

Solmu

Matematiikkalehti
2/2013

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



Solmu 2/2013

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

Biocenter Oulu, Oulun yliopisto

Antti Viholainen, tutkijatohtori, antti.viholainen@uef.fi

Fysiikan ja matematiikan laitos, Itä-Suomen yliopisto

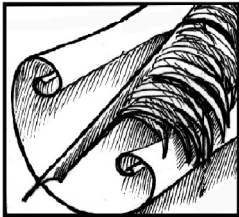
Numeroon 3/2013 tarkoitetut kirjoitukset pyydämme lähettämään 2.9.2013 mennessä.

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 opetussuunnitelmasta (Markku Halmetoja).....	4
$P = NP$ -ongelma – mikä se on? (Tuomas Korppi)	7
Käänteistä marjanpoimintaa (Jukka Liukkonen).....	11
Kompleksiluvut ja kolmannen asteen yhtälön ratkaisut (Lauri Ajanki).....	15
Binomikaava (Pekka Alestalo)	18
Binomijakaumasta (Markku Halmetoja).....	21
Laskentoa ja jääkiekkoa (Matti Lehtinen)	23
Sekalaisia kilpailutehtäviä (Heikki Pokela).....	25
Supremum (Tuomas Korppi)	27



Pitkän matematiikan opetussuunnitelmasta

Pääkirjoitus

Helsingin yliopiston matematiikan ja tilastotieteen laitoksen johtaja, professori Mats Gyllenberg kuuluu josakin yhteydessä sanoneen, että ”yhtään ihmiskunnan suurista ongelmista ei ratkaista ilman matematiikan apua”. Ajatusta voi täydentää toteamalla, että tuskin on olemassa yhtään tällaista ongelmaa, jonka ratkaisemisessa tarvittava matematiikka ei tavalla tai toisella pohjautuisi edellisen Solmun pääkirjoituksessa [1] luvion pitkän matematiikan opetussuunnitelman pohjaksi ehdottamaani asialistaan. Seuraavassa pohditaan tätä seitsemän kohdan ohjelmaa hieman yksityiskohtaisemmin. Sen sisältö vastaa suurelta osin nykyistä opetussuunnitelmaa, mutta asiat ovat oppimisen ja myös fysiikan kannalta paremmassa järjestyksessä. Nykyiset valtakunnalliset syventävät kurssit sisältyvät karsittuna esittämäni pakolliseen oppimäärään.

1. Opiskelu alkaa reaalitylukujen laskulakien ja ominaisuuksien esittelyllä. Verrannollisuus ja prosenttilaskut kerrataan harjoitustehtävissä. Pääsisältönä on perehtyminen algebrallisten, eksponentti- ja logaritmifunktioiden ominaisuuksiin. Niihin liittyvien lausekkeiden, yhtälöiden ja epäyhtälöiden käsittely suoritetaan samassa laajuudessa kuin nykyisinkin. Lasketaan myös funktioiden ja lukujonojen raja-arvoja. Tämä ei raskautaa oppimäärää, vaan pikemminkin lisää ymmärrystä esimerkiksi rationaalifunktioiden määrittelyehdoista. Määritellään funktion jatkuvuus ja todetaan jatkuvan funktion perusominaisuudet. Juurifunktiot ja potenssi, missä eksponenttina ei ole kokonaisluku, käsitellään ennen eksponenttifunktion perehtymistä. Logaritmien osalta keskitytään pääasiassa Briggsin logaritmiin, mutta

johdetaan myös kantaluvun vaihtosääntö. Luonnollinen logaritmi opiskellaan myöhemmin analyysin yhteydessä. Käänteisfunktioita käsitellään esimerkkien kautta.

2. Logiikka ja lukuteoria otetaan osaksi pakollista oppimäärää, sillä, kuten monet ovat todenneet, matematiikan opetuksen on seurattava aikaansa. Logiikan alkeet, induktio, Boolean algebra ja joukko-opin peruskäsitteet ovat kongruenssiopin lisäksi tämän osion keskeisiä asioita. Sovelluksina esitellään lukuteoriaan perustuvia salakirjoitusjärjestelmiä, erityisesti RSA-algoritmi. Sivustolla <http://avoinoppikirja.fi> oleva oppikirja [2] kattaa suunnilleen nämä asiat.

3. Suora ja epäsuora todistus on opittu edeltävässä logiikan osiossa, joten valmiudet deduktiiviseen geometrian opiskeluun ovat olemassa. Päätelyn pohjaksi annetaan tiettyjä selviöinä pidettäviä lauseita. Eräiden Eukleideen-Hilbertin aksioomien lisäksi niitä ovat mm. samankohdaisia kulmia koskeva lause sekä kolmioiden yhtenevyys- ja yhdenmuotoisuuslauseet. Tarkoituksena ei ole problematisoida intuitiivisesti selviä totuuksia vaan näyttää muutaman esimerkin avulla, miten välttämät todistuvat loogisesti tietyistä perusteista lähtien. Pääasiana on oppia soveltamaan algebraa ja yhdenmuotoisuutta geometrisissa ongelmissa. Monikulmioiden pinta-aloja johdetaan suorakulmiosta lähtien. Yleisempien kappaleiden tilavuudet annetaan valmiina, joskin eräitä niistä voi johtaa kirjoituksessa [3] esitetyllä tavalla. Opitaan sini- ja kosinilauseet, ja tässä yhteydessä laajennetaan trigonometristen funktioiden määritelmät mielivaltaisille kulmille. Vektoreita tarkastellaan alustavasti jo nyt määrittelemällä niiden sum-

ma ja erotus, luvulla kertominen ja yhdensuuntaisuus, miltä pohjalta voidaan käsitellä vektorin jakaminen tasossa komponentteihin. Vektorioppi antaa perspektiiviä erälle geometrian lauseille ja niitä tarvitaan myös fysiikassa. Sen opiskelu on helpompaa, jos hallitsee kulloinkin tarvittavat matemaattiset käsitteet. Lukiossa matematiikan on kuljettava fysiikan edellä.

Nämä kolme asiakokonaisuutta muodostavat ensimmäisen lukiovuoden oppimäärän. Opettajalla on oltava mahdollisuus oman harkintansa mukaan kiihdyttää tai hidastaa etenemisnopeutta opettamansa ryhmän tarpeita vastaavaksi. Matematiikan opiskelu tulisiikin järjestää jaksottomaksi käsittämään viisi tai kuusi oppituntia viikossa koko lukuvuoden ajan, onhan pitkä matematiikka sen valinneille äidinkielen ohella koulun tärkein oppiaine. Aikaa käytetään pikemminkin syvyyssuunnassa tapahtuvaan opiskeluun, joten perusasiat ehditään käymään läpi kaikkialla lukuvuoden loppuun mennessä. Tällöin esimerkiksi koulun vaihto ei aiheuta merkittäviä ongelmia. Luultavasti eräissä muissakin oppiaineissa on tarvetta palata jaksottomaan opiskeluun. Koulun hallinnon on tässä joustettava, sillä sen tehtävähän on taata oppimisen edellytykset eikä tuhota niitä opetusta byrokratisoimalla.

4. ja 5. Trigonometria, kompleksiluvut, vektorioppi ja analyttinen geometria muodostavat monin tavoin toisiinsa kietoutuvan kokonaisuuden, joka on parasta aloittaa vektoreilla. Opiskellaan aluksi muotoa $x\mathbf{i} + y\mathbf{j}$ olevien vektorien yhteen- ja vähennyslasku, reaalityyppillä kertominen, pituus ja yhdensuuntaisuus. Trigonometriset funktiot on jo määritelty yksikköympyrän avulla, joten radiaaniin tutustumisen jälkeen voidaan todistaa kosinin ja sinin yhteen- ja vähennyslaskukaavat, kuten kirjoituksessa [4] on tehty. Trigonometrinen funktioiden perusominaisuuksien johtamisen jälkeen päästään perehtymään yhtälöihin sekä ilman derivointia ratkeaviin ääriarvotehtäviin. Kompleksiluvut esitetään xy -tason lukupareina, joille määritellään alussa opitun vektorilaskennan lisäksi kertolasku. Luonnollisesti opitaan myös kompleksiluvun tavanomainen esitystapa, napakoordinaattiesitys ja de Moivre'n kaava. Polynomien jaollisuusoppi täydennetään algebran peruslauseen avulla. Vektorilaskentaa voidaan nyt jatkaa esittelemällä aluksi xyz -koordinaatisto tavanomaisine kantavektoreineen. Komponenttiesitysten rinnalle otetaan koordinaattiesitykset ja niiden avulla suoritettavat laskutoimitukset. Määritellään skalaaritulo ja todistetaan sitä koskevat laskusäännöt. Määritellään vektoritulo ja annetaan sitä koskevat laskusäännöt ilman todistuksia. Esitetään suuntaisjärmiön tilavuus skalaarikolmitulon itseisarvona. Analyttisen geometrian osuus aloitetaan xy -tason suoran vektori yhtälöllä, joka voidaan saman tien todeta dimensiosta riippumattomaksi. Vektori yhtälöstä johdetaan suoran parametrisointi ja siitä edelleen tavanomainen yhtälö. Kulmakertoimeen ja sen trigonometriseen merkitykseen päästään suuntavektorin avulla. Johdetaan xy -tason suoran

normaali yhtälö vaatimalla, että annetun pisteen kautta kulkeva suora on kohtisuorassa tunnettua vektoria vastaan. Samalla tavalla saadaan xyz -koordinaatiston tasolle normaali yhtälö. Johdetaan kaava pisteen etäisyydelle xy -tason suorasta ja xyz -koordinaatiston tasosta. Hyödynnetään vektoreita mahdollisimman tehokkaasti kaikissa muissakin suorissa ja tasoissa koskevilla kysymyksillä. Lineaarisia yhtälöryhmiä ratkaistaan sekä algebrallisesti että geometrisesti. Toisen asteen käyriä käsitellään nykyistä perusteellisemmin. Ellipsi, paraabeli ja hyperbeli määritellään yhdenmukaisesti uraominaisuuden kautta ja niille johdetaan parametriesityksiä. Niiden tangentteja määritetään tavanomaisen diskriminanttitarkastelun lisäksi laskemalla käyrien sekanttien kulmakertoimien raja-arvoja. Näin saadaan differentiaalilaskennan perusajatus kirkastettua niin, ettei se välittömästi katoa muodollisten derivoimissääntöjen alle.

6. Todennäköisyyslaskenta aloitetaan kombinatoriikan alkeilla. Binomilause todistetaan (ks. [5]), sillä sitä tarvitaan myöhemmin myös potenssin derivoimissääntöä johdettaessa. Tilastollisen aineiston keskiarvo ja keskihajonta käsitellään, koska niitä tullaan tarvitsemaan normaali jakauman yhteydessä. Joukko-opin käsitteet ja merkinnät tulevat luontevasti käyttöön todennäköisyyttä määriteltäessä ja laskusääntöjä johdettaessa. Todennäköisyyslaskennan keskeistä sisältöä geometrisen, tilastollisen ja ehdollisen todennäköisyyden lisäksi ovat äärellisiin kenttiin liittyvät diskreetit satunnaisuuttajat. Niiden todennäköisyysjakaumista esitetään myös massatulkinta, mikä selkiyttää odotusarvon ja varianssin käsitteitä. Toistokokeisiin liittyvien tehtävien yhteydessä kertautuvat eksponentti- ja logaritmifunktioiden ominaisuudet.

Opiskelun precalculusvaihe on näin saatu päätökseen, ja on luotu luja pohja korkeamman matematiikan opiskelulle. Sen voi aloittaa jo toisen opiskeluvuoden keväällä välittömästi todennäköisyyslaskennan tultua käsitellyksi. Aikataulut ovat järjestelykysymyksiä.

7. Analyysin opiskelu aloitetaan derivaatan määritelmällä, jonka soveltamista harjoitellaan perusteellisesti. Yleisten derivoimissääntöjen todistamisen jälkeen päädytään johtamaan alkeisfunktioiden derivaatat. Samalla harjoitellaan myös integraalifunktion muodostamista, kuten opetussuunnitelmaehdotuksessa [6] esitetään. Näiden laskutoimitusten opiskelu samanaikaisesti estänee niiden sekaantumisen myöhemmissä opinnoissa. Luonnollisesti integrointitekniikkaa on harjoiteltava vielä erikseen ennen määrätyn integraalin käsitelyä. Funktioiden kulkuun liittyvät asiat perustellaan väliarvolauseen avulla. Tavanomaisten sovellusten lisäksi käsitellään yhtälön numeerinen ratkaiseminen Newtonin menetelmällä, sillä siinä tulee taas kerran esille differentiaalilaskennan ydin. Tähän kaikkeen riittää aikaa, koska opiskelua ei tarvitse alati keskeyttää uusien funktiotyyppien esittelyyn. Määrätty integraali määritellään ala- ja yläsummia käyttäen. Induktiota opetel-

taessa on todistettu erilaisia kokonaislukujen potenssisummaa, joiden avulla voidaan todeta, että tietyllä välillä esimerkiksi funktion $g(x) = x^3$ tasavälisillä alaja yläsummilla on yhteinen raja-arvo. Tämän jälkeen oppilaan on helppo hyväksyä, että sama pätee ainakin jatkuville funktioille. Ennen määrätyn integraalin ja integraalifunktion välisen yhteyden johtamista lasketaan integraalien likiarvoja puolisuunnikasmenetelmällä. Se havainnollistaa hyvin sitä, mistä integraalilaskennassa on kysymys. Määrätyn integraalin osalta nykyiseen oppimäärään lisätään fysiikan sovelluksia, ensimmäisen kertaluvun separoituvia differentiaaliyhtälöitä, epäoleelliset integraalit ja jatkuvia satunnaismuuttujia koskeva todennäköisyyslaskennan osuus, joka huipentuu normaalijakauman käsittelyyn. Viimeisenä käsitellään sarjat, koska nyt on mahdollista testata niiden suppenemista myös integraalitestein.

Tällaisen pitkän matematiikan oppimäärän kunnollinen suorittaminen takaa pääsyn matematiikan taitoja edellyttäviin korkeakouluopintoihin ja suurella todennäköisyydellä myös niissä menestymisen. Tehokas opiskelu edellyttää taitavasti laadittua oppimateriaalia. Harjoitustehtävissä laadun on korvattava määrä. Hyvä periaate on, että matematiikkaa sovelletaan matematiikkaan, eli aikaisemmin opitut asiat esiintyvät osina myöhempiä harjoitustehtäviä. Näin oppimäärä ei pirstaloidu erillisiin osiin. Arkielämän sovellusten tulee olla järkeviä. Oikein mitoitettu oppimateriaali ja hyvä kouluopetus ei pureksi kaikkea valmiiksi. Harjoitustehtäviä ratkaisemalla oivalletaan asioiden välisiä yhteyksiä ja opitaan laskurutiineja, mitä kukaan ei voi tehdä kenenkään puolesta. Matematiikka kasvaa osaksi harastajansa keskushermostoa, ja näin juuri sen on oltava, jos joskus aikoo osallistua ”ihmiskunnan suurten ongelmien ratkaisemiseen”. Muussa tapauksessa niiden pohtiminen jää hyödyttömäksi taivasteluksi.

Ylioppilaskoe saisi perustua pelkästään tässä ehdotettuun pakolliseen oppimäärään, joskin sen lisäksi voidaan opiskella koulukohtaisia syventäviä oppimääriä. Sopivia aihepiirejä löytyy analyttisestä geometriasta, sillä esimerkiksi toisen asteen käyriä on mukava tutkia napakoordinaatistossa ja vektorituloon liittyvät todistukset ovat myös syventävää oppiainesta. Geometriaakaan ei ole tyhjentävästi opiskeltu pakollisen osuuden yhteydessä ja lukuteoriaa voi aina opiskella lisää. Analyysin rinnalla voidaan opiskella differentiaaliyhtälöitä. Vektoriopin jatkoksi sopii erinomaisesti myös lineaarialgebra. Sen voi jakaa konkreettiseen kaksi- ja kolmiulotteiseen osaan ja abstraktimpaan osaan, jossa vektoreita ja matriiseja tarkastellaan yleisemmin.

On outoa, että oppimateriaalien tekeminen on jätetty sisältöä koskevan kontrollin tavoittamattomiin yksityiseksi liiketoiminnaksi. Matematiikan kannalta olisi parempi, jos opetushallitus värväisi ammattimattamatikoita laatimaan ja tarkistamaan vapaasti käytettävät

koko lukion kattavat oppikirjat. Avoin-kirja-projektissa työskentelevät saattaisivat olla ydinjoukko niiden laatimisessa. Tämän kirjoituksen seitsenkohtainen ohjelma on kaikin puolin sopiva jäsenitys yksityiskohtaiselle opetussuunnitelmalle ja siihen pohjautuvalle oppikirjasarjalle, sillä siinä esitetyt asiat on joka tapauksessa opittava ja ne on asetettu kohtuullisen loogiseen järjestykseen. Mitä muuta lukion pitkä matematiikka voisi olla?

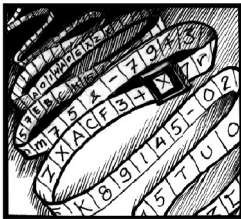
Sanomattakin on selvää, että pitkän matematiikan opiskelu on aloitettava välittömästi lukion alkaessa. Mihin kahdesta neljään kaikille yhteisiin kursseihin ei ole mahdollisuutta eikä motiivia. Ne johtaisivat yksinomaan tyhjäkäyntiin ja turhautumiseen, sillä matemaattisesti heikoin lukioon tuleva oppilasaines ei hallitse alkeitakaan kirjaimilla laskemisesta ja numeeriset taidotkin ovat hukassa. Mikään ei enää lukiossa saa hidastaa oppimaan haluavien ja kykenevien etenemistä.

Lukion lyhyen matematiikan oppimäärää on kehitettävä nykyistä paremmin vastaamaan matemaattisesti heikompien oppilaiden tarpeita. Se voisi sisältää arkielämän laskentaa käsittelevän kokonaisuuden, jonka päälle olisi mahdollisuus valita lisäkursseja, joilla opitaan yhteiskunnallisten yliopisto-opintojen, OKL:n ja eräiden amk-opintojen kannalta olennaisia asioita. Lyhyestä matematiikasta lisää seuraavassa Solmussa.

Markku Halmetoja

Viitteet

- [1] Markku Halmetoja, Lopultakin, vai eikö sittenkään, http://solmu.math.helsinki.fi/2013/1/paak_1_13.pdf
- [2] Anna-Maija Partanen, Antti Rasila, Mika Setälä, Vapaa matikka 11, http://avoinoppikirja.fi/tiedostot/lukio/matematiikka/vapaa_matikka_11_v1.pdf
- [3] Markku Halmetoja, Induktio, ympyrä, kartio ja pallo, http://solmu.math.helsinki.fi/2012/3/induktio_ympyra_kartio_pallo.pdf
- [4] Markku Halmetoja, Lukion trigonometriaa, <http://solmu.math.helsinki.fi/2012/1/trigonometriaa.pdf>
- [5] Pekka Alestalo, Binomikaava, <http://solmu.math.helsinki.fi/2013/2/binomi.pdf>
- [6] Heikki Pokela, Ehdotus lukion uudeksi opetussuunnitelmaksi, <http://www.luma.fi/artikkelit/1009/ehdotus-uudeksi-opetussuunnitelmaksi>



$P = NP$ -ongelma – mikä se on?

Tuomas Korppi

Johdanto

Tässä kirjoitelmassa esittelemme erään kuuluisimmista avoimista matemaattisista ongelmista. Kyse on $P = NP$ -kysymyksestä, joka kysyy, voidaanko tiettyjä tietokoneella suoritettavia laskentoja suorittaa nopeasti. Yhtälössä P tarkoittaa nk. polynomisessa ajassa laskettavia ongelmia ja NP nk. polynomisessa ajassa ei-deterministisesti laskettavia ongelmia. Nämä käsitteet määritellään myöhemmin tässä tekstissä. Yhtälö $P = NP$ siis väittää, että nämä kaksi ongelmaluokkaa ovat samat. Onko näin? Sitä kukaan ei tiedä.

Koska kyse on matemaattisesta ongelmasta, ratkaisuksi vaaditaan todistusta jommalle kummalle seuraavista:

- **Todistus sille, että kyseiset luokat ovat samat.** Tämä voitaisiin todistaa mm. tekemällä tiettyjä NP -luokkaan kuuluvia ongelmia nopeasti ratkova tietokoneohjelma.
- **Todistus sille, että luokat ovat eri.** Tämä tarkoittaisi todistusta sille, että on mahdotonta tehdä tiettyjä NP -luokkaan kuuluvia ongelmia nopeasti ratkovaa tietokoneohjelmaa.

Jos joku saa $P = NP$ -kysymyksen ratkaistua, Clay Mathematics Institute on luvannut ratkaisusta miljoonan dollarin palkinnon. Yllättävää kyllä, palkinto

olisi periaatteessa mahdollista saada riittävän hyvällä Miinaharava-pelin analyysillä.

Laskennasta

Tässä kirjoitelmassa tarkoitamme tietokoneohjelmalla ohjelmaa, joka saa aluksi yhden syötteen, joka on äärellinen merkkijono¹, laskee sitä aikansa, ja lopuksi palauttaa joko merkkijonon ”Kyllä” tai merkkijonon ”Ei”. Tavallisessa tietokoneessa on rajallinen määrä muistia, ja tavallisissa yhteyksissä on rajallinen määrä aikaa laskennalle, mutta laskennan teoreettisessa tarkastelussa oletetaan, että nämä suureet ovat riittävän suuria käsitellä olevan laskennan loppuunviemiseksi, olivatpa ne kuinka suuria tahansa, kunhan ne ovat äärellisiä. Samoin ohjelman saama syöte saa olla kuinka pitkä tahansa, kunhan se on äärellinen.

Polynominen aika

Olkoon T tietokoneohjelma edellisessä luvussa kuvailussa mielessä. Merkitään $f(1)$:llä pisintä aikaa, jonka ohjelma käyttää yhden merkin mittaisen syötteen käsittelemään. Yhden merkin mittaisia syötteitä on useita, ja merkitsemme siis $f(1)$:llä maksimia kaikkien yhden

¹Yhteen merkkijonoon voidaan koodata vaikka millä mitalla tietoa, eli ohjelmamme voi saada syötteeksi esimerkiksi useita lukuja vaikkapa puolipisteellä erotettuna.

merkin mittaisten syötteiden vaatimista ajoista. Merkitään $f(2)$:lla pisintä aikaa, jonka ohjelma käyttää kahden merkin mittaisen syötteen käsittelyyn ja niin edelleen. Näin saamme funktion $f: \mathbb{N} \rightarrow \mathbb{N}$ (voidaan olettaa, että laskenta-ajat ovat kokonaislukuja, ja voidaan asettaa $f(0) = 0$).

Tyypillisesti $\lim_{n \rightarrow \infty} f(n) = \infty$, ja meitä kiinnostava kysymys on:

Kuinka nopeasti f lähenee ääretöntä?

Sanomme, että ohjelman T vaatima aika on *polynominen*, jos on olemassa (kokonaiskertoiminen) polynomi Q , jolle $f(n) \leq Q(n)$ kaikilla n . Tässä sillä, mikä on ykköistä edustava ajanjakso f :n määritelmässä ei ole merkitystä. Samat ohjelmat ovat polynomisia, valittiinpa tuo ajanjakso lyhyeksi tai pitkäksi.

Jos ohjelman T vaatima aika on polynominen, ohjelmaa T pidetään yleensä nopeana. Tämä johtuu siitä, että n :n kasvaessa minkä tahansa polynomin $Q(n)$ arvo kasvaa kohti ääretöntä suhteellisen hitaasti. Polynomisen ohjelma onkin oikeasti nopea, jos polynomin Q aste on pieni. Jos polynomin Q aste on suuri, voi ohjelma olla käytännössä liian hidas, vaikka se olisikin polynomisen.

Jos ohjelman T vaatima aika ei ole polynominen, se on niin hidas, että laskenta yhtään pidemmällä syötteillä on käytännössä toivotonta. Eksponenttifunktio $f(n) = 2^n$ kasvaa nopeammin kuin mikään polynomi. Voidaan siis todistaa, että jos Q on polynomi, on olemassa sellainen $n_0 \in \mathbb{N}$, että kaikilla $n > n_0$ pätee $f(n) > Q(n)$. Ei-polynomisten tietokoneohjelmien aikavaatimukset ovatkin melko usein joitakin eksponenttifunktion johdannaisia.

Esimerkki 1. *Olkoon T ohjelma, joka saa syötteenään listan lukuja sekä luvun k , ja joka tutkii käymällä listan läpi, onko luku k listassa. Tällaiselle ohjelmalle parhaan polynomin Q aste on yksi, eli T on polynomisen ja nopea.*

Esimerkki 2. *Tässä esimerkissä puhutaan alkulukutesteistä, eli ohjelmista, jotka saavat syötteenään kymmenjärjestelmässä esitetyn luvun ja palauttavat tiedon siitä, onko kyseessä alkuluku. Huomautamme, että kun puhumme siitä, onko joku alkulukutesti polynomisen, emme tarkoita, että onko ohjelman suoritus aika korkeintaan joku syötteenä saadun luvun polynomi, vaan sitä, onko ohjelman suoritus aika korkeintaan joku syötteenä saadun luvun kymmenjärjestelmäsesityksen pituuden polynomi. Esimerkiksi luvun 1000000 kymmenjärjestelmäsesityksessä on seitsemän merkkiä, mikä on huomattavasti vähemmän kuin miljoona.*

Jos käymme läpi kaikki kaikki luonnolliset luvut, jotka ovat korkeintaan syötteenä annetun luvun neliöjuuri, ja testaamme jokaisen kohdalla, onko kyseessä syötteen

tekijä, saamme aikaan alkulukutestin, mutta sen vaatima laskenta-aika on niin pitkä, että testimme ei ole polynomisen. Jos n on syötteenä saadun luvun kymmenjärjestelmäsesityksen pituus, syötteenä saadun luvun neliöjuurta pienempiä lukuja on yli $10^{n/2-2} = \frac{1}{100}\sqrt{10}^n$, mikä on suurempi kuin 2^n , kun n on riittävän suuri.

Paras tunnettu varmasti toimiva alkulukutesti on polynomisen, mutta paras sille tunnettu polynomi Q on astetta seitsemän. Näin suuri aste tarkoittaa sitä, että käytännössä tätä ohjelmaa ei käytetä alkulukujen testaamiseen, vaan alkulukutesteinä käytetään nopeampia ohjelmia, jotka toimivat vain tietyllä todennäköisyydellä, joka tosin saadaan huomattavan korkeaksi.

Päätösongelmat

Olkoon M (jossain äärellisessä aakkostossa esitettyjen) äärellisten merkkijonojen joukko, ja M', M'' joukon M jako kahteen osaan eli *päätösongelma*. Olkoon $m \in M$. Meitä kiinnostaa, kumpaan osaan, M' vai M'' , m kuuluu. Olkoon T tietokoneohjelma, joka ratkaisee tämän, eli T on ohjelma, joka saa syötteenään m :n, ja T kertoo, kumpaan osaan, M' vai M'' , syöte m kuuluu. Oletamme siis, että T toimii näin kaikkien M :n alkuioiden kohdalla. Tällaisessa tapauksessa sanomme, että T ratkaisee päätösongelman M', M'' .

Jos jollekin päätösongelmalle M', M'' on mahdollista kirjoittaa sen ratkaiseva tietokoneohjelma, joka toimii polynomisessa ajassa, sanomme, että M', M'' on polynomisen. Polynomisten päätösongelmien luokkaa merkitään kirjaimella P .

Kauppamatkustajan ongelma

Tutkitaan seuraavaa päätösongelmaa: On annettu joukko kaupunkia sekä hinnat kaikkien kahden kaupungin välisille matkoille. On lisäksi annettu maksimihinta h . Kauppamatkustajan ongelma kuuluu: Voiko tehdä kiertomatka, joka alkaa jostain kaupungista ja päättyy samaan kaupunkiin niin, että jokaisessa kaupungissa käydään kerran ja kierroksen yhteishinta on korkeintaan h ?

Jos haluamme saada tämän päätösongelman edellisessä kappaleessa esitettyyn formalismiin, M' siis kuvaa niitä systeemejä s (jossain merkkijonokoodauksessa esitettyinä; tässä siis sisältää tiedot kaupungeista, niiden välisten matkojen hinnoista sekä maksimihinnan h), joille kyseisenlainen kiertomatka on olemassa, ja M'' kuvaa muita systeemejä.

Kukaan ei tiedä, onko tämä päätösongelma polynomisen, eli onko nopein mahdollinen tämän päätösongelman ratkaiseva tietokoneohjelma polynomisen. Lukijalla kävi ehkä mielessä, että ongelma voitaisiin rat-

kaista käymällä kaikki mahdolliset reitit läpi ja katsoamalla jokaisen reitin kohdalla, onko sen hinta korkeintaan h . Syötteen pituuden kasvaessa tällaisen laskennan viemä aika kasvaa kuitenkin nopeammin kuin mikään syötteen pituuden polynomi, eli tämä ei kelpaa polynomiseksi ratkaisuksi. Polynomisessa ajassa tämän ongelman ratkaisevan tietokoneohjelman pitäisi siis olla huomattavasti ovelammin laadittu.

Kuitenkin seuraavanlainen polynominen tietokoneohjelma T on olemassa: Olkoon s kuten edellä ja k kiertomatka systeemissä s . T saa syötteenään parin s, k ja ratkaisee, onko k sellainen kierros, että sen hinta on korkeintaan h .

Ei-deterministinen polynominen aika

Olkoon M', M'' päätösongelma. Oletetaan, että jokaiselle $m \in M'$ on olemassa toinen merkkijono m' , jota kutsutaan m :n *todistajaksi*. Sallimme myös sen, että merkkijonolla voi olla useita todistajia. Lisäksi oletamme, että m :n lyhyimmän todistajan pituus on korkeintaan joku m :n pituuden polynomi. Lisäksi oletamme, että jos $m \in M''$, m :llä ei ole todistajia.

Esimerkiksi Kauppatarkkailijan ongelma on tällainen päätösongelma: Systeemin s todistaja on kiertomatka k , jonka hinta on korkeintaan h .

Sanomme, että M', M'' on ei-deterministinen polynominen päätösongelma, jos on olemassa polynomisessa ajassa toimiva tietokoneohjelma T , joka saa syötteenään parin m, m' ja ratkaisee, onko m' jonon m todistaja. Ei-determinististen polynomisten päätösongelmien luokkaa merkitään NP . Kuten edellisen luvun viimeisessä kappaleessa totesimme, Kauppatarkkailijan ongelma on ei-deterministinen polynominen päätösongelma.

Huomautamme, että jos M', M'' on ei-deterministinen polynominen päätösongelma, on olemassa tietokoneohjelma T , joka ratkaisee tämän päätösongelman, joskin epärealistisen hitaasti. T muodostetaan seuraavasti: Olkoon Q polynomi siten, että jos m on pituutta n oleva syöte, jolla on todistaja, m :llä on korkeintaan pituutta $Q(n)$ oleva todistaja. Nyt kun tietokoneohjelmalle T annetaan syöte m , se käy kaikki korkeintaan pituutta $Q(n)$ olevat merkkijonot läpi ja kokeilee jokaisen kohdalla, onko kyseessä m :n todistaja. Syötteen pituuden kasvaessa tällaisen laskennan viemä aika kasvaa kuitenkin nopeammin kuin mikään syötteen pituuden polynomi, eli tämä ei kelpaa polynomiseksi ratkaisuksi.

Sivuhuomautuksena vielä mainittakoon, että nimitys ei-deterministinen polynominen tulee siitä, että tällaiset ongelmat voidaan ratkaista polynomisessa ajassa kuvitteellisilla tietokoneohjelmilla, jotka toimivat

”ei-deterministisesti” eli osaavat arvata oikein. NP -pätösongelma voidaan ratkaista ei-deterministisesti niin, että ensin arvataan oikein todistaja ja sen jälkeen tarkastetaan polynomisessa ajassa, että arvattiin oikein.

Onko $P = NP$?

Nyt saamme muotoiltua $P = NP$ -kysymyksen. Se siis kysyy, onko luokka P sama kuin luokka NP . Jos T on jonkin päätösongelman M', M'' ratkaiseva polynominen tietokoneohjelma, voidaan ajatella, että jokaisen M' :uun kuuluvan syötteen todistaja on tyhjä merkkijono, joten T toimii myös ei-deterministisessä polynomisessa ajassa. Siis P sisältyy luokkaan NP . Kysymys siis kuuluu: Voidaanko jokainen ei-deterministinen polynominen päätösongelma ratkaista polynomisessa ajassa, siis ohjelmalla, joka saa syötteen vain alkuperäisen syötteen eikä todistajakandidaattia? Kukaan ei tiedä. Yleisesti uskotaan, että nämä kaksi luokkaa ovat eri, mutta kukaan ei osaa todistaa, että kaikkia NP -ongelmia on mahdotonta ratkaista polynomisessa ajassa.

Sen verran kuitenkin tiedetään, että jos Kauppatarkkailijan ongelma saataisiin ratkaistua polynomisessa ajassa, ratkaisusta osattaisiin muokata minkä tahansa NP -pätösongelman polynominen ratkaisu. Tällaisia NP -pätöongelmia, joiden polynominen ratkaisu ratkaisisi $P = NP$ -kysymyksen kertaheitolla on muitakin. Esimerkkinä tällaisesta mainittakoon seuraava:

Esimerkki 3. *Miinaharava-pelin tilanteella tarkoitamme mielivaltaisen kokoista Miinaharava-pelin tilannetta, jossa osa ruuduista on avattu ja osa avaamatta, ja kussakin avatussa ruudussa on numero, joka voi olla myös nolla. Lisäksi tilanteessa on asetettu lippuja osaan niistä ruuduista, joissa on miina. On myös mahdollista, että yhtään lippua ei ole asetettu. Oletamme kuitenkin, että liput on asetettu oikein, eli jokaisessa sellaisessa ruudussa, jossa on lippu, on myös miina.*

Nyt päätösongelmamme on seuraava: On annettu Miinaharava-pelin tilanne. Onko olemassa (muiden kuin liputettujen) miinojen sellaisia sijainteja, että ne sopivat annettuun tilanteeseen?

Lopuksi

NP ei suinkaan ole vaikeimpien mahdollisten päätösongelmien luokka. On olemassa päätöongelmia, jotka ovat ratkaistavissa tietokoneella², mutta jotka ovat niin vaikeita, että ne eivät kuulu edes luokkaan NP . Päätöongelmille on määritetty paljon muitakin luokkia kuin

²Joskin käytännön kannalta epärealistisen hitaasti.

P ja NP , ja $P = NP$ -kysymyksen lisäksi myös paljon muita luokkia koskevia kysymyksiä on vastaamatta. $P = NP$ -kysymys on pelkästään näistä kuuluisin.

On olemassa myös päätösongelmia, joita mikään tietokoneohjelma ei ratkaise. Tällaisiin tutustuimme kirjoitelmassa Korppi [1].

Pähkinöitä

1. Olkoon $f: \mathbb{N} \rightarrow \mathbb{N}$ funktio, jolle on olemassa polynomi Q ja luonnollinen luku n_0 siten, että $f(n) \leq Q(n)$ aina, kun $n \geq n_0$. Osoita, että on olemassa polynomi Q' siten, että $f(n) \leq Q'(n)$ kaikilla $n \in \mathbb{N}$. (Tämä tehtävä osoittaa, että tässä kirjoitelmassa annettu polynomisen aikavaatimuksen määritelmä on yhtäpitävä kirjallisuudesta yleisemmin löytyvän määritelmän kanssa.)

2. Tutkitaan Esimerkissä 3 esitettyä Miinaharavaa koskevaa päätösongelmaa. Osoita, että kyseinen ongelma kuuluu luokkaan NP .
3. Osoita, että jos Esimerkissä 3 esitetty Miinaharavaa koskeva päätösongelma saataisiin ratkaistua polynomisessa ajassa, saataisiin polynomisessa ajassa ratkaistua myös seuraava päätösongelma: On annettu Miinaharava-pelin tilanne ja suljettu ruutu r . Onko varmaa, että ruudussa r ei ole miinaa?

4. Onko $P = NP$?

Viitteet

- [1] Korppi, Tuomas, *Mitä ei voida laskea?*, Solmu 1/2013

Verkko-Solmun oppimateriaalit

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

Kilpailumatematiikan opas (Matti Lehtinen)

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 1: Mekaniikkaa (Markku Halmetoja ja Jorma Merikoski)

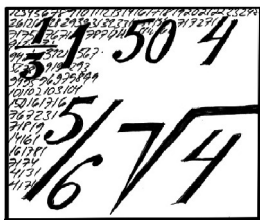
Matemaattista fysiikkaa lukiolaiselle 2: Sähköoppia (Markku Halmetoja ja Jorma Merikoski)

Lukuteorian helmiä lukiolaisille (Jukka Pihko)

Matematiikan peruskäsitteiden historia (Erkki Luoma-aho)

Matematiikan historia (Matti Lehtinen)

Reaalianalyysiä englanniksi (William Trench)



Käänteistä marjanpoimintaa

Jukka Liukkonen

Metropolia Ammattikorkeakoulu

Mistä on kysymys?

Mustikan pinnalla on normaalisti ohut ultraviolettivaloa heijastava vahakerros. Näkyvän valon aallonpituudella kerros aiheuttaa sen, että marja näyttää siniseltä. *Tervamustikaksi* kutsutulta kiiltävänmustalta värimuunnokselta vahakerros puuttuu. Teeret ja punakylkirastaat suosivat sinisiä mustikoita, sillä linut ovat mieltyneitä ultraviolettivaloon. Tervamustikat ovat melko harvalukuisia, mutta joillain alueilla niitä tavataan runsaastikin.

Sammeli on käynyt keräämässä kipollisen mustikoita. Velipoika Miihkali yrittää arvata, mistä Sammeli on mustikkansa hakenut. Ahkujärven rannoilla kasvavista mustikoista $p_A \cdot 100\%$ on tervamustikoita, Bieggajängän laitamien mustikkasadossa tervamustikoiden osuus on $p_B \cdot 100\%$. Muita mustikkapaikkoja lähi- maastossa ei ole. Sammelin keräämässä *otoksessa* tervamustikoiden osuus kaikista mustikoista ei välttämättä ole lähelläkään mainittuja prosenttimääriä, mutta keskittyäksemme Miihkalin käyttämään päättelymenetelmään tarkastelemme pelkistettyä tilannetta, jossa Sammelin marjasaaliin tervamustikkapitoisuus on tasan $p_A \cdot 100\%$ tai tasan $p_B \cdot 100\%$. Edellisessä tapauksessa marjat tulkitaan Ahkujärven ja jälkimmäisessä Bieggajängän sadon osaksi. Sammeli ei anna Miihkalin tutkia kipponsa sisältöä, vaan näyttää hänelle kiposta summamustikassa ottamansa marjan yksi kerrallaan palauttaen mustikan aina takaisin kippoon. Tällaista

kutsutaan *otannaksi takaisinpanolla*. Se jatkuu kunnes laskintaan näpräilevä Miihkali lopulta rohkaistuu ilmoittamaan hyvinkin valistuneen arvauksen mustikoiden alkuperästä. Normaalikäsitteilyssä mustikan vahakerros kuluu helposti pois, mutta nyt oletamme vahan pysyvän. Millainen on Miihkalin menetelmä?

Matemaattinen malli

Todennäköisyyslaskennan kielellä ilmaistuna kyseessä on *toistokoe*, jossa perättäiset toistot ovat toisistaan *riippumattomat*. Mustan (M) ja sinisen (S) värin todennäköisyydet ehdoilla, että marja on poimittu Ahkujärveltä (A) tai vastaavasti Bieggajängältä (B), ovat

$$P(M|A) = \frac{P(M \cap A)}{P(A)} = p_A, \quad P(S|A) = 1 - p_A,$$

$$P(M|B) = p_B, \quad P(S|B) = 1 - p_B.$$

Sulkeaksemme pois mielenkiinnottomat erikoistapaukset oletamme, että $0 < p_A < 1$, $0 < p_B < 1$ ja $p_A \neq p_B$. Olkoon V_n marjojen värien jono siinä vaiheessa, kun Miihkali on nähnyt n mustikkaa, ja $m(n)$ mustan värin esiintymiskertojen lukumäärä jonossa V_n . Jos esimerkiksi kaksi ensimmäistä mustikkaa ovat sinisiä ja kolmas musta, värijono on $V_3 = (S, S, M)$, ja $m(3) = 1$.

Tällaisen jonon esiintymistodennäköisyydet ovat

$$P(V_3|A) = P(S|A)P(S|A)P(M|A) = p_A(1 - p_A)^2,$$

$$P(V_3|B) = P(S|B)P(S|B)P(M|B) = p_B(1 - p_B)^2.$$

Yleisesti

$$P(V_n|A) = p_A^{m(n)}(1 - p_A)^{n-m(n)},$$

$$P(V_n|B) = p_B^{m(n)}(1 - p_B)^{n-m(n)}.$$

Todennäköisyyden kertolaskusäännöstä

$$P(A|V_n)P(V_n) = P(V_n|A)P(A)$$

saadaan Bayesin kaava

$$P(A|V_n) = \frac{P(V_n|A)P(A)}{P(V_n)}.$$

Kokonaistodennäköisyyden kaava

$$P(V_n) = P(V_n|A)P(A) + P(V_n|B)P(B)$$

antaa Bayesin kaavalle muodon

$$P(A|V_n) = \frac{P(V_n|A)P(A)}{P(V_n|A)P(A) + P(V_n|B)P(B)}$$

$$= \frac{1}{1 + \frac{P(V_n|B)P(B)}{P(V_n|A)P(A)}}. \quad (1)$$

Jos näiden todennäköisyyksien jono lähestyisi nollaa otannan edistyessä, olisi varmaankin kyse Bieggajängän mustikoista. Jos jono lähestyisi ykköistä, mustikat luultavasti olisivat Ahkujärveltä peräisin.

Mallin suppeneminen

Suppenemistarkastelut saattavat tuntua hankalilta tottumattomasta lukijasta. Edes jonkinlaiseen täsmällisyyteen pyrkivän esityksen yksityiskohtien ymmärtäminen ei ole oleellista itse asian kannalta. Yritämme selvittää, milloin jonolla $P(A|V_n)$ on raja-arvo, ja mikä se on. Ehdollisten todennäköisyyksien $P(V_n|B)$ ja $P(V_n|A)$ suhde on

$$\frac{P(V_n|B)}{P(V_n|A)} = \frac{p_B^{m(n)}(1 - p_B)^{n-m(n)}}{p_A^{m(n)}(1 - p_A)^{n-m(n)}}$$

$$= \left[\left(\frac{p_B}{p_A} \right)^{\frac{m(n)}{n}} \left(\frac{1 - p_B}{1 - p_A} \right)^{1 - \frac{m(n)}{n}} \right]^n.$$

Lukumäärien $m(n)$ ja n suhde $m(n)/n$ on mustan värin suhteellinen frekvenssi jonossa V_n . Jos marjat ovat Ahkujärven mustikoita, suurten lukujen lain ns. vahvan version nojalla suhteellinen frekvenssi lähestyy raja-arvoon todennäköisyyttä p_A siinä mielessä, että

$$P\left(\frac{m(n)}{n} \rightarrow p_A\right) = 1.$$

Tällöin sanotaan, että $m(n)/n$ *konvergoi melkein varmasti* (engl. *almost surely*) kohti lukua p_A , ja merkitään

$$\frac{m(n)}{n} \xrightarrow{\text{a.s.}} p_A.$$

On periaatteessa mahdollista, että kiposta sattumalta tulee poimituksi esim. koko ajan vain sinisiä marjoja, jolloin $m(n)/n = 0 \rightarrow 0 \neq p_A$, mutta tämänkaltaisen tilanne on äärimmäisen harvinainen, sen todennäköisyys on 0. Seuraavassa tarkastelemme vain niitä värijonoja, joille $m(n)/n \rightarrow p_A$ tavanomaisessa mielessä, kun $n \rightarrow \infty$. Sellaisille jonoille johtamamme tulokset pätevät todennäköisyydellä 1 kaikkien värijonon joukossa. Edellä oletimme marjojen sisältyvän Ahkujärven satoon. Bieggajängän mustikoiden tapauksessa tarkastelemme vastaavasti vain niitä värijonoja, joilla $m(n)/n \rightarrow p_B$. Voimme siis kirjoittaa

$$\lim_{n \rightarrow \infty} \left[\frac{P(V_n|B)}{P(V_n|A)} \right]^{\frac{1}{n}}$$

$$= \begin{cases} \left(\frac{p_B}{p_A} \right)^{p_A} \left(\frac{1 - p_B}{1 - p_A} \right)^{1 - p_A} & \text{tapauksessa } A, \\ \left(\frac{p_B}{p_A} \right)^{p_B} \left(\frac{1 - p_B}{1 - p_A} \right)^{1 - p_B} & \text{tapauksessa } B. \end{cases} \quad (2)$$

Suhteen $P(V_n|B)/P(V_n|A)$ raja-arvon määrittämiseksi tarvitsemme pari aputulosta eli lemmaa:

Lemma 1. Olkoon $0 < x < 1$, $0 < y < 1$ ja $x \neq y$. Tällöin

$$(a) \left(\frac{x}{y} \right)^y \left(\frac{1 - x}{1 - y} \right)^{1 - y} < 1,$$

$$(b) \left(\frac{x}{y} \right)^x \left(\frac{1 - x}{1 - y} \right)^{1 - x} > 1.$$

Todistus: Jälkimmäinen väite (b) seuraa edellisestä käänteislukuihin siirtymällä, joten riittää todistaa (a). Se on yhtäpitävä epäyhtälön

$$f(x) = x^y(1 - x)^{1 - y} < y^y(1 - y)^{1 - y} \quad (3)$$

kanssa. Tässä $f(y) = y^y(1 - y)^{1 - y}$. Funktion f derivaatta muuttujan x suhteen on

$$f'(x) = yx^{y-1}(1 - x)^{1 - y} + x^y(1 - y)(1 - x)^{-y} \cdot (-1)$$

$$= \left(\frac{1 - x}{x} \right) \left(\frac{1 - x}{x} \right)^{-y} y + \left(\frac{1 - x}{x} \right)^{-y} (y - 1)$$

$$= \left[\left(\frac{1 - x}{x} + 1 \right) y - 1 \right] \left(\frac{1 - x}{x} \right)^{-y}$$

$$= \left[\frac{y}{x} - 1 \right] \left(\frac{1 - x}{x} \right)^{-y}.$$

Tässä tulossa jälkimmäinen tekijä on positiivinen, joten ensimmäinen tekijä määrää tulon etumerkin. Täten $f'(x) > 0$ eli f on aidosti kasvava, kun $0 < x < y$.

Vastaavasti $f'(x) < 0$ eli f on aidosti vähenevä, kun $y < x < 1$. $\square$

Lemman perusteella siis

$$\left(\frac{p_B}{p_A}\right)^{p_A} \left(\frac{1-p_B}{1-p_A}\right)^{1-p_A} < 1,$$

ja

$$\left(\frac{p_B}{p_A}\right)^{p_B} \left(\frac{1-p_B}{1-p_A}\right)^{1-p_B} > 1.$$

Lemma 2. Olkoon $\lim_{n \rightarrow \infty} a_n = a$, missä $0 < a \neq 1$. Tällöin

$$\lim_{n \rightarrow \infty} a_n^n = \begin{cases} 0, & 0 < a < 1, \\ \infty, & a > 1. \end{cases}$$

Todistus: Perustamme todistuksen lukujonon raja-arvon määritelmään. Olkoon $\lambda = (a+1)/2$ lukujen a ja 1 keskiarvo. Tapauksessa $0 < a < 1$ on olemassa sellainen positiivinen kokonaisluku n_1 , että $0 < a_n < \lambda < 1$ aina, kun $n > n_1$. Indeksien arvoilla $n > n_1$ pätee $0 < a_n^n < \lambda^n \rightarrow 0$.

Tapauksessa $a > 1$ on olemassa sellainen positiivinen kokonaisluku n_2 , että $a_n > \lambda > 1$ aina, kun $n > n_2$. Indeksien arvoilla $n > n_2$ pätee $a_n^n > \lambda^n \rightarrow \infty$. $\square$

Soveltamalla lemmaa raja-arvoyhtälöön (2) saamme yhtälön

$$\lim_{n \rightarrow \infty} \frac{P(V_n|B)}{P(V_n|A)} = \begin{cases} 0 & \text{tapauksessa } A, \\ \infty & \text{tapauksessa } B. \end{cases}$$

Lopuksi otamme taas kaikki värijonot mukaan, jolloin tavallisen suppenemisen tilalle astuu melkein varma suppeneminen. Kaavan (1) perusteella

$$P(A|V_n) = \frac{1}{1 + \frac{P(V_n|B)P(B)}{P(V_n|A)P(A)}} \xrightarrow{\text{a.s.}} \begin{cases} 1 & \text{tapauksessa } A, \\ 0 & \text{tapauksessa } B. \end{cases} \quad (4)$$

Laskentakaava

Tarkoituksenamme on johtaa käytännöllinen *iteraatioon* eli toistoon perustuva kaava todennäköisyyksien $P(A|V_n)$ laskemiseksi. Olkoon F_n jonon V_n viimeinen alkio. Kun F_n poistetaan jonosta V_n , jäljelle jää jono

V_{n-1} . Kaavasta (1) saadaan Bayesin kaavan avulla

$$\begin{aligned} P(A|V_n) &= \frac{P(V_n|A)P(A)}{P(V_n|A)P(A) + P(V_n|B)P(B)} \\ &= \frac{P(F_n|A)P(V_{n-1}|A)P(A)}{P(F_n|A)P(V_{n-1}|A)P(A) + P(F_n|B)P(V_{n-1}|B)P(B)} \\ &= \frac{P(F_n|A) \frac{P(V_{n-1}|A)P(A)}{P(V_{n-1})}}{P(F_n|A) \frac{P(V_{n-1}|A)P(A)}{P(V_{n-1})} + P(F_n|B) \frac{P(V_{n-1}|B)P(B)}{P(V_{n-1})}} \\ &= \frac{P(F_n|A)P(A|V_{n-1})}{P(F_n|A)P(A|V_{n-1}) + P(F_n|B)P(B|V_{n-1})}. \end{aligned}$$

Symmetriasuhteista vastaavat yhtälöt pätevät myös vaihtamalla A ja B keskenään:

$$\begin{aligned} P(A|V_n) &= \frac{P(F_n|A)P(A|V_{n-1})}{P(F_n|A)P(A|V_{n-1}) + P(F_n|B)P(B|V_{n-1})}, \\ P(B|V_n) &= \frac{P(F_n|B)P(B|V_{n-1})}{P(F_n|A)P(A|V_{n-1}) + P(F_n|B)P(B|V_{n-1})}. \end{aligned}$$

Merkitsemme $P_0(A) = P(A)$, $P_0(B) = P(B)$, $P_n(A) = P(A|V_n)$ ja $P_n(B) = P(B|V_n)$, kun $n > 0$. Näillä merkinnöillä todennäköisyyksille saadaan helppokäyttöinen iteratiivinen laskentakaava

$$\begin{cases} P_0(A) = P(A) \\ P_0(B) = P(B) \\ \begin{cases} P_n(A) = \frac{P(F_n|A)P_{n-1}(A)}{P(F_n|A)P_{n-1}(A) + P(F_n|B)P_{n-1}(B)} \\ P_n(B) = \frac{P(F_n|B)P_{n-1}(B)}{P(F_n|A)P_{n-1}(A) + P(F_n|B)P_{n-1}(B)} \end{cases} \end{cases} \quad (5)$$

Alin yhtälö on mukana vain symmetrian havainnollistamisen takia. Laskennassa se kannattaa korvata yhtälöllä $P_n(B) = 1 - P_n(A)$. Jos jompikumpi todennäköisyyksistä $P_n(A)$ ja $P_n(B)$ on tasan 1, jolloin toinen on tasan 0, iteroinnin jatkaminen ei enää muuta todennäköisyyksiä. Verrattuna laskentakaavaan (1) iteraatio (5) on kätevä siinä mielessä, että koko havaintojonoa V_n ei tarvitse säilyttää muistissa, vaan ainoastaan jompikumpi edellisistä todennäköisyyksistä $P_{n-1}(A)$ ja $P_{n-1}(B)$. Toinen riittää, sillä $P_{n-1}(A) + P_{n-1}(B) = 1$. Tietysti $P(M|A)$, $P(M|B)$, $P(S|A)$ ja $P(S|B)$ tarvitaan myös, mutta ne säilyvät samoina koko laskennan ajan. Kun vaiheen $n-1$ jälkeen tulee uusi havainto (so. katsotaan seuraavan mustikan väri F_n), vaiheen $n-1$ *posterioritodennäköisyydet* $P_{n-1}(A)$ ja $P_{n-1}(B)$ otetaan vaiheen n *prioritodennäköisyyksiksi*, ja lasketaan uudet *posterioritodennäköisyydet* $P_n(A)$ ja $P_n(B)$. Kertoimia $P(F_n|A)$ ja $P(F_n|B)$ kutsutaan nimellä *uskottavuus* (engl. *likelihood*), ja nimittäjä $P(F_n|A)P_{n-1}(A) + P(F_n|B)P_{n-1}(B)$ on *normeerausvakio*. Viimeksi mainitun ainoana tehtävänä on varmistaa, että $P_n(A) + P_n(B) = 1$.

Esimerkki 4. Tervamustikoiden osuudet kaikista mustikoista ovat tavallisesti sen verran pieniä, että havainnollista esimerkkiä ajatellen musta mustikka toistuu aivan liian harvoin. Sen takia tässä simulaatiossa liioitellaan: Ahkujärven marjoista 60 % ja Bieggajängän marjoista 30 % oletetaan tervamustikoiksi. Sammeli keräsi marjat Ahkujärveltä, mutta Miihkali ei sitä etukäteen tiedä.

n	F_n	$P_n(A)$	$P_n(B)$	Kommentti
0		0.45	0.55	Arvattu priorijakauma
1	S	0.3185841	0.6814159	Sininen tukee Bieggajängää
2	S	0.2108346	0.7891654	
3	M	0.3482467	0.6517533	Musta tukee Ahkujärveä
4	M	0.5165919	0.4834081	
5	M	0.6812537	0.3187463	
6	M	0.8104115	0.1895885	
7	M	0.8952788	0.1047212	
8	M	0.9447463	0.0552537	
9	S	0.9071536	0.0928464	Sininen tukee Bieggajängää
10	M	0.9513168	0.0486832	Musta tukee Ahkujärveä
11	S	0.9178054	0.0821946	Sininen tukee Bieggajängää
12	S	0.8645118	0.1354882	
13	S	0.7847669	0.2152331	
14	S	0.6756932	0.3243068	
15	M	0.8064641	0.1935359	Musta tukee Ahkujärveä
16	M	0.8928648	0.1071352	
17	S	0.8264577	0.1735423	Sininen tukee Bieggajängää
18	S	0.7312771	0.2687229	
19	M	0.8447834	0.1552166	Musta tukee Ahkujärveä
20	M	0.9158619	0.0841381	

Aika hyvin asettuivat todennäköisyydet oikean vaihtoehdon eli Ahkujärven kannalle jo 20 ensimmäisellä iteraatiokierroksella. Ise asiassa paras tulos saatiin jo kierroksella 8, mutta sen jälkeen tuli sattumalta paljon sinisiä mustikoita, jotka houkuttelivat todennäköisyyttä Bieggajängän suuntaan. Suurten lukujen laki alkaa kuitenkin "vääjäämättä" (so. todennäköisyydellä 1) toimia jossain vaiheessa. Kierroksen 20 jälkeen Miihkali tietää yli 90 %:n varmuudella, että kyse on Ahkujärven mustikoista – vai tietääkö sittenkään? Viimeiseltä riviltä

nähdään todennäköisyys sille, että marjat on poimitu Ahkujärveltä ehdolla, että Sammelin suorittamassa "jälkipoiminnassa" on saatu värisarakkeen mukainen mustikkajono. Todennäköisyydet ovat päteviä vain, mikäli ensimmäisen rivin priorijakauma on todellisen tilanteen mukainen. Priorijakauma tarkoittaa, että 45 % Sammelin poimintaretkistä suuntautuu Ahkujärvelle ja loput 55 % Bieggajängälle. Vaikka priorijakauma olisi arvattu täysin pieleen, iteraation jossain vaiheessa alkaa selvästi näkyä, kummasta paikasta marjat ovat peräisin. Väärästä priorijakaumasta lähteneen iteraation antamat ehdolliset välitodennäköisyydet ovat enemmän tai vähemmän roskaa, mutta tavoitteenahan onkin lopputulos, siis kumman vaihtoehdon kohdalle todennäköisyys lopulta kasaantuu.

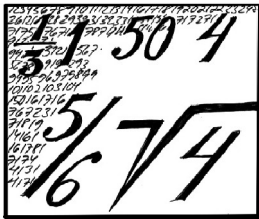
Yleistykset

Edellä esitetty oli kenties yksinkertaisin mahdollinen esimerkki tilastollisesta inversiosta. Se yleistyy ilmeisellä tavalla tilanteisiin, joissa mustikkapaikkoja on K kpl, siis esim. $A_1, \dots, A_K$. Nyt kahden todennäköisyyden $P_n(A)$ ja $P_n(B)$ muodostaman jakauman paikalla on todennäköisyyksistä $P_n(A_1), \dots, P_n(A_K)$ muodostuva jakauma. Malliin on myös helppoa ottaa useampi väri. Iteraatio (5) ei muutu paljon:

$$\begin{cases} P_0(A_1) = P(A_1) \\ \vdots \\ P_0(A_K) = P(A_K) \end{cases}$$

$$\begin{cases} P_n(A_1) = \frac{P(F_n|A_1)P_{n-1}(A_1)}{\sum_{k=1}^K P(F_n|A_k)P_{n-1}(A_k)} \\ \vdots \\ P_n(A_K) = \frac{P(F_n|A_K)P_{n-1}(A_K)}{\sum_{k=1}^K P(F_n|A_k)P_{n-1}(A_k)} \end{cases}$$

Värien lisääntyminen merkitsee vain muuttujan F_n mahdollisten arvojen lisääntymistä. Tällöin pitää tietää myös näiden arvojen todennäköisyydet jokaisen marjapaikan A_k kohdalla. Kun marjastusesimerkistä irrottaudutaan ja etäännyttään, saadaan yleistykset kaikenulotteisille diskreeteille ja jatkuville jakaumille. Nämä yleistykset toimivat yötäpäivää lukemattomien arkikäytössä olevien laitteiden prosessoreissa, mutta näistä asioista kertomisen jätän viisaammille.



Kompleksiluvut ja kolmannen asteen yhtälön ratkaisut

Lauri Ajanki

Helsingin yliopisto

Johdanto

Reaalilukua α voidaan graafisesti ajatella x -akselin eli *reaaliakselin* pisteenä $(\alpha, 0)$. Näin saamme samaistuksen reaalilukujen ja reaaliakselin välille. Kompleksiluvut määritellään tason yleisinä pisteinä (a, b) . Kompleksiluvuille määritellään yhteen- ja kertolasku kaavoilla

$$\begin{aligned}(a, b) + (c, d) &= (a + c, b + d) \\ (a, b)(c, d) &= (ac - bd, ad + bc).\end{aligned}$$

Näin määriteltynä kompleksiluvut muodostavat luonnollisen laajennoksen reaaliluvuille. Esimerkiksi jokainen reaaliluku x on samaistuksen $x = (x, 0)$ kautta myös kompleksiluku. Reaaliluvulla 1 kertominen ei muuta kompleksilukua (a, b) , sillä määritelmän nojalla $(1, 0)(a, b) = (1 \cdot a - 0 \cdot b, 1 \cdot b + 0 \cdot a) = (a, b)$. Huomaa myös, että molemmat laskutoimitukset ovat vaihdannaisia eli ne toteuttavat ehdot

$$\begin{aligned}(a, b) + (c, d) &= (c, d) + (a, b) \\ (a, b)(c, d) &= (c, d)(a, b).\end{aligned}$$

Luvulla $(0, 1)$ on ominaisuus $(0, 1)(0, 1) = (-1, 0) = -1$. Tätä lukua sanotaan *imaginaariyksiköksi* ja merkitään lyhyemmin merkinnällä i . Lyhyemmin merkittynä saamme siis tuloksen $i^2 = -1$. Imaginaariyksikön avulla jokainen kompleksiluku voidaan esittää muodossa

$$(a, b) = (a, 0) + (0, b) = (a, 0) + (0, 1)(b, 0) = a + ib,$$

joka on usein kätevämpi esitysmuoto. Tarkemmin kompleksilukuja on Solmussa käsitellyt Matti Lehtinen, katso [3].

Kompleksiluvuilla on paljon reaaliluvuista poikkeavia ominaisuuksia: edellä jo havaittiin, että yhtälöllä $x^2 + 1 = 0$ on kompleksinen ratkaisu $x = i$. Voidaankin osoittaa, että polynomiyhtälöillä on aina kompleksiratkaisuja: *algebran peruslauseen* mukaan jokaisella n -asteisella polynomiyhtälöllä on tasan n kappaletta kompleksiratkaisuja kun ne lasketaan kertalukuineen, ks. [2]. Mikä on yhtälön $x^2 + 1 = 0$ toinen ratkaisu? Tarkastellaan tässä erästä lähtökohdiltaan reaalista ilmiötä, jonka tutkimiseen tarvitsemme kompleksilukuja.

Kuutiojuuria ja de Moivre'n kaava

1500-luvun matematiikan historian suuria kehitysvaiheita oli kolmannen ja neljännen asteen yhtälöiden ratkaisukaavojen löytyminen. Italialainen Gerolamo Cardano julkaisi vuonna 1545 nimeään kantavan ratkaisukaavan muotoa $x^3 = mx + n$ oleville yhtälöille. Kaavan mukaan

$$x = \sqrt[3]{\frac{n}{2} + \sqrt{\frac{n^2}{4} - \frac{m^3}{27}}} + \sqrt[3]{\frac{n}{2} - \sqrt{\frac{n^2}{4} - \frac{m^3}{27}}}.$$

Kaavan alkuperäisestä keksijästä käytiin aikanaan kiihkas julkinen sananvaihto useamman matemaatikon välillä. Suositeltavana taustalukemisenä kolmannen ja neljännen asteen yhtälöiden ratkaisukaavojen löytymisestä sekä alkuperäiseen keksijään liittyvästä kiistasta

mainittakoon Mario Livion suomennettu teos Yhtälö, jota ei voinut ratkaista [4].

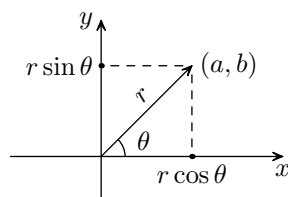
Ratkaisukaava ei kuitenkaan ole aivan niin yksinkertainen kuin päällisin puolin näyttää ja sen oikeellisuus herättikin aikanaan ihmetystä. Viitteitä tästä antaa yhtälö $x^3 = 6x + 4$. Kyseinen yhtälö voidaan toki ratkaista ilman kaavaakin: kokeilemalla havaitaan, että vakio-termin tekijöistä $x = -2$ on eräs ratkaisu. Muut ratkaisut löydetäisiin tekijöihinjaolla. Tässä kirjoituksessa on kuitenkin tarkoitus tutkia, miten ratkaisukaava käyttäytyy mainitun yhtälön tapauksessa. Lähteenä on käytetty vastaavaa esitystä teoksessa [1].

Koska funktio $f(x) = x^3 - 6x - 4$ on jatkuva ja vaihtaa merkkiään väleillä $[-3, -\frac{3}{2}]$, $[-1, 0]$ sekä $[1, 3]$, on näillä väleillä oltava nollakohdat. Monotonisuuden nojalla kullakin välillä on tasan yksi nollakohta. Suora sijoitus kaavaan antaa

$$\begin{aligned} x &= \sqrt[3]{\frac{4}{2} + \sqrt{\frac{16}{4} - \frac{216}{27}}} + \sqrt[3]{\frac{4}{2} - \sqrt{\frac{16}{4} - \frac{216}{27}}} \\ &= \sqrt[3]{2 + \sqrt{-4}} + \sqrt[3]{2 - \sqrt{-4}} \\ &= \sqrt[3]{2 + 2i} + \sqrt[3]{2 - 2i}. \end{aligned} \quad (1)$$

Päädymme siis kahden kompleksisen kuutiojuuren summaan. Ratkaisuja tiedetään kuitenkin olevan kolme kappaletta ja niiden kaikkien pitäisi olla reaalisia – jotain näyttäisi olevan pielessä. Cardanon kaava on kuitenkin oikein, kaavassa (1) itse asiassa esiintyy kolme reaalilukua. Tämän näkemiseksi tarvitsemme hieman trigonometriaa.

Kun ajattelemme kompleksilukua tason pisteenä (a, b) , saadaan sen etäisyys origosta Pythagoraan mukaan kaavalla $r = \sqrt{a^2 + b^2}$. Origosta poikkeavan kompleksiluvun *vaihekulma* on kulma, joka jää positiivisen x -akselin sekä origon ja pisteen (a, b) määräämän janan väliin. Origolle ei määritellä vaihekulmaa. Vaihekulma on kätevin määrittää kuvan avulla: esimerkiksi ensimmäisessä neljänneksessä sijaitsevan pisteen vaihekulma θ toteuttaa ehdon $\tan \theta = \frac{b}{a}$.



Vaihekulma ei ole yksikäsitteinen: jos θ on eräs pisteen (a, b) vaihekulma, myös $\theta + 2\pi n$ kelpaa vaihekulmaksi millä tahansa kokonaisluvulla n . Usein vaihekulma rajoitetaan jollekin 2π -mittaiselle puoliavovälille. Nyt suorakulmaisille koordinaateille a ja b saadaan esitysmuodot $a = r \cos \theta$, $b = r \sin \theta$ ja kompleksiluku

voidaan esittää muodossa $z = a + ib = r(\cos \theta + i \sin \theta)$. Tätä esitystä kutsutaan napakoordinaattiesitykseksi.

Napakoordinaattien perustuloksia on *de Moivre'n kaava*, jonka mukaan kokonaisluvulla n pätee

$$(\cos \theta + i \sin \theta)^n = \cos n\theta + i \sin n\theta.$$

Kaavan todistus tapahtuu induktiolla. Palataan nyt selvittämään, mitä ovat kuutiojuuret kaavassa (1). Käsitellään ensin juurta $\sqrt[3]{2 + 2i}$. Kuutiojuuren määrittelyn nojalla $\sqrt[3]{z}$ tarkoittaa sitä lukua w , joka toteuttaa ehdon $w^3 = z$. Tehtävänä on siis määrittää luku, jonka kolmas potenssi on $2 + 2i$. Tämä onnistuu de Moivre'n kaavan avulla. Luvun $2 + 2i$ napakoordinaattiesitykseksi saadaan $\sqrt{8}(\cos \frac{\pi}{4} + i \sin \frac{\pi}{4})$. Merkitään $w = r(\cos \theta + i \sin \theta)$ ja muodostetaan yhtälö

$$\begin{aligned} (r(\cos \theta + i \sin \theta))^3 &= \sqrt{8}(\cos \frac{\pi}{4} + i \sin \frac{\pi}{4}) \\ \Leftrightarrow r^3(\cos 3\theta + i \sin 3\theta) &= \sqrt{8}(\cos \frac{\pi}{4} + i \sin \frac{\pi}{4}). \end{aligned}$$

Vertaamalla yhtälön molempia puolia havaitaan, että täytyy olla

$$\begin{aligned} r^3 &= \sqrt{8} \text{ ja } 3\theta = \frac{\pi}{4} + 2\pi n, \\ \Leftrightarrow r &= \sqrt[3]{\sqrt{8}} \text{ ja } 3\theta = \frac{\pi}{4} + 2\pi n, \\ \Leftrightarrow r &= \sqrt{2} \text{ ja } \theta = \frac{\pi}{12} + \frac{2\pi n}{3} = \frac{\pi(1 + 8n)}{12}, \quad n \in \mathbb{Z}. \end{aligned}$$

Ratkaisuja on siis useita. Havaitaan kuitenkin, että arvolla $n = 3$ saadaan $\theta = \frac{25\pi}{12} = \frac{\pi}{12} + 2\pi$, josta sini ja kosini ovat samat kuin kulmasta $\theta = \frac{\pi}{12}$. Siis arvosta $n = 3$ alkaen saadut ratkaisut alkavat ”kiertämään kehää”. On siis kolme eri lukua, joiden kuutio on $2 + 2i$ – napakoordinaateissa ne ovat $\sqrt{2}(\cos \frac{\pi}{12} + i \sin \frac{\pi}{12})$, $\sqrt{2}(\cos \frac{3\pi}{4} + i \sin \frac{3\pi}{4})$ sekä $\sqrt{2}(\cos \frac{17\pi}{12} + i \sin \frac{17\pi}{12})$.

Vastaavasti luku $2 - 2i$ on napakoordinaateissa $\sqrt{8}(\cos(-\frac{\pi}{4}) + i \sin(-\frac{\pi}{4})) = \sqrt{8}(\cos \frac{\pi}{4} - i \sin \frac{\pi}{4})$, joten de Moivre'n kaava antaa

$$\begin{aligned} (r(\cos \theta + i \sin \theta))^3 &= \sqrt{8}(\cos \frac{\pi}{4} - i \sin \frac{\pi}{4}) \\ \Leftrightarrow r^3(\cos 3\theta + i \sin 3\theta) &= \sqrt{8}(\cos \frac{\pi}{4} - i \sin \frac{\pi}{4}) \\ \Leftrightarrow r &= \sqrt{2} \text{ ja } 3\theta = \frac{\pi}{4} + 2\pi n \\ \Leftrightarrow r &= \sqrt{2} \text{ ja } \theta = \frac{\pi(1 + 8n)}{12}, \quad n = 0, 1, 2. \end{aligned}$$

Eli juuren $\sqrt[3]{2 - 2i}$ arvot ovat $\sqrt{2}(\cos \frac{\pi}{12} - i \sin \frac{\pi}{12})$, $\sqrt{2}(\cos \frac{3\pi}{4} - i \sin \frac{3\pi}{4})$ sekä $\sqrt{2}(\cos \frac{17\pi}{12} - i \sin \frac{17\pi}{12})$.

Sijoitetaan saadut luvut kaavaan (1). Jos lukua n vastaa ratkaisu z_n , niin saadaan

$$\begin{aligned} z_0 &= \sqrt{2} \left(\cos \frac{\pi}{12} + i \sin \frac{\pi}{12} \right) + \sqrt{2} \left(\cos \frac{\pi}{12} - i \sin \frac{\pi}{12} \right) \\ &= 2\sqrt{2} \cos \frac{\pi}{12} = 2\sqrt{2} \cdot \frac{1}{4}(\sqrt{6} + \sqrt{2}) \\ &= \frac{1}{2}(2\sqrt{3} + 2) = 1 + \sqrt{3} \end{aligned}$$

$$\begin{aligned} z_1 &= \sqrt{2} \left(\cos \frac{3\pi}{4} + i \sin \frac{3\pi}{4} \right) + \sqrt{2} \left(\cos \frac{3\pi}{4} - i \sin \frac{3\pi}{4} \right) \\ &= 2\sqrt{2} \cos \frac{3\pi}{4} = 2\sqrt{2} \left(-\frac{1}{\sqrt{2}} \right) = -2 \end{aligned}$$

$$\begin{aligned} z_2 &= \sqrt{2} \left(\cos \frac{17\pi}{12} + i \sin \frac{17\pi}{12} \right) \\ &\quad + \sqrt{2} \left(\cos \frac{17\pi}{12} - i \sin \frac{17\pi}{12} \right) \\ &= 2\sqrt{2} \cos \frac{17\pi}{12} = 2\sqrt{2} \left(-\frac{1}{4}(\sqrt{6} - \sqrt{2}) \right) \\ &= -\frac{1}{2}(2\sqrt{3} - 2) = -(\sqrt{3} - 1) = 1 - \sqrt{3} \end{aligned}$$

eli kolme reaalilukua. Sijoittamalla saadut luvut takaisin yhtälöön $x^3 = 6x + 4$ nähdään, että ne todella ovat yhtälön ratkaisut.

Kirjoittaja opiskelee matematiikan opettajaksi.

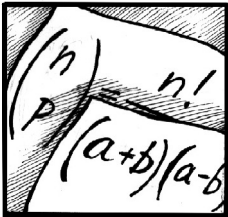
Viitteet

- [1] William Dunham: Euler – The Master of Us All, The Mathematical Association of America, 1999.
- [2] Tuomas Hytönen: Algebran peruslause lukiolaisille, Solmu 3/2011.
- [3] Matti Lehtinen: Kaikki tarpeellinen kompleksiluvuista, Solmu 1/2006.
- [4] Mario Livio: Yhtälö, jota ei voinut ratkaista – Mitä matematiikka paljasti symmetrian kielen, Terra Cognita, 2005.

Diplomitehtävien oheislukemistoa

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

Lukujärjestelmistä
 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



Binomikaava

Pekka Alestalo

Matematiikan ja systeemianalyysin laitos
Aalto-yliopiston perustieteiden korkeakoulu

Tässä kirjoituksessa vertaillaan kahta tapaa lähestyä binomikaavaa (2). Niistä ensimmäinen perustuu lukumäärien laskemiseen, jota kutsutaan kombinatoriikaksi. Toinen tapa viittaa puolestaan analyysiin, jolla matematiikassa yleensä tarkoitetaan jotakin derivaattaa tai integraaliin liittyvää.

Kombinatorinen binomikaava

Kertoma $n! = n(n-1)(n-2)\dots 3 \cdot 2 \cdot 1$ on eräs tärkeimmistä lukumäärän laskemiseen liittyvistä lausekkeista. Se antaa vastauksen esimerkiksi kysymykseen, kuinka monella eri tavalla n ihmistä voidaan asettaa jonoon. Monien eri syiden vuoksi on luontevaa määrittellä $0! = 1$; esimerkiksi tyhjä joukko on sopimuksen mukaan kaikkien joukkojen osajoukko. Lisäksi on syytä muistaa, että joukossa alkioiden järjestyksellä ei ole merkitystä; järjestetyn joukon oikea matemaattinen nimitys on nimenomaan jono.

Kertomalausekkeiden sieventämisessä tarvitaan usein seuraavaa tulosta. Esimerkiksi

$$\frac{5!}{3!} = \frac{5 \cdot 4 \cdot 3 \cdot 2}{3 \cdot 2} = 5 \cdot 4,$$

ja samalla periaatteella saadaan yleinen kaava

$$n(n-1)\dots(n-m+1) = \frac{n!}{(n-m)!},$$

kun $0 \leq m \leq n$.

Olkoot $0 \leq k \leq n$ luonnollisia lukuja (nolla mukana). Kombinatorinen määritelmä binomikertoimelle $\binom{n}{k}$ on lukumäärä sille, kuinka monella eri tavalla n :n alkion joukosta voidaan valita k :n alkion osajoukko. Lauseke $\binom{n}{k}$ luetaan ” n yli k ”; englanniksi ” n over k ” tai ” n choose k ”, joista jälkimmäinen viittaa suoraan näiden lukujen kombinatoriseen taustaan. Esimerkiksi viiden hengen ryhmästä saadaan $\binom{5}{2}$ erilaista sulkapallon kaksinpeliä.

Monet binomikerrointen ominaisuudet on helppo päätellä ilman eksplisiittistä kaavaa

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}, \quad (1)$$

joka johdettaneen kaikissa lukiokirjoissa vertaamalla k :n alkion jonojen lukumäärää vastaavien k :n alkion osajoukkojen lukumäärään.

Tehtävä 1. Päättele binomikerrointen

$$\binom{n}{0}, \binom{n}{n}, \binom{n}{1} \text{ ja } \binom{n}{n-1}$$

arvot kombinatorisesti. Tarkista tulokset kaavan (1) avulla.

Tehtävä 2. Esitä kombinatorinen perustelu kaavalle

$$\binom{n}{k} = \binom{n}{n-k}.$$

Binomikerrointen nimi ei kuitenkaan viittaa kombinatoriseen määritelmään, vaan binomikaavaan

$$\begin{aligned}(a+b)^n &= \sum_{k=0}^n \binom{n}{k} a^{n-k} b^k \\ &= \binom{n}{0} a^n + \binom{n}{1} a^{n-1} b + \dots \\ &\quad + \binom{n}{n-1} a b^{n-1} + \binom{n}{n} b^n \\ &= a^n + n a^{n-1} b + \dots + n a b^{n-1} + b^n, \quad (2)\end{aligned}$$

kun n on luonnollinen luku ja a, b ovat reaalityypin lukuja.

Huomatus: Summamerkkin käyttöön liittyy yleensä sopimus, jonka mukaan $0^0 = 1$. Muuten esimerkiksi binomikaavan ensimmäinen termi a^n (indeksillä $k=0$) pitäisi kirjoittaa muusta summasta erilleen siltä varalta, että $b=0$.

Binomikaava todistetaan yleensä ns. matemaattisen induktion avulla, mutta kombinatorinen päättely on hyvin suoraviivainen. Kun lauseke

$$(a+b)^n = (a+b)(a+b)\dots(a+b)$$

kerrotaan auki, niin $a^{n-k}b^k$ -tyyppisiä termejä saadaan täsmälleen silloin, kun tulon n :stä tekijästä valitaan täsmälleen k kappaletta b -termejä, jolloin kaikki loput $n-k$ kappaletta ovat a -termejä. Termien järjestyksellä ei tulossa ole väliä, joten $a^{n-k}b^k$ -termejä saadaan yhteensä $\binom{n}{k}$ kappaletta.

Yllä oleva päättely miellyttää kombinatoriseen ajatteluun tottuneita, ja tälle ihmistyyppille myös binomikerrointen ominaisuus

$$\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k} \quad (3)$$

on helppo ilman lausekkeiden sieventämistä, kun kysytään: Monellako eri tavalla voidaan $n+1$ alkion joukosta valita k kappaletta? Vastaus löytyy esimerkiksi seuraavalla tavalla. Ajatellaan alkiot palloina, joista yksi on musta ja loput n valkoisia (mutta keskenään erilaisia). Erilaiset k :n alkion valinnat jakaantuvat silloin kahteen ryhmään; niihin, joissa ei ole mustaa palloa (A-ryhmä), ja kaikkiin muihin, joissa on musta pallo ja $k-1$ valkoista (B-ryhmä). Tällöin A-ryhmän valintoja on $\binom{n}{k}$ kappaletta, koska musta pallo on pelkkää ilmaa A-ryhmälle. B-ryhmän valintoja on taas $\binom{n}{k-1}$ kappaletta, sillä mustan pallon lisäksi valitaan vain $k-1$ valkoista palloa n :stä mahdollisesta. Ryhmät A ja B ovat täysin erilliset, joten niiden lukumäärien summana saadaan kaikkien valintojen lukumäärä. Huomaa myös, ettei pallojen väritykseen liity niiden järjestämistä.

Tehtävä 3. Piirrä kuvio edellisen päättelyn tilanteesta ja tutki välivaiheet huolellisesti. Tarvittaessa voit kokeilla asiaa pienillä luvuilla n ja k .

Tehtävä 4. Todista kaava (3) kirjoittamalla binomikerroimet kertomien avulla ja sieventämällä lausekkeet.

Tehtävä 5. Kertaa, miten kaavan (3) avulla saadaan Pascalin kolmion muodostussääntö, kun n on rivinumero ja $k=0,1,\dots,n$ on kolmion sivun suuntaisten sarakkeiden järjestysnumero.

Tehtävä 6. Neperin luku e määritellään (yleensä) raja-arvona

$$e = \lim_{n \rightarrow \infty} \left(1 + \frac{1}{n}\right)^n.$$

a) Osoita binomikaavan avulla, että $e \geq 2$. b) Osoita binomikaavan avulla, että $e > 2$.

Analyttinen binomikaava

Osa ihmisistä hahmottaa raa'an kaavoilla laskemisen kombinatorista päättelyä helpommin. Binomikaava voidaan todistaa myös tällä tavalla.

Tavallisin todistus etenee ns. matemaattisen induktion avulla potenssin n suhteen. Siinä tarvitaan ym. kaavaa (3) ja melko mutkikasta summalausekkeiden sieventelyä. Koska se on mielestäni hankalampi kuin seuraava päättely, niin sivuutan sen kokonaan.

Todetaan aluksi, että yleinen binomikaava (2) seuraa yksinkertaisemmasta kaavasta

$$(1+x)^n = \sum_{k=0}^n \binom{n}{k} x^k \quad (4)$$

sijoittamalla tähän $x=b/a$, kertomalla tulos puolittain lausekkeella a^n ja tekemällä tarvittavat potenssien sievennykset.

Kaavaa (4) kannattaa tarkastella kahden n -asteisen polynomin yhtäsuuruutena: siinä väitetään, että polynomit $P(x) = (1+x)^n$ ja $Q(x) = \sum_{k=0}^n \binom{n}{k} x^k$ ovat samat.

Tehtävä 7. Todista seuraava tulos: Jos n -asteisille polynomeille

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$$

ja

$$q(x) = b_n x^n + b_{n-1} x^{n-1} + \dots + b_1 x + b_0$$

on voimassa $p(0) = q(0)$ ja lisäksi

$$p^{(m)}(0) = q^{(m)}(0) \text{ kaikilla } 1 \leq m \leq n,$$

niin $a_m = b_m$ kaikilla m ja polynomit ovat samat. Tässä siis $p^{(m)}(0)$ tarkoittaa polynomin $p(x)$ kertaluvun m derivaattaa kohdassa $x=0$.

Kaavan (4) todistamiseksi riittää siis tarkistaa tehtävän 7 ehdot. Selvästi $P(0) = (1+0)^n = 1$ ja

$$Q(0) = \sum_{k=0}^n \binom{n}{k} 0^k = 1,$$

koska $0^0 = 1$.

Lisäksi arvoilla $1 \leq m \leq n$ on voimassa

$$\begin{aligned} P'(x) &= n(1+x)^{n-1}, \\ P''(x) &= n(n-1)(1+x)^{n-2}, \\ &\vdots \\ P^{(m)}(x) &= n(n-1)\dots(n-m+1)(1+x)^{n-m}, \end{aligned}$$

joten

$$\begin{aligned} P^{(m)}(0) &= n(n-1)\dots(n-m+1)(1+0)^{n-m} \\ &= n(n-1)\dots(n-m+1) = \frac{n!}{(n-m)!} \end{aligned}$$

käyttämällä alussa esitettyä kertoman ominaisuutta. Toisaalta

$$\begin{aligned} Q'(x) &= \sum_{k=1}^n \binom{n}{k} k x^{k-1}, \\ Q''(x) &= \sum_{k=2}^n \binom{n}{k} k(k-1) x^{k-2}, \end{aligned}$$

$\vdots$

$$\begin{aligned} Q^{(m)}(x) &= \sum_{k=m}^n \binom{n}{k} k(k-1)\dots(k-m+1)x^{k-m} \\ &= \binom{n}{m} m! + \sum_{k=m+1}^n \binom{n}{k} k(k-1)\dots \\ &\quad (k-m+1)x^{k-m}, \end{aligned}$$

joten

$$\begin{aligned} Q^{(m)}(0) &= \binom{n}{m} m! = \frac{n!}{m!(n-m)!} m! \\ &= \frac{n!}{(n-m)!} = P^{(m)}(0). \end{aligned}$$

Väite on siis todistettu, ja kaava (4) on tosi.

Lisätietoja esimerkiksi englanninkielisen Wikipedian sivulla http://en.wikipedia.org/wiki/Binomial_coefficient

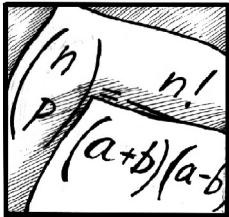
Matematiikan hämmästyttävä tehokkuus luonnontieteissä

Nobelin fysiikan palkinnon saaja E. P. Wigner kirjoitti artikkelissa, jonka otsikko on Matematiikan hämmästyttävä tehokkuus luonnontieteissä:

”Matematiikan kielen ihmeellinen sopivuus fysiikan lakien formulointiin on suurenmoinen lahja, jota emme ymmärrä emmekä ansaitse, meidän tulisi olla kiitollisia siitä ja toivoa, että se pysyy voimassa myös tulevaisuudessa ja että sitä voidaan laajentaa monille muillekin tieteen aloille, seurasi siitä sitten mielihyvää tai hämmennystä.”

N. Bourbakin artikkelissa ”Matematiikan arkkitehtuuri” sanotaan:

”Nykyfysiikan viimeiset keksinnöt näyttävät vahvistavan, mitä odottamattomimmalla tavalla, kokeellisesti havaittavien ilmiöiden ja matemaattisten struktuurien välisen läheisen yhteyden. Kuitenkaan emme tiedä yhtään mitään tämän tosiasian perusteista ja ehkä emme koskaan tule tietämäänkään.”



Binomijakaumasta

Markku Halmetoja

Mäntän lukio

Binomijakautuneen satunnaismuuttujan odotusarvon ja varianssin laskeminen suoraan määritelmiin tukeutuen on laskuteknisesti haastava tehtävä ja lukion oppikirjoissa ne yleensä annetaankin valmiina kaavoina. Tässä kirjoituksessa esitetään differentiaalilaskentaa soveltava oikotie kyseisten parametrien johtamiseksi. Lukijan mukavuutta ajatellen kerrataan aluksi eräitä yleisiä käsitteitä.

Lukuja

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}, \quad k = 0, \dots, n$$

kutsutaan binomikertoimiksi, sillä jos n on positiivinen kokonaisluku, niin

$$(1+x)^n = \sum_{k=0}^n \binom{n}{k} x^k. \quad (1)$$

Binomikaava (1) todistuu mukavasti esimerkiksi induktiolla binomikertoimien yhteenlaskusääntöä

$$\binom{n}{k-1} + \binom{n}{k} = \binom{n+1}{k} \quad (2)$$

soveltaen. Yhtälön (1) avulla saadaan jatkossa tarvittava yleisempi binomikaava

$$(a+b)^n = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k}. \quad (3)$$

Aktiivinen lukija suorittaa yhtälöihin (1), (2) ja (3) liittyvät todistukset yksityiskohtaisesti tai katsoo ne Pekka Alestalon kirjoituksesta [1].

Satunnaismuuttujan X todennäköisyysjakaumasta ilmenee, millä todennäköisyydellä muuttuja saa minkäkin arvon. Jos muuttujan arvojoukko on äärellinen, niin jakauma esitetään usein taulukkona

$X :$	x_1	$\dots$	x_k	$\dots$	x_n
$p :$	p_1	$\dots$	p_k	$\dots$	p_n

missä siis $P(X = x_k) = p_k$ ja $p_1 + \dots + p_n = 1$.

Todennäköisyydet p_k on mukava ajatella x -akselin pisteisiin x_k asetetuiksi massoiksi, joiden kokonaismäärä on 1. Tällöin satunnaismuuttujan odotusarvo

$$\mu = \mathbb{E}X = \sum_{k=1}^n x_k \cdot P(X = x_k) = p_1 x_1 + \dots + p_n x_n$$

on massan painopiste ja varianssi

$$\sigma^2 = \mathbb{D}^2 X = (x_1 - \mu)^2 p_1 + \dots + (x_n - \mu)^2 p_n$$

sen hitausmomentti painopisteen suhteen. Varianssi on siis varsin luonnollinen mittari kertomaan todennäköisyyden keskittymisestä odotusarvon läheisyyteen. Aktiivinen lukija muuntaa varianssin kaavan jatkossa tarvittavaan muotoon

$$\sigma^2 = -\mu^2 + \sum_{k=1}^n p_k x_k^2. \quad (4)$$

Kerrataan lyhyesti myös binomitodennäköisyys. Siihen tullaan suorittamalla n riippumatonta toistoa kokeesta, jonka tulostodennäköisyydet ovat A ja $\bar{A}$. Jos A :n esiintymistodennäköisyys yksittäisessä toistossa on p ja satunnaismuuttuja X on A :n esiintymiskertojen lukumäärä n :ssä toistossa, niin

$$P(X = k) = \binom{n}{k} p^k (1-p)^{n-k}, \quad k = 0, 1, \dots, n.$$

Tällöin sanotaan, että satunnaismuuttuja X on binomijakautunut parametrein n ja p , ja merkitään

$$X \sim \text{Bin}(n, p).$$

Kaavaa (3) soveltaen nähdään, että binomitodennäköisyyksien summa

$$\sum_{k=0}^n \binom{n}{k} p^k (1-p)^{n-k} = (p + 1 - p)^n = 1.$$

Binomijakautuneen muuttujan odotusarvo

$$\begin{aligned} \mu &= \sum_{k=0}^n k \cdot P(X = k) \\ &= \sum_{k=0}^n k \cdot \binom{n}{k} p^k (1-p)^{n-k}, \end{aligned} \quad (5)$$

ja varianssin määrittämisessä kaavaa (4) soveltaen on laskettava summa

$$\sum_{k=0}^n k^2 \cdot \binom{n}{k} p^k (1-p)^{n-k}. \quad (6)$$

Aktiivinen lukija tutkii millaisiin komplikaatioihin summien (5) ja (6) käsittely johtaa, sillä siten saa perspektiiviä seuraavaan yksinkertaiseen esitykseen.

Olkoon X diskreetti satunnaismuuttuja, jolla on äärellinen arvojoukko $\{x_1, \dots, x_n\}$ ja $P(X = x_k) = p_k$. Määritellään sen *generoiva funktio* g seuraavasti:

$$g(t) = p_1 t^{x_1} + \dots + p_n t^{x_n}, \quad (t > 0).$$

Derivoimalla saadaan

$$g'(t) = p_1 x_1 t^{x_1-1} + \dots + p_n x_n t^{x_n-1},$$

joten

$$\mu = \mathbb{E}X = g'(1).$$

Varianssin laskemisessa tarvitaan g :n toinen derivaatta

$$g''(t) = p_1 x_1 (x_1 - 1) t^{x_1-2} + \dots + p_n x_1 (x_n - 1) t^{x_n-2}.$$

Sen arvo pisteessä $t = 1$

$$g''(1) = \sum_{k=1}^n p_1 x_k (x_k - 1) = \sum_{k=1}^n p_k x_k^2 - g'(1),$$

joten

$$\sum_{k=1}^n p_k x_k^2 = g'(1) + g''(1).$$

Tämän avulla varianssin kaava (4) saadaan muotoon

$$\begin{aligned} \sigma^2 &= -\mu^2 + \sum_{k=1}^n p_k x_k^2 \\ &= -g(1)^2 + g'(1) + g''(1) \\ &= g''(1) + g'(1) - g(1)^2. \end{aligned}$$

Binomijakauman generoiva funktio

$$\begin{aligned} g(t) &= \sum_{k=0}^n P(X = k) \cdot t^k \\ &= \sum_{k=0}^n \binom{n}{k} p^k (1-p)^{n-k} \cdot t^k \\ &= \sum_{k=0}^n \binom{n}{k} (pt)^k (1-p)^{n-k} \\ &= (pt + 1 - p)^n. \end{aligned}$$

Sen derivaattojen

$$\begin{aligned} g'(t) &= np(pt + 1 - p)^{n-1} \\ g''(t) &= n(n-1)p^2(pt + 1 - p)^{n-2} \end{aligned}$$

avulla saadaan muuttujan X odotusarvo

$$\mu = \mathbb{E}X = g'(1) = np$$

ja varianssi

$$\begin{aligned} \sigma^2 &= \mathbb{D}^2 X = g''(1) + g'(1) - g(1)^2 \\ &= n(n-1)p^2 + np - (np)^2 \\ &= (np)^2 - np^2 + np - (np)^2 \\ &= np - np^2 \\ &= np(1-p). \end{aligned}$$

Viitteet

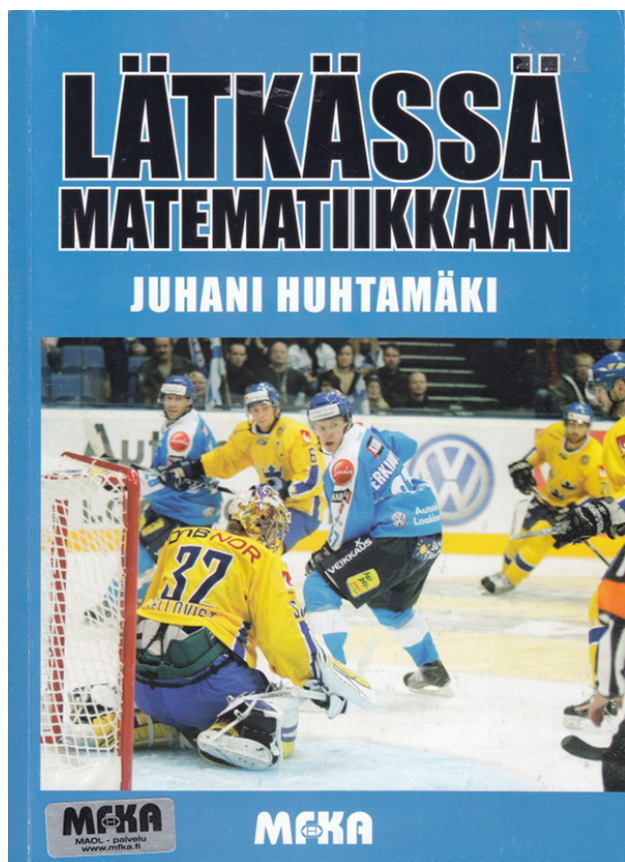
- [1] Pekka Alestalo, Binomikaava, Solmu 2/2013, <http://solmu.math.helsinki.fi/2013/2/binomi.pdf>



Laskentoa ja jääkiekkoa

Matti Lehtinen
Helsingin yliopisto

Juhani Huhtamäki: Lätkässä matematiikkaan.
MFKA-Kustannus Oy, 2010, 96 sivua. Hinta MFKA:n verkkokaupassa 15,30 euroa.



Pojat syrjäytyvät, sehän on yksi keskeisiä koulutuksen huolenaiheita. Matemaattisten aineiden opettajien liiton kustannusyhtiö MFKA on lähtenyt osaltaan ponnistelemaan tätä trendiä vastaan julkaisemalla laskennon harjoituskokoelmia, joiden teemana on urheilu. Sarjan ensimmäinen, vuonna 2010 painettu osa *Lätkässä matematiikkaan* on ottanut teemakseen nykyään ilmeisesti merkittävimmän urheiluviihteen muodon, jääkiekon. Myös jalkapalloaiheinen tehtäväkokoelma on ilmestynyt.

Lätkässä matematiikkaan -kirjassa on 110 laskutehtävää. Laskuja laskemaan on ajateltu luokkien 6–9 oppilaat. Tehtävät on kaikki painettu aukeamien vasemmanpuoleisille sivuille; oikeanpuoleiset on varattu kirjan käyttäjälle ratkaisutilaksi. Työkirja siis, eikä kerran täytettynä enää toimi toisen käyttäjän käsissä.

Tehtävät on ryhmitelty yhdeksään lukuun, joille on keksitty jääkiekkoaiheiset otsikot, osin englanninkieliset. Teemoina ovat peruslaskutoimitukset, yksikönmuunnokset, nopeudet (edelleen pääasiassa yksikönmuunnoksia), prosenttilaskenta, jonka eri aspekteille on omistettu luvuista neljä, tasogeometria (muutama pinta-alatehtävä) ja yhdeksäs luku, joka sisällysluettelon mukaan kattaa symmetrian, Pythagoraan lauseen, avaruusgeometrian, yhtälöt ja yhtälöparit ja vielä tilastot. Kaikkiin tehtäviin on annettu numeeriset vastaukset, muttei sen tarkempia ohjeita tai selityksiä.

Kaikki tehtävät on jotenkin sijoitettu jääkiekon maailmaan, jossa erilaisten numeeristen tietojen tilastointi

on tavanomaista ja runsasta. Lisääkö tämä asian mielenkiintoa, on vaikea sanoa. Tyypillisten tehtävien ”AK Kazanin kahdessa peräkkäisessä ottelussa oli yleisöä 11 345 ja 11 786. Montako prosenttia enemmän oli yleisöä jälkimmäisessä ottelussa?” tai ”Jokereiden pelimatka TPS:n vieraaksi on 165 km. Pelimatka Tapparan vieraaksi on 104,85 prosenttia Turun matkasta. Kuinka paljon pidempi matka on Tampereelle?” lukuarvotulokset eivät ainakaan minusta ole kovin mielenkiintoisia. Mutta on tehtävissä toki relevantimpiakin. Mielenkiintoista on varmaan laskea, kuinka pian siniviivalta ammuttu kiekko on maalivahdin kohdalla (vaikka tehtävässä sivulla 22 ei oteta kantaa siihen, mistä kohtaa siniviivaa laukaus lähtee) tai paljonko vettä kuluu, kun jäähdytyskone levittää sitä kaukaloon 1,20 millimetrin vesikerroksen (mutta tiedetäänkö paksuus todella millimetrin sadasosan tarkkuudella?).

Yksi *Lätkässä matematiikkaan* -kaltaisten kirjojen ongelma on vääjäämätön ajan kuluminen. Realistiset tiedot koskevat myöhäisimmillään pelikautta 2007–08, ja pelaajia, joiden saavutukset tulevat ajan mittaan himmenemään historian hämärään. Mikään ei tietysti estä kirjaa käyttävää opettajaa korvaamasta lukuja ajan-

kohtaisemmillla.

Kirjaa on maustettu sinne tänne ripotelluin pikkutiedoin ja muutamin ongelmatehtävin. Useimmat ovat ”SEND + MORE = MONEY” -tehtävän kaltaisia korvaa kirjain numerolla -tehtäviä. Nämä ovat muiden tehtävien tasoon nähden huomattavan vaikeita. Moniin on myös olemassa enemmän kuin yksi ratkaisu. Tätä ei vastausosastossa ole otettu huomioon.

Lätkässä matematiikkaan on varsin selvästi poikakirja. Vain yhdessä tehtävässä näkyy mainittavan toinen sukupuoli, ja silloinkin kysytään ottelun naispuolisten katsojien määrää. Jääkiekkoon vihkiytymättömän lukijan silmään pistävät jotkin varmaan alan normaaliin kielenkäyttöön kuuluvat ilmaukset kuten ”ampui tutkaan”. Pientä mutta tuskin häiritsevää horjuvuutta on merkinnöissä. Ja kyllähän *ympyrälieriö* on yhdyssana.

Matematiikasta syrjäytymässä oleva poika tuskin omaaloitteisesti etsiytyy hyödyllisen harjoituskirjan luokse. Mahtanevatko peruskoulun ylläpitäjät myöskään tällaisia kirjoja ostella. Olisi varmaan hyvä, jos niin tekisivät.

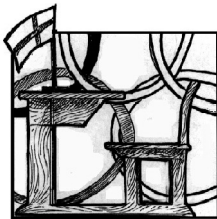
Solmun matematiikkadiplomit

Peruskoululaisille tarkoitettut Solmun matematiikkadiplomit I – VIII tehtävineen 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)



Sekalaisia kilpailutehtäviä

Heikki Pokela

Tapiolan lukio

Edellisen numeron tehtävistä

Tämän vuoden ensimmäisessä Solmussa jätettiin lukijan ratkottaviksi pari tehtävää. Ensimmäisessä piti etsiä kaikki kokonaisluvut x , jotka toteuttavat yhtälön

$$2^x(4 - x) = 2x + 4. \quad (1)$$

Koska 2^x on positiivinen, on lausekkeiden $2x + 4$ ja $4 - x$ oltava samanmerkkiset. Niillä ei ole yhteisiä nol-lakohtia, joten tutkittavaksi jää x :n arvot $-1, 0, 1, 2$ ja 3 . Näistä yhtälön (1) toteuttavat $x = 0$, $x = 1$ ja $x = 2$. Myös muita ratkaisutapoja löytyy, mutta todennäköisesti suurin osa niistä johtaa hyvin pitkään algebraliseen pyörittelyyn. Kilpailutehtäville on tyypillistä, että yksi ratkaisutapa on lyhyt, muut pitkiä.

Toisena tehtävänä oli osoittaa, että jos m ja s ovat positiivisia kokonaislukuja joiden tulo on 2000^{2001} , niin yhtälöllä

$$mx^2 - sy^2 = 3 \quad (2)$$

ei ole kokonaislukuratkaisuja. (Kilpailutehtävä Make-doniasta)

Tehtävä voidaan ratkaista ristiriitatodistuksella. Oletetaan, että (2) toteutuu joillakin positiivisilla kokonaisluvuilla x ja y , ja että m ja s ovat tehtävän ehdot toteuttavia lukuja. Koska $2000 = 16 \cdot 125$, voimme kirjoittaa

$$ms = (2^4 5^3)^{2001} = 2^{8004} 5^{6003}.$$

Kakkosen saaminen tekijäksi on hyödyllistä, sillä nyt voidaan ottaa parillisuus ja parittomuus työkaluksi tehtävän ratkaisussa. Koska ms on parillinen, eivät m ja s voi molemmat olla parittomia. Jos s on parillinen, on m :n oltava pariton, sillä $mx^2 = 3 + sy^2$ on pariton. Voimme siis tässä tapauksessa kirjoittaa $m = 5^\alpha$, missä α on kokonaisluku, joka toteuttaa ehdon $0 \leq \alpha \leq 6003$. Tästä seuraa, että $s = 2^{8004} 5^{6003-\alpha}$, joten alkuperäinen yhtälö saadaan muotoon

$$5^\alpha x^2 = 3 + 2^{8004} 5^{6003-\alpha} y^2. \quad (3)$$

Yhtälön oikea puoli on kongruentti luvun 3 kanssa modulo 4. Vasemmalla puolella on x^2 , joka neliönä on 0 tai 1 modulo 4, joten siitä ei 5:llä kertomalla saa lukua, joka olisi kongruentti 3:n kanssa modulo 4.

Jos puolestaan m on parillinen, niin s on pariton. Siis $s = 5^\beta$ jollakin kokonaisluvulla β , joka toteuttaa $0 \leq \beta \leq 6003$. Nyt $m = 2^{8004} 5^{6003-\beta}$, ja alkuperäinen yhtälö on

$$3 + 5^\beta y^2 = 2^{8004} 5^{6003-\beta} x^2. \quad (4)$$

Yhtälöstä (4) nähdään, että β ei voi toteuttaa ehtoa $0 < \beta < 6003$, sillä tässä tapauksessa seuraisi $5 \mid 3$, mikä on mahdotonta. Jos $\beta = 0$, niin

$$y^2 \equiv -3 \equiv 2 \pmod{5}.$$

Jos $\beta = 6003$, niin $x^2 \equiv 3 \pmod{5}$, koska

$$2^{8004} = 4^{4002} \equiv (-1)^{4002} \equiv 1 \pmod{5}.$$

Siispä tämäkin vaihtoehto johtaa ristiriitaan, sillä lukujen neliöt ovat kongruentteja lukujen 0, 1 tai 4 kanssa modulo 5. Aktiivinen lukiolainen voi varmistaa asian laskemalla lukujen $5n$, $5n + 1$, $5n + 2$, $5n + 3$ ja $5n + 4$ neliöt.

Maol loppukilpailu 2013

Loppukilpailuun kutsuttiin syksyllä pidetyistä alkusarjoista kolme ensimmäisen vuoden, kuusi toisen vuoden ja noin kaksitoista kolmannen vuoden lukio-opiskelijaa. Varsinkin näille kolmelle nuorimmalle kutsutulle edessä oli todella haastetta, sillä loppukilpailu ei tunne sarjakakoa. Kuitenkaan he eivät yleensä jää aivan tulostulostan loppupäähän, saati pisteittä. Joskus joku heistä pääsee kymmenen parhaan joukkoon. Niin kävi tänäkin vuonna.

Viidestä tehtävästä viimeistä oli vuotta aiemmin käyty Etelä-Korean matematiikkakilpailujen loppukilpailussa, ja se käsitteli lukuteoriaa.

Etsi kaikki kokonaislukukolmikot (m, p, q) , jotka toteuttavat yhtälön

$$2^m p^2 + 1 = q^5. \quad (5)$$

ja joissa lisäksi $m > 0$ sekä p ja q ovat alkulukuja.

Ratkaisu lähtee liikkeelle siirtämällä ykkönen oikealle puolelle. Koska $q^5 - 1$ on jaollinen $(q - 1)$:llä, $q - 1$ on muotoa $2^n p^k$, missä $n \leq m$ ja k on 0, 1 tai 2. Tällaisten eksponenttiehtojen asettaminen tulee melko usein vastaan kilpatehtävien yhtälöissä, joissa etsitään kokonaislukuratkaisuja. Yhdistämällä edellisen tuloksen ja yhtälön (5) saamme yhtälöparin

$$\begin{cases} 2^m p^2 = q^5 - 1 \\ 2^n p^k = q - 1. \end{cases} \quad (6)$$

Jakamalla yhtälöt (6) puolittain saadaan

$$2^{m-n} p^{2-k} = \frac{q^5 - 1}{q - 1} = q^4 + q^3 + q^2 + q + 1, \quad (7)$$

missä oikea puoli on pariton, joten $m = n$. Binomikaavaa soveltamalla saadaan

$$2^m p^2 + 1 = q^5 = (2^m p^k + 1)^5 \geq 2^{5m} p^{5k} + 1,$$

mistä seuraa

$$2^m p^2 \geq 2^{5m} p^{5k}$$

ja edelleen

$$p^{2-5k} \geq 2^{4m} \geq 1.$$

Eksponenteista tulee vaatimukseksi $2 - 5k \geq 0$. Aiemmin k :lle saatu ehto antaa ainoaksi vaihtoehdoksi $k = 0$ ja siten $q - 1 = 2^m$. Alkuperäinen yhtälö on nyt

$$2^m p^2 + 1 = (2^m + 1)^5. \quad (8)$$

Avaamalla yhtälössä (8) sulut, vähentämällä ykköset ja jakamalla luvulla 2^m saadaan

$$p^2 = 2^{4m} + 5 \cdot 2^{3m} + 10 \cdot 2^{2m} + 10 \cdot 2^m + 5. \quad (9)$$

Jos nyt $m \geq 2$, niin yhtälöstä (9) seuraa

$$p^2 \equiv 5 \pmod{8},$$

minkä aktiivinen lukiolainen toteaa mahdottomaksi. Täten $m = 1$. Sijoittamalla ratkaistut luvut aiempiin yhtälöihin saadaan lopuksi $(m, p, q) = (1, 11, 3)$.

Pari tehtävää pohdittavaksi

Funktionaalitehtävät edellyttävät kuvauksiin liittyvien perusominaisuuksien ymmärtämistä. Tällaisia ominaisuuksia ovat mm. käänteiskuvaus ja useat sisäkkäiset funktio-operaatiot. Seuraavaa tehtävää ei ehkä heti arvasta funktionaalitehtäväksi.

Olkoon $a = \sqrt[1992]{1992}$. Kumpi luvuista

$$a^{a^{\dots^a}} \text{ vai } 1992 \quad (10)$$

on suurempi? Yhtälön vasemmalla puolella on 1992 kappaletta a -kirjaimia.

Lausekkeiden arvoihin, siis lukuihin, liittyvät pohdinnat kuten numeroiden määrät, ensimmäiset tai viimeiset numerot ratkeavat yleensä kongruenssin laskusäännöillä. Joskus binomikaava ja induktio riittävät, kuten seuraavassa tehtävässä.

Määritä luvun

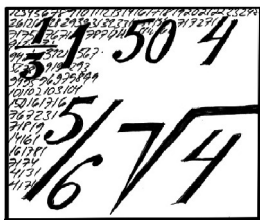
$$2^5 + 2^{5^2} + 2^{5^3} + \dots + 2^{5^{1991}} \quad (11)$$

kaksi viimeistä numeroa, kun luku kirjoitetaan kymmenjärjestelmässä.

Vihjeeksi edelliseen vaikkapa se, että kannattaa katsoa, mihin kahteen numeroon kaksi ensimmäistä termiä päättyvät kymmenjärjestelmässä. Päätelmän voi yrittää sen jälkeen yleistää induktiolla.

Kilpailutehtävien ratkaisuihin esiintyvät usein kongruenssi, induktio, parillisuus, neliön ei-negatiivisuus, kehäkulmat, yhdenmuotoisuus, sopivien lukujen sijoittaminen funktionaaliyhtälöiden sisälle, polynomiyhtälöiden juurten ominaisuudet ja muutamat muut perusasiat. Hienous lienee juuri tässä. Varsin rajatulla matematiikan osa-alueella, kilpailumatematiikalla, voidaan kehittää nuoren lukiolaisen matemaattista oppimiskykyä melko rajattomasti. Haasteet kilpailumatematiikassa eivät lopu kesken.

Ratkaisuihin palattaneen jonkin seuraavan Solmun palstoilla.



Supremum

Tuomas Korppi

Johdanto

Lukijan mielestä rationaali- ja reaalilukujoukot tuntuivat ehkä samanlaisilta. Rationaali- ja reaaliluvuilla lasketaan suunnilleen samalla tavalla. Kummastakin löytyy mielivaltaisen suuria lukuja ja mielivaltaisen pieniä positiivisia lukuja sekä tietysti vastaavat negatiiviset luvut. On kuitenkin eräs ominaisuus, joka tekee reaaliluvuista rationaalilukuja paremman systeemin jatkuvan muutoksen kuvailemiseen ja moneen muuhunkin tarkoitukseen. Tämä ominaisuus voidaan ilmaista niin, että jokaisella epätäydellä, ylhäältä rajoitetulla joukolla reaalilukuja on pienin yläraja. Ilmaus voi tässä vaiheessa tuntua lukijasta kryptiseltä, ja tutustummekin tähän ominaisuuteen tässä kirjoitelmassa. Käytän huomattavasti mukaillen erästä keskustelussa [1] esitettyä lähestymistapaa.

Opettavainen satu

Olipa kerran poika nimeltä Pekka, joka ei tuntenut muita lukuja kuin rationaaliluvut. Lukijan muistin virkistämiseksi mainittakoon, että rationaaliluvut ovat niitä lukuja, jotka saadaan kahden kokonaisluvun osamääränä, eli muun muassa $\frac{1}{5}$, $\frac{5}{1}$, $\frac{-2}{3}$ ja $\frac{0}{1}$ ovat rationaalilukuja.

Eräänä päivänä Pekka lähti kävelemään pois päin kotitalostaan. Kutsumme sitä hetkeä, jona Pekka lähti kävelemään, hetkeksi 0, ja Pekka kiihdytti kävelyään

niin, että Pekan etäisyys kotitalosta saadaan kaavalla

$$\text{Etäisyys} = \text{Aika}^2.$$

Hetkellä 1,5 Pekka havaitsi, että hän on etäisyydellä $1,5^2 = 2,25$ kotitalostaan. Pekka päätteli, että on ollut hetki h_0 , jona hän on ollut etäisyydellä 2 kotitalostaan. Nyt h_0 toteuttaa yhtälön

$$h_0^2 = 2.$$

Kuitenkin Pekka tiesi, että tällä yhtälöllä ei ole ratkaisuja rationaalilukujen joukossa. Koska Pekka tunsikin vain rationaaliluvut, hän oli ymmällään.

Eräänä toisena päivänä Pekka teki kävelyn, jossa hän lähti kotitalostaan, käveli aikansa ja palasi kotitaloonsa. Kutsumme edelleen sitä hetkeä, jona Pekka lähti kävelemään, hetkeksi 0. Tällä kertaa Pekka käveli niin, että hänen etäisyytensä kotitalosta saadaan kaavalla

$$\text{Etäisyys} = \text{Aika} - \text{Aika}^3.$$

Hetkellä 0 hän oli kotitalossaan, ja hetkellä 1 hän oli palannut kotitaloonsa. Pekka päätteli, että näiden hetkien välillä on hetki h_1 , jona hän on ollut kauimpana kotitalostaan. Pekka oli opiskellut matematiikkaa, ja hän tiesi, että h_1 on funktion

$$f(x) = x - x^3$$

derivaatan nollakohta. Nyt

$$f'(x) = 1 - 3x^2,$$

joten

$$h_1^2 = \frac{1}{3}.$$

Pekka tiesi, että tälläkään yhtälöllä ei ole ratkaisuja rationaalilukujen joukossa, joten Pekka oli taas ymmällään. Sen pituinen se.

Ongelman muotoilu

Kuten useissa saduissa, myös tässä sadussa on opetus: rationaaliluvut ovat hyvin puutteellinen lukujärjestelmä jatkuvan liikkeen kuvailuun. Lukija lieene törmännyt sellaisiin reaalityihin, jotka olisivat auttaneet Pekan hämmennykseen: $h_0 = \sqrt{2}$ ja $h_1 = \sqrt{\frac{1}{3}}$. Nämä eivät olekaan rationaalilukuja. Lukija lieene törmännyt myös muihin reaalityihin, jotka eivät ole rationaalilukuja. Esimerkkejä tällaisista ovat e ja π .

Edellä olemme esimerkinomaisesti maininneet joitakin reaalitylukuja. Nyt kysymys, joka meitä kiinnostaa, kuuluu

Mitä kaikkia lukuja meidän on hyväksyttävä reaalityluiksi, jotta saisimme reaalityluista hyvän (mm.) jatkuvaa liikettä kuvailevan systeemin?

Rationaaliluvut ovat myös reaalitylukuja, mutta ne eivät yksin riitä. Mitä muuta tarvitaan? Luettelon antaminen kaikista reaalityluista vaikuttaa toivottomalta projektilta¹, joten tahdomme jonkun yleisen periaatteen, jolla voidaan tuottaa kaikki reaalityluvut.

Palaamme tähän kysymykseen hetken päästä, mutta ensin tutkimme motivoivana esimerkkinä hiukan $\sqrt{2}$:ta.

$\sqrt{2}$:sta

Tutkimme sitä aukkoa, jonka $\sqrt{2}$:n puute rationaalilukujen systeemiin jättää.

Osoitamme ensin, että ei ole olemassa rationaalilukua r , jolle $r^2 = 2$. Tästä seuraa, että $\sqrt{2}$ ei ole rationaaliluku.

Todistus: Teemme vastaoletuksen, että on olemassa rationaaliluku r , jolle $r^2 = 2$. Nyt r voidaan esittää muodossa $\frac{a}{b}$, missä a ja b ovat kokonaislukuja. Voimme lisäks olettaa, että edellämäinittua esitystä on sievennetty niin paljon, että a :lla ja b :llä ei ole yhteisiä tekijöitä. Koska $(\frac{a}{b})^2 = 2$, pätee $a^2 = 2b^2$. Siis a^2 on jaollinen kahdella, joten a on jaollinen kahdella, ja koska esitys oli sievennetty, b ei ole jaollinen kahdella. Siis

a^2 on jaollinen neljällä. Mutta koska b ei ole jaollinen kahdella, $2b^2$ ei ole jaollinen neljällä, ristiriita. Siis vastaoletus on väärä, ja rationaalilukua r , jolle $r^2 = 2$, ei ole olemassa. $\square$

Tutkitaan sitten sellaisia rationaalilukuja $\frac{a}{b} > 0$, joille $(\frac{a}{b})^2 < 2$. Koska neliöjuurifunktio on kasvava, tällaisille luvuille pätee myös $\frac{a}{b} < \sqrt{2}$. Valitaan nyt niin suuri $n \in \mathbb{N}$, että $\frac{1}{10^n} < \sqrt{2} - \frac{a}{b}$, eli $\frac{a}{b} + \frac{1}{10^n} < \sqrt{2}$. Tästä seuraa $(\frac{a}{b} + \frac{1}{10^n})^2 < 2$. Vedämme seuraavan johtopäätöksen: Jos $\frac{a}{b}$ on mikä tahansa positiivinen rationaaliluku, jolle $(\frac{a}{b})^2 < 2$, on olemassa toinen, suurempi rationaaliluku $\frac{a}{b} + \frac{1}{10^n}$, jolle $(\frac{a}{b} + \frac{1}{10^n})^2 < 2$.

Vastaavalla päättelyllä voidaan näyttää seuraava: Jos $\frac{a}{b}$ on mikä tahansa positiivinen rationaaliluku, jolle $(\frac{a}{b})^2 > 2$, on olemassa toinen, pienempi rationaaliluku $\frac{a}{b} - \frac{1}{10^n}$, jolle $(\frac{a}{b} - \frac{1}{10^n})^2 > 2$.

Siis niiden positiivisten rationaalilukujen $\frac{a}{b}$ joukossa A , joille $(\frac{a}{b})^2 < 2$, ei ole suurinta alkioita, ja niiden positiivisten rationaalilukujen $\frac{a}{b}$ joukossa B , joille $(\frac{a}{b})^2 > 2$, ei ole pienintä alkioita.

Edellisestä vedämme seuraavan, jatkon kannalta olennaisen johtopäätöksen: Ei ole olemassa pienintä rationaalilukua $\frac{a}{b}$, joka olisi vähintään niin suuri kuin kaikki A :n alkioita, eikä ole olemassa suurinta rationaalilukua $\frac{a}{b}$, joka olisi korkeintaan niin pieni kuin kaikki B :n alkioita.

Joukkojen A ja B välissä on siis aukko, johon $\sqrt{2}$ kuului. Seuraavassa luvussa esitämme periaatteen, jolla kaikki tällaiset aukot voidaan tilkitä.

Kuinka reaalityluvut saadaan aikaan?

Tässä luvussa esitämme vihdoin sen periaatteen, joka tuottaa kaikki reaalityluvut. Aloitamme kuitenkin parilla määritelmällä.

Olkoon A epätyhjä joukko rationaalilukuja. Sanomme, että A on ylhäältä rajoitettu rationaalilukujen joukossa, jos on olemassa rationaaliluku q , jolle $a \leq q$ kaikilla joukon A alkioilla a .

Olkoon A epätyhjä joukko rationaalilukuja. Sanomme, että reaalityluku r on joukon A yläraja, jos kaikilla joukon A alkioilla a pätee $a \leq r$. Sanomme, että reaalityluku r' on joukon A pienin yläraja eli *supremum*, jos seuraavat kaksi ehtoa pätevät

- r' on joukon A yläraja.
- Jos reaalityluku r'' on joukon A yläraja, niin $r' \leq r''$.

Nyt kaikki reaalityluvut saadaan tuotettua seuraavalla periaatteella:

¹Ja sitä se onkin; tämä voidaan jopa todistaa.

Periaate 1. Jos A on epättyhjä joukko rationaalilukuja, joka on ylhäältä rajoitettu rationaalilukujen joukossa, niin on olemassa reaaliluku r , joka on joukon A pienin yläraja.

Tutkitaan vielä Pekan tilannetta. Hän siis tarvitsee reaaliluvut $\sqrt{2}$ ja $\sqrt{\frac{1}{3}}$. Määritellään joukko A_0 niin, että se on niiden positiivisten rationaalilukujen a joukko, joille $a^2 < 2$. Nyt $\sqrt{2}$ saadaan joukon A_0 pienimpänä ylärajana. Vastaavasti, jos A_1 on niiden positiivisten rationaalilukujen a joukko, joille $a^2 < \frac{1}{3}$, niin $\sqrt{\frac{1}{3}}$ saadaan joukon A_1 pienimpänä ylärajana.

Toivon, että tässä vaiheessa lukijasta ei tunnu siltä, että ammunne tykillä karpästä. Olemme kunnolla perustelleet ainoastaan kahden reaaliluvun $\sqrt{2}$:n ja $\sqrt{\frac{1}{3}}$:n tarpeen, mutta Periaate 1 tuottaa reaalilukuja vaikka millä mitalla. Kuitenkin kaikki näin syntyvät reaaliluvut tarvitaan, jotta saadaan kehitettyä kunnollinen jatkuva muutosta kuvaava teoria.

Desimaalikehitelmät

Lukija on saattanut törmätä reaalilukujen luonnehdintaan desimaalikehitelminä, jotka mahdollisesti ovat päättymättömiä. Tässä luvussa selitämme, miksi tämä reaalilukujen luonnehdinta tuottaa saman tuloksen kuin Periaate 1. Käsittelemme vain ei-negatiivisia lukuja. Negatiiviset luvut voidaan käsitellä samantapaisella menetelmällä.

Olkoon $a, a_1a_2a_3 \dots$ desimaalikehitelmä, missä a on kokonaisosa ja $a_1, a_2, a_3, \dots$ desimaalit. Muodostetaan rationaalilukujoukko A , jonka jäsenet ovat seuraavat rationaaliluvut, joita on mahdollisesti äärettömän monta

$$\begin{array}{l} a, a_1 \\ a, a_1a_2 \\ a, a_1a_2a_3 \\ \vdots \end{array}$$

Nyt joukko A nähdään helposti ylhäältä rajoitetuksi, ja sen pienin yläraja on juuri reaaliluku, jonka desimaalikehitelmä on $a, a_1a_2a_3 \dots$.

Kääntäen, olkoon x reaaliluku, joka on rationaalilukujoukon A pienin yläraja. Muodostetaan rationaalilukujoukko A' siten, että $a \in A'$, jos on olemassa $b \in A$, jolle $b \geq a$. Nyt x on joukon A' pienin yläraja. Olkoon a suurin kokonaisluku, joka kuuluu joukkoon A' . Olkoon a, a_1 suurin yksidesimaalinen desimaalikehitelmä, joka kuuluu joukkoon A' . Olkoon a, a_1a_2 suurin kaksidesimaalinen desimaalikehitelmä, joka kuuluu joukkoon A' . Tässä siis tosiaan luku a on sama kuin luvun a, a_1 kokonaisosa, ja luvun a, a_1a_2 kokonaisosa ja ensimmäinen desimaali ovat samat kuin luvulla a, a_1 . Jatkaamalla prosessia saadaan aikaan kaikki x :n desimaalit.

Reaalilukujen ominaisuuksia

Olkoon A joukko reaalilukuja. Määritellään A :n yläraja ja pienin yläraja (eli *supremum*), samoin ylhäältä rajoitettuus samoin kuin teimme sen rationaalilukujoukoille. Sen avulla, että Periaate 1 tuottaa kaikki reaaliluvut, voidaan todistaa seuraava teoreema:

Teoreema 2. Olkoon A epättyhjä, ylhäältä rajoitettu joukko reaalilukuja. Tällöin on olemassa reaaliluku r , joka on joukon A pienin yläraja.

Tämän teoreeman todistus jätetään harjoitustehtäväksi. Todistusstrategia on selitetty luvussa Pähkinöitä.

Periaatteella 1 tuotetut reaaliluvut auttavat myös Pekan pälkähästä sekä moniin muihin samankaltaisiin tilanteisiin. Voidaan nimittäin todistaa seuraavaksi esitettävät teoreemat. Annamme teoreemoille perustelut, jotka kenties saavat ne tuntumaan uskottavilta. Jos perustelut aiheuttavat lukijalle hahmotusvaikeuksia, kuvien piirtäminen auttaa. Lukijan kannattaa huomata, että perustelumme eivät ole matemaattisia todistuksia.

Teoreema 3. Olkoon $f: \mathbb{R} \rightarrow \mathbb{R}$ jatkuva funktio. Olkoon $a < b$ kaksi reaalilukua ja c reaaliluku, joka on lukujen $f(a)$ ja $f(b)$ välissä. Tällöin on olemassa reaaliluku y , $a \leq y \leq b$, jolle $f(y) = c$.

Perustelu: Oletetaan $f(a) \leq f(b)$. Olkoon A niiden reaalilukujen z joukko, jotka ovat vähintään yhtäsuuria kuin a ja korkeintaan yhtäsuuria kuin b , ja joille $f(z) \leq c$. Nyt luku y saadaan joukon A pienimpänä ylärajana.

Jos $f(a) > f(b)$, muodostetaan $g(x) = -f(x)$, $c' = -c$ ja sovelletaan edellisen kappaleen tulosta olioille g, c', a, b .

Teoreema 4. Olkoon $a < b$ reaalilukuja ja $f: [a, b] \rightarrow \mathbb{R}$ jatkuva funktio. Tällöin on olemassa $x \in [a, b]$ siten, että funktio f saa pisteessä x suurimman arvonsa.

Perustelu: Olkoon c funktion f kuvajoukon supremum. Tässä vaiheessa emme vielä tiedä, että kuvajoukko on ylhäältä rajoitettu. Asetetaan ylhäältä rajoittamattoman osajoukon supremumiksi ∞ , eli jos kuvajoukko on rajoittamaton, $c = \infty$.

Valitaan $a_0 = a$ ja $b_0 = b$.

Olkoon x_0 välin $[a_0, b_0]$ keskipiste. Tutkitaan välejä $[a_0, x_0]$ ja $[x_0, b_0]$. Vähintään toisen näistä väleistä kuvajoukon supremum on c . Valitaan a_1 :ksi ja b_1 :ksi tämän välin päätepisteet, $a_1 < b_1$. (Jos edellä kummankin välin kuvajoukon supremum on c , valitaan vain toinen näistä väleistä.)

Olkoon x_1 välin $[a_1, b_1]$ keskipiste. Tutkitaan välejä $[a_1, x_1]$ ja $[x_1, b_1]$. Vähintään toisen näistä väleistä kuvajoukon supremum on c . Valitaan a_2 :ksi ja b_2 :ksi tämän välin päätepisteet, $a_2 < b_2$. (Jos edellä kummankin välin kuvajoukon supremum on c , valitaan vain toinen näistä väleistä.)

Jatkamalla prosessia äärettömiin, saadaan ääretön kasvava jono $a_0, a_1, a_2, \dots$ ja ääretön vähenevä jono $b_0, b_1, b_2, \dots$. Lisäksi välin $[a_i, b_i]$ pituus lähenee nolaa, kun $i \rightarrow \infty$. Valitaan x :ksi joukon $\{a_0, a_1, a_2, \dots\}$ supremum, joka sijaitsee jokaisella välillä $[a_i, b_i]$, $i \in \mathbb{N}$. Nyt $f(x) = c$, ja koska f saa arvon c , $c \neq \infty$.

Tarkat todistukset käydään yleensä läpi ensimmäisillä yliopiston matematiikan kursseilla.

Pähkinöitä

Kaikissa pähkinöissä saat käyttää vapaasti kaikkia tässä kirjoitelmassa mainittuja tuloksia sekä muita tunte-miasi matematiikan tuloksia.

- Olkoon A neliö, jonka sivun pituus on 1. Laske A :n lävistäjän pituus ja totea, että rationaaliluvut eivät ole riittäviä edes yksinkertaisen geometrian tekemiseen.
- Osoita, että $\sqrt{\frac{1}{3}}$ ei ole rationaaliluku.
- Olkoon A joukko reaalilukuja. Sanomme, että $x \in \mathbb{R}$ on joukon A alaraja, jos $x \leq a$ kaikilla $a \in A$. Sanomme, että A on alhaalta rajoitettu, jos sillä on alaraja. Olkoon A epätyhjä, alhaalta rajoitettu joukko reaalilukuja. Osoita, että joukolla A on suurin alaraja.
- Luvussa Desimaalikehitelmät konstruointiin joukko A' . Osoita, että seuraava pätee: Jos $a \in A'$, ja r on mikä tahansa rationaaliluku, jolle $r < a$, niin $r \in A'$.
- Kappaleessa Desimaalikehitelmät konstruointiin desimaalikehitelmä joukon A ylärajalle. Konstruktiossa oletettiin perustelematta seuraava: Jos a on n ensimmäistä desimaalia sisältävä konstruktion vaihe ja b on $n + 1$ ensimmäistä desimaalia sisältävä konstruktion vaihe, niin b :n n ensimmäistä desimaalia ovat samat kuin a :n n ensimmäistä desimaalia. Todista kyseinen väite.
- Olkoon q rationaaliluku ja A niiden rationaalilukujen joukko, jotka ovat korkeintaan yhtäsuuria kuin q . Osoita, että q on joukon A pienin yläraja.
- Todista Teoreema 2. Sinun kannattaa seurata seuraavaa strategiaa:
 - Todista, että jos r_0, r_1 ovat reaalilukuja, $r_0 < r_1$, niin on olemassa rationaaliluku q , jolle $r_0 < q \leq r_1$. Tässä kannattaa käyttää hyväksi sitä, että Periaate 1 tuottaa *kaikki* reaaliluvut.
 - Todista, että jos A on ylhäältä rajoitettu joukko reaalilukuja, on olemassa rationaaliluku q , joka on joukon A yläraja. Tässä voit käyttää hyväksi sitä, että Periaate 1 tuottaa *kaikki* reaaliluvut.
 - Olkoon A ylhäältä rajoitettu joukko reaalilukuja. Muodosta niiden rationaalilukujen q joukko B , joille on olemassa $a \in A$, jolle $q \leq a$. Päättele käyttäen edellistä pykälää, että B :llä on yläraja, joka on rationaaliluku.
 - Olkoon A ja B kuten edellisessä pykälässä. Olkoon q joukon B yläraja. Osoita, että q on joukon A yläraja. Käytä hyväksi pykälää a.
 - Olkoon A ja B kuten edellisessä pykälässä. Olkoon q joukon B pienin yläraja (tällainen on olemassa pykälän c ja Periaatteen 1 nojalla). Osoita, että q on joukon A pienin yläraja.
- Tämä tehtävä koostuu kolmesta kohdasta.
 - Olkoon A niiden rationaalilukujen joukko, jotka ovat pienempiä kuin 1, ja x joukon A pienin yläraja. Sovella luvussa Desimaalikehitelmät mainittua menetelmää ja konstruoi luvulle x desimaalikehitelmä.
 - Olkoon B niiden rationaalilukujen joukko, jotka ovat korkeintaan yhtäsuuria kuin 1, ja y joukon B pienin yläraja. Sovella luvussa Desimaalikehitelmät mainittua menetelmää ja konstruoi luvulle y desimaalikehitelmä.
 - Osoita, että edellä $x = y$. Strategia: Tee vastaoletus $x \neq y$ ja päättelee $x < y$. Osoita, että lukujen x ja y keskiarvolle k (joka on reaaliluku, voit olettaa tämän tunnetuksi) pätee $x < k < y$. Käytä edellisen tehtävän pykälää a ja päättelee, että on olemassa rationaaliluku q , jolle $x < q \leq k$, ja johda tästä ristiriita.

Viitteet

- [1] Täydellisyysaksiooma,
<http://solmu.math.helsinki.fi/cgi-bin/yabb2/YaBB.pl?num=1209209108/0#0>