematiikasta tai tilastotieteestä valmistuneita maistereita/tohtoreita on niukasti. Siksi haluankin suositella matematiikan ja tilastotieteen maisteriopintoja pohjaopinnoiksi biologiasta kiinnostuneille opiskelijoille.

Esimerkki tyypillisestä lineaarisesta regressiomallista on

$$y_i = b_0 + \sum_{j=1}^p x_{ij}b_j + e_i \quad (i = 1, \dots, n).$$

Tässä y_i on näkyvän tason havainto tutkittavasta perinnöllisestä ominaisuudesta yksilöllä i , b_0 on vakioter-
mi, joka halutaan selvittää, x_{ij} on geneettisen tason

mittausarvo (esimerkiksi -1 genotyyppille AA, 0 genotyyppille AB ja 1 genotyyppille BB) yksilöllä i DNA:n kohdassa j . Kulmakerroin b_j kuvaa mittauspisteen vaikutusta tutkittavaan ominaisuuteen kohdassa j , joka halutaan selvittää kaikissa DNA:n kohdissa. Jäännöstermit e_i oletetaan samoin jakautuneiksi ja keskenään riippumattomiksi siten, että ne kukin noudattavat samanlaista normaalijakaumaa, $e_i \sim N(0, \sigma^2)$, varianssilla σ^2 . Tämä jäännöstermeille tehty oletus antaa yleisesti kriteerin mallin sopivuuden tarkasteluun aineistossa $((y_i, x_{ij}), i = 1, \dots, n; j = 1, \dots, p)$, jonka perusteella myös tuntemattomille muuttujille voidaan tuottaa arviot. Jotta arviot voidaan tuottaa myös tilanteessa, kun $p > n$, lisäksi tarvitaan muuttujan valintaa tai *a priori* -informaatiota.

Muuta aiheesta suomenkielellä:

Juga, J., Sillanpää M. J., Mäntysaari E. (2012) ”Lypsykarjan genominen valinta” kirjassa: ”Maailma muuttuu: muuttuuko maatalous.” Sivut 165–172. Mervi Sepänen (ed.).

Verkko-Solmun oppimateriaalit

Osoitteesta <http://solmu.math.helsinki.fi/oppimateriaalit.html> löytyvät oppimateriaalit:

Reaalianalyysiä englanniksi (William Trench)

Geometrian perusteita (Matti Lehtinen)

Geometria (K. Väisälä)

Lukualueiden laajentamisesta (Tuomas Korppi)

Jaksolliset desimaaliesitykset algebrallisesta näkökulmasta (Jaska Poranen ja Pentti Haukanen)

Algebra (Tauno Metsänkylä ja Marjatta Näätänen)

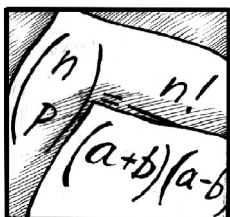
Algebra (K. Väisälä)

Matemaattista fysiikkaa lukiolaiselle (Markku Halmetoja ja Jorma Merikoski)

Lukuteorian helmiä lukiolaisille (Jukka Pihko)

Matematiikan peruskäsitteiden historia (Erkki Luoma-aho)

Matematiikan historia (Matti Lehtinen)



EkspONENTTijakaumasta

Jorma Merikoski

Informaatitieteiden yksikkö, Tampereen yliopisto
jorma.merikoski@uta.fi

EkspONENTTijakauman tiheysfunktio

$$f(x) = \begin{cases} ae^{-ax}, & \text{kun } x \geq 0, \\ 0, & \text{kun } x < 0, \end{cases}$$

missä $a > 0$. On helppo osoittaa, että f todellakin on tiheysfunktio ja että tämän jakauman sekä odotusarvo että keskihajonta on $1/a$. On myös helppo osoittaa, että eksponenttijakauman kertymäfunktio

$$F(x) = \begin{cases} 1 - e^{-ax}, & \text{kun } x \geq 0, \\ 0, & \text{kun } x < 0. \end{cases}$$

Lukiossa eksponenttijakaumaa käsitellään vain ohimennen (ks. esim. [1, teht. 299]), jos ollenkaan, mutta se ansaitsisi enemmän huomiota. Nimittäin satunnaismuuttuja on ”muistiton”, jos ja vain jos se noudattaa eksponenttijakaumaa. Tämä seuraa kiinnostavalla tavalla eksponenttifunktion ominaisuuksista. Käsittelemme tätä asiaa enimmäkseen Rossin kirjan [2, luku 5.2.2] perusteella.

Mitä tarkoittaa satunnaismuuttujan muistittomuus? Olettakaamme, että tietty laite L on pysynyt käyttökunnossa melko kauan. Lisääkö vai vähentääkö tällainen tieto todennäköisyyttä sille, että L toimii edelleen hyvin? Voitaisiin ajatella, että se vähentää, koska L on jo tullut näin ”vanhaksi”. Toisaalta voitaisiin ajatella päinvastoin, että se lisää, koska L on jo osoittautunut näin ”kestäväksi”. Kumpi vastaus on oikea, riippuu

tietenkin L :stä ja tarkasteltavien ajanjaksojen pituuksista. Mutta tämä esimerkki oikeuttaa myös ”kompromissiin” näiden vastausten välillä eli ajattelemaan, ettei tällaisella tiedolla ole vaikutusta. Silloin todennäköisyys sille, että L toimii edelleen, ei riipu siitä, kuinka kauan L on jo toiminut. Toisin sanoen L :n jäljellä oleva ”elinaika” on ”muistiton” sikäli, ettei se riipu L :n ”iästä”.

Yleisesti sanomme, että satunnaismuuttuja X on *muistiton*, jos

$$P(X > s + t \mid X > t) = P(X > s)$$

eli

$$P(X > s + t) = P(X > s)P(X > t)$$

kaikilla $s, t \geq 0$.

EkspONENTTijakauma on helppo osoittaa muistittomaksi. Nyt herää mielenkiintoinen käänteisongelma: Onko olemassa muita muistittomia jakaumia? Näytämme, ettei ole.

Tarkastelemme satunnaismuuttujaa X , jonka kertymäfunktio on F . Merkitsemme $\bar{F}(x) = P(X > x)$. Tällöin X on muistiton, jos ja vain jos

$$\bar{F}(s + t) = \bar{F}(s)\bar{F}(t)$$

kaikilla $s, t \geq 0$. Määritämme aluksi kaikki ne oikealta jatkuvat funktiot g (kertymäfunktion täytyy olla oikealta jatkuva), jotka toteuttavat *funktionaalisyhtälön*

$$g(s+t) = g(s)g(t) \quad (1)$$

kaikilla $s, t \geq 0$.

Aluksi huomaamme, että välttämättä

$$g\left(\frac{2}{n}\right) = g\left(\frac{1}{n} + \frac{1}{n}\right) = g\left(\frac{1}{n}\right)g\left(\frac{1}{n}\right) = g\left(\frac{1}{n}\right)^2$$

kaikilla $n \in \mathbb{Z}_+$. Edelleen näemme induktiolla, että

$$g\left(\frac{m}{n}\right) = g\left(\frac{1}{n}\right)^m \quad (2)$$

kaikilla $m, n \in \mathbb{Z}_+$. Asettamalla nyt $m = n$ saamme

$$g(1) = g\left(\frac{1}{n}\right)^n$$

eli

$$g\left(\frac{1}{n}\right) = g(1)^{\frac{1}{n}}. \quad (3)$$

Yhtälöiden (2) ja (3) perusteella

$$g\left(\frac{m}{n}\right) = g(1)^{\frac{m}{n}} \quad (4)$$

kaikilla $m, n \in \mathbb{Z}_+$ eli

$$g(x) = g(1)^x, \quad (5)$$

kun $x > 0$ on rationaalinen. Lisäksi tämä pätee arvolla $x = 0$, koska g on oikealta jatkuva. Mutta (5) pätee myös x :n ollessa irrationaalinen. Nimittäin tässä tapauksessa on olemassa sellainen jono (x_k) x :ää suurempia rationaalilukuja, että $x = \lim_{k \rightarrow \infty} x_k$, joten g :n oikeanpuolisen jatkuvuuden, yhtälön (4) ja eksponenttifunktion jatkuvuuden perusteella

$$\begin{aligned} g(x) &= g\left(\lim_{k \rightarrow \infty} x_k\right) \\ &= \lim_{k \rightarrow \infty} g(x_k) \\ &= \lim_{k \rightarrow \infty} g(1)^{x_k} \\ &= g(1)^{\lim_{k \rightarrow \infty} x_k} = g(1)^x. \end{aligned}$$

Siis (5) on voimassa kaikilla ei-negatiivisilla reaaliluvuilla x .

Merkitsemällä $a = -\ln g(1)$ saamme

$$g(x) = e^{-ax}. \quad (6)$$

Siis g :n täytyy olla muotoa (6), missä $a \in \mathbb{R}$ on mielivaltainen. Toisaalta jokainen tämänmuotoinen funktio toteuttaa selvästi funktionaaliyhtälön (1). Näin ollen tuon funktionaaliyhtälön kaikki oikealta jatkuvat ratkaisut ja vain ne ovat muotoa (6) (ja siis jatkuvia).

Kertymäfunktioita F koskeva vastaava ehto on

$$\bar{F}(x) = e^{-ax}$$

eli

$$F(x) = 1 - e^{-ax}$$

kaikilla $x \geq 0$. Mutta nyt täytyy olla $a > 0$, jotta F olisi kertymäfunktio. On helppo nähdä, että $F(x) = 0$, kun $x < 0$. Olemme siis osoittaneet, että eksponenttijakauma on ainoa muistiton jakauma.

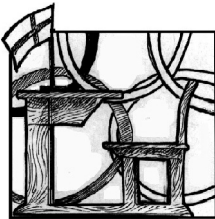
Seuraava esimerkki on asiallisesti sama kuin [2, esim. 5.2]. Olkoon P jokin sellainen paikka, jossa ”asiakkaita” palvellaan kahdelta ”luukulta” tai muusta ”palvelupisteestä”. Kun A tulee P :hen, kummallakin luukulla on asiakas; olkoot he B ja C . Ottamansa jonotusnumeron perusteella A pääsee asioimaan heti sen jälkeen, kun B tai C on lopettanut. Saatuaan asiansa toimitetuksi A poistuu heti. Millä todennäköisyydellä joko B tai C vielä jatkaa silloin asiointiaan?

Tätä tehtävää ei tietenkään voida ratkaista ilman lisäoletuksia. On yksinkertaisinta olettaa, että luukulla asiointin kesto noudattaa eksponenttijakaumaa tietyllä parametrilla a . Kun A pääsee luukulle, asiointi toisella luukulla kestää vielä ajan, joka eksponenttijakauman muistittomuuden takia noudattaa tätä samaa eksponenttijakaumaa. Olkoon X siellä asioiva B tai C . Tällöin A :n ja X :n välinen tilanne on täysin symmetrinen, joten kysytty todennäköisyys on $\frac{1}{2}$.

Mutta eikös todennäköisyyden sille, että X saa asiansa toimitetuksi ennen A :ta, pitäisi olla suurempi kuin $\frac{1}{2}$, koska X on jo ehtinyt jonkin aikaa asioida A :n aloittaessa? Oikeastaan todennäköisyys $\frac{1}{2}$ saattaa vaikuttaa suorastaan järjettömältä. Kuitenkin järjellisyys tai järjettömyys riippuu täysin siitä, miten hyvin tai huonosti eksponenttijakauma sopii mallintamaan asiointin kestoa. Lukijan mietittäväksi jää keksiä esimerkki, jossa tämä jakauma sopii hyvin, ja toinen esimerkki, jossa se sopii huonosti. Tämä tehtävä on helppo, mutta lukija saa myös vaikean tehtävän: Onko funktionaaliyhtälöillä (1) epäjatkuvia ratkaisuja?

Viitteet

- [1] M. Halmetoja, K. Häkkinen, J. Merikoski, L. Pippola, H. Silfverberg, T. Tossavainen, *Matematiikan taito 13: Differentiaali- ja integraalilaskennan jatkokurssi*, WSOY, 2008.
- [2] S. M. Ross, *Introduction to Probability Models*. 7th Ed., Acad. Pr., 2000.



Jännelikulmioiden juhlaa – Tyttöjen matematiikkaolympialaisten tehtäväsatoa

Anne-Maria Ernvall-Hytönen

Matematiikan ja tilastotieteen laitos, Helsingin yliopisto

Cambridgessa järjestettiin 10–16.4.2012 kautta aikain ensimmäiset Euroopan tyttöjen matematiikkaolympialaiset. Kilpailun idea oli saatu Kiinasta, jossa tyttöjen kilpailuja on ollut jo pitkään. Kilpailun tarkoitus oli kannustaa tyttöjä matematiikkakilpailuihin tarjoamalla yksi mukava väliporras matkalla kansainvälisiin matematiikkaolympialaisiin. Ajatus on hyvä: kansainvälisissä matematiikkaolympialaisissa tyttöjen määrä on vain n. 10 %, jolloin moni tyttö väistämättä tuntee itsensä joukosta poikkeavaksi. Tehtävät ovat haastavia. Tarkoituksella.

Kilpailuun osallistui joukkue kuudestatoista Euroopan maasta, sekä Indonesiasta, Saudi-Arabiasta ja Yhdysvalloista. Suomea edustivat Pihla Karanko, Katja Kulmala, Neea Palojärvi ja Jiali Yan. Joukkueenjohtajana toimi FT Anne-Maria Ernvall-Hytönen ja varajohtajana FL Esa Vesalainen. Jiali Yan saavutti pronssimitaliin oikeuttavan sijan, ja Neea Palojärvi sai kunniamaininnan. Kilpailun voittivat Bulgarian Pavlena Nenova ja Yhdysvaltain Danielle Wang. Suomen joukkueen osallistumisen mahdollisti Teknologiateollisuuden sata-vuotissäätiön sekä Matematiikan rahaston tuki.

Keskustellaanpa vielä hetki tehtävien valinnan filosofista ennen itse tehtäviin siirtymistä. Kilpailu on kaksipäiväinen, molempina päivinä neljä tehtävää ja aikaa neljä ja puoli tuntia. Molempina päivinä on tarkoitus olla yksi helppo tehtävä, eli tehtävät 1 ja 5. Matematiikkakilpailujen tyypilliset alat – algebra, geometria, kombinatoriikka ja lukuteoria – ovat kaikki edus-

tettuna molempina päivinä. Algebra ei täälläkään ole varsinaista algebraa siinä mielessä kuin se yliopistossa ymmärretään, vaan kokonaisuus kilpailumatematiikan osa-aloja, kuten funktionaaliyhtälöitä, epäyhtälöitä, polynomeja, jonoja jne. Kilpailun tehtävät oli valinnut komitea, eikä siis joukkueenjohtajista koostuva raati. Tehtävasarja oli hyvä, mutta en voi väittää kannattavani kyseistä mallia, jossa joukkueenjohtajien valta on redusoitu veto-oikeuden käyttöön tehtävän kohdalla, mikäli ehdokas on jo tunnettu. Joukkueenjohtajat tietenkin myös käänsivät tehtävät.

Viimeisen tehtävän (tehtävä 8) on tarkoitus olla hyvin hankala, kuten tehtävänvalintakomitean johtaja Geoff Smith luonnehti: ”Siltä varalta, että täällä on uusi Lisa Sauermann, että hänelläkin on jotain tekemistä.” (Lisa Sauermann on IMO:n historian Hall of Famen kärki, joka hallitsi kilpailuja muutamat viime vuodet.) Toinen huomattava asia on, että molemmissa geometrian tehtävissä seikkailee jännelikulmio. Jännelikulmiot ovat toki erinomaisen hyödyllisiä, mutta hieman yllättävältä tämä silti tuntuu. Kuitenkin ehkäpä vielä yllättävämpää oli, että tulokinnan mukaan kolme tai neljä tehtävää oli enemmän tai vähemmän kombinatorisia.

Tehtävät

Tehtävä 1. Olkoon ABC kolmio, jonka ympäri piirretyn ympyrän keskipiste on O . Pisteet D , E ja F ovat

sivujen BC , CA ja AB sisäpisteitä, tässä järjestyksessä, niin että DE on kohtisuorassa CO :ta vastaan ja DF on kohtisuorassa BO :ta vastaan. (Se, että piste on sisäpiste, tarkoittaa esimerkiksi, että piste D on suoralla BC , ja että D on pisteiden B ja C välissä tuolla suoralla.) Olkoon K kolmion AFE ympäri piirretyn ympyrän keskipiste. Osoita, että suorat DK ja BC ovat kohtisuorassa toisiaan vastaan.

Tehtävä 2. Olkoon n positiivinen kokonaisluku. Määritä luvun n funktiona suurin mahdollinen positiivinen kokonaisluku m , jolla on seuraava ominaisuus: Taulukko, jossa on m riviä ja n saraketta voidaan täyttää reaali-luvuilla niin, että mille tahansa kahdelle eri riville $[a_1, a_2, \dots, a_n]$ ja $[b_1, b_2, \dots, b_n]$ pätee

$$\max(|a_1 - b_1|, |a_2 - b_2|, \dots, |a_n - b_n|) = 1.$$

Tehtävä 3. Etsi kaikki funktiot $f: \mathbb{R} \rightarrow \mathbb{R}$, joilla

$$f(yf(x+y) + f(x)) = 4x + 2yf(x+y)$$

kaikilla $x, y \in \mathbb{R}$.

Tehtävä 4. Kokonaisluvuista koostuvaa joukkoa A kutsutaan summatäydeksi, jos $A \subset A + A$, eli jos jokainen joukon A alkio $a \in A$ on joukon A jonkin alkioparin $b, c \in A$ summa (b ja c eivät välttämättä ole erisuuria). Kokonaisluvuista koostuvan joukon A sanotaan olevan nollasummavapaa, jos 0 on ainoa kokonaisluku, jota ei voida esittää joukon A äärellisen epätyhjän osajoukon alkioiden summana. Onko olemassa summatäyttä nollasummavapaata kokonaisluvuista koostuvaa joukkoa?

Tehtävä 5. Luvut p ja q ovat alkulukuja ja toteuttavat ehdon

$$\frac{p}{p+1} + \frac{q+1}{q} = \frac{2n}{n+2}$$

jollakin positiivisella kokonaisluvulla n . Etsi kaikki mahdolliset erotuksen $q - p$ arvot.

Tehtävä 6. Äärettömän monta ihmistä on rekisteröityneenä yhteisöverkkoon, jonka nimi on Pärstäkerroin. Jotkut kahden eri käyttäjän muodostamat parit ovat rekisteröityneet ystäviksi, mutta jokaisella käyttäjällä on vain äärellinen määrä ystäviä. Jokaisella käyttäjällä on ainakin yksi ystävä. (Ystävyys on symmetristä, eli jos A on käyttäjän B ystävä, niin B on käyttäjän A ystävä.) Jokaisen on valittava yksi ystävistään parhaaksi ystäväkseen. Jos A valitsee käyttäjän B parhaaksi ystäväkseen, ei siitä (valitettavasti) seuraa, että B valitsisi käyttäjän A parhaaksi ystäväkseen. Sellaista joka on valittu parhaaksi ystäväksi, kutsutaan 1-parhaaksi ystäväksi. Yleisemmin, jos $n > 1$ on positiivinen kokonaisluku, niin käyttäjä on n -paras ystävä, jos hänet on valittu sellaisen käyttäjän parhaaksi ystäväksi, joka on $(n-1)$ -paras ystävä. Sellaista, joka on k -paras ystävä kaikilla positiivisilla kokonaisluvuilla k , kutsutaan suosituksi.

(a) Todista, että jokainen suosittu käyttäjä on jonkun suosittu käyttäjän paras ystävä.

(b) Osoita, että jos käyttäjillä voi olla äärettömän paljon ystäviä, niin on mahdollista, että suosittu käyttäjä ei ole yhdenkään suosittu käyttäjän paras ystävä.

Tehtävä 7. Olkoon ABC teräväkulmainen kolmio, jonka ympäri piirretty ympyrä on Γ ja ortokeskus H . Olkoon K sellainen ympyrän Γ piste, joka on eri puolella janaa BC kuin A . Olkoon L pisteen K peilaus suoran AB suhteen, ja olkoon M pisteen K peilaus suoran BC suhteen. Olkoon E toinen kolmion BLM ympäri piirretyn ympyrän ja ympyrän Γ leikkauspiste. Osoita, että suorat KH , EM ja BC leikkaavat samassa pisteessä. (Kolmion ortokeskus on korkeusjanojen leikkauspiste.)

Tehtävä 8. Sana on jonkin aakkoston kirjainten äärellinen jono. Sana on *toistava*, jos se on saatu kirjoittamalla peräkkäin vähintään kaksi identtistä sanaa (esimerkiksi *ababab* ja *abcabc* ovat toistavia, mutta *ababa* ja *aabb* eivät ole). Osoita, että jos sanalla on sellainen ominaisuus, että minkä tahansa kahden vierekkäisen kirjaimen paikan vaihtaminen keskenään tekee siitä toistavan, niin sen kaikki kirjaimet ovat samoja. (Huomaa, että on mahdollista vaihtaa kahden vierekkäin sijaitsevan identtisen kirjaimen paikkaa säilyttäen sana samana.)

Ratkaisut

Ratkaisu 1. Kehäkulmalauseen nojalla $\angle COB = 2\angle A$. Lisäksi $OB = OC$, joten $\angle OBC = \angle BCO = 90^\circ - \angle A$. Samoin $\angle FKE = 2\angle A$ ja $\angle KFE = \angle FEK = 90^\circ - \angle A$. Koska DE ja CO ovat kohtisuorassa toisiaan vasten, pätee $\angle EDC = 90^\circ - \angle DCO = 90^\circ - \angle BCO = \angle A$, ja vastaavasti $\angle BDF = \angle A$, joten $\angle FDE = 180^\circ - 2\angle A$. Täten $KFDE$ on jännene-kulmio, joten samaa jännettä vastaaville kulmille pätee $\angle KDE = \angle KFE = 90^\circ - \angle A$. Siis $\angle KDC = 90^\circ$, joten DK on kohtisuorassa suoraa BC vastaan.

Ratkaisu 2. Missään vaaditut ominaisuudet täyttyvässä taulukossa ei sarakkeen suurin ja pienin alkio voi erota kuin korkeintaan yhdellä. Siispä, jos jokainen sarakkeen arvo, joka ei ole suurin eikä pienin, vaihdetaan (ihan miten vaan) sarakkeen suurimmaksi tai pienimmäksi arvoksi, ei se muuta minkään sellaisten a_i , b_i arvoja, joilla $|a_i - b_i| = 1$, eikä se myöskään muuta mitään erotusta suuremmaksi kuin yksi, joten taulukolla on yhä vaadittu ominaisuus. Kuitenkin tällaisen muutoksen jälkeen, riippumatta siitä, mitä minkäkin sarakkeen pienin ja suurin arvo ovat, on jokaisessa sarakkeessa vain kaksi mahdollista vaihtoehtoa, suurempi ja pienempi. Koska tehtävän ehdon mukaan mitkään kaksi riviä eivät voi olla identtisiä, erilaisia rivejä voi olla korkeintaan 2^n kappaletta. Tämä on siis ehdoton maksimi. Toisaalta, tämä voidaan saavuttaa ottamalla taulukkoon kaikki n :n alkion mittaiset luvuista 0 ja 1 koostuvat rivit.

Ratkaisu 3. Kun $y = 0$, saadaan $f(f(x)) = 4x$, joten f on bijektio. Lisäksi

$$f(0) = f(4 \cdot 0) = f(f(f(0))) = 4f(0),$$

ja täten $f(0) = 0$. Kun $x = 0$ ja $y = 1$, saadaan tehtävänannon yhtälön sekä ensimmäisen yhtälön avulla

$$4 = f(f(1)) = 2f(1),$$

joten $f(1) = 2$, ja $f(2) = f(f(1)) = 4$. Sijoituksella $y = 1 - x$ saadaan

$$f(2(1 - x) + f(x)) = 4x + 4(1 - x) = 4 = f(2)$$

kaikilla $x \in \mathbb{R}$. Koska f on injektio, saadaan $f(x) = 2 - 2(1 - x) = 2x$. On helppo tarkistaa, että tämä funktio toteuttaa alkuperäisen ehdon. Siispä $f(x) = 2x$ kaikilla $x \in \mathbb{R}$ on etsitty funktio.

Ratkaisu 4. Ehkä yllättävästikin tällainen joukko on olemassa. Asetetaan

$$A = \{F_{2n} \mid n = 1, 2, \dots\} \cup \{-F_{2n+1} \mid n = 1, 2, \dots\},$$

missä F_k on k :s Fibonaccin luku ($F_1 = 1$, $F_2 = 1$, $F_{k+2} = F_{k+1} + F_k$, kun $k \geq 1$), ja osoitetaan, että tämä käy esimerkistä. Nyt $F_{2n} = F_{2n+2} + (-F_{2n+1})$ ja $-F_{2n+1} = (-F_{2n+3}) + F_{2n+2}$, kun $n \geq 1$, joten A on summatäysi (ja peräti yksikäsitteisellä esityksellä). Fibonaccin luvuille pätee $F_2 = F_1$, $F_3 = F_2 + 1$. Näistä ja luvut määrittelevästä palautuskaavasta saadaan induktiolla $F_{2k} = F_{2k-1} + F_{2k-3} + \dots + F_1$ ja $F_{2k+1} = F_{2k} + F_{2k-2} + \dots + F_2 + 1$. Näistä ominaisuuksista seuraa, että 0 ei ole kahden A :n alkion summa. Jos näin olisi, olisi myös

$$\sum_{i=1}^s F_{2n_i} = \sum_{j=1}^t F_{2n_j+1}.$$

Molemmissa summissa on oltava enemmän kuin yksi yhteenlaskettava, joten se summista, jossa suurin yhteenlaskettava on suurempi, on itseisarvoltaan aidosti suurempi kuin toinen.

Riittää siis osoittaa, että kaikki nollasta poikkeavat kokonaisluvut voidaan esittää joukon A erisuurten alkioiden summana, eli lukujen $1, -2, 3, -5, 8, -13, 21, \dots$ avulla. Tämä voidaan tehdä käyttäen niin kutsuttua ahnetta algoritmia: Kun esitetään luku n , aloitetaan valitsemalla $m = \pm F_k$, missä $|m| \geq |n|$, lukujen n ja m etumerkit ovat samat, ja m on itseisarvoltaan pienin nämä ehdot toteuttava luku. Tämän jälkeen jatketaan induktiivisesti, käsitellen seuraavaksi lukujen m ja n erotus. On helppo nähdä, että mitään lukua ei käytetä kahdesti: Osoitetaan tämä induktiolla. Tapaus $k = 2$ (eli $m = 1$) on alkutilanne. Induktio-oletus on, että niillä n , joilla algoritmi alkaa alkiolla $\pm F_\ell$, kun $\ell \leq k$, ei mitään alkiota jouduta käyttämään kahdesti, eikä myöskään jouduta käyttämään alkioita $\pm F_j$, kun

$j > \ell$. Induktion saattaminen loppuun on suoraviivaista.

Ratkaisu 5. Tämä tehtävä on ratkaistavissa tarkastelemalla lukujen p , q ja n parillisuutta, ja jakamalla tarkastelu osiin. Käydään tässä kuitenkin läpi hieman lyhyempi, joskin ehkä hieman enemmän kekseliäisyyttä vaativa ratkaisu.

Kun tehtävän yhtälön molemmilta puolilta vähennetään 2, ja kerrotaan yhtälö tämän jälkeen luvulla -1 , saadaan

$$\frac{1}{p+1} - \frac{1}{q} = \frac{4}{n+2}.$$

Täten $q > p + 1$. Edelleen

$$q - p - 1 = \frac{4(p+1)q}{n+2}.$$

Koska q ei voi olla luvun $p+1$ tekijä (eli vasen puoli ei ole luvulla q jaollinen), on luvun q oltava luvun $n+2$ tekijä. Kirjoitetaan $\frac{n+2}{q} = u$, missä u on positiivinen kokonaisluku. Nyt

$$q - p - 1 = \frac{4(p+1)}{u},$$

joten $uq - u(p+1) = 4(p+1)$. Täten $p+1$ on luvun uq tekijä. Koska q on alkuluku ja $q > p+1$, ei $p+1$ voi olla luvun q tekijä, vaan sen on oltava u :n tekijä. Kirjoitetaan $v = \frac{u}{p+1}$. Nyt

$$q - p = 1 + \frac{4}{v} \in \{2, 3, 5\}.$$

Kaikki kolme tapausta ovat mahdollisia, sillä kolmikoksi (p, q, n) voidaan valita $(3, 5, 28)$ tai $(2, 5, 28)$ tai $(2, 7, 19)$. Huomaa, että kaikki alkulukukaksoset tuottavat ratkaisun kolmikolla $(p, p+2, 2(2p^2+6p+3))$.

Ratkaisu 6. Merkitään henkilön A parasta ystävää $f(A)$:lla. Olkoon lisäksi $f^0(x) = x$, ja $f^{k+1}(x) = f(f^k(x))$, eli kuka tahansa, joka on k -paras ystävä, on $f^k(A)$ jollekin A . Olkoon X suosittu, ja olkoon x_k sellainen henkilö, jolle $f^k(x_k) = X$. Koska henkilöllä X on vain äärellinen määrä ystäviä, äärettömän monen henkilöistä $f^{k-1}(x_k)$ (jotka kaikki siis ovat valinneet henkilön X parhaaksi ystäväkseen) on oltava samoja, jonka siis myös täytyy olla suosittu.

Jos taas on mahdollista olla äärettömän paljon ystäviä, niin tarkastellaan henkilöitä X_i positiivisilla kokonaisluvuilla i ja henkilöitä $P_{i,j}$, missä $i < j$ ja j on positiivinen kokonaisluku. Valitkoon X_i henkilön X_{i+1} parhaaksi ystäväkseen, ja valitkoon taas $P_{i,i}$ henkilön X_1 parhaaksi ystäväkseen, ja valitkoon $P_{i,j}$ henkilön $P_{i+1,j}$ parhaaksi ystäväkseen, kun $i < j$. Nyt kaikki henkilöt X_i ovat suosittuja, mutta X_1 ei ole suosittu henkilön paras ystävä.

Ratkaisu 7. Koska $BMEL$ on jänneleikelmä, pätee $\angle BEM = \angle BLM$. Lisäksi tehtävänannon konstruktion mukaan $|BK| = |BL| = |BM|$, joten

$$\begin{aligned}\angle BLM &= 90^\circ - \frac{1}{2}\angle MBL \\ &= 90^\circ - \left(180^\circ - \frac{1}{2}\angle KBL - \frac{1}{2}\angle KBM\right) \\ &= \left(\frac{1}{2}\angle KBL + \frac{1}{2}\angle KBM\right) - 90^\circ \\ &= (180^\circ - \angle B) - 90^\circ \\ &= 90^\circ - \angle B.\end{aligned}$$

Huomataan myös, että $\angle BEM = \angle BAH$, joten suorien EM ja AH leikkauspiste N on ympyrällä Γ . Olkoon X suorien KH ja BC leikkauspiste, ja olkoon N' suorien MX ja AH leikkauspiste. Koska BC puolittaa jängteen KM , kolmio KM on tasakylkinen. Koska suorat AH ja MK ovat yhdensuuntaisia, kolmio HXN' on tasakylkinen. Koska suorat AH ja BC ovat kohtisuorassa toisiaan vasten, on N' pisteen H peilaus suoran BC suhteen. Tunnetusti tällainen peilaus on ympäripiirretty ympyrällä, eli ympyrällä Γ , joten $N = N'$. Täten pisteet E, M, N ja M, X, N' ovat samalla suoralla MN , eli suora EM kulkee pisteen X kautta.

Ratkaisu 8. Tätä tehtävää voi lähestyä hyvin monella eri tavalla. Esitetään nyt ratkaisu, joka ei ole käsittämättömän pitkä, ja joka ei käytä mitään kovin syvälistä tietämystä.

Kutsutaan sanaa vakioksi, jos sen kaikki kirjaimet ovat samoja. Tarkastellaan epävakioita sanaa W , jonka pituus $|W| = w$, ja johdetaan tästä (ennen pitkää) ristiriita tehtävän väitteen kanssa, eli tehdään vasta oletus-todistus. Koska sanassa W on ainakin kaksi erisuurta kirjainta, olkoon $W = AabB$, missä $a \neq b$. Voidaan olettaa, että $B = cC$, epätyhjää sana, eli $W = AabcC$ (emme oletetaan mitään sanoista A ja C , edes epätyhjyyttä). Sopivilla vaihdoilla saadaan toistavat sanat $W' = AbacC = P^{w/p}$, jonka jakson P pituus p jakaa luvun w , $1 < p < w$ ja $W'' = AacbC = Q^{w/q}$, jonka jakson Q pituus q jakaa luvun w , $1 < q < w$. Kuitenkin, jos sana UV on toistava, niin on myös sana VU toistava, ja samalla jakson mitalla (mutta jakso ei välttämättä ole sama). Voimmekin siis jatkossa työskennellä toistavien sanojen $W'_0 = CAbac$ (jakso P' , jakson pituus p) ja $W''_0 = CAacb$ (jakso Q' , jakson pituus q) kanssa. Nyt pääajatus on se, että kahden toistavan sanan yhteinen alkuosa ei voi olla liian pitkä.

Jos sana $a_1a_2 \dots a_w = T^{w/t}$ on toistava, jaksolla T ja jakson pituudella $t \mid w$, $1 \leq t \leq w$. niin silloin sana (ja sen alasanat ovat t -jaksoisia, eli $a_k = a_{k+t}$ kaikilla $1 \leq k \leq w - t$). Siis päi sana CA on sekä p -jaksoinen että q -jaksoinen.

Tässä kohtaa voisi käyttää Wilf-Finen lausetta, mutta koska se ei yleissivistykseen kuulu, muotoillaan ja

todistetaan hieman heikompi väite.

Väite. Olkoot p ja q positiivisia kokonaislukuja, ja olkoon N sana, jonka pituus on n , ja joka on sekä p -jaksollinen että q -jaksollinen. Jos $n \geq p + q$, niin N on $\text{syt}(p, q)$ -jaksollinen.

Todistus. Osoitetaan ensin, että kaksi epätyhjää sanaa kommutoi, eli $UV = VU$, jos ja vain jos on olemassa sana W , joka toteuttaa ehdot $|W| = \text{syt}(|U|, |V|)$, $U = W^{|U|/|W|}$ ja $V = W^{|V|/|W|}$. On ilmeistä, että tällaisen sanan olemassaolosta seuraa kommutointi. Riittää siis osoittaa, että kommutointi edellyttää tätä. Käytetään induktiota luvulle $|U| + |V|$. Alkuaskeleessa $|U| + |V| = 2$, eli $|U| = |V| = 1$, jolloin ilmeisesti $W = U = V$. Kun $|U| + |V| > 2$, jos $|U| = |V|$, niin tällöin on pädeävä $U = V$, jolloin tilanne on selvä. Jos $|U| \neq |V|$, niin voidaan olettaa, että $|U| < |V|$, jolloin $V = UV'$, eli $UVV' = UV'U$, eli $UV' = V'U$, ja koska $|V'| < |V|$, pätee $2 \leq |U| + |V'| < |U| + |V|$, jolloin induktio-oletuksen nojalla löytyy sana W , jolla $U = W^{|U|/|W|}$ ja $V' = W^{|V'|/|W|}$, joten $V = UV' = W^{(|U|+|V'|)/|W|} = W^{|V|/|W|}$.

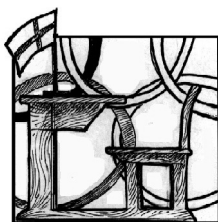
Voidaan nyt olettaa, että $p \leq q$, $q = kp + r$, ja pätee $N = QPS$, missä $|Q| = q$ ja $|P| = p$. Jos $r = 0$, on tilanne selvä. Jos taas näin ei ole, niin voidaan kirjoittaa $P = UV$ ja $Q = V(UV)^k$, missä $|V| = r$, ja koska $UV = VU$, niin $PQ = QP$, jolloin ylläolevan tuloksen mukaan on olemassa sana W , jonka pituus on $\text{syt}(p, q)$, ja jonka avulla voidaan kirjoittaa $P = W^{p/\text{syt}(p, q)}$ ja $Q = W^{q/\text{syt}(p, q)}$, eli sana N on $\text{syt}(p, q)$ -jaksoinen.

Väite on nyt todistettu, ja voimme palata tehtävän ratkaisuun. Tarvitaan siis $|CA| \leq p + q - 1$, eli $w \leq p + q + 2$, sillä muutoin sanat W'_0 ja W''_0 olisivat identtisiä, mikä on mahdotonta. Koska $p \mid w$ ja $1 < p < w$, pätee $2p \leq w \leq p + q + 2$, eli $p \leq q + 2$. Vastaavasti $q \leq p + 2$. Täten $\max(p, q) \leq \min(p, q) + 2$. Ehdosta $k \max(p, q) = w \leq p + qp/2 \leq 2 \max(p, q) + 2$ saadaan $(k - 2) \max(p, q) \leq 2$, mutta $\max(p, q) \leq 2$ on mahdoton, sillä kolmen kirjaimen loppuosa acb ei ole jaksollinen. Ja täten sen on kuuluttava sanaan Q' , eli $q \geq 3$. Täten $k = 2$, ja $w = 2 \max(p, q)$.

Jos $\max(p, q) = \min(p, q)$, niin $w = 2p = 2q$, mikä on ristiriita.

Jos $\max(p, q) = \min(p, q) + 1$, niin $3 \min(p, q) \leq w = 2 \max(p, q) = 2 \min(p, q) + 2$, eli $\min(p, q) \leq 2$, joten $\min(p, q) = 2$ ja $\max(p, q) = 3$, ja ylläolevan havainnon nojalla voidaan todeta $q = 3$ ja $p = 2$, eli $c = b$. Tästä seuraa, että $w = 2 \max(p, q) = 6$, joten $CA = aba = abb$, mikä on ristiriita.

Jos $\max(p, q) = \min(p, q) + 2$, niin $3 \min(p, q) \leq w = 2 \max(p, q) = 2 \min(p, q) + 4$, eli $\min(p, q) \leq 4$. Koska $\min(p, q) \mid w = 2 \max(p, q)$, niin on pädeävä joko $\min(p, q) = 2$ ja $\max(p, q) = 4$, jolloin $w = 8$, mikä on ristiriita, tai $\min(p, q) = 4$ ja $\max(p, q) = 6$, jolloin $w = 12$. Tämä on myös ristiriita.



Yksi helppo, viisi vaikeaa? – Kansainväliset matematiikkaolympialaiset 2012

Matti Lehtinen

Helsingin yliopisto

Kansainväliset matematiikkaolympialaiset pidettiin heinäkuussa 2012 53. kerran. Kilpailujen historiassa tämä oli kolmas kerta, kun toimittiin eteläisen pallonpuoliskon talvessa, ilmastossa, jossa esimerkiksi Suomen koululaiset ovat tottuneet oppia saamaan ja osaamistaan osoittamaan. Kilpailijoita oli 548, maita 100, Etelä-Korea oli paras ja Suomi sijalla 65; Suomen Otte Heinävaara sai hopeamitalin. Nämä ja muut tilastotiedot löytyvät Matematiikkaolympialaisten virallisilta verkkosivuilta http://www.imo-official.org/year_info.aspx?year=2012.

Olympialaisissa ratkotaan aina kuusi tehtävää kahdessa neljän ja puolen tunnin mittaisessa kokeessa. Tehtävät päättää kaikkien osallistujamaiden joukkueenjohtajista koostuva tuomaristo. Tuomaristo on sidottu asian tuntijaraadin etukäteen laatimaan 30 tehtävän ehdokaslistaan, ja sen pohjana puolestaan ovat kaikista osallistujamaista pyydetty ehdotukset. Niitä oli tänä vuonna saatu 136 kaikkiaan 40 maasta. Kuuden tehtävän joukkoon on tapana valita ainakin yksi edustaja kullakin neljältä kilpailumatematiikan vakiintuneelta osalta, nimittäin algebrasta, geometriasta, kombinatoriikasta ja lukuteoriasta. Tapana on myös luokitella tehtävät helpoiksi, keskinkertaisiksi ja vaikeiksi. Kutenkin tällaista on sarjaan pyritty saamaan kaksi kappaletta. Kun helpot tehtävät ratkaisevat melkein kaikki kilpailijat ja vaikeita ei juuri kukaan, niin paremmuusjärjestys on usein jäänyt riippumaan vain kahdesta keskinkertaisesta tehtävästä. Tämän vuoden tuoma-

risto oli tiedostanut ongelman ja pyrki lisäämään keskinkertaisten tehtävien osuutta helppojen ja vaikeiden kustannuksella. Lopputulokset osoittivat, että tässä ei aivan onnistuttu: kahden vaikeimman tehtävän ratkaisu onnistui vain kymmenkunnalle viidestä ja puolesta sadasta kilpailijasta.

Olymplatehtävien ratkaisuihin voi tutustua esimerkiksi Suomen matemaattisen yhdistyksen Valmenusjaoston sivuilla osoitteessa <http://solmu.math.helsinki.fi/olympia/IMO/2012/ratk2012.pdf>.

Tässä kirjoituksessa pyritään tuomaan esiin ratkaisun löytämisen kannalta olennaisia asioita. Etenkin vaikeimpien tehtävien kohdalla yksityiskohtiin asti ei mennä.

Helpoimmaksi tehtäväksi ennakoitiin olympialaisten tehtävää 1, jonka aihepiiri oli klassinen geometria:

Kolmion ABC kärkeä A vastassa olevan sivuympyrjän keskipiste on J . Sivuympyrän ja sivun BC sivuamispiste on M . Ympyrä sivuaa suoraa AB pisteessä K ja suoraa AC pisteessä L . Suorien LM ja BJ leikkauspiste on F ja suorien KM ja CJ leikkauspiste on G . Olkoon vielä S suorien AF ja BC ja T suorien AG ja BC leikkauspiste. Todista, että M on janan ST keskipiste.

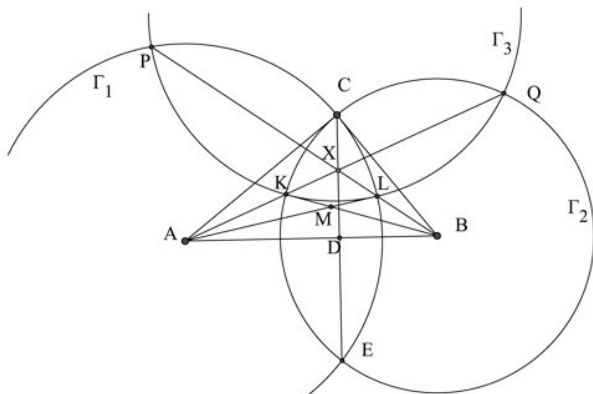
Tehtävätekstiin liittyi vielä sivuympyrän määritelmä. Kolmion sivuympyröitähän ovat ne kolme ympyrää, jotka sivuavat yhtä kolmion sivuista ja kahden muun jatkeita.

On vielä torjuttava yhtäsuuruuden mahdollisuus. Yhtäsuuruuden toteutumiselle olisi välttämätöntä, että $a_k = \frac{1}{k-1}$ kaikilla k , $2 \leq k \leq n$, mutta silloin lukujen a_k tulo ei voisi olla 1.

Tehtävän pistejakauma oli hyvin kaksihuippuinen. Tarpeellisen oivalluksen tehneet saivat yleensä täydet pisteet. Niitä annettiin 172:lle kilpailijalle. Toisaalta 263 kilpailijaa jäi kokonaan pisteittä.

Neljäs useamman kuin muutaman kilpailijan ratkaisu tehtävä oli toisen päivän toinen tehtävä, sekin hyvin klassisentyypistä kilpailugeometriaa.

Kolmiossa ABC on $\angle BCA = 90^\circ$ ja D on C :stä piirretyn korkeusjanan kantapiste. Olkoon X janan CD sisäpiste. Olkoon K se janan AX piste, jolle $BK = BC$ ja L se janan BX piste, jolle $AL = AC$. Olkoon M AL :n ja BK :n leikkauspiste. Osoita, että $MK = ML$.



Tehtävän varsin lyhyt ja elegantti ratkaisu perustuu olennaisesti pisteen potenssille ympyrän suhteen. Ensin on vain löydettävä ympyrät. Tehtävän ehto antaa kaksi: A -keskisen, C :n ja L :n kautta kulkevan Γ_1 :n ja B -keskisen, C :n ja K :n kautta kulkevan Γ_2 :n. Ympyrät leikkaavat C :n lisäksi pisteessä E , BX leikkaa Γ_1 :n L :n lisäksi pisteessä P ja AX Γ_2 :n K :n lisäksi pisteessä Q . Piste X on ympyröiden yhteisellä jängteellä CE , joten sillä on sama potenssi $CX \cdot XE$ molempien ympyröiden suhteen. Erityisesti $KX \cdot XQ = LX \cdot XP$. Mutta nyt pisteen potenssia voidaan soveltaa vähemmän tavalliseen suuntaan, osoittamaan, että neljä pistettä on samalla ympyrällä. Jos Γ_3 on pisteiden P, K, L kautta kulkeva ympyrä ja KX leikkaa tämän ympyrän myös pisteessä Q' , niin $PX \cdot XL = KX \cdot XQ'$. Aikaisemman yhtälön perusteella päätellään, että $Q' = Q$, ts. että P, K, L ja Q ovat kaikki ympyrällä Γ_3 . Koska $AC \perp BC$, A :n potenssi Γ_2 :n suhteen on $AC^2 = AK \cdot AQ$. Mutta silloin myös $AL^2 = AK \cdot AQ$; kun tämä tulkitaan A :n potenssiksi Γ_3 :n suhteen, niin nähdään, että AL on Γ_3 :n tangentti. Samoin on KB , ja väite $MK = ML$ seuraa heti.

Tämä tehtävä osoittautui olennaisesti vaikeammaksi kuin sarjan toinen geometriatehtävä. Täydet pisteet sai 86 kilpailijaa, mutta kokonaan pisteittä jäi 349.

Ensimmäisen kilpailupäivän viimeinen tehtävä kuului aihealueeseen kombinatoriikka. Siinä esiteltiin melko eksoottinen peli.

Valehteluleikki on peli, jossa on kaksi pelaajaa A ja B . Pelin säännöt perustuvat positiivisiin kokonaislukuihin k ja n , jotka ovat molempien pelaajien tiedossa.

Pelin alussa A valitsee kokonaisluvut x ja N , $1 \leq x \leq N$. A pitää luvun x salassa, mutta ilmoittaa B :lle rehellisesti luvun N . B pyrkii saamaan tietoa luvusta x tekemällä A :lle kysymyksiä. Jokaisessa kysymyksessä hän esittää jonkin positiivisten kokonaislukujen joukon S (samaa joukkoa on voitu käyttää jo aikaisemmassa kysymyksessä) ja kysyy A :lta, kuuluuko x joukkoon S . B voi tehdä niin monta kysymystä kuin haluaa. A :n on heti vastattava jokaiseen B :n kysymykseen joko kyllä tai ei, mutta hän voi valehdella niin usein kuin haluaa. Ainoa rajoitus on, että jokaisen $k+1$:n peräkkäisen vastauksen joukossa on oltava ainakin yksi rehellinen. Kysyttyään niin monta kysymystä kuin on halunnut, B ilmoittaa positiivisten kokonaislukujen joukon X , jossa on enintään n alkioita. Jos x kuuluu joukkoon X , B voittaa. Muussa tapauksessa hän häviää. Todista, että

1. jos $n \geq 2^k$, niin B :llä on voittostrategia;
2. jokaista tarpeeksi suurta k :ta kohden on olemassa sellainen $n \geq 1,99^k$, että B :llä ei ole voittostrategiaa.

Tehtävän kahdella osiolla on varsin erityyppinen ratkaisu. Ensimmäiseen kysymykseen vastaamiseksi riittää, kun osoitetaan, että B voi lähteä joukosta $T_0 = \{1, 2, \dots, N\}$ ja alkio kerrallaan poistaa siitä sellaisia alkioita y , joista hän tietää, että $y \neq x$; tätä voi tehdä niin kauan kuin joukossa on jäljellä 2^k alkioita. Voidaan olettaa, että jäljellä on joukko $T = \{1, 2, \dots, 2^k, \dots, m\}$. B kysyy ensin enintään $k+1$ kertaa kysymyksen "onko $x = 2^k$?". Jos A vastaa aina "ei", niin ainakin yksi vastaus on oikein, joten $x \neq 2^k$. Jos taas A vastaa ainakin kerran "kyllä", B esittää seuraavaksi k kysymystä, joista jokainen on "onko x :n binääriesityksen i :s numero 0?". Jos A :n kaikki $k+1$ vastausta (mukana siis $x = 2^k$ -kysymykseen annettu "kyllä") olisivat väärä, niiden komplementtien avulla olisi rakennettavissa x . Koska vastauksista ainakin yksi on oikea, komplementeista rakentuva y ei ole x , ja tämä y voidaan poistaa T :stä ja jos T :ssä yhä on enemmän kuin n alkioita, toistaa prosessi. Toisen kysymyksen vastaus perustuu siihen, että jos $1 < c < 2$, ja $n = \lfloor (2-c)c^{k+1} \rfloor - 1$, niin B ei pysty kysymyksillään saamaan riittävästi tietoa. Sanomme, että A valehtelee luvusta i , jos hän vastaa B :n kysymykseen " $x \in S$?" kyllä, ja $i \notin S$, tai ei, ja $i \in S$. Jälkimmäiseen kysymykseen vastauksen tarjoaa A :n vastausstrategia, joka ei riipu x :stä, ja jonka mukaan A ei koskaan valehtelee

enemmän kuin k kertaa mistään luvusta i . Näin B ei missään vaiheessa saa tarpeeksi tietoa x :stä. Tällöin A valitsee luvun $N = n + 1$ ja muodostaa funktion

$$\phi = \sum_{i=1}^N c^{m_i},$$

missä eksponentit m_i ilmoittavat, kuinka monta peräkkäistä kertaa A on valehdellut i :stä. Osoittautuu, että jos A valitsee aina seuraavan vastauksensa niin, että ϕ saa pienimmän mahdollisen arvon, niin aina $\phi < c^{k+1}$, joten jokainen $m_i \leq k$. Jos erityisesti $1,99 < c < 2$, niin $n > 1,99^k$.

Tehtävään vastasi täysien pisteiden arvoisesti 8 kilpailijaa. Kolmisenkymmentä pystyi vastaamaan ensimmäiseen osioon, mutta 481 kilpailijaa jäi pisteittä.

Olympialaisten viimeinen tehtävä valittiin sarjaan lukuteorian osastosta, mutta tehtävä on melko algebralinen.

Määritä kaikki positiiviset kokonaisluvut n , joille on olemassa sellaiset ei-negatiiviset kokonaisluvut

$a_1, a_2, \dots, a_n$, että

$$\frac{1}{2^{a_1}} + \frac{1}{2^{a_2}} + \dots + \frac{1}{2^{a_n}} = \frac{1}{3^{a_1}} + \frac{2}{3^{a_2}} + \dots + \frac{n}{3^{a_n}} = 1. \quad (1)$$

Osoittautuu, että tehtävän ratkaisuehdot kelpaavat kaikki sellaiset luvut n , joille pätee $n \equiv 1 \pmod{4}$ tai $n \equiv 2 \pmod{4}$. Sen että ehto on välttämätön, näkee melko välittömästi laventamalla jälkimmäistä yhtälöä tarpeeksi korkealla 3:n potenssilla ja tulkitsemalla saatua yhtälöä $\pmod{2}$. Saadaan, että $1 + 2 + \dots + n$ on pariton, joka on yhtäpitävää edellä väitetyn kanssa.

Toisin päin päättely perustuu havaintoihin

$$\frac{1}{2^{a+1}} + \frac{1}{2^{a+1}} = \frac{1}{2^a} \quad \text{ja} \quad \frac{x}{3^{a+1}} + \frac{y}{3^{a+1}} = \frac{z}{3^a},$$

jos $x + y = 3z$. Näitä käyttäen yhtälö (1) voidaan suurempien n :ien tapauksessa redusoida tapaukseen, jossa n korvautuu luvulla $n - 12$, ja viimein todeta, että kun $n \in \{2, 5, 6, 9, 10, 13, 14\}$, vaaditut luvut löytyvät.

Tehtävään löysi ratkaisun 10 kilpailijaa; 474 jäi kokonaan pisteittä.

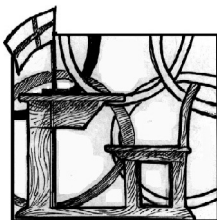
Solmun matematiikkadiplomit

Peruskoululaisille tarkoitetut Solmun matematiikkadiplomit I – VII tehtävineen sekä diplomin VIII tehtävät ovat tulostettavissa osoitteessa

<http://solmu.math.helsinki.fi/diplomi.html>

Opettajalle lähetetään pyynnöstä vastaukset koulun sähköpostiin. Pynnön voi lähettää osoitteella

[marjatta.naatanen\(at\)helsinki.fi](mailto:marjatta.naatanen(at)helsinki.fi)



Määrätyn integraalin opettamisesta differentiaalisesti

Kyösti Tarvainen

matematiikan yliopettaja

Metropolia ammattikorkeakoulu

Johdanto

Kirjoituksessa esitetään, miten määrättyjen integraalien lausekkeita johdetaan *differentiaalisesti* tekniikan ja fysiikan sovellutuksissa ja miten tämä menettely perustellaan rationaalisesti. Lukion kirjoissa esitetään sellaisia differentiaalisia johtoja, joissa tarkastellaan ”äärettömän pieniä” suureita. Niitä ei kuitenkaan ole tapana käyttää fysiikan tai tekniikan sovellutuksissa. Ammattikorkeakoulun opettajana en myöskään ole nähnyt, että ylioppilas olisi johtanut määrätyn integraalin lausekkeen käyttäen ”äärettömän pieniä” suureita. Syynä on varmaan se, että ne ovat niin hämäriä ja pieniä, ettei niihin saa otetta.

Kuten seuraavassa esitetään, differentiaaliset johdot ovat virtaviivaistettuja esityksiä yksityiskohtaisemmista tarkasteluista, joissa määrätyn integraalin lauseke määritetään lähtien liikkeelle likiarvosummista. Siksi differentiaalisen menettelyn hallinta edellyttää sitä, että on johtanut useita integraalilausekkeita yksityiskohtaisten summatarkastelujen kautta. Ne vievät sen verran aikaa, että lukiossa varmaankin tulisi keskittyä niihin ja jättää differentiaaliset tarkastelut ammattikorkeakoulu- ja yliopisto-opintoihin. Nykyisissä yhdysvaltalaisissa calculus-kirjoissakin on yleensä luovuttu differentiaalisista tarkasteluista.

Seuraavassa esitetään ensin, miten määrätty integraali johdetaan yksityiskohtaisesti, ja sitten, miten lyhyemmin differentiaalisesti.

Yksityiskohtainen määrätyn integraalin lausekkeen johtaminen

Määrättyyn integraaliin johtavissa tapauksissa tilanne on yleisesti sanottuna seuraavanlainen. Meidän on laskettava x -akselin väliin $[a, b]$ liittyvän suureen arvo. Vaikeutena on se, että tehtävään liittyy x :stä riippuva funktio $f(x)$, mutta kuitenkin tehtävä on sellainen, että osaamme ratkaista sen siinä tapauksessa, että funktio f on vakio.

Edelleen olkoon tehtävä sellainen, että voimme määrittää laskettavan suureen likiarvon seuraavasti. Jaetaan väli $[a, b]$ n :ään yhtä pitkään osaväliin, joiden pituutta merkitään Δx :llä. Merkitään osavälien alkupisteitä $x_1 (= a), x_2, x_3, \dots, x_n$. Laskettavan suureen arvo k :nnella osavälillä (*kertymä* k :nnella osavälillä) olkoon likimäärin $f(x_k)\Delta x$. Oletetaan edelleen, että laskettavan suureen arvo saadaan summana osavälien kertymistä, joten sille saadaan likiarvo osavälien kertymien likiarvojen summana $\sum_{k=1}^n f(x_k)\Delta x$.

Oletetaan, että geometrisesti tai fysikaalisesti voimme päätellä, että tämä likiarvo lähestyy laskettavan suureen tarkkaa arvoa, kun osavälien lukumäärä n kasvaa rajatta. Tällöin tarkkaa arvoa merkitään määrättynä integraalina $\int_a^b f(x) dx$.

Differentiaalisen johtotavan perustelu

Tekniikan ja fysiikan sovellutuksissa ei noudateta yksityiskohtaisesti edellä selostettua menettelyä, koska silloin aina toistuisivat samanlaiset merkinnät ja päätte-lyt. Lopputulos, muotoa $\int_a^b f(x) dx$ oleva lauseke, halutaan saada paperille nopeammin.

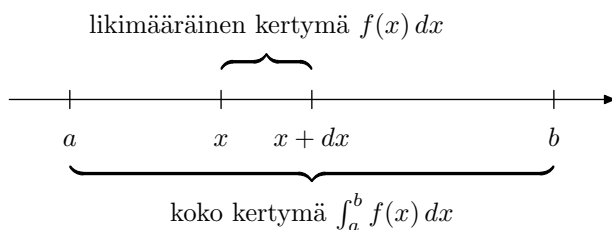
Lopputuloksen alku $\int_a^b$ on aina helppo kirjoittaa tarkasteluvälin perusteella. Loppu dx on myös helppo kirjoittaa. Ainoa ongelma on se, että mikä on funktion $f(x)$ lauseke.

Palataan yksityiskohtaiseen johtoon: mistä ilmestyi lopputuloksen funktio $f(x)$? Vastaus: se oli likiarvolas- kussa se funktio, jonka arvolla (osavälin alkupisteessä) kerrottiin osavälin pituus.

Toisin sanoen saamme funktion $f(x)$ selville, kun tarkastelemme mielivaltaista lyhyttä osaväliä ja katsomme, millä sen pituus täytyy kertoa, jotta saamme likiarvon laskettavan suureen kertymälle tällä osavälillä. Tähän perustuu differentiaalinen menettely.

Kuten heti ilmenee, tarkasteltavan mielivaltaisen osavälin alkupistettä kannattaa merkitä x :llä ja välin pituutta dx :llä. Kun määritetään laskettavan suureen likimääräistä kertymää tällä välillä, saadaan selville (jos tapaus ylipäättään johtaa määrättyyn integraaliin), millä dx on kerrottava, jotta saadaan kertymän likiarvo. Näin saadaan likiarvo $f(x) dx$, jonka eteen meidän onkin vain lisättävä integraalimerkki, jossa on koko välin rajat.

Perinpohjainen johto on näin tyypistynyt kahden rivin mittaiseksi. Jotta ymmärtäisi differentiaalisen johdon ja osaisi käyttää sitä, on luonnollisesti ensin käytävä läpi useita yksityiskohtaisia integraalilausekkeiden johtoja. Kuva 1 havainnollistaa differentiaalista tapaa johtaa määrätyn integraalin lauseke.



Kuva 1. Määrätyn integraalin lausekkeen differentiaalinen johtamistapa.

Esimerkki. Johdetaan määrätyn integraalin lauseke auton aikavälillä $[a, b]$ ajaman matkan pituudelle s , kun auton nopeus ajan t funktiona on $v(t)$. Differentiaalinen johto:

- lyhyellä aikavälillä $[t, t + dt]$ auto kulkee matkan $v(t) dt$
- koko matka $s = \int_a^b v(t) dt$.

Huomautuksia differentiaaliseen johtoon

Huomautus 1. Differentiaalisesta johdosta on jätetty pois likiarvosummien tarkastelu, mutta ainakin tekniikan ammattiaineiden opettajien tapana on viitata summiin seuraavalla epätarkalla sanonnalla. Sen jälkeen, kun esimerkiksi edellisessä esimerkissä on johdettu osavälillä $[t, t + dt]$ kertyvän matkan pituus $v(t) dt$, sanotaan: ”koko matka välillä $[a, b]$ on summa eli (sic) integraali $\int_a^b v(t) dt$ ”.

Huomautus 2. Ammattiaineiden opettajien tapana ei ole esittää virhetarkasteluja likiarvolle $v(t) dt$; eivätkä he ylipäättään edes mainitse sitä, että kyseessä on likiarvo, koska se on selvä asia näissä yhteyksissä. Likiarvotarkasteluja voi kuitenkin jokainen itse tehdä. Artikkelissa [1] esitetään muutamia tarkastelutapoja. Usein voidaan nojautua siihen, että likiarvon suhteellinen virhe menee nollaan osavälin pituuden lähestyessä nollaa.

Esimerkin tapauksessa tämä on fysikaalisesti selvä asia, kun ajatellaan sitä, että erittäin pienellä aikavälillä auton nopeus muuttuu melko tasaisesti. Jos esimerkiksi $dt = 1$ sekunti ja tällä aikavälillä nopeus esimerkiksi kasvaa 0,2 %, niin matkan kertymässä $v(t) dt$ on karkeasti ottaen myös noin 0,2 %:n virhe. Kun aikaväli pienenee puoleen, nopeus ehtii kasvaa vain noin puolet eli 0,1 %, jolloin kertymän $v(t) dt$ suhteellinen virhekin noin puolittuu. Näin edelleen puolittumisia ajatellen, näemme että $v(t) dt$:n suhteellinen virhe lähestyy nollaa, kun dt lähestyy nollaa. Viitteessä [1] olevan Lauseen 1 perusteella tämä takaa sen, että $v(t) dt$ on riittävän tarkka likiarvo.

Ammattiaineiden opettajat näyttävät käyttävän vielä yksinkertaisempaa ajattelutapaa: heille termin $v(t) dt$ tarkkuuden vakuudeksi riittää se, että se olisi tarkka arvo kertymälle välillä $[t, t + dt]$, jos funktiolla v olisi tällä välillä vakioarvona välin alkupisteen arvo $v(t)$. Tällainen ajattelutapa näyttää toimivan kaikissa käytännön sovellutuksissa. Viitteessä [2] on matemaattisesti todistettu, miten samantapainen ehto takaa määrätyn integraalin lausekkeen pätevyyden.

Huomautus 3. Vaikka differentiaalinen tapa johtaa integraalilausekkeita on rankasti lyhennetty versio yksityiskohtaisesta johdosta, se on osoittautunut luotettavaksi: ei ole kohdattu esimerkkiä, jossa suhteellisen huolellinen henkilö tekisi virheen. Tosin joskus huolimaton opiskelija on valinnut tarkasteluväliksi $[x, x + dx]$ sellaisen erikoisen välin, että siihen liittyvän kertymän lauseke $f(x) dx$ ei päde kaikilla osaväleillä.

Huomautus 4. Aiemmin monissa calculus-kirjoissa esitettiin differentiaalisen johtotavan erilaisia formalisoituja muotoja. Mutta nykyään yleiseksi tavaksi näyttää tulleen se, että jokaisessa sovellutuksessa johdetaan likiarvosumman lauseke, mistä nähdään tarkan arvon integraalilauseke. Tämä olisi varmaan hyvä menettely

myös lukiossa. Väisäläkin [3] käytti sitä, kun hän pinta-alan lisäksi käsitteli tilavuuden. Väisälä hallitsi differentiaalisien menettelyjen, kuten hänen elegantti vektorianalyysin oppikirjansa osoittaa, mutta hän varmaankin arvioi, että vielä lukiossa sitä ei ole syytä esittää.

Korkeakouluissa matematiikan ja ammattiaineiden välillä on määrättyjen integraalien kohdalla yleensä ikävä kuilu: matematiikassa ne opetetaan täsmällisesti puhtaasti matemaattisesti, mutta ammattiaineissa ja fysiikassa ne johdetaan lyhyesti differentiaalisesti. Matematiikan opettajien tehtävänä on rakentaa silta tämän kuilun yli perustelemalla differentiaalinen johtotapa, koska he voivat tehdä sen lähtien omista matemaattisista määrittelyistään. Ammattiaineiden opettajat eivät yleensä tunne näitä matemaattisia lähtökohtia eivätkä siten voi perustella differentiaalisia johtoja, jotka ammattiaineissa näyttävätkin ikään kuin vain periytyvän sukupolvelta seuraavalle.

Huomautus 5. Samantapainen kuilu on myös differentiaaliyhtälöiden kohdalla. Niiden differentiaalisissa johdoissa esiintyy kuitenkin niin erilaisia approksimaatioita, ettei niille voi esittää yleistä perustelua, kuten edellä määrättyille integraaleille. Siten differentiaaliyh-

tälöiden kohdalla on yleisesti vain lähdettävä siitä, että differentiaalisella tarkastelutavalla voidaan nopeasti johtaa differentiaaliyhtälö, jonka pätevyyttä voidaan sitten tarvittaessa tarkistaa pidemmällä, matemaattisesti täsmällisemmällä tavoilla. Lindelöfin kirjassa [4] on esitetty muutaman esimerkin valossa, miten differentiaaliyhtälö johdetaan nopeasti differentiaalisesti ja toisaalta matemaattisen täsmällisesti.

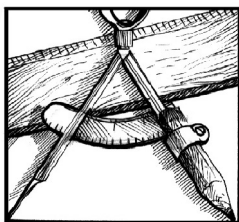
Viitteet

- [1] K. Tarvainen, *Määrätyn integraalin opettamisesta likiarvotarkasteluin*, Solmu 2/2012.
- [2] K. Tarvainen, Justifying differential derivations when setting up definite integrals, *International Journal of Mathematical Education in Science and Technology*, Vol. 39, No 1, 61–68, 2008.
- [3] K. Väisälä, *Algebran oppi- ja esimerkkikirja 2*, WSOY, 1963.
- [4] E. Lindelöf, *Johdatus korkeampaan analyysiin*, WSOY, 1956.

Diplomitehtävien oheislukemistoa

Osoitteessa <http://solmu.math.helsinki.fi/diplomi.html> on diplomitehtäville oheislukemistoa, joka varmasti kiinnostaa muitakin kuin diplomien tekijöitä:

Desimaaliluvut, mitä ne oikeastaan ovat?
 Murtolukujen laskutoimituksia
 Negatiivisista luvuista
 Hiukan osittelulaista
 Lausekkeet, kaavat ja yhtälöt
 Äärettömistä joukoista
 Erkki Luoma-aho: Matematiikan peruskäsitteiden historia
 Gaussin jalanjäljissä
 K. Väisälä: Algebra
 Yläkoulun geometriaa
 Geometrisen todistamisen harjoitus
 K. Väisälä: Geometria
 Lukuteorian diplomitehtävät



Induktio, ympyrä, kartio ja pallo

Markku Halmetoja

Mäntän lukio

Ympyrän ja pallon pinta-ala sekä pallon ja kartion tilavuus jäävät koulussa ulkoa opituiksi kaavoiksi lukion integraalilaskennan kurssiin asti. Kartion tilavuutta tosin voidaan havainnollistaa äyskäröimällä kolme kartiollista vettä vastaavaan lieriöön, mutta tämä todistus ei ole ”vedenpitävä”; se voidaan tehdä vain äärelliselle määrälle kartioita mittaustarkkuuden rajoissa. Nämä asiat voitaisiin kuitenkin kohtuullisen helposti käsitellä jo peruskoulussa eriyttävänä oppiaineena. Seuraavassa kerrotaan miten se tehdään. Esitys perustuu kahteen erittäin vanhaan aritmeettiseen totuuteen, ja pohjatietoina tarvitaan lisäksi suoran lieriön tilavuus, yhdenmuotoisuusopin alkeet sekä Pythagoraan lause.

Aritmetiikalla ei aluksi näyttäisi olevan yhtymäkoh-
taa mainittuihin geometrisiin objekteihin, mutta yhteys paljastuu tekemisen myötä. Ilmiö on matematiikassa varsin yleinen. Monia matematiikan aloja on vuosikymmeniäkin kehitelty toisistaan riippumatta, kunnes joku on löytänyt niiden välille yllättävän yhteyden. Pienemmässä mittakaavassa tämä nähdään myös koulumatematiikassa: aikaisemmin opittuja asioita putkahtelee tavantakaa esiin uusia asioita käsiteltäessä. Siksi täytyy kaikkeen matematiikassa opittuun suhtautua tietyllä kunnioituksella.

Induktio

Olet varmaankin nähnyt uutislähetyksen kevennysosassa japanilaisten opiskelijoiden pystyttävän muutamia miljoonia dominopalikoita jonoon, minkä jälkeen he

kaatavat jonon ensimmäisen palikan, jolloin kaikki palikat kaatuvat yksitellen. Näillä tempauksilla yritetään päästä Guinnessin ennätysten kirjaan ja päästäänkin, mikäli saadaan palikoita kaatumaan enemmän kuin muut ovat aikaisemmin saaneet. Matematiikassa on mahdollista kuitenkin pistää paljon paremmaksi, sillä voimme ensimmäisen palikan avulla kaataa äärettömän monta seuraavaa palikkaa. Kaatamismenetelmää kutsutaan *matemaattiseksi induktioksi* tai lyhyesti vain induktioksi. Sen juoni selviää seuraavasta esimerkistä.

Esimerkki. Todistettava, että kokonaislukujen summa

$$S_n = 1 + 2 + \dots + n = \frac{1}{2}n(n+1). \quad (2)$$

Tutkitaan yhtälöä (2) aluksi pienillä n :n arvoilla. Esimerkiksi

$$S_1 = 1 = \frac{1}{2} \cdot 1 \cdot (1+1) \quad \text{ja}$$

$$S_2 = 1 + 2 = \frac{1}{2} \cdot 2 \cdot (2+1),$$

joten väite on tosi n :n arvoilla 1 ja 2. Tämä havainto vastaa ensimmäisen ja toisenkin palikan kaatamista. Miten sitten loput palikat saadaan nurin? Osoittamalla, että jos väite on tosi arvolla $n = k$, niin sen seurausena se on tosi myös arvolla $n = k + 1$. Kutsutaan tätä toistaiseksi *kaatumissäännöksi*. Nyt voidaan päätellä seuraavasti: Koska väite kokeilun perusteella on tosi arvolla $n = 2$, niin kaatumissäännön perusteella se on tosi myös arvolla $n = 2 + 1 = 3$. Koska väite nyt *tiedetään todeksi* arvolla $n = 3$, niin se kaatumissäännön mukaan on tosi myös arvolla $n = 3 + 1 = 4$. Näin voidaan jatkaa loputtomiin. Siis kaikki palikat kaatuvat,

eli yhtälö on tosi kaikilla n :n positiivisilla kokonaisluokuarvoilla.

Kaatumissäännön oikea nimi on *induktioaskel* ja se täytyy vielä todistaa, jotta tämä ajatusrakennelma olisi aukoton. Oletetaan siis, että väite on tosi arvolla $n = k$, jolloin

$$S_k = 1 + 2 + \dots + k = \frac{1}{2}k(k+1).$$

Nyt

$$\begin{aligned} S_{k+1} &= 1 + 2 + \dots + k + (k+1) \\ &= \frac{1}{2}k(k+1) + (k+1) \\ &= (k+1)\left(\frac{1}{2}k+1\right) \\ &= \frac{1}{2}(k+1)(k+2) \\ &= \frac{1}{2}(k+1)((k+1)+1), \end{aligned}$$

eli väite on tosi myös arvolla $n = k+1$. Induktioaskel on näin todistettu.

Positiivisten kokonaislukujen neliöille on voimassa hie-man hankalamman näköinen yhtälö

$$1^2 + 2^2 + \dots + n^2 = \frac{1}{6}n(n+1)(2n+1), \quad (3)$$

jota myös tarvitsemme jatkossa. Puhtaasti esteettisistä syistä mainittakoon vielä kolmaskin:

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

Todistamalla yhtälöt (3) ja (4) opit induktion. Se kannattaa tehdä, sillä kyseessä on yksi tärkeimmistä matematiikan todistusmenetelmistä. Induktiosta kerrotaan myös kirjoituksessa [1].

Ympyrä

Kaikki ympyrät ovat keskenään yhdenmuotoisia, joten kahdessa annetussa ympyrässä vastinpituuksien suhde on vakio. Jos siis kehät ovat p ja p' ja halkaisijat d ja d' , niin on voimassa verranto

$$\frac{d}{d'} = \frac{p}{p'}$$

joka p'/d :llä kertomalla tulee muotoon

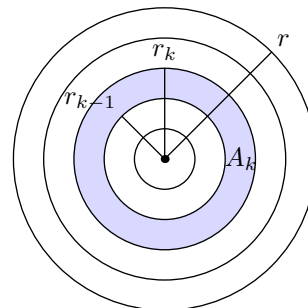
$$\frac{p'}{d'} = \frac{p}{d}.$$

Kehän ja halkaisijan suhde yhdessä ympyrässä on sama kuin toisessa ympyrässä, eli tämä suhde on ympyrän koosta riippumaton luku. Se merkitään kreikkalaisella kirjaimella π , ja sen kaksidesimaalinen likiarvo on 3,14. Siis, jos ympyrän kehä ja halkaisija ovat p ja d , niin

$$\frac{p}{d} = \pi.$$

Tästä seuraa, että $p = \pi d$, ja koska $d = 2r$, edelleen $p = 2\pi r$. Tämä puhtaasti geometriseen päättelyyn pohjautuva ympyrän kehän pituuden perustelu voidaan täsmentää analyttisesti vasta yliopisto-opinnoissa.

Miten lasketaan r -säteisen ympyrän pinta-ala? Tutkailaan aluksi kuviossa näkyviä sisäkkäisiä renkaita, joiden kehät jakavat säteen n :ään



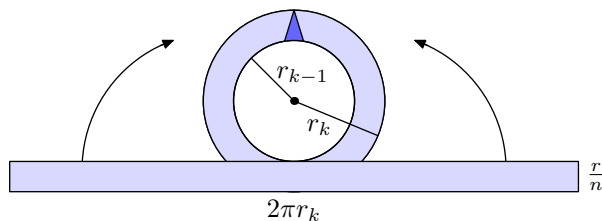
yhtäsuureen osaan. Jokaisessa renkaassa sisä- ja ulko-kehän välinen etäisyys on siten $\frac{r}{n}$. Ympyrän pinta-ala on renkaiden pinta-alojen summa:

$$A_{\odot} = A_1 + A_2 + \dots + A_n.$$

Arvioimalla renkaiden pinta-aloja saamme arvion myös ympyrän pinta-alasta. Kuviossa tummennettuna näkyvän k :nnen renkaan sisä- ja ulkosäteet ovat

$$r_{k-1} = \frac{(k-1)}{n} r \quad \text{ja} \quad r_k = \frac{k}{n} r.$$

Sisä- ja ulkokehän pituudet ovat $2\pi r_{k-1}$ ja $2\pi r_k$. Kun ulkokehän pituinen suorakulmio, jonka korkeus on $\frac{r}{n}$, kierretään renkaan päälle, se peittää sen



täysin, ja osa peittyy kuvion osoittamalla tavalla kahteen kertaan. Suorakulmion pinta-ala on suurempi kuin renkaan pinta-ala, ja kaikkien näiden suorakulmioiden pinta-alojen summa on siksi suurempi kuin ympyrän pinta-ala. Yhteenlaskettavat suorakulmioiden pinta-alat sievenevät muotoon

$$2\pi r_k \frac{r}{n} = 2\pi \frac{k}{n} r \frac{r}{n} = \frac{2\pi r^2}{n^2} k,$$

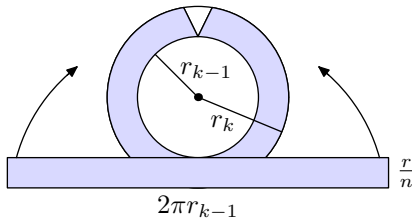
missä $k = 1, 2, \dots, n$, ja niiden summa

$$\frac{2\pi r^2}{n^2} (1 + 2 + \dots + n) = \frac{2\pi r^2}{n^2} \frac{n(n+1)}{2} = \pi r^2 \left(1 + \frac{1}{n}\right).$$

Ympyrän pinta-alalle saadaan siis yläraja

$$A_{\odot} < \pi r^2 \left(1 + \frac{1}{n}\right). \quad (5)$$

Kun sisäkehän pituinen suorakulmio, jonka korkeus on $\frac{r}{n}$, kierretään



renkaan päälle, se ei peitä sitä täysin, vaan jää kuvion osoittamalla tavalla vajaaksi. Suorakulmion pinta-ala on pienempi kuin renkaan pinta-ala, ja kaikkien näiden suorakulmioiden pinta-alojen summa on siksi pienempi kuin ympyrän pinta-ala. Yhteenlaskettavat suorakulmioiden pinta-alat sievenevät muotoon

$$2\pi r_{k-1} \frac{r}{n} = 2\pi \frac{(k-1)}{n} r \frac{r}{n} = \frac{2\pi r^2}{n^2} (k-1),$$

missä $k = 1, 2, \dots, n$, ja niiden summa

$$\begin{aligned} \frac{2\pi r^2}{n^2} (0 + 1 + 2 + \dots + (n-1)) &= \frac{2\pi r^2}{n^2} \frac{(n-1)n}{2} \\ &= \pi r^2 \left(1 - \frac{1}{n}\right). \end{aligned}$$

Ympyrän pinta-alalle saadaan siis alaraja

$$\pi r^2 \left(1 - \frac{1}{n}\right) < A_{\odot}. \quad (6)$$

Yhdistämällä epäyhtälöt (5) ja (6) saamme kaikilla n :n positiivisilla kokonaislukuarvoilla voimassaolevan kaksoisepäyhtälön

$$\pi r^2 \left(1 - \frac{1}{n}\right) < A_{\odot} < \pi r^2 \left(1 + \frac{1}{n}\right).$$

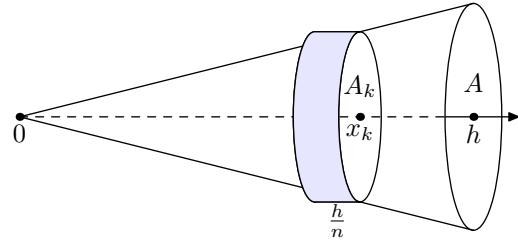
Antamalla n :n kasvaa hyvin suureksi, tulevat kaksoisepäyhtälön vasemmalla ja oikealla puolella olevat πr^2 :n kertoimina olevat luvut yhä lähemmäs ja lähemmäs lukua 1. Lukion matematiikassa tämä ilmaistaan niin, että näiden lausekkeiden *raja-arvo* on 1, kun n lähestyy ääretöntä. Ala- ja ylärajalla on siis yhteinen raja-arvo πr^2 , kun n kasvaa, ja koska $A_{\odot}$ kaikilla n :n arvoilla on niiden välissä, ei ole muuta mahdollisuutta kuin että

$$A_{\odot} = \pi r^2.$$

Ympyrän pinta-ala on niin tärkeä asia, että aktiivisen lukijan kannattaa miettiä vielä seuraavaa pientä sitä valaisevaa tutkimustehtävää: *Voidaanko ympyrän pinta-ala laskea niin, että ajatellaan renkaat puolisuunnikkakiksi, joiden korkeus on $\frac{r}{n}$ ja kantoina ovat renkaan sisä- ja ulkokehän pituudet? Tällöin ei tarvittaisi alaraja- ja ylärajoja, vaan pinta-ala saataisiin suoraan laskeamalla puolisuunnikkaiden alat yhteen. Jos tämä onnistuu, niin kuinka moneksi renkaaksi ympyrä pitää jakaa?*

Kartio

Olkoon h kartion korkeus ja A sen pohjan pinta-ala. Kuvion kartio näyttää ympyräpohjaiselta, mutta pohjan muodolla ei ole merkitystä. Kartiota leikkaava pohjan suuntainen taso erottaa siitä kärjen puolelle alkuperäisen kartion kanssa yhdenmuotoisen kartion. Niiden pohjat ovat yhdenmuotoisia



tasokuvioita, joiden pinta-alojen suhde on vastinpi-tuuksien, esimerkiksi korkeusjanojen, suhteen neliö. Jaetaan korkeusjana pohjan suuntaisilla tasoilla n :ään yhtäsuureen osaan. Kohdassa $x_k = \frac{k}{n}h$ olevan leikkauskuvion pinta-alan A_k ja pohjan pinta-alan A suhde on siis

$$\frac{A_k}{A} = \left(\frac{kh}{n} : h\right)^2 = \left(\frac{k}{n}\right)^2.$$

Tästä seuraa

$$A_k = A \left(\frac{k}{n}\right)^2.$$

Kohdassa x_k olevan lieriön tilavuus on

$$A_k \frac{h}{n} = A \frac{k^2}{n^2} \frac{h}{n} = \frac{Ah}{n^3} k^2, \quad k = 1, 2, \dots, n.$$

Koska kartio jää näiden lieriöiden yhdessä muodostaman kappaleen sisään, on lieriöiden tilavuuksien summa kartion tilavuutta suurempi. Siis

$$\begin{aligned} V_{\text{kartio}} &< \frac{Ah}{n^3} (1^2 + 2^2 + \dots + n^2) \\ &= \frac{Ah}{n^3} \frac{n(n+1)(2n+1)}{6} \\ &= \frac{Ah}{6} \left(1 + \frac{1}{n}\right) \left(2 + \frac{1}{n}\right), \end{aligned}$$

joten saamme kartion tilavuudelle ylärajan

$$V_{\text{kartio}} < \frac{Ah}{6} \left(2 + \frac{1}{n^2} + \frac{3}{n}\right). \quad (1)$$

Aktiivinen lukija voi samalla tavalla johtaa kartion sisään jäävien lieriöiden tilavuuksien summasta kartion tilavuudelle alarajan

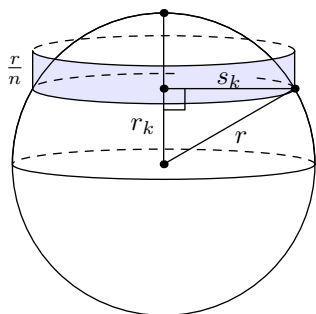
$$\frac{Ah}{6} \left(2 + \frac{1}{n^2} - \frac{3}{n}\right) < V_{\text{kartio}}, \quad (2)$$

ja päätellä näin saatujen epäyhtälöiden (1) ja (2) avulla, että

$$V_{\text{kartio}} = \frac{1}{3} Ah.$$

Pallo

Pallon tilavuuden määrittämiseksi leikataan sitä yhdensuuntaisilla tasoilla niin, että säde r jakaantuu n :ään yhtäsuureen osaan. Kuvioon



merkittyjen tietojen avulla aktiivinen lukija osaa nyt itsenäisesti johtaa pallon tilavuudelle alarajan

$$2\pi r^3 \left(\frac{2}{3} - \frac{1}{6n^2} - \frac{1}{2n} \right) < V_{\text{pallo}}$$

ja ylärajan

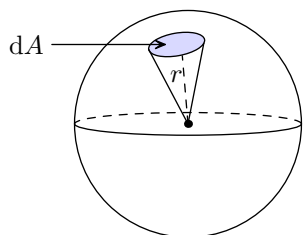
$$V_{\text{pallo}} < 2\pi r^3 \left(\frac{2}{3} - \frac{1}{6n^2} + \frac{1}{2n} \right),$$

ja päätellä niiden perusteella, että

$$V_{\text{pallo}} = \frac{4}{3}\pi r^3.$$

Pallon pinta-ala voidaan määrittää täsmällisesti matemaattisen analyysin keinoin vasta yliopisto-opinnoissa. Seuraava kuvaileva esitys on laadittu kirjan [4] pohjalta.

Pallon pinta-alan laskemiseksi peitetään se pallon kokoon nähden



pienillä osapinnoilla eli *pinta-alkioilla* A_k , joiden summa

$$A_1 + A_2 + \dots + A_n = A_{\text{pallo}}.$$

Pinta-alkioita ajatellaan itse asiassa olevan äärettömän monta, jolloin niitä merkitään symbolisesti dA ja niiden summaa venytetyllä S-kirjaimella:

$$\int_{\text{pallo}} dA = A_{\text{pallo}}.$$

Kahdella pinta-alkiolla saattaa olla yhteisiä reunapisteitä, mutta ei yhteisiä sisäpisteitä. Kun pinta-alkion dA reunapisteet yhdistetään pallon keskipisteeseen, saadaan kartio, jonka pohjan pinta-ala on dA ja korkeus on r . Tällaisen *tilavuusalkion* tilavuus on noin $dV = \frac{r}{3}dA$. Likimääräisyys johtuu siitä, että pinta-alkiot eivät ole tasomaisia. Jos ne kuitenkin ovat hyvin pieniä, niin niiden tulkitseminen tasomaisiksi aiheuttaa vain olemattoman virheen. Pallon tilavuus on näiden tilavuusalkioiden summa:

$$V_{\text{pallo}} = \int_{\text{pallo}} dV = \frac{r}{3} \int_{\text{pallo}} dA = \frac{r}{3} A_{\text{pallo}},$$

mistä seuraa, että

$$A_{\text{pallo}} = 4\pi r^2.$$

Lopuksi

Nähdyt esimerkit, tai oikeammin niiden tässä nähty käsittely, kuuluvat integraalilaskennan esihistoriaan. Jo Arkhimedes¹ päätteli pinta-aloja ja tilavuuksia periaatteessa samalla tavalla, mutta puhtaasti geometrisin käsittein. Pari muunnelmaa hänen esittämästään ympyrän pinta-alan todistuksesta löytyy kirjasta [3, s. 179] ja kirjoituksesta [2]. Nykyaikaisen integraalilaskennan perusteet julkaisi ensimmäisenä Leibniz² vuonna 1675. Hän löysi yhteyden käyrän rajoittaman pinta-alan ja käyrää sivuavan suoran määrittämisen välille. Perustelusti voidaan todeta, että se tiede ja teknologia, jonka tänään koemme jokapäiväisessä elämässämme, on pitkälti juuri tuon yksittäisen keksinnön seurausta. Esihistorian tunteminen puolestaan antaa erinomaisen pohjan lukiossa alkavalle integraalilaskennan opiskelulle.

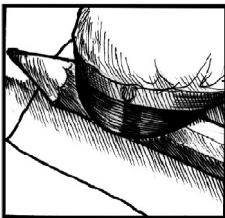
Kiitokset dosentti Heikki Apiolalle rakentavista kommentteista.

Viitteet

- [1] <http://solmu.math.helsinki.fi/2008/diplomi/gauss.pdf>
- [2] http://solmu.math.helsinki.fi/2008/diplomi/ylakoulun_geometriaa.pdf
- [3] Teuvo Aittokallio, *Patikkaretkiä matematiikan maisemaan*, Kaarina 2009.
- [4] Kalle Väisälä, *Lukion geometria*, WSOY 1966.

¹ Arkhimedes (287–212 eaa.), kreikkalainen matemaatikko.

² Gottfried Leibniz (1646–1716), saksalainen matemaatikko ja filosofi.



Pari vanhaa ylioppilastehtävää

Lehtori K.

Vanhoista ylioppilastehtäväkokoelmista löytyy helmiä. Vuonna 1910 kysyttiin syksyn kokeessa yhtälöryhmää

$$\begin{cases} x - ay + a^2z = a^3 \\ x - by + b^2z = b^3 \\ x - cy + c^2z = c^3. \end{cases}$$

Suurin osa kokelaista lienee ryhtynyt eliminoimaan tuntemattomia, ja ratkeahan tehtävä niinkin. Sen laatija on kuitenkin ollut muissa aatoksissa. Yhtälöryhmä voidaan nimittäin kirjoittaa muotoon

$$\begin{cases} a^3 - za^2 + ya - x = 0 \\ b^3 - zb^2 + yb - x = 0 \\ c^3 - zc^2 + yc - x = 0, \end{cases}$$

mistä näkyy, että luvut a, b, c ovat polynomin

$$p(t) = t^3 - zt^2 + yt - x \quad (3)$$

kolme nollakohtaa. Tässä polynomissa muuttujan korkeimman potenssin kerroin on 1, joten sen tuloesitys on

$$p(t) = (t - a)(t - b)(t - c). \quad (4)$$

Polynomi (4) on aukikerrottuna

$$p(t) = t^3 - (a + b + c)t^2 + (ab + bc + ca)t - abc. \quad (5)$$

Vertailemalla kertoimia esitystavoissa (3) ja (5) nähdään, että

$$\begin{cases} x = abc \\ y = ab + bc + ca \\ z = a + b + c. \end{cases}$$

Sensoreilla ja tehtävän laatijalla lienee ollut aluksi hauskaa kokelaiden monimutkaisia ratkaisuja katsellessaan, mutta lopulta hymy on varmaan hyytynyt, sillä kaikki monenkin sivun mittaiset ratkaisut on täytynyt käydä yksityiskohtaisesti läpi, jotta arvostelussa toteutuisi oikeudenmukaisuus.

Hauskalta näyttäviä yhtälöryhmiä oli ollut ylioppilaskokeessa jo aikaisemminkin. Vuoden 1903 kevään kokeessa oli seuraava tehtävä:

Ratkaise yhtälöryhmä

$$\begin{cases} ax + by + cz = d \\ bx + ay + cz = d \\ cx + by + az = d, \end{cases}$$

kun a, b ja c ovat keskenään erisuuret.

Kirjassa [1] tehtävälle annetaan yksikäsitteinen ratkaisu, ja siinä yhteydessä kysytään, miksi tehtävässä luvut a, b ja c edellytetään keskenään erisuuriksi. Jätämme aktiivisen lukijan pohdittavaksi, onko tehtävän ratkaisu todellakin näin ongelmaton.

Viitteet

- [1] R. Laurén, E. Kannisto, *Matemaattiset tehtävät ylioppilastutkinnossa vuosina 1895–1935*, kahdeksas painos, Gummerus osakeyhtiö, 1935.