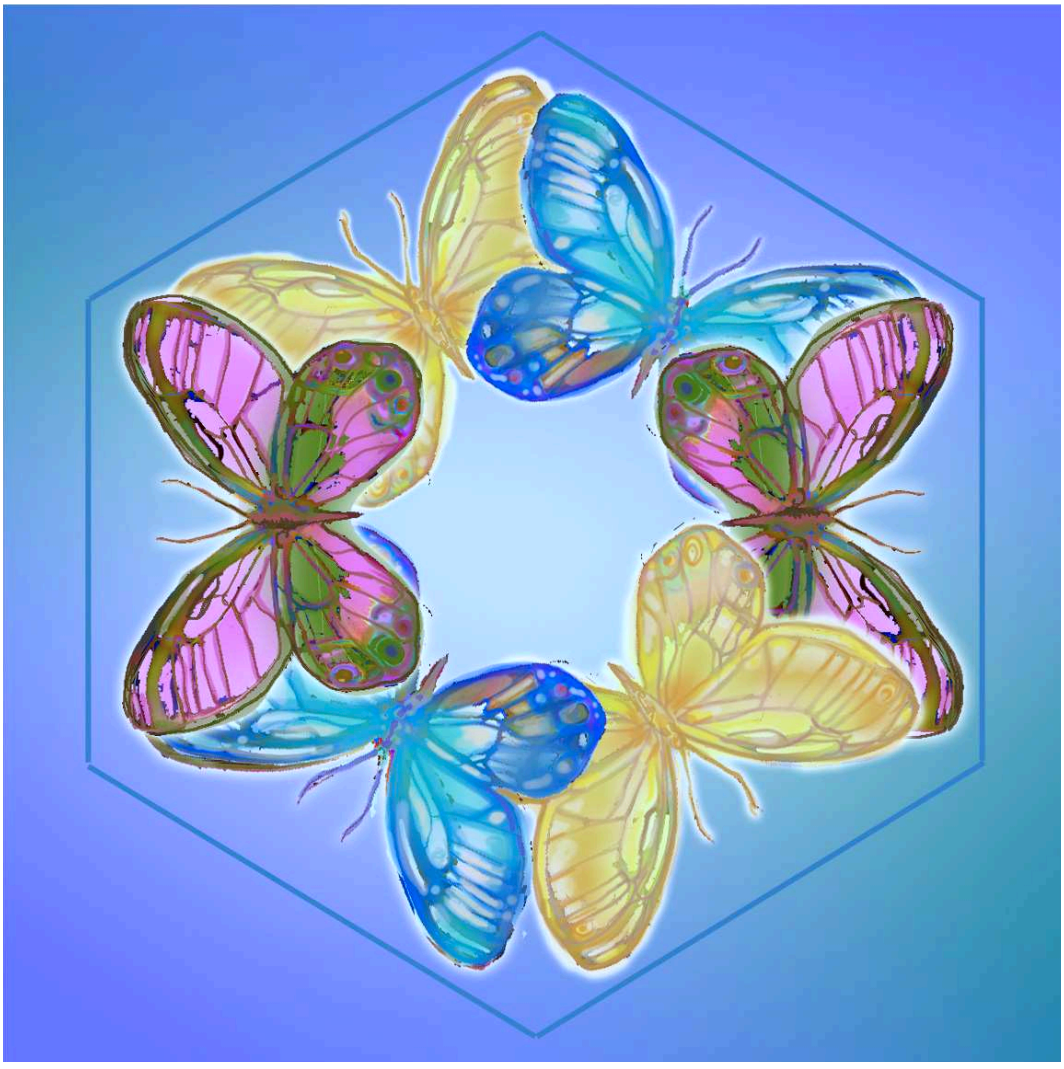
Solmu

Matematiikkalehti
2/2008

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



Solmu 2/2008

ISSN 1458-8048 (Verkkolehti)
ISSN 1459-0395 (Painettu)

Matematiikan ja tilastotieteen laitos
PL 68 (Gustaf Hällströmin katu 2b)
00014 Helsingin yliopisto

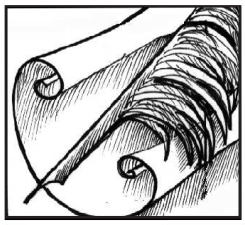
http://solmu.math.helsinki.fi/

Numeroon 3/2008 tarkoitetut kirjoitukset pyydämme lähettämään 10.9.2008 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



Matematiikan opetuksesta – jälleen kerran

Koulu kehittyy. Yhtenäinen peruskoulu on entistä yhtenäisempi: hallinnollinen raja ala- ja yläasteen välillä on poistettu. Tämä on avannut vision: opettajien jako luokanopettajiin ja aineenopettajiin poistukoon myös.

En tiedä, kuinka vakavasti luokanopettajat tavoittelevat esimerkiksi vieraan kielen opetuksen saattamista luokanopettajan haltuun koko peruskoulun ajaksi. Luultavasti yhteiskunnan vallitsevat yleiset käsitykset nousevat tässä vastaan. Englannin opetusta ei varmaan haluta delegoida kasvatustieteen kandidaateille. Pahoin pelkään, että "yleinen ymmärrys" voi kuitenkin johtaa uskomukseen, että matematiikan opetus on siirrettävissä koko peruskoulun ajaksi luokanopettajakoulutuksen saaneiden opettajien huostaan.

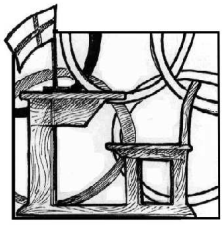
Peruskoulun tavoite oli poistaa opetuksen epätasa-arvoa antamalla kaikille nuorille sama mahdollisuus oppiin ja niihin mahdollisuuksiin elämässä, joita sivistys mukanaan tuo. On oikeastaan surullista ja hämmentävää, että tämä mahdollisuuksien avartuminen tarkoitti itse asiassa mahdollisuuksien supistumista. Kun keskikoulu tarjosi sen suorittaneille kohtuullisen hyvän lähtökohdan lukioon tai opistotasoisiin ammattiopintoihin, niin peruskoulun tuottama tieto on selvästi matalampitasoista. Tämän näkee matematiikassa: lukion oppimäärän täyttävät asiat, jotka ennen peruskoulun aikaa kuuluivat keskikoulun oppisisältöihin ja jotka tuolloin voitiin lukiossa ja ammatillisessa koulutuksessa olettaa oppilaan omaksumaksi tiedoksi, jonka varaan sitten oli mahdollista rakentaa lisää. Nykyinen lukion opetussuunnitelma ja sen realisaatiot pyörivät paljolti näissä perusasioissa, ja pitemmälle menevän tiedon esittämiselle ja erityisesti sen omaksumiselle jää valitettavan vähän aikaa.

Tässä valpas lukija esittää vastaväitteen: entä PISA-tutkimus ja sen tuottama korkeatasoisen opetuksen maailmanmaine? PISAan perehtyneet tietävät, että PISA ei oikeastaan millään tavalla mittaa sitä matematiikan ymmärrystä ja osaamista, joka matematiikan opetuksen tavoitteena on kautta aikojen ollut niin Suomessa kuin muuallakin. Ei ole tietenkään syytä vähäksyä hyvää PISA-menestystä. Se osoittaa, että tutkimusotokseen valikoituneet suomalaisnuoret osaavat lukea ja jossain määrin myös ymmärtää lukemaansa. Hieno juttu, noin yleiseltä kannalta, mutta matematiikka on olennaisesti muuta. Samoin matematiikan soveltaminen kaikkiin niihin reaalitieteisiin, joiden rakennus olennaisesti lepää matematiikan perustalla.

Toisaalla tässä lehdessä esitellään lukion opetussuunnitelman ongelmakohtia. Voimassa olevien opetussuunnitelmien synty oli erikoinen: opetussuunnitelmaluonnos muuttui prosessin aikana suuntaan jos toiseenkin, kunnes viranomaispäätökseksi tuli opetussuunnitelma, jonka saattoi aavistella olevan vähintään ongelmallinen. Nyt kun opetussuunnitelmaa on muutama vuosi käytännössä kokeiltu, pelot ovat osoittautuneet aiheellisiksi.

Opetussuunnitelma on iso juttu. Siihen liittyy monenlaista työtä ja intressiä, ei vähiten oppikirjankustannusliiketoiminnan kannalta. Opetussuunnitelman tulisi olla stabiili. Suunnitelmia onkin muuteltu vain melko pitkien aikojen välein. Mutta kun ilmeisiä virheitä on tapahtunut, ne tulisi korjata. Jos toisessa vaakakupissa ovat kustantamojen intressit ja toisessa oppilaat ja suomalainen osaaminen, ei ole vaikeata päättää mitä on tehtävä. Eikö niin, Opetusministeriö ja Opetushallitus?

Matti Lehtinen **Pääkirjoitus**



Pitkän matematiikan opetussuunnitelmat kriittisessä tarkastelussa

Matti Lehtinen
Maanpuolustuskorkeakoulu

Nykyisin voimassaolevat lukion opetussuunnitelman perusteet on annettu käyttöön Opetushallituksen määräyksellä 33/011/2003, ja ne astuivat voimaan 1.8.2005. Kun lukion oletuskesto on kolme vuotta, niin nyt alkaa täyttyä aika, jonka kuluessa uutta opetussuunnitelmaa on sovellettu yhteen lukioikäluokkaan ja kokemuksia on saatu. Solmunkin ympärillä on käyty keskustelua näistä kokemuksista. Referoin tässä kirjoituksessa ennen kaikkea Mäntän lukion lehtorin Markku Halmetojan ja Kiimingin lukion lehtorin Maisa Spangarin esittämiä ajatuksia matematiikan pitkän oppimäärän opetussuunnitelmista. Myös muiden esittämiä mielipiteitä esiintyy joukossa.

Matematiikan pitkän ja lyhyen oppimäärän tavoitteilla on olennainen ero: jälkimmäinen on yleissivistystä ja kansalaistaitoa, mutta pitkällä matematiikalla luodaan edellytyksiä jatko-opinnoille aloilla, joissa matematiikalla on merkittävä osuus. Pitkän matematiikan suorittaneiden määrää on koetettu lisätä helpottamalla kursseja ja alentamalla ylioppilastutkinnon rimaa. Näin saatu määrällinen voitto on kuitenkin laadussa hävitty. Mahdollisuus läpäistä pitkän matematiikan ylioppilaskoe todella vaatimattomin suorituksin syö järjestelmän uskottavuutta.

Molemmat opettajat korostavat sitä, että matematiikka on yhtenäinen, peruskoulusta lukioon jatkuva oppiaine. Peruskoulun asia olisi opettaa perusasiat, luvuilla, myös murtoluvuilla laskeminen, ei vain mekaanisina temppuina, vaan ymmärrys mukana. Ei olisi pahaksi, jos peruskoulu opettaisi kunnolla rationaalilausekkeiden käsittelyn ja geometrian perusteet. Yksi ehdoton vaatimus olisi matematiikan saaminen aineenopettajan hoitoon jo nykykäytäntöä aikaisemmin. Spangarin mielestä peruskoulun matematiikanopetus keskittyy vain ja ainoastaan mekaaniseen laskentoon, ilman käsitystä itse matematiikasta. Näin saattaa käydä, että peruskoulussa hyvinkin menestynyt oppilas saattaa kohdata lukion oppimäärän ja vaatimattomankin tason shokkina.

Opettajien mielestä nykyinen opetussuunnitelma harrastaa monissa paikoin haitallista oppimisen myöhentämistä. Esimerkiksi rationaalilausekkeiden ja -yhtälöiden algebran oppiminen jää differentiaalilaskennan kurssiin, joka puolestaan merkitsee sitä, että analyysin perusasioille kuten raja-arvoille ja erotusosamäärille jää liian vähän aikaa. Samoin on laita logaritmin: sitä ei suinkaan käsitellä loogisessa yhteydessään eksponenttifunktion kera, vaan vasta kurssilla 8, ja ajasta tulee pula taas. – Samanlaista opetuksen myöhentämistä on tapahtunut myös peruskoulussa, ja tämä osin selittää peruskoulusta lukioon tulevien matematiikan osaamisvajautta. Mikä peruskoulussa kaiken kaikkiaan mättää, on laaja kysymys, jonka selvittely ei kokonaisuudessaan ole tässä mahdollista.

Halmetoja keräisi kaikki keskeiset työkaluluontoiset algebralliset asiat lukion kahteen ensimmäiseen kurssiin:

tällöin myöhempiin, käsitteellisempiin asioihin perehtyminen olisi luontevampaa.

Trigonometrian jakautuminen kursseihin 3 ja 9 on Halmetojan mielestä luonnotonta: mitään syytä pantata trigonometristen funktioiden yleistä määrittelyä yksikköympyrän avulla tai Pythagoraan lauseen trigonometrista versiota kurssiin 9 saakka ei ole. Geometrian kurssi lähes väistää geometrian ja matematiikan keskeistä sisältöä, todistamista.

Analyyttisen geometrian ja vektoriopin sisältävät kurssit olisi Halmetojan ja Spangarin mielestä syytä vaihtaa toiseen järjestykseen: monet analyyttisen geometrian asiat olisivat kovasti helpompia, jos vektoriajattelun ja -tekniikan geometria olisi jo käytössä. Ja perin suotavaa olisi tiedonjako kartioleikkauksistakin – jos analyyttisen geometrian kurssin lineaariyhtälöryhmäosuus siirrettäisiin vektorikurssiin, tilaa saataisiin. Lineaaristen yhtälöiden ratkaisun teoria on joka tapauksessa ymmärrettävissä geometrian avulla.

Todennäköisyyslaskentakurssi 6 tuo mukanaan jatkuvatkin jakaumat, vaikka niiden käsittelyn olennaisin työkalu, integraalilaskenta, opetetaan vasta kurssissa 10. Todennäköisyyskurssi voisi keskittyä diskreettiin todennäköisyyslaskentaan ja hakea synergiaa myös mekaniikan (painopiste, hitausmomentti) ja todennäköisyyslaskennan (odotusarvo, varianssi) analogioista.

Kurssin 7 oikea nimi olisi Differentiaalilaskenta eikä derivaatta. Nykyisen opetussuunnitelman linjausten mukaan kaikki edelliset kurssit ovat helpohkoja, mutta tässä kurssissa ollaan sitten totuuden edessä. Halmetojan ja Spangarin näkemyksen mukaan tähän kurssiin ei olisi tarpeen enää sisällyttää työkaluna rationaalilausekkeiden algebraa, joka olisi käsitelty jo kurssissa 2. Sen sijaan derivaatan olemus ja merkitys muutosnopeutena olisi selvästi tuotava esiin jo opetussuunnitelmassa.

Kurssin 8 kevennykseksi koituisi logaritmin ensiesittely aikaisemmin. Kurssiin 9 olisi helposti liitettävissä tärkeimpien trigonometrian kaavojen johto, lähtökohtana vektorien $(\cos x, \sin x)$ ja $(\cos y, \sin y)$ pistetulosta suoraan saatava $\cos(x - y) = \cos x \cos y + \sin x \sin y$. Lukujonojen ja sarjojen käsittely eri kursseissa (9 ja 13) ei ole onnistunut ratkaisu.

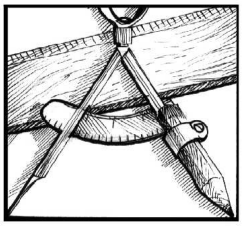
Kurssin 10, Integraalilaskenta, oppisisältöihin olisi saatava eksplisiittisesti keskeisten ympyrään ja palloon liittyvien pinta-ala- ja tilavuuskaavojen johto.

Kurssi 11, Lukuteoria ja logiikka, tulisi sijoittaa ensimmäisen opiskeluvuoden kurssiksi. Sen sisältöihin tulisi lisätä induktio.

Kurssin 12 sisältöihin tulisi ehdottomasti lisätä kompleksiluvut. Sen sijaan numeerinen derivointi on tässä turha sisältö.

Kurssin 13, differentiaali- ja integraalilaskennan jatkokurssin, sisältöihin olisi liitettävissä raja-arvon täsmällinen määrittely epäyhtälön $|f(x) - a| < \epsilon$ ratkaisua tarkastelemalla.

Matematiikka on oma oppiaineensa, eikä sen opetus, ainakaan pitkän matematiikan opetus, välttämättä onnistu opettajalta, joka on hankkinut pätevyytensä luonnontieteiden parissa, ympäristössä, jossa matematiikka on ollut tarvittavan laskennon aputiede. Hyvään opetukseen ei riitä oppikirjojen kattavien opettajamateriaalien kopioiminen oppilaiden eteen. Opetussuunnitelman puutteet antavat erittäin suuren merkityksen opettajan ammattitaidolle ja omalle aineentuntemukselle.



Ruprecht von der Pfalzin probleema

Simo K. Kivelä

Ruprecht von der Pfalz oli 1600-luvulla elänyt saksalais-englantilainen prinssi. Isä oli saksalainen kuningas Fredrik V, äiti Englannin kuninkaan Jaakko I:n tytär. Ruprecht eli nuoruutensa maanpaossa Hollannissa, myöhempinä vuosinaan osallistui eri tavoin vuosisadan levottomuuksiin, ennen muuta Englannissa tasavaltalaisten ja kuningasmielisten välisiin taisteluihin. [1]

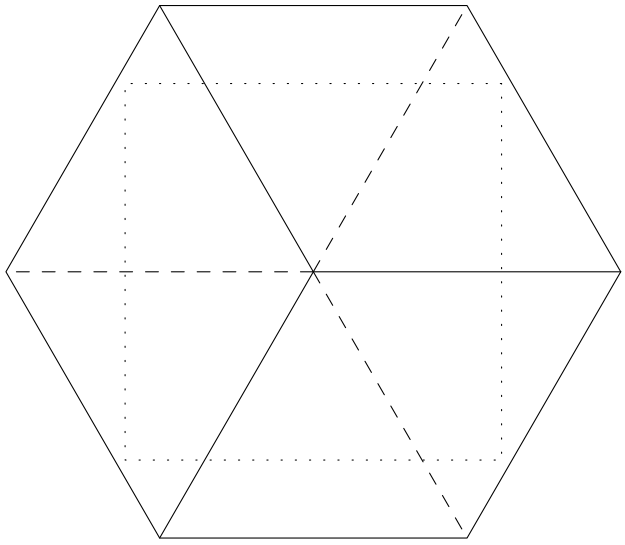
Sotajoukkojen johtamisen ohella Ruprecht oli kiinnostunut myös taiteista ja luonnontieteiden tutkimisesta. Hänen nimensä on jäänyt elämään *Ruprecht von der Pfalzin probleemassa*:

Millainen reikä on työstettävä (massiiviseen) kuutioon, jotta siitä voidaan työntää läpi toinen samankokoinen kuutio?

Ensi näkemällä tuntuu siltä, että probleemalla ei voi olla ratkaisua. On kuitenkin melko helppoa osoittaa, että ratkaisu on olemassa.

Ratkaisun olemassaolo

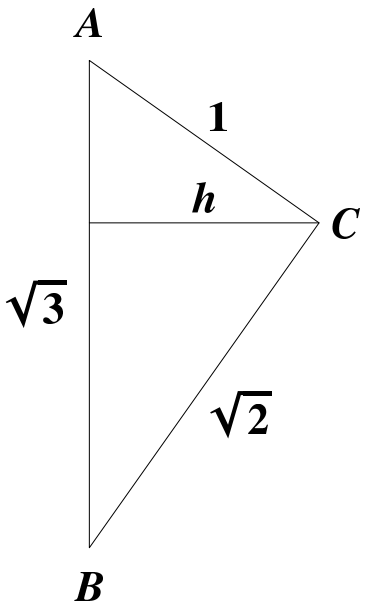
Asetetaan kuutio seisomaan kärjelleen vaakasuoralle tasolle. Tällöin vastakkainen kärki on täsmälleen seisontakärjen yläpuolella, ja jos kuutio projisioidaan yhdensuuntaisprojektiolla kohtisuoraan vaakasuoralle tasolle, sen ääriviiva on säännöllinen kuusikulmio. (Kuva 1.)



Kuva 1: Kärjellään seisova kuutio päältä nähtynä. Alapuolella olevat särmät katkoviivoilla. Pisteviivoilla piirretty neliö on toinen samankokoinen kuutio, joka lepää sivutahkonsa varassa.

Sivusta katsottuna kuution oikea puolisko on kuvan 2 mukainen. Piste A on kuution ylin ja B sen alin kärki, AC on kuution särmä, jonka pituudeksi yksinkertaisuuden vuoksi oletetaan 1. Jana BC on kuution sivutahkon lävistäjä ja siis pituudeltaan $\sqrt{2}$. Kuution avaruuslävistäjän AB pituus on $\sqrt{3}$. Koska kolmio ABC on suorakulmainen, voidaan korkeusjanan pituus helposti laskea: $h = \sqrt{\frac{2}{3}}$. Tämä on kuvan 1 kuusikulmion ympäri piirretyn ympyrän säde.

Simo Kivelä on Teknillisen korkeakoulun eläkkeellä oleva matematiikan lehtori. Hänen sähköpostiosoitteensa on `simo.kivela@tkk.fi`.



Kuva 2: Kärjellään seisovan kuution oikean puoliskon leikkaus. Pisteet A ja B ovat ylin ja alin kärki, piste C äärimmäinen kärki oikealla.

Kuvassa 1 pisteviivalla piirretty neliö esittää kuutiota, joka lepää vaakasuoralla tasolla yhdellä sivutahkollaan ja jonka särmän pituus on myös 1. Kun kuusikulmion ympäri piirretyn ympyrän säde h tunnetaan, on helppoa laskemalla todeta, että neliö sopii kuusikulmion sisään. Jos siis alkuperäiseen kuutioon työstetään lävistäjän AB suunnassa poikkileikkaukselta neliönmuotoinen reikä, jossa neliön sivun pituus on 1, voidaan tästä reiästä työntää läpi toinen samankokoinen kuutio.

Reiällisen kuution havainnollistaminen geometrisesti

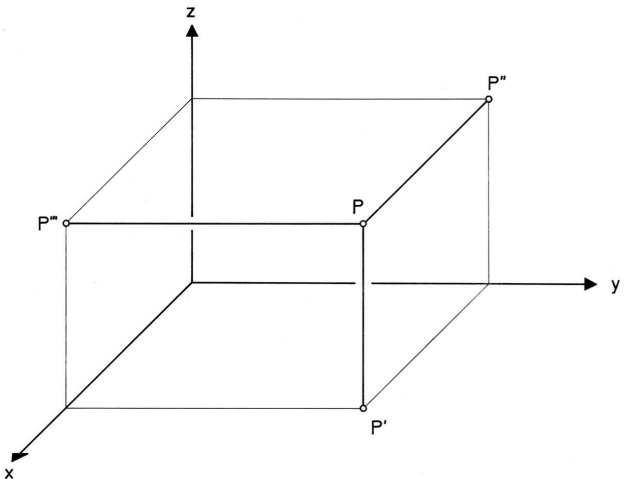
Vaikka kuva 1 esittääkin kuutiota ja siihen työstettyä reikää sopivasta suunnasta katsottuna, ei kuvan perusteella ole aivan helppoa päätellä, miltä reiällinen kuutio oikeastaan näyttää. Voidaan myös kysyä, voitaisiinko reikä työstää jossakin muussakin kuin lävistäjän suunnassa.

Havainnollisia kuvia voidaan muodostaa periaatteessa kahdella tavalla. Perinteinen — jo muutamia vuosisatoja vanha — menettely perustuu sopivan yhdensuuntaisprojektiokuvan konstruoimiseen *deskriptiivisen geometrian* menetelmillä. Modernimpi vaihtoehto on tietotekniikan hyödyntäminen, jolloin luontevin työkalu on jokin kolmiulotteisen geometrian käsittelyyn sopiva ohjelmisto. Tällaisia ovat monet ns. matemaattiset laskentaohjelmistot, mutta myös teollisuuden suunnittelutehtävissä käytettävät CAD- (Computer Aided Design) ohjelmistot, joissa monien muiden ominaisuuksien ohella on työkalut geometristen konstruktioiden tekemiseen.

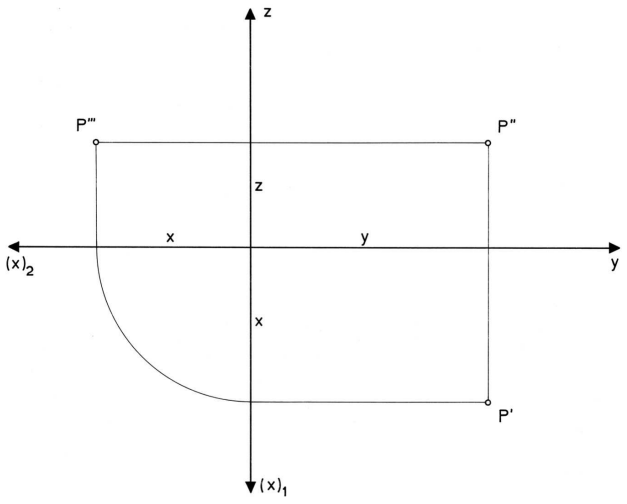
Mongen projektio, deskriptiivisen geometrian perustyökalu

Gaspard Monge oli Napoleonin aikalainen, upseeri ja matemaatikko, joka osallistui Napoleonin sotaretkiin ja kehitti sotilaallista käyttöä varten geometriset suunnittelumenetelmät, jotka kantavat hänen nimeään. Hän loi nämä jo ennen Ranskan vallankumousta, mutta ne olivat sotasalaisuuksia ja julkaistiin vasta joitakin vuosia vallankumouksen jälkeen. [2, 3]

Mongen projektiossa kohde – geometrinen tilanne, kappale, suunniteltava esine tai laite – projisioidaan yhdensuuntaisprojektiolla kohtisuorasti toisaalta xy-tasoon, toisaalta yz-tasoon. Edellistä kutsutaan *perus-*, jälkimmäistä *pystyprojektioksi.* Kolmantena voi olla kohtisuora projektio xz-tasoon (*sivuprojektio*), mutta tätä harvoin tarvitaan. (Kuva 3.)

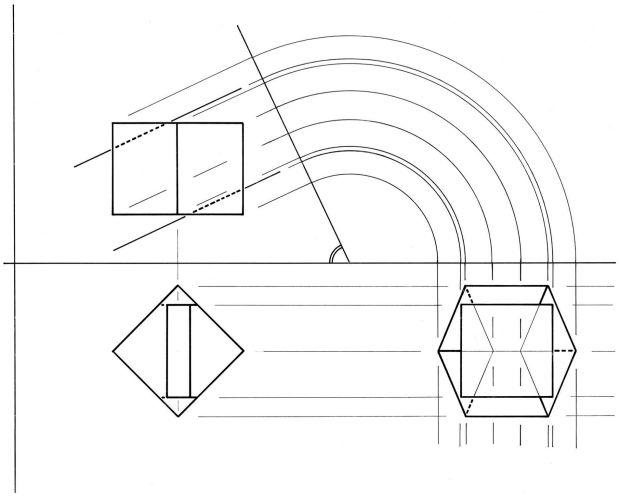


Kuva 3: Mongen projektion syntyminen.



Kuva 4: Mongen projektion perus-, pysty- ja sivuprojektio.

Kaikki kolme projektiota esitetään samassa tasossa (piirustuspaperin tasossa) siten, että perusprojektio käännetään y-akselin ympäri ja sivuprojektio z-akselin ympäri yz-tasoon, jolloin syntyy kuvan 4 mukainen tilanne. Tässä on esitettynä vain yhden pisteen projektiot, mutta isommat kohteet projisioidaan periaatteessa pisteittäin.



Kuva 5: Ruprecht von der Pfalzin probleeman ratkaisu Mongen projektiossa.

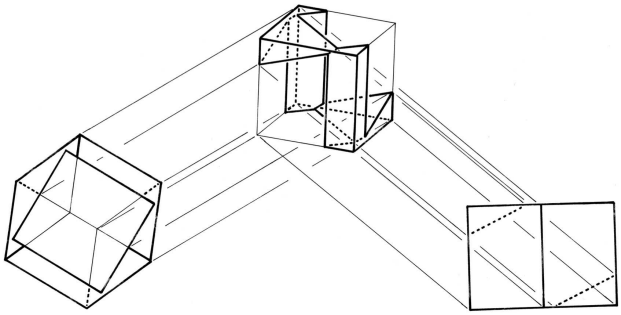
Kuvassa 5 on Ruprecht von der Pfalzin probleema ratkaistuna Mongen projektiossa. Alkuperäinen kuutio näkyy perusprojektiossa 45° kierrettynä. Pystyprojektiossa näytetään, miten kuutio projisioidaan kohtisuorasti kaltevalle tasolle. Tämän kaltevuuskulmaa voidaan helposti muuttaa eikä se kuvassa olekaan sellainen, että projisiointisuunta olisi sama kuin kuution lävistäjän suunta. Kalteva taso leikkaa xy-tasoa pitkin x-akselin suuntaista suoraa ja se kierretään xy-tasoon tämän suoran ympäri. Tällöin perusprojektion puolelle saadaan näkyviin kuution projektio kaltevaan tasoon. Tämän sisään mahtuu neliö, jonka sivu on yhtä pitkä kuin kuution särmä. Näin on osoitettu, että valitussa suunnassa kuutioon voidaan työstää reikä, josta samankokoinen kuutio mahtuu läpi. Viitteessä [4] on sama ratkaisu Java-sovelmana.

Havainnollista kuvaa reiällisestä kuutiosta ei tässäkään ole saatu. Käytettävissä on kuitenkin kolmekin yhdensuuntaisprojektioprojektiokuvaa reiällisestä kuutiosta.

Schmidin–Eckhartin menetelmä

Havainnollinenkin kuva kuutiosta on mahdollista saada suhteellisen yksinkertaisella piirtämismenettelyllä.

1900-luvun alkupuolella itävaltalaiset Th. Schmid ja L. Eckhart esittivät menetelmän, jolla kohteen kahden projektiokuvan perusteella voidaan muodostaa uusi yhdensuuntaisprojektiokuva kohteesta. Lähtökohtana olevat projektiokuvat asetetaan piirustustasoon sopivaan asemaan ja kumpaakin kuvaa varten valitaan kiinteä suunta; nämä eivät saa olla yhdensuuntaiset. Tietyn pisteen kuvapiste uudessa kuvassa saadaan asettamalla suuntien mukaiset suorat alkuperäisten kuvien vastinpisteiden kautta ja määrittämällä näiden leikkauspiste. Uusi kuva voidaan tällä tavoin piirtää piste pisteeltä.



Kuva 6: Ruprecht von der Pfalzin probleeman ratkaisu Schmidin–Eckhartin menetelmällä laadittuna.

Lähtökohtana olevat kuvat voidaan periaatteessa asettaa mihin tahansa asemaan ja suunnat valita miten tahansa. Tuloksena syntyy yleensä uusi yhdensuuntaisprojektiokuva kohteesta; erikoistapauksessa se voi litistyä suoraksi. Kuva voi kuitenkin liittyä niin vinoon yhdensuuntaisprojektioon (jossa projektiosäde ei ole kohtisuorassa kuvatasoa vastaan), että se ei ole kovin havainnollinen. Sopivien asemien ja suuntien määrittämiseen on kuitenkin olemassa menetelmät.

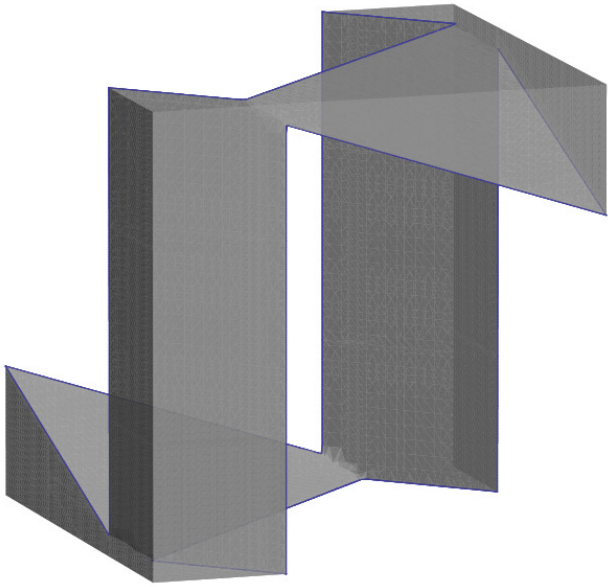
Kuva 6 esittää reiällisen kuution kuvan konstruoimisen lähtemällä kahdesta Mongen projektion avulla saadusta projektiokuvasta.

Tarkempia tietoja Schmidin–Eckhartin menetelmästä, joka saksaksi tunnetaan nimillä *Einschneideverfahren* ja *Schnellrißverfahren*, on löydettävissä viitteistä [6, 5]. Jälkimmäisessä on Java-sovelma, jolla asetteluja ja suuntia voidaan muuttaa.

Reiällisen kuution havainnollistaminen laskemalla

Edellä esitetty menettely on luonteeltaan geometrinen, piirtämiseen perustuva. Tietotekniikan käyttö on pikemminkin algebrallista, usein varsin vaativaan laskemiseen perustuvaa.

Kuva 7 esittää Ruprecht von der Pfalzin probleeman ratkaisua, joka on laskettu ja piirretty laskentaohjelma Mathematicalla [7].



Kuva 7: Mathematicalla tehty Ruprecht von der Pfalzin probleeman ratkaisu.

Kuvaa varten laadittu koodi on annettu alla. Kuutio on tällöin asetettu siten, että sen keskipiste on origossa, särmät akseleiden suuntaisia ja särmän pituus = 2.

```
n = {1, 1, a}; h = {1, 1, 0};
rtk = Solve[ArcCos[n.h/Sqrt[n.n]/Sqrt[h.h]]
   == 25 Degree, a] // N;
n = n/Sqrt[n.n] /. rtk[[2]];
k = {0, 0, 1};
ex = Cross[k, n]; ex = ex/Sqrt[ex.ex];
ey = Cross[n, ex];
rtk = Solve[{x, y, z}
   == a ex + b ey + c n, {a, b, c}];
reika = Max[Abs[a], Abs[b]] /. rtk[[1]];
kuutio = Max[Abs[x], Abs[y], Abs[z]];
kuva1 = ContourPlot3D[reika == 1,
   {x, -2, 2}, {y, -2, 2}, {z, -2, 2},
   RegionFunction -> Function[{x, y, z},
      kuutio <= 1],
   Mesh -> None,
   BoundaryStyle -> Automatic,
   ContourStyle -> Opacity[0.8],
   Lighting -> "Neutral",
   ColorFunction -> Function[{x, y, z},
      GrayLevel[0.5]]];
kuva2 = ContourPlot3D[kuutio == 1,
   {x, -2, 2}, {y, -2, 2}, {z, -2, 2},
   RegionFunction -> Function[{x, y, z},
      reika >= 1],
   Mesh -> None,
   BoundaryStyle -> Automatic,
   ContourStyle -> Opacity[0.8],
   Lighting -> "Neutral",
   ColorFunction -> Function[{x, y, z},
   GrayLevel[0.5]]];
ruprkuva = Show[kuva1, kuva2, Boxed -> False,
   Axes -> None, ImageSize -> 600,
   ViewPoint -> {-30, 10, 6}]
```

Koodin muuttujien merkitykset ovat seuraavat:

- Vektori $\vec{n}$ ilmoittaa työstettävän reiän suunnan. Parametri a on määrätty siten, että kaltevuuskulma vaakatasoon (vektori $\vec{h}$) nähden on 25°.
- Vektorit $\vec{e}_x$ ja $\vec{e}_y$ ilmoittavat reiän poikkileikkausneliön sivujen suunnat. $\vec{e}_x$, $\vec{e}_y$ ja $\vec{n}$ ovat yksikkövektoreita. $\vec{k}$ on pystysuora vektori, jota tarvitaan näiden laskemisessa.
- Kuution pinta määritellään yhtälöllä $\max\{|x|,|y|,|z|\} = 1$. Vastaavalla tavalla määritellään työstettävän reiän pinta muodossa $\max\{|a|,|b|\} = 1$, missä muuttujille a ja b on ensin laskettu lausekkeet (jälkimmäinen muuttuja `rtk`).
- Muuttuja `kuva1` esittää työstettävän reiän pintaa niiltä osin kuin se sijaitsee kuution sisällä ja `kuva2` kuution pinnan niitä osia, jotka jäävät jäljelle, kun reikä on työstetty. Yhdistämällä nämä muuttujaan `ruprkuva` saadaan kuva 7.

Viitteet

[1] Ruprecht von der Pfalz, Herzog von Cumberland, `http://de.wikipedia.org/wiki/Ruprecht_von_der_Pfalz,_Herzog_von_Cumberland` (saks.)

[2] Gaspard Monge, `http://www-groups.dcs.st-and.ac.uk/~history/Biographies/Monge.html` (engl.)

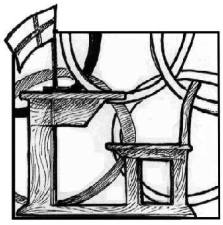
[3] Gaspard Monge, `http://www.bibmath.net/bios/index.php3?action=affiche&quoi=monge` (ransk.)

[4] Simo Kivelä, Ruprecht von der Pfalzin probleema, Cabri-Geometriaan pohjautuva Java-sovelma, `http://matta.hut.fi/matta2/cabri/ruprecht.html`

[5] Hermann Vogel, Allgemeines Einschneideverfahren, `http://www-m10.ma.tum.de/~vogel/KG_Metall_Bau/Daten/Einschnitt_a.html` (saks.)

[6] Walter Wunderlich, Darstellende Geometrie II, 234 s., Hochschultaschenbücher, Bibliographisches Institut AG, Mannheim, 1967 (saks.)

[7] Mathematica, laskentaohjelma, `http://www.wolfram.com/`



Montessori ja Varga-Neményi -opetustyyleistä

Marjatta Näätänen
Matematiikan ja tilastotieteen laitos
Helsingin yliopisto

Solmuun on jo vuosia kerätty tiedostoja unkarilaisesta Varga-Neményi -alkuopetusmenetelmästä. Tänä vuonna on saatu myös tiedostoja Maria Montessorin opetustyylistä. Tässä kirjoituksessa verrataan lyhyesti näitä kahta toisiinsa. Kiitän asiantuntevista kommenteista Outi Suorttia ja Anni Lampista.

Molemmat matematiikan alkuopetustyylit sisältävät paljon samoja aineksia: kaikkien aistien ja hienomotoriikan harjoittaminen, fyysinen aktiivisuus, ikäkauden mahdollisuuksien huomioiminen, runsas ja harkittu apuvälineiden käyttö. Apuvälineiden käytössä Montessori oli edelläkävijä, hänen työtään erityisesti värisauvojen käytön suhteen jatkoi Cuisenaire. Montessorilla sauvoilla on ominaisuutena niiden pituus, Georges Cuisenaire laajensi sauvojen käyttöä neljän peruslaskutoimituksen havainnollistamisesta murtolukujen, pinta-alan, tilavuuden ja neliöjuuren havainnollistamiseen sekä yhtälöiden ratkaisemiseen. Caleb Gattegno kehitti ja levitti näitä ideoita ja Varga seurasi tätä käytäntöä, joten värisauvojen käytön suhteen on eroja.

Montessoriopetuksessa siirrytään sauvoista helmimateriaaliin. Niillä lasketaan peruslaskutoimitukset, paitsi jakolaskua, jolle on omat välineensä. Helmillä voidaan laskea neliöitä, kuutioita, peruslaskutoimituksia eri lukujärjestelmillä, havainnollistaa murto- ja desimaalilukuja. Montessorin opetuksessa tutustutaan suuriin lukuihin jo esikouluiässä ja keskitytään peruslaskutoimitusten hallintaan myös suurilla luvuilla. Varga-Neményi -opetuksessa pohjustetaan matematiikan perusteita pitkään pienellä lukualueella, 1. luokalla lukualue on 0 - 20 ja 2. luokalla 0 - 100. Jo alkuvaiheessa hankitaan kokemuksia myös muista kuin kymmenjärjestelmästä.

Unkarilaisilla on toisena perusvälineenä loogiset palat logiikan harjoittamista varten.

Montessorin välineet ovat hienostuneita ja materiaalit houkuttelevat koskettamaan niitä, unkarilaisten voivat olla halpoja jokapäiväisiä esineitä, vaikka munakennoja ja papuja. Myös Montessorissa on tarjolla jokapäiväisiä esineitä matematiikkapelien nimellä. Kumpikin tyyli käyttää etenemistä konkreettisesta, omasta kokemuksesta lähtien matematiikan käsitteitä pohjustaen. Perustana on usko siihen, että lapsella on oma rajaton valmius ja halu oppia ja tätä omaa keksimistä tuetaan.

Montessori korostaa varsinkin alussa yksittäistä, hiljaista työskentelyä. Tehtäviä tehdään myös usein pareittain tai pienissä ryhmissä, tai lapset vain seuraavat pidemmälle ehtineen lapsen työskentelyä. Unkarilaisessa tyylissä korostetaan asiasta puhumista, opettajan johdattelemaa keskustelua ja usein jokaisella lapsella on käytössään samanlaiset välineet yhtä aikaa ja koko luokka on mukana samassa toiminnassa. Montessori ei käytä kotitehtäviä, unkarilaiset käyttävät.

Aina, kun mahdollista, harjoitellaan Varga-Neményi -menetelmässä kumpaankin suuntaan menemällä; esi-

merkiksi kerro kuvasta, tee laskutehtävä – kääntäen, lähtemällä laskutehtävästä oppilas tekee siihen sopivan kuvan tai asetelman. Apuvälineiden käyttö päätyy asian esittämiseen ”matematiikan kielellä”.

Maria Montessorin esittämä käsitys oppimisesta ja hänen pedagogiansa opetustyyli olivat jo vuosisadan alussa samankaltaiset kuin parikymmentä vuotta myöhemmin aloittaneen Vygotskin. Unkarilainen opetustyyli sai vaikutteita Vygotskiltä – kuten lähteminen lapsen lähiympäristöstä ja tästä laajentaen.

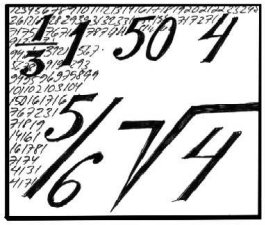
Välineiden suunnitelmallisen käytön avulla lapsi etenee matematiikan oppimisessa kuin valmista polkua kulkien. Hän voi myös palata aikaisempiin välineisiin, jos lisäharjoittelua tarvitaan.

Seuraavassa on Solmuun kerättyjä tiedostoja Maria Montessorin opetustyylistä:

Numerossa 1/2008 ilmestynyt kirjoitus Maria Montessorista:
`http://solmu.math.helsinki.fi/2008/1/montessori.pdf`

Yleisesitys Montessori-opetustyylistä:
`http://solmu.math.helsinki.fi/2008/montessori/montessorikasvatuksen_olemuksesta.pdf`

Geometrian peruskäsitteiden opettamiseen keskittyvä esitys Montessori-opetustyylistä:
`http://solmu.math.helsinki.fi/2008/montessori/montessorikasvatuksen_olemuksesta_geometria.pdf`



Onko $\sqrt{-1}$ olemassa? Keskipituinen kertomus lukujen olemuksesta, 2. osa

Antti Valmari
Ohjelmistotekniikan laitos
Tampereen teknillinen yliopisto

Tiivistelmä

Tämän kirjoituksen tavoitteena on kertoa lukujen olemuksesta ja matemaattisen määrittelemisen luonteesta tavallista helppotajuisemmin. Kirjoituksessa pohditaan muun muassa, miksi $\frac{1}{0}$ ei ole luku, mutta $\sqrt{-1}$ on. Myös selviää, miksi uusien lukujen keksiminen on loppunut kompleksilukuihin.

Nollan käänteisarvo

Nyt kun vähennyslasku on määritelty siten, että jokainen vähennyslasku on laskettavissa, on luonnollista yrittää tehdä sama jakolaskulle. Tunnetusti ykkönen on kertolaskun suhteen samankaltaisessa roolissa kuin nolla yhteenlaskun. Olemme jo muotoilleet tämän lakina (8): ”On olemassa luku 1 siten, että jokaisella luvulla a pätee $a \cdot 1 = a$”. Lakia täytyy kuitenkin täydentää ehkä yllättävällä vaatimuksella:

(11) $1 \neq 0$

Tämä on todellakin tarpeen vaatia! Nimittäin järjestelmä, jossa on vain yksi olento 0 toteuttaa kaikki lait (1), ..., (10) ja jatkossa annettavat lait (12), ..., (17). Siinä kaikki laskutoimitukset tuottavat saman tuloksen 0.

Seuraava yhteenlaskua matkiva askel olisi julistaa, että jokaista lukua a kohti on olemassa luku $\frac{1}{a}$ siten, että $a \cdot \frac{1}{a} = 1$. Kuten hyvin tiedetään, matemaatikot ovat kuitenkin rajanneet nollan pois tästä säännöstä:

(12) Jos $a \neq 0$, niin on olemassa luku $\frac{1}{a}$ siten, että $a \cdot \frac{1}{a} = 1$.

Miksi $\frac{1}{0}$ eli nollan käänteisarvo on jätetty pois? Olemme oppineet, että matemaatikko saa määritellä uusia olentoja ihan niinkuin haluaa, eikä ole tarpeen miettiä, ovatko ne ”oikeasti” olemassa. Eikö nollan käänteisarvo voitaisi ottaa mukaan ihan vain julistamalla, että sekin on olemassa? Päästäisiin eroon siitä riesasta, että nollalla ei saa jakaa!

Nollan käänteisarvo voidaan ottaa käyttöön, jos halutaan. Valitettavasti seuraukset ovat ikäviä. Nollan käänteisarvo on olento $\frac{1}{0}$ siten, että $0 \cdot \frac{1}{0} = 1$. Käyttämällä tätä lakia, kertolaskun liitännäisyyttä sekä kokonaislukujen ominaisuuksia $2 \cdot 0 = 0$ ja $2 \cdot 1 = 2$ saadaan $1 = 0 \cdot \frac{1}{0} = (2 \cdot 0) \cdot \frac{1}{0} = 2 \cdot (0 \cdot \frac{1}{0}) = 2 \cdot 1 = 2$. Tätä ei voida hyväksyä, koska se muuttaisi tavallisten lukujen

ominaisuuksia. Kakkonen ei ole ykkönen! Koska tavallisten lukujen lakeja ei saa muuttaa, niin ei ole muuta keinoa saada $0 \cdot \frac{1}{0} = 1$ voimaan kuin luopua kertolaskun liitännäisyydestä silloin, kun laskussa on mukana $\frac{1}{0}$. Tässä tapauksessa siis $(2 \cdot 0) \cdot \frac{1}{0} \neq 2 \cdot (0 \cdot \frac{1}{0})$.

Tämä harmillinen tulos voidaan esittää myös jakolaskun lakien rikkoutumisena $\frac{2 \cdot 0}{0} \neq 2 \cdot \frac{0}{0}$. Säännöstä "nollalla ei saa jakaa" päästiin eroon, mutta nollalla jakamiseen pitää soveltaa eri lakeja kuin muihin jakolaskuihin. Siis nollalla jako pitää silti käsitellä erikoistapauksena. Tavoiteltu hyöty jäi saamatta.

Eivätkä ongelmat lopu tähän. Olkoon x mikä tahansa luku. Lakien (9), (2) ja (7) nojalla saadaan $x \cdot 1 = x \cdot (1 + 0) = x \cdot (0 + 1) = x \cdot 0 + x \cdot 1$. Lisäämällä molemmille puolille $-(x \cdot 1)$ ja soveltamalla lakeja (10), (3), (10), (9) ja (5) saadaan $0 = x \cdot 1 + (-(x \cdot 1)) = (x \cdot 0 + x \cdot 1) + (-(x \cdot 1)) = x \cdot 0 + (x \cdot 1 + (-(x \cdot 1))) = x \cdot 0 + 0 = x \cdot 0 = 0 \cdot x$. Siis $0 \cdot x = 0$. Tämäkin on ristiriidassa tavoitteen $0 \cdot \frac{1}{0} = 1$ kanssa. Tässä laskussa ei käytetty kertolaskun liitännäisyyttä, joten jokin toinenkin laki on uhrattava, jotta $0 \cdot \frac{1}{0} = 1$ saadaan voimaan.

Nollan käänteisarvo $\frac{1}{0}$ ei siis ole samanlainen hyödyllinen kiltti apulainen kuin negatiiviset luvut, vaan pahantapainen olento, joka rikkoo ainakin kahta rationaalilukujen noudattamaa lakia eikä tuo sitä hyötyä, jota varten se kutsuttiin mukaan. On parempi potkaista se ulos. Niin matemaatikot ovat tehneet. Jos jossakin on sovelluksia, joissa nollan käänteisarvon ominaisuudet ovat enemmän hyödyksi kuin haitaksi, niin siellä sen voi ja kannattaa ottaa käyttöön. Se käyttäytyy kuitenkin niin eri tavalla kuin tavalliset luvut, että silloinkin on parempi olla kutsumatta sitä luvuksi.

Esimerkiksi raja-arvojen yhteydessä käytetään usein olentoja ∞ ja $-\infty$, jotka voitaisiin ajatella nollan käänteisarvoksi ja sen vastaluvuksi. Jos niille määritellään yhteenlasku, niin se tehdään yleensä niin, että jos a on reaaliluku, niin $a + \infty = \infty + a = \infty$ ja $a + (-\infty) = (-\infty) + a = -\infty$. Mutta tällöin $(1 + \infty) + (-\infty) = \infty + (-\infty) = 0$ ja $1 + (\infty + (-\infty)) = 1 + 0 = 1$, joten liitännäisyyslaki ei päde. Liitännäisyyslaki on niin tärkeä laki, että matemaatikot luopuvat mieluummin laista (1) kuin siitä. Ei siis yleensä määritellä, että $-\infty$ on ∞:n vastaluku, vaan että $\infty + (-\infty)$ ei ole määritelty.

Edellä on puhuttu nollan käänteisarvosta ikäänkuin se olisi yksikäsitteinen, ennalta määrätty olento. Sen tarkka luonne määräytyy kuitenkin vasta sitten, kun on annettu niin paljon sääntöjä, että sen käyttäytyminen kaikissa tilanteissa on määräytynyt. $f$skeisessä esimerkissä $\infty + 1 = \infty$, mutta jossain toisessa sovelluksessa voi olla parempi valita $\frac{1}{0} + 1 \neq \frac{1}{0}$. Nollalla voi siis olla erilaisia käänteisarvoja eri tarkoituksia varten. Niille kaikille on kuitenkin yhteistä, että ne rikkovat kertolaskun liitännäisyyttä ja ainakin yhtä muuta rationaalilukujen lakia. Tämä johtuu siitä, että ainoa edellä olevissa laskelmissa käytetty nollan käänteisarvon ominaisuus on, että $0 \cdot \frac{1}{0} = 1$.

Millä oikeudella sitten vaadittiin, että nollan käänteisarvon on noudatettava lakia $0 \cdot \frac{1}{0} = 1$? Eikö sen tilalle voi valita jonkin muun lain? Kyllä voi, mutta niin määriteltyä olentoa ei ole mitään järkeä kutsua "nollan käänteisarvoksi". Matematiikassa "a:n käänteisarvolla" on johdonmukaisesti tarkoitettu sellaista olentoa $\frac{1}{a}$, että $a \cdot \frac{1}{a} = 1$. (Tapana on myös vaatia $\frac{1}{a} \cdot a = 1$, mutta sitä ei tarvitse sanoa erikseen silloin, kun kertolasku on vaihdannainen.) Määritellä saa mitä tahansa. Määritellyn olennon nimi pitää kuitenkin valita siten, että se ei ole ristiriidassa aikaisempien nimivalintojen kanssa.

Mitä luvut ovat?

Totesimme, että nollan käänteisarvon voi määritellä monellakin tavalla, mutta se käyttäytyy joka tapauksessa niin eri tavalla kuin oikeat luvut, että sitä ei pidä kutsua luvuksi. Mikä sitten kelpaa luvuksi?

Matematiikassa on tarkasti määritelty merkitys käsitteille "luonnollinen luku", "kokonaisluku", "rationaaliluku", "reaaliluku" ja niin edelleen, mutta ei käsitteelle "luku". Tästä seuraa, että matemaatikko voi ottaa käyttöön uudenlaisia olentoja ja alkaa kutsua niitä luvuiksi. Tästä ei kuitenkaan seuraa, että mitä tahansa kutsutaan luvuiksi. Uusien olentojen pitää muistuttaa tuttuja lukuja tarpeeksi paljon ja olla niihin tarpeeksi läheisessä suhteessa, jotta matemaatikot kelpuuttavat ne luvuiksi. Vaikka ei ole määritelty, miten paljon on tarpeeksi paljon, matemaatikot ovat tähän asti aina päässeet asiasta yhteisymmärrykseen.

Lukua ei tee luvuksi sen "omat" ominaisuudet, vaan jäsenyys järjestelmässä, jonka kaikki olennot yhdessä noudattavat jotakin kokoelmaa lakeja. Luvun -2 ominaisuus $2 + (-2) = 0$ puhuu paitsi -2:sta, myös luvuista 2 ja 0 sekä yhteenlaskusta. Laki "on olemassa $-a$" tarkoittaa itse asiassa, että "$-a$" on mukana puheena olevassa järjestelmässä. Peruskysymys ei siis ole, onko jokin olento luku, vaan onko jokin olentojen järjestelmä lukujoukko. (Tapana on sanoa "lukujoukko", vaikka "lukujärjestelmä" olisi parempi sana, sillä mukaan kuuluvat lukujen lisäksi ainakin yhteenlasku ja kertolasku.) Esimerkiksi ilmauksilla "luonnolliset luvut" ja "rationaaliluvut" viitataan tällaisiin järjestelmiin. Luvuilla täytyy voida laskea, tai muuten niitä ei sanota luvuiksi!

Kaikki tutut lukujärjestelmät noudattavat ainakin lakeja (1), ..., (8). Näitä lakeja käytetään laskuissa niin rutiininomaisesti, että jos yksikin niistä menetettäisiin, laskemisen luonne muuttuisi ihan toisenlaiseksi. Esimerkiksi vektoreilla ja matriiseilla on osittain toiset lait. Välillä on hankala muistaa, miten niillä saa ja ei

saa laskea. Mutta niitäpä ei kutsutakaan luvuiksi. Kuten edellä nähtiin, nollan käänteisarvoa ei voida ottaa käyttöön menettämättä ainakin kahta laeista (1), ..., (8).

Edellä totesimme, että lait (1), ..., (8) riittävät määräämään, että luvut 1, 2, 3, ... käyttäytyvät yhteen- ja kertolaskuissa kuten luonnolliset luvut, *jos kaikki nämä luvut ovat erisuuria*. Vaikka lakien (8) ja (1) ansiosta luvut 1, $1+1$, $(1+1)+1$, ... ovat kaikki varmasti olemassa, tähänastiset lait eivät riitä takaamaan, että ne ovat erisuuria. Laskemalla muuten normaalisti, mutta asettamalla $5 = 0$ (mistä seuraa $6 = 1$, $7 = 2$ ja niin edelleen) saadaan järjestelmä, jossa on viisi olentoa, joiden laskutoimitukset käyttäytyvät seuraavasti (olemme panneet olentojen päälle pienen viivan muistutukseksi, että ne eivät ole tuttuja lukuja):

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Tämä järjestelmä noudattaa kaikkia lakeja (1), ..., (12). Lakien (1), (2), (4), (5), (8), (9), (10) ja (12) voimassaolo on hyvin helppo tarkastaa näistä taulukoista. Koska järjestelmän olennot ovat erit, on laki (11) voimassa. Lakien (3), (6) ja (7) tarkastaminen vaatii enemmän työtä, mutta kyllä nekin pätevät.

Tämän viisialkioisen ja muiden samantapaisten järjestelmien alkioita ei ole tapana kutsua luvuiksi. Matemaatikon sana mille tahansa järjestelmälle, joka noudattaa lakeja (1), ..., (12) on *kunta*. Rationaalilukujen järjestelmä, reaalilukujen järjestelmä ja tämä viisialkioinen järjestelmä ovat kuntia. Kokonaislukujen järjestelmä ei ole kunta, koska laki (12) ei päde, eli kaikilla nollasta poikkeavilla alkioilla ei ole käänteisalkioita.

Jos jokin lukujen järjestelmä halutaan määritellä yksikäsitteisesti, niin tarvitaan lisää lakeja, joilla suljetaan väärät kunnat pois. Reaalilukujen tapauksessa tämä tehdään kahdessa vaiheessa. Ensin vaaditaan, että reaaliluvut voidaan asettaa suuruusjärjestykseen, joka käyttäytyy laskutoimitusten suhteen tutulla tavalla. Jokaiselle reaaliluvulle a, b ja c pätee:

(13) Tasan yksi seuraavista pätee: $a < b$, $a = b$ tai $b < a$.

(14) Jos $a < b$ ja $b < c$, niin $a < c$.

(15) Jos $a < b$, niin $a + c < b + c$.

(16) Jos $0 < a$ ja $0 < b$, niin $0 < ab$.

Tällä vaatimuksella saadaan aikaan, että 1, $1+1$, $(1+1)+1$, ... todellakin ovat kaikki eri lukuja. Nimittäin, lakien (9) ja (8) ansiosta 0 ja 1 ovat olemassa, ja laki (11) sanoo, että $1 \neq 0$. Lain (13) nojalla joko $0 < 1$ tai $1 < 0$. Jos $0 < 1$, niin lakien (10), (2) ja (15) nojalla $1 = 1 + 0 = 0 + 1 < 1 + 1$ eli $1 < 1 + 1$. Lisäämällä ykkönen kummallekin puolelle ja soveltamalla lakia (15) uudelleen saadaan $1+1 < (1+1)+1$. Tätä toistamalla saadaan $1 < 1+1 < (1+1)+1 < ((1+1)+1)+1 < \ldots$. Jos olisikin $1 < 0$, niin samanlaisella päättelyllä saataisiin $\ldots < ((1 + 1) + 1) + 1 < (1 + 1) + 1 < 1 + 1 < 1$.

Nyt tarvitsee vielä osoittaa, että jos $a_1 < a_2 < a_3 < \ldots$ tai $\ldots < a_3 < a_2 < a_1$, niin luvut a_i ovat kaikki keskenään erisuuria. Ensimmäisessä tapauksessa soveltamalla lakia (14) toistuvasti saadaan $a_1 < a_3$, $a_1 < a_4$ ja niin edelleen. Vanhastaan tiedettiin, että $a_1 < a_2$. Lain (13) nojalla näistä seuraa, että $a_1 \neq a_2$, $a_1 \neq a_3$, $a_1 \neq a_4$ ja niin edelleen. Samalla tavalla voidaan osoittaa, että $a_2 \neq a_3$, $a_2 \neq a_4$, $a_2 \neq a_5$ ja niin edelleen, ja yleensä, että $a_i \neq a_j$ kun $i < j$. Samanlainen päättely toimii myös jälkimmäisessä tapauksessa.

Tämän tuloksen ansiosta lakeja (1), ..., (9), (11), (13), (14) ja (15) noudattava järjestelmä sisältää vääjäämättä luonnollisten lukujen kanssa samalla tavalla käyttäytyvän osajärjestelmän. Jälleen kerran noudatamme sitä periaatetta, että koska kyseistä osajärjestelmää ei mitenkään voi erottaa luonnollisista luvuista, sanomme, että se *on* luonnolliset luvut. Lakien (10) ja (12) ansiosta mukana ovat muutkin rationaaliluvut, myös negatiiviset, ja niiden yhteen-, vähennys-, kerto- ja jakolaskuista tulevat ne tulokset, jotka koulussa opittiin. Toisaalta rationaaliluvut toteuttavat lait (1), ..., (16), joten rationaalilukujen järjestelmä on pienin nämä lait toteuttava järjestelmä.

Edellä otettiin huomioon mahdollisuus, että $1 < 0$. Ilman lakia (16) tämä olisi todellakin mahdollista! Sen huomaa siitä, että jos "$<$" käännetään toisinpäin muotoon "$>$", niin lait (13), ..., (15) ovat yhä voimassa, mutta (16) rikkoutuu. Siis vasta laki (16) on se, joka kertoo, kumminpäin luvut on asetettu suuruusjärjestykseen.

Mahdollisuus $1 < 0$ voidaan sulkea pois seuraavasti. Edellä osoitettiin, että $x \cdot 0 = 0$. Siitä seuraa, että $0 = x \cdot 0 = x \cdot (1 + (-1)) = x \cdot 1 + x \cdot (-1) = x + x \cdot (-1)$. Siis $x \cdot (-1)$ on x:n vastaluku eli $-x$. Niinpä $(-1) \cdot (-1) = -(-1) = 1$. Jos $1 < 0$, niin lisäämällä kummallekin puolelle -1 saadaan $0 < -1$. Niinpä laki (16) vaatii, että $0 < (-1) \cdot (-1) = 1$. Siis samanaikaisesti $1 < 0$ ja $0 < 1$. Se rikkoo lakia (13). Vaihtoehto $1 < 0$ on siis

mahdoton, joten ainoa jäljelle jäävä vaihtoehto $0 < 1$ on oikea.

Reaalilukujen järjestelmä tulee täysin määritellyksi, kun lisätään vielä yksi laki, niin sanottu *täydellisyysaksiooma*. Se on nykyaikainen muotoilu asiasta, jonka nimi on *Dedekindin leikkaus*, ja jonka keksi Richard Dedekind 1800-luvun jälkipuoliskolla [1, s. 788–789]. Se on monimutkainen ilmaista täsmällisesti, mutta sen perusajatus on seuraava. Ajatellaan, että kaikki reaaliluvut jaetaan millä tahansa periaatteella kahteen epätyhjään osaan, "pienet luvut" ja "suuret luvut", siten, että jokainen pieni luku on pienempi kuin jokainen suuri luku. Täydellisyysaksiooma sanoo, että joko pienten lukujen joukossa on suurin tai suurten lukujen joukossa on pienin.

Tämän ymmärtämiseksi tarkastelkaamme jakoa, jossa "pienet luvut" sisältävät kaikki negatiiviset luvut, nollan, sekä ne positiiviset luvut, joiden neliö on enintään 2. "Suuret luvut" ovat tietysti loput positiiviset luvut.

Jos rationaaliluvuille tehdään tällainen jako, niin $\sqrt{2}$ ei ole kummassakaan osassa, koska se ei ole rationaaliluku. Pienten lukujen osa sisältää loputtomiin sen toinen toistaan tarkempia alalikiarvoja, kuten 1, 1,4, 1,41 ja 1,4142135. (Jokainen näistä on rationaaliluku. Esimerkiksi $1{,}4142 = \frac{14142}{10000}$.) Otetaan mikä tahansa pieni luku, niin sitä suurempi pieni luku löydetään valitsemalla $\sqrt{2}$:n alalikiarvo, jossa on tarpeeksi monta desimaalia. Mikään pienistä luvuista ei siis ole suurin pieni luku. Vastaavasti suurten lukujen osa sisältää loputtomiin tarkkenevia ylälikiarvoja, kuten 2, 1,5, 1,42 ja 1,4142136. Otetaan mikä tahansa suuri luku, niin tarpeeksi monidesimaalinen $\sqrt{2}$:n ylälikiarvo on sitä pienempi. Siis mikään suurista luvuista ei ole pienin suuri luku. Huomaamme, että rationaalilukujen joukko ei noudata täydellisyysaksioomaa.

Reaalilukujen tapauksessa täydellisyysaksiooma pakottaa ainakin yhden luvun olemassaolon, joka on joko suurin pienistä tai pienin suurista. Tämä luku ei ole mikään edellä luetelluista rationaalisista likiarvoista. Lakien (13), ..., (16) vuoksi tämän luvun neliön on pakko olla enintään yhtäsuuri kuin minkä tahansa suuren luvun neliön ja ainakin yhtäsuuri kuin minkä tahansa positiivisen pienen luvun neliön. Neliö ei siis voi olla muuta kuin 2, joten tämän luvun on oltava $\sqrt{2}$.

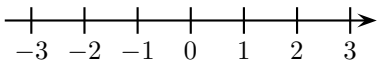
Samalla kun täydellisyysaksiooma pakottaa mukaan kaikki luvut, jotka sijaitsevat rationaalilukujen väleissä, se varmistaa, että mukaan ei tule olentoja, jotka olisivat suurempia kuin kaikki rationaaliluvut. Nimittäin, jos tällainen olento olisi mukana, reaaliluvut voitaisiin jakaa "pieniin" ja "suuriin" siten, että pieniä ovat kaikki rationaaliluvut ja niitä pienemmät luvut. Mikään rationaaliluku q ei ole pienistä luvuista suurin, koska myös $q + 1$ on rationaaliluku ja $q + 1 > q$. Mikään muu pieni luku ei voi olla suurin pieni luku, koska se on jotain rationaalilukua pienempi. Siis pienten lukujen joukossa ei ole suurinta. Niinpä täydellisyysaksiooman vuoksi suurten lukujen joukossa on oltava pienin luku. Olkoon sen nimi ω. Lain (15) nojalla $\omega - 1 < \omega$. Koska ω on pienin suuri luku, on $\omega - 1$ pieni luku, eli on olemassa rationaaliluku q siten, että $\omega - 1 \leq q$. Mutta silloinhan $\omega \leq q+1$, mikä on ristiriidassa sen kanssa, että suurena lukuna ω ei ole rationaaliluku eikä mitään rationaalilukua pienempi. Siis suurten lukujen osan on pakko olla tyhjä, eli ei ole olemassa reaalilukua, joka on suurempi kuin kaikki rationaaliluvut.

Vastaavalla tavalla nähdään, että ei ole olemassa reaalilukua, joka on pienempi kuin kaikki rationaaliluvut.

Reaalilukujen joukko noudattaa täydellisyysaksioomaa siitä yksinkertaisesta syystä, että täydellisyysaksiooma on otettu mukaan reaalilukujen joukon määritelmään. Tätä ei voitu tehdä noin vain, vaan ensin piti varmistua, että se sopii yhteen reaalilukujen muiden lakien kanssa. Eihän nollan käänteisarvoakaan voitu ottaa mukaan, koska se ei sopinut yhteen tärkeiden lakien kanssa. Tämä tarkastus on valitettavasti liian monimutkainen asia tässä käsiteltäväksi.

(17) Täydellisyysaksiooma

Reaaliluvut voidaan asettaa molempiin suuntiin päättymättömälle suoralle. Se tunnetaan nimellä *lukusuora*.



Kompleksiluvut

Nyt voimme vihdoin ja viimein keskittyä olennon $\sqrt{-1}$ ongelmaan. Aluksi toteamme, että ainakaan reaaliluku se ei ole. Nimittäin, nolla se ei tietenkään ole, koska $0 \cdot 0 = 0 \neq -1$. Laki (16) takaa, että se ei ole mikään positiivinen reaaliluku. Negatiiviset vaihtoehdot saadaan suljettua pois osoittamalla, että kahden negatiivisen luvun tulo on positiivinen. Olkoot $a < 0$ ja $b < 0$. Lisäämällä molempiin vastaluvut molemmille puolille saadaan $0 < -a$ ja $0 < -b$. Lain (16) mukaan siis $0 < (-a)(-b)$. Toisaalta $(-a)(-b) = (a(-1))(b(-1)) = \ldots = (ab)((-1)(-1)) = (ab)1 = ab$. Siis $0 < ab$.

Kuitenkin yhtälöiden ratkaisemisesta saadut kokemukset houkuttelevat laskemaan olennolla $\sqrt{-1}$ ja muilla negatiivisten lukujen neliöjuurilla ikäänkuin ne olisivat lukuja. Esimerkiksi Geronimo Cardano ratkaisi vuoden 1545 kirjassaan kolmannen asteen yhtälöitä $x^3 = px+q$ tavalla, joka vastaa kaavaa $x = \sqrt[3]{A+B} + \sqrt[3]{A-B}$,

missä $A = \frac{q}{2}$ ja $B = \sqrt{\frac{q^2}{4} - \frac{p^3}{27}}$ [1, s. 399–405]. (Cardano myönsi kirjassaan, että hän ei ollut tuloksen keksijä.) Yhtälön $x^3 = 3x + 2$ tapauksessa tämä johtaa nätisti välivaiheiden $A = 1$ ja $B = 0$ kautta oikeaan ratkaisuun $x = 2$. Mutta tapauksessa $x^3 = 15x + 4$ tämä tuottaa tulokseksi $x = \sqrt[3]{2 + \sqrt{-121}} + \sqrt[3]{2 - \sqrt{-121}}$. Cardano ei tästä selvinnyt, vaikka hän tiesi, että $x = 4$ on yhtälön ratkaisu.

Rafael Bombelli hyväksyi tuloksen $\sqrt[3]{2 + \sqrt{-121}} + \sqrt[3]{2 - \sqrt{-121}} = 4$ päteväksi [1, s. 408]. Hän arvasi rohkeasti, että $\sqrt[3]{2 \pm \sqrt{-121}}$ ovat muotoa $a \pm b\sqrt{-1}$. Koska niiden summa on 4, on $a = 2$. Laskemalla $(2 \pm b\sqrt{-1})^3 = 8 \pm 12b\sqrt{-1} - 6b^2 \mp b^3\sqrt{-1} = (8 - 6b^2) \pm (12b - b^3)\sqrt{-1}$ havaitaan, että kaikki täsmää, jos $8 - 6b^2 = 2$ ja $(12b - b^3)\sqrt{-1} = 11\sqrt{-1} = \sqrt{-121}$. Tähän päästään sijoittamalla $b = 1$. Siis $\sqrt[3]{2 + \sqrt{-121}} = 2 + \sqrt{-1}$. Tämä ei auttanut yhtälön $x^3 = px + q$ ratkaisemisessa silloin, kun $\frac{q^2}{4} - \frac{p^3}{27} < 0$, mutta oli askel kompleksilukujen ominaisuuksien ymmärtämisen suuntaan.

Bombelli siis laski olennolla $\sqrt{-1}$ ikäänkuin se olisi luku, joka noudattaa samoja sääntöjä kuin muutkin luvut. Olennosta $\frac{1}{0}$ saamiemme kokemusten vuoksi tiedämme, että sellainen ei välttämättä ole turvallista. Meillä on kuitenkin yksi etu, jota Bombellilla ei ollut: tiedämme, että olennainen kysymys on, missä määrin lait (1), ..., (17) säilyvät.

Näimme, että jokaisen lakeja (13), ..., (16) noudattavan luvun neliö on 0 tai positiivinen. Nyt nimenomaan haluamme luvun, jonka neliö on negatiivinen. Näin ollen, vaikka kaikki tätä ennen käyttöönotetut luvut noudattavat lakeja (13), ..., (16), nyt niistä on pakko luopua ainakin osittain. Koska niiden tehtävä on asettaa luvut suuruusjärjestykseen, on yksinkertaisinta todeta, että $\sqrt{-1}$ on reaalilukujen suuruusjärjestyksen — siis lukusuoran — ulkopuolella, ja sitten unohtaa ne kaikki.

Lain (17) tehtävä on varmistaa, että kaikki reaaliluvut ovat mukana reaalilukujen järjestelmässä. Sitä ei voi sellaisenaan soveltaa uusille luvuille, koska se käyttää hyväkseen lukujen suuruusjärjestystä, jonka juuri menetimme. Toisaalta, jos vaadimme, että uusi järjestelmä on reaalilukujen laajennos, niin kaikki reaaliluvut ovat mukana ja lain (17) tehtävä on suoritettu.

Tutkikaamme siis, mitä seuraa, jos oletetaan reaalilukujen lisäksi sellaisen luvun i olemassaolo, että $i^2 = -1$, ja pidetään samanaikaisesti kiinni laeista (1), ..., (12). Syntyykö ristiriita, vai saadaanko aikaan toimiva lukujärjestelmä? Tai ehkä syntyy monta erilaista toimivaa lukujärjestelmää?

Lain (4) vuoksi uutta lukua i täytyy voida kertoa reaaliluvuilla. Siis bi on olemassa, kun b on reaaliluku. Uusia lukuja täytyy voida myös laskea yhteen reaalilukujen kanssa. Tällä tavalla saadaan lausekkeita muotoa $a + bi$. Voidaan osoittaa, että ne kaikki vastaavat eri lukuja. Nimittäin, jos $a_1 + b_1 i = a_2 + b_2 i$, niin $(b_1 - b_2)i = a_2 - a_1$. Jos $b_1 - b_2 \neq 0$, tästä saadaan edelleen $i = \frac{a_2 - a_1}{b_1 - b_2}$, joka on reaaliluku. Mutta i ei ole reaaliluku, joten $b_1 - b_2 = 0$ eli $b_1 = b_2$. Siitä seuraa $a_2 - a_1 = (b_1 - b_2)i = 0i = 0$. Niinpä $a_1 = a_2$.

Siis kun $b \neq 0$, niin jokainen olento muotoa $a + bi$ on uusi luku, joka pitää ottaa mukaan järjestelmään. ($a + 0i$ on tietenkin vanha tuttu reaaliluku a.) Niinpä niilläkin on voitava laskea yhteen- ja kertolaskuja. Tuleeko niistä tulokseksi lisää uusia lukuja, jotka on pakko ottaa mukaan, ja niin edelleen loputtomiin?

Yhteenlaskun vaihdannaisuus- ja liitännäisyyslain sekä osittelulain ansiosta kahden tällaisen olennon summa paljastuu samanlaiseksi olennoksi: $(a_1 + b_1 i) + (a_2 + b_2 i) = a_1 + b_1 i + a_2 + b_2 i = a_1 + a_2 + b_1 i + b_2 i = (a_1 + a_2) + (b_1 + b_2)i$. Yhteenlasku ei siis tuota enää lisää uusia olentoja. Myöskään kertolasku ei tuota lisää uusia olentoja, koska $(a_1 + b_1 i)(a_2 + b_2 i) = a_1 a_2 + a_1 b_2 i + b_1 a_2 i + b_1 b_2 i^2 = (a_1 a_2 - b_1 b_2) + (a_1 b_2 + b_1 a_2)i$.

Uusilla olennoilla pitää olla vasta- ja käänteisluvut. Onneksi on helppo huomata, että $-a - bi$ on olennon $a + bi$ vastaluku. Käänteisluvuksi kelpaa $\frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i$, mikä voidaan tarkastaa laskulla $(a + bi)(\frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i) = (\frac{a^2}{a^2+b^2} + \frac{b^2}{a^2+b^2}) + (-\frac{ab}{a^2+b^2} + \frac{ba}{a^2+b^2})i = \frac{a^2+b^2}{a^2+b^2} = 1$. Se on olemassa, kun $a \neq 0$ tai $b \neq 0$, koska silloin $a^2 + b^2 > 0$.

Ei siis ole enää tarvetta ottaa mukaan lisää olentoja.

Olemme osoittaneet, että jos reaalilukujen joukko halutaan laajentaa kunnaksi, jossa on luku i siten, että $i^2 = -1$, niin on vain yksi tapa edetä. Mukana ovat kaikki parit muotoa $a + bi$, missä a ja b ovat reaalilukuja, ja yhteen- ja kertolaskut lasketaan näin:

$$\begin{aligned} & (a_1 + b_1 i) + (a_2 + b_2 i) \\ = \; & (a_1 + a_2) + (b_1 + b_2)i \end{aligned}$$

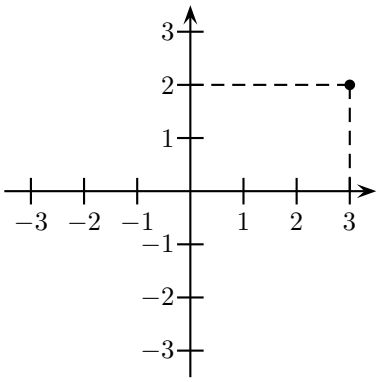
$$\begin{aligned} & (a_1 + b_1 i)(a_2 + b_2 i) \\ = \; & (a_1 a_2 - b_1 b_2) + (a_1 b_2 + b_1 a_2)i \end{aligned}$$

Vielä on tarpeen tarkastaa, että näin syntyvä järjestelmä todella on kunta, ja että emme vahingossa muuttaneet reaalilukujen käyttäytymistä. Jos sijoitetaan vasta- ja käänteisluvun kaavoihin $b = 0$, saadaan $-a - 0i = -a$ ja $\frac{a}{a^2+0^2} - \frac{0}{a^2+0^2}i = \frac{1}{a}$, kuten pitääkin. Jos sijoitetaan summan ja tulon kaavoihin $b_1 = b_2 = 0$, huomataan, että tulokseksi saadaan tutut reaalilukujen summa ja tulo. Lait (1), (4), (10) ja (12) tuli jo tarkastettua, ja loppujen tarkastaminen on rutiinityötä.

Lukujen $a + bi$ järjestelmä on siis reaaliluvut sisältävä kunta. Se tunnetaan nimellä *kompleksiluvut*. Luvut muotoa bi, missä $b \neq 0$, ovat *imaginaariluvut*. Päättelystämme seuraa, että kompleksiluvuille ei ole vaihtoehtoa. Jos reaaliluvut laajennetaan kunnaksi, jossa

on alkio, jonka neliö on -1, niin silloin kaikki kompleksiluvut tulevat vääjäämättä mukaan.

Sveitsiläinen Leonhard Euler (1707–1783) ymmärsi kompleksiluvut hyvin. Häneltä on peräisin luvun $\sqrt{-1}$ merkki i sekä hämmästyttävä tulos $e^{\pi i} = -1$, joka liittää toisiinsa luonnollisen logaritmijärjestelmän kantaluvun e, ympyrän kehän ja halkaisijan suhteen π ja imaginaariyksikön i [1, s. 622]. Mutta kompleksiluvut hyväksyttiin yleisesti vasta kun Carl Friedrich Gauss, joka on eräs historian suurimmista matemaatikoista, näytti vuonna 1832, että ne vastaavat tason pisteitä [1, s. 710]. Caspar Wessel oli tosin keksinyt saman jo vuonna 1797, mutta hänen tuloksensa ei saanut ansaitsemaansa huomiota, kenties siksi, että hän ei julkaissut sitä kansainvälisessä tiedelehdessä vaan Tanskan akatemian sarjassa. Lukua $a + bi$ vastaa x-y-koordinaatiston piste (a, b). Esimerkiksi kuvan piste vastaa lukua $3 + 2i$.



3-ulotteisia lukuja?

Näimme, että reaaliluvut vastaavat (luku)suoran pisteitä ja kompleksiluvut vastaavat tason pisteitä. Suora on yksi- ja taso on kaksiulotteinen olento, joten reaaliluvut ovat yksi- ja kompleksiluvut ovat kaksiulotteisia lukuja. Maailma, jossa elämme, on kolmiulotteinen. Niinpä seuraava luonnollinen askel olisi kehittää kolmiulotteisia lukuja. Tässä luvussa huomaamme kuitenkin, että sellaisia ei voi olla olemassa. Siihen päästäksemme meidän on ensin tutkittava hieman polynomeja ja niiden nollakohtia.

Lauseketta $a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$, missä a_i:t ovat lukuja, kutsutaan *polynomiksi*. Jos $a_n \neq 0$, se on *n:nnen asteen* polynomi. Esimerkiksi $x^3 - 2x^2 + 16$ on kolmannen asteen polynomi. Polynomin *nollakohta* on sellainen luku x, että $a_n x^n + \cdots + a_0 = 0$. Luvut a_i ovat polynomin *kertoimet*. Polynomin $x^3 - 2x^2 + 16$ kertoimet ovat 1, -2, 0 ja 16. Sillä on kolme nollakohtaa: -2, $2 + 2i$ ja $2 - 2i$.

Edellä mainittu Gauss todisti vuonna 1799 julkaistussa väitöskirjassaan hienon tuloksen: jokaisella polynomilla, jonka kertoimet ovat kompleksilukuja ja jonka aste on ainakin yksi, on ainakin yksi nollakohta, joka on kompleksiluku [1, s. 698–699]. Tämä tulos on niin tärkeä, että sitä kutsutaan algebran peruslauseeksi. Valitettavasti todistus on liian monimutkainen tässä esitettäväksi.

Olkoon x_1 polynomin $a_n x^n + \cdots + a_0$ nollakohta. Jos luvut $b_{n-1}, \ldots, b_0$ on valittu siten, että $b_{n-1} = a_n$ ja muutoin $b_{j-1} = x_1 b_j + a_j$, niin pienellä kertolaskulla voidaan tarkastaa, että $a_n x^n + \cdots + a_0 = (x - x_1)(b_{n-1} x^{n-1} + \cdots + b_0)$. Myös $b_{n-1} x^{n-1} + \cdots + b_0$ on polynomi. Jos sen aste on vähintään yksi, niin silläkin on nollakohta x_2 ja se voidaan jakaa muotoon $(x - x_2)(c_{n-2} x^{n-2} + \cdots + c_0)$. Tällä tavalla jatkamalla nähdään, että jokainen polynomi voidaan kirjoittaa muodossa $a_n x^n + \cdots + a_0 = (x - x_1)(x - x_2) \cdots (x - x_n) a_n$, missä $x_1, x_2, \ldots, x_n$ ovat polynomin nollakohtia. Polynomilla ei voi olla näiden lisäksi muita nollakohtia, koska muilla x:n arvoilla oikea puoli on nollasta poikkeavien lukujen $x - x_1$, $x - x_2$ ja niin edelleen sekä a_n tulo, ja siksi nollasta poikkeava.

Kompleksilukujen laskusäännöistä on helppo tarkastaa, että jos kompleksilukujen yhteen- tai kertolaskussa vaihdetaan kaikkien imaginaariosien etumerkit, niin tulos säilyy muuten ennallaan, paitsi että tuloksenkin imaginaariosan etumerkki vaihtuu. Toisin sanoen, jos $(a_1 + b_1 i) + (a_2 + b_2 i) = a + bi$, niin $(a_1 - b_1 i) + (a_2 - b_2 i) = a - bi$, ja jos $(a_1 + b_1 i)(a_2 + b_2 i) = a + bi$, niin $(a_1 - b_1 i)(a_2 - b_2 i) = a - bi$. Tästä seuraa, että jos polynomin kertoimet $a_0, \ldots, a_n$ ovat reaalilukuja ja polynomin arvo x:n arvolla $a + bi$ on $c + di$, niin polynomin arvo x:n arvolla $a - bi$ on $c - di$.

Erityisesti, jos $a + bi$ on reaalikertoimisen polynomin nollakohta, niin $c + di = 0$, joten $c = d = 0$ ja $c - di = 0$, joten myös $a - bi$ on kyseessä olevan polynomin nollakohta. Nollakohtia $a + bi$ ja $a - bi$ vastaavien tekijöiden $x - (a + bi)$ ja $x - (a - bi)$ tulo on $x^2 - 2ax + a^2 + b^2$. Se on toisen asteen polynomi, jonka kertoimet ovat reaalilukuja. Tästä seuraa, että jokainen reaalikertoiminen vähintään astetta yksi oleva polynomi voidaan esittää ensimmäistä ja toista astetta olevien reaalikertoimisten polynomien tulona. Esimerkkipolynomillemme $x^3 - 2x^2 + 16$ tämä tulo on $(x + 2)(x^2 - 4x + 8)$.

Tämän päättelyn lopputulos koskee pelkästään reaalilukuja eikä lainkaan imaginaarilukuja, joten se olisi ollut kiinnostava niidenkin menneen ajan matemaatikoiden mielestä, jotka eivät hyväksyneet imaginaarilukuja. He eivät olisi kuitenkaan uskaltaneet ottaa tulosta käyttöön ilman todistusta, jossa ei käytetä imaginaarilukuja. Sellaista ei ole helppo löytää. Tässä on jälleen esimerkki siitä, että imaginaarilukuja tarvitaan välivaiheena matkalla tulokseen, joka ei käsittele imaginaarilukuja.

Nyt voidaan tutkia, mitä tapahtuu, jos reaalilukujen laajentamisen lähtökohtana ei olisikaan i, joka on polynomin $x^2 + 1$ nollakohta, vaan jonkin muun reaali-

kertoimisen polynomin nollakohta. Polynomina voi olla $x^4 + 1$ tai mikä tahansa muu reaalikertoiminen polynomi, jolla ei ole nollakohtaa reaalilukujen joukossa. Merkitsemme sen hypoteettista nollakohtaa symbolilla $\ddot{\imath}$.

Kuten edellä nähtiin, kyseessä oleva polynomi voidaan jakaa reaalikertoimisiin ensimmäisen ja toisen asteen tekijöihin. Luku $\ddot{\imath}$ on jonkin niistä nollakohta. Se ei voi olla ensimmäisen asteen tekijän $x - x_j$ nollakohta, koska silloin se olisi reaaliluku x_j. Se on siis jonkin toisen asteen tekijän $x^2 + px + q$ nollakohta, eli $\ddot{\imath}^2 + p\ddot{\imath} + q = 0$. Toisen asteen yhtälön ratkaisukaavasta tiedämme, että $p^2 - 4q < 0$ eli $4q - p^2 > 0$, koska muutoin polynomin $x^2 + px + q$ nollakohdat olisivat reaalilukuja, eikä uudelle luvulle $\ddot{\imath}$ olisi tilaa. Nyt voimme laskea $(p + 2\ddot{\imath})^2 = p^2 + 4p\ddot{\imath} + 4\ddot{\imath}^2 = 4(\ddot{\imath}^2 + p\ddot{\imath} + q) - 4q + p^2 = 4 \cdot 0 - 4q + p^2 = -(4q - p^2)$. Niinpä $\left(\frac{p+2\ddot{\imath}}{\sqrt{4q-p^2}}\right)^2 = \frac{-(4q-p^2)}{4q-p^2} = -1$.

Siis mukaan tunkeutui väkisin luku, jonka neliö on -1! Edellä näimme, että tällaisen luvun olemassaolo määrää kompleksiluvut yksikäsitteisesti. Huomaamme, että nollakohdan olettaminen *mille tahansa* reaalikertoimiselle polynomille, jolla ei sellaista ole reaalilukujen joukossa, johtaa aina samaan kompleksilukujen järjestelmään.

Nyt on helppo osoittaa, että kolmiulotteisia lukuja ei ole olemassa — eikä neli-, viisi-, kuusi- tai muitakaan, missä ulottuvuuksien määrä on äärellinen ja vähintään kolme. Päästäksemme reaaliluvuista eteenpäin tarvitsemme ainakin yhden uuden luvun $\ddot{\imath}$. Se ei saa olla minkään reaalikertoimisen polynomin nollakohta, koska muuten tulokseksi tulee kompleksiluvut, kuten äsken näimme. Näinollen esimerkiksi $\ddot{\imath}^4$ ei ole mikään niistä luvuista, jotka voidaan esittää muodossa $a + b\ddot{\imath} + c\ddot{\imath}^2 + d\ddot{\imath}^3$, koska muutoin se olisi polynomin $x^4 - dx^3 - cx^2 - bx - a$ nollakohta. Samasta syystä $a_1 + b_1\ddot{\imath} + c_1\ddot{\imath}^2 + d_1\ddot{\imath}^3 \neq a_2 + b_2\ddot{\imath} + c_2\ddot{\imath}^2 + d_2\ddot{\imath}^3$ paitsi kun $a_1 = a_2$, $b_1 = b_2$, $c_1 = c_2$ ja $d_1 = d_2$. Jokainen luvuista $\ddot{\imath}$, $\ddot{\imath}^2$, $\ddot{\imath}^3$, ... tarvitsee siis käyttöönsä oman uuden ulottuvuuden, eikä mikään äärellinen ulottuvuuksien määrä riitä.

Jos laajentaminen aloitetaan kompleksiluvuista, niin silloinkaan $\ddot{\imath}$ ei voi olla minkään kompleksikertoimisen polynomin nollakohta, koska sen kaikki nollakohdat löytyvät kompleksilukujen joukosta, kuten Gauss todisti. Samalla lailla kuin äsken nytkin saadaan tulokseksi, että jokainen luvuista $\ddot{\imath}$, $\ddot{\imath}^2$, $\ddot{\imath}^3$, ... luo oman ulottuvuuden.

Jos ulottuvuuksia sallitaan rajaton määrä, niin kompleksiluvuille löytyy laajennos, joka on kunta. Nimittäin lausekkeet muotoa polynomi jaettuna polynomilla, jossa kertoimet ovat kompleksilukuja ja jakaja on jokin muu polynomi kuin 0, ovat nekin olentoja, joita voi laskea yhteen ja kertoa keskenään. Kuinka ollakaan, niidenkin muodostama järjestelmä on kunta. Polynomien osamäärät ovat käsitteenä kuitenkin niin kaukana tutuista luvuista, että niitä ei kutsuta luvuiksi. (Jos tämä temppu tehdään rationaalikertoimisille polynomeille, saadaan rationaalilukujen laajennos, jossa on alkio, joka on suurempi kuin kaikki kokonaisluvut. Tämä osoittaa, että täydellisyysaksiooma on todellakin tarpeen todistettaessa, että mikään reaaliluku ei ole kaikkia rationaalilukuja suurempi.)

Kompleksiluvuille ei siis ole vaihtoehtoja. Ne on otettava joko sellaisenaan, tai on tyydyttävä reaalilukuihin tai johonkin reaalilukujen osajoukkoon, tai sitten on pakko siirtyä samantien rajatonulotteisiin olentoihin. Ei ole olemassa hieman kompleksilukujen kaltaista mutta kuitenkin erilaista järjestelmää. Ei ole olemassa kolmiulotteisia kompleksilukuja. Kompleksi- ja imaginaariluvut ovat omituisen joustamattomia ollakseen vain imaginaarisia — eli kuvitteellisia.

Lopuksi

Matemaatikot määrittelevät käsitteitä rakentamalla niitä aikaisemmista käsitteistä. Tässä kertomuksessa rakensimme negatiiviset rationaaliluvut positiivisista. Matemaatikko voi määritellä käsitteen myös luettelemalla siltä vaadittavat ominaisuudet. Reaalilukujen määrittelemiseksi riittää luetella tässä tekstissä esitetyt 17 lakia.

Kun käsite määritellään luettelemalla lakeja, on vaarana, että lait ovat keskenään ristiriidassa. Näin käy esimerkiksi, jos asetetaan laeiksi (1), ..., (11) sekä (12) siten muutettuna, että myös $\frac{1}{0}$ on olemassa. Jos lait ovat ristiriidassa, käsitteelle voidaan todistaa kaksi ominaisuutta, jotka eivät mitenkään voi olla yhtäaikaa voimassa — esimerkiksi $1 = 0$ ja $1 \neq 0$. Käsite on silloin mahdoton. Sitä ei ole olemassa.

Tämä periaate toimii myös toisinpäin. Lakikokoelma on varmasti ristiriidaton, jos voidaan antaa esimerkki käsitteestä, joka toteuttaa sen. Lait (1), ..., (12) ovat varmasti ristiriidattomat, koska kohdassa "Mitä luvut ovat?" esitettiin viisialkioinen järjestelmä, joka toteuttaa ne. Toinen, tutumpi esimerkki ne toteuttavasta käsitteestä on rationaaliluvut. Viisialkioisessa järjestelmässä on se etu, että koska alkioita on vain viisi, jokainen laki voidaan tarkastaa erikseen jokaisella alkiolla, alkioiden parilla tai alkioiden kolmikolla. (Liitännäisyyslait ja osittelulaki puhuvat kolmesta alkiosta yhtäaikaa.) Lukija voi halutessaan tehdä tarkastuksen viimeistä yksityiskohtaa myöten. Rationaalilukuja on äärettömästi, joten tarkastusta ei voi tehdä jokaiselle rationaalilukukolmikolle erikseen, vaan on käytettävä epäsuoria keinoja.

Esimerkin antaminen on siis hyvä keino osoittaa, että lakikokoelma ei ole ristiriitainen.

Lakikokoelmilla määritteleminen on usein käsitteen käytön kannalta kätevämpi lähtökohta kuin rakentamalla määritteleminen. Lisäksi usein on olemassa monta käsitettä, jotka toteuttavat saman lakikokoelman — näimme, että on olemassa paljon erilaisia kuntia. Jos tällaisten käsitteiden ominaisuuksia tutkitaan lakikokoelmasta aloittaen, selville saadut asiat koskevat *kaikkia* lakikokoelman mukaisia käsitteitä — siis esimerkiksi kaikkia kuntia. Saadaan enemmän tuloksia samalla vaivalla. Lakikokoelmista aloittaminen auttaa yleensä myös paremmin ymmärtämään asioiden välisiä yhteyksiä.

Sitäpaitsi käsitteiden rakentamiseen aikaisemmista käsitteistä liittyy se ongelma, että niin ei voi tehdä, ennen kuin on määritelty ensimmäinen käsite, jolla päästään alkuun. Tämä ensimmäinen käsite voi olla esimerkiksi joukot tai luonnolliset luvut. Se täytyy määritellä lakikokoelman avulla.

Joukkoja ja luonnollisia lukuja on rajattomasti, joten niiden lakeja ei voi tarkastaa jokainen tapaus erikseen, niinkuin teimme viisialkioiselle esimerkkikunnalle. Usko joukkojen tai luonnollisten lukujen lakien ristiriidattomuuteen perustuu toisaalta siihen, että ne ovat hyvin yksinkertaisia ja uskottavan tuntuisia (ainakin matemaatikoiden mielestä!), ja toisaalta siihen, että niiden varaan on voitu rakentaa valtava määrä matematiikkaa ilman, että tuhoisia ristiriitoja on pulpahtanut esiin. Ristiriitaisuuksia on välillä ilmennyt, mutta aina ne on kyetty ratkaisemaan. Matematiikan ristiriidattomuuden puolesta puhuu myös se, että kännykät, avaruusraketit ja ydinvoimalaitokset toimivat (ainakin suurimman osan aikaa), vaikka ne on suunniteltu matematiikan avulla.

Molemmat tavat määritellä käsitteitä ovat siis tarpeen, ja ne ovat matematiikan tutkimuksessa vuorovaikutuksessa keskenään.

Matemaatikko saa siis määritellä käsitteitä aivan kuten haluaa, kunhan varoo ristiriitoja. Eikö tästä seuraa, että matematiikka on yhtä mielivaltaista kuin šhakkipelin säännöt?

Tämä kirjoitus on toivottavasti vakuuttanut lukijan siitä, että ei seuraa. Vaikka määritelmiä voi yrittää asettaa mielivaltaisesti, syntyvien käsitteiden ominaisuuksia ei voi säädellä mielivaltaisesti. Kuntaan ei pysty lisäämään nollan käänteisarvoa, vaikka kuinka maanittelisi. Kolmiulotteisia lukuja ei saa aikaan, vaikka kuinka yrittäisi. Jos niitä yrittää väkisin, saa aikaan ristiriitoja. Jos tekee määritelmään pienen muutoksen huolellisesti ristiriitoja välttäen, niin helposti käy niin, että saakin tulokseksi alkuperäisen käsitteen vain hieman naamioituna, kuten kävi yrityksessämme määritellä toisenlaisia kompleksilukuja olettamalla nollakohta polynomille x^4+1. Jos tekee määritelmään niin suuren ristiriidattoman muutoksen, että määritelty käsite muuttuu, niin muutosta ei pysty hienosäätämään halutuksi, vaan käsite loksahtaa johonkin toiseen niistä käsitteistä, jotka ovat mahdollisia.

Matemaattiset käsitteet ovat siis huomattavasti vähemmän vapaasti valittavissa kuin määritelmät. Ne ikäänkuin elävät omaa elämäänsä määritelmistä piittaamatta.

Kiitokset

Kiitän Tuomas T. Korppia aloitteen tekemisestä tämän kirjoituksen kirjoittamiseksi sekä osallistumisesta ideointiin.

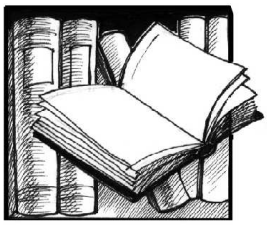
Viitteet

[1] Boyer, Carl: *Tieteiden kuningatar, matematiikan historia.* Osa I sivut 1–469. Osa 2 sivut 471–982. Suomentanut Kimmo Pietiläinen. Art House, 1994.

[2] Cormen, Thomas H. & Leiserson, Charles E. & Rivest, Ronald L.: *Introduction to Algorithms.* The MIT Press, 1990.

[3] Nurmi, Timo & Rekiaro, Ilkka & Rekiaro, Päivi: *Suomalaisen sivistyssanakirja.* Gummerus Kirjapaino Oy, Jyväskylä 1995.

[4] Stroustrup, Bjarne: *The C++ Programming Language, Third Edition.* Addison-Wesley, 1997.



Suomen matematiikan pioneereja

Matti Lehtinen
Maanpuolustuskorkeakoulu

Olli Lehto: Tieteen aatelia. Lorenz Lindelöf ja Ernst Lindelöf. Otava 2008. 398 sivua. 44,30 e.

Hiljattain katselin television tietokilpailuohjelmaa, jossa vastaajien on arvioitava, tietävätkö suomalaiset laajemmin oikeita vastauksia esitettyihin kysymyksiin. Sain tietää, että enemmistö suomalaisista ei enää tiedä, kuka on kehittänyt pesäpallon. (Oikea vastaus on Lauri eli Tahko Pihkala). Kuinka moni matematiikan alalla Suomessa nykyään enää muistaa, että matematiikan tieteenä ja tutkimuksena saattoivat Suomessa alkuun isä ja poika Lindelöf. Olli Lehdon uusi kirja palauttaa tämän tosiasian mieleen.

Suomen matematiikan isänä voi monesta syystä pitää Ernst Lindelöfiä: hän toi Suomeen funktioteorian ja kasvatti tutkijat, jotka hänen ohellaan nostivat Suomen maailmankärkeen tällä matematiikan osa-alueella, ja Lindelöfin opetustoiminta, ennen muuta hänen mainiot oppikirjansa, vaikuttivat laajasti maamme matemaattisen tiedon tason kohoamiseen. Ja Lorenz Lindelöf puolestaan ei ole vain Ernst Lindelöfin isä, vaan laajasti matematiikan ulkopuolellakin toiminut ja monin tavoin maamme historiaan vaikuttanut henkilö.

Aika kuluu ja sukupolvet vaihtuvat. Kun tämän kirjoittaja 1960-luvulla aloitteli opintojaan, Ernst Lindelöfin oppikirjoja sai vielä kirjakaupoista ja hänen oppilaittensa oppilaat opettivat Helsingin yliopistossa. Näihin kuuluu akateemikko Olli Lehto, joka on jälleen tehnyt merkittävän kulttuuriteon pelastamalla Lindelöfien, isän ja pojan, elämäntyön kansien väliin. Aikaisemminhan olemme jo saaneet nauttia hänen tallentaminaan Rolf Nevanlinnan ja Väisälän kolmen tiedemiesveljeksen, Vilhon, Yrjön ja Kallen elämäkerroista.

Ernst Lindelöfin matemaatikkomaineen tunteva lukija saattaa hämmästyä kirjan materiaalijakaumaa. Varsinaisesta tekstiosuudesta noin 220 sivua käsittelee Lorenz Lindelöfiä ja vain 130 Ernst Lindelöfiä. Selitys on osin kohteiden toimintakentissä. Lorenz Lindelöf (1827–1908) eli huomattavan monipuolisen elämän. Hän syntyi köyhässä Karvian pappilassa, opiskeli Helsingin yliopistossa tähtitieteilijäksi ja aloitti uraansa Pulkovan observatoriossa Pietarissa, pätevöityi pikavauhtia matematiikan professoriksi, loi käytännössä ensimmäisenä suomalaisena kansainvälisiä matemaattisia suhteita, kohosi yliopiston rehtoriksi, osallistui merkittävänä vaikuttajana säätyvaltiopäiviin kolmessa eri säädyssä, aateloitiin ja nousi aatelissäädyn johtoon, maamarsalkaksi, oli Helsingin kaupunginvaltuuston puheenjohtajanakin, toimi vuosikymmeniä Kouluylihallituksen johtajana, sekä Suomen Tiedeseuran sihteerinä eli käytännössä tuolloin Suomen ainoan yleistieteellisen yhteisön johdossa. Kouluhallituksen ja sen seuraajan opetushallituksen seinien sisällä eivät sittemmin olekaan vaikuttaneet matemaattisesti huippupätevät johtajat.

Ernst Lindelöfin (1870–1946) ura ei ollut yhtä monipolvinen. Hänkin tuli nuorena matematiikan professoriksi, teki neljännesvuosisadan ajan matemaattis-

ta tutkimustyötä, joka on jättänyt enemmän jälkiä matematiikan kansainväliseen sanastoon kuin kenenkään muun suomalaisen (Lindelöfin peitelause, Lindelöfin avaruus, Lindelöfin hypoteesi, Phragmén-Lindelöfin lause, Picard-Lindelöfin approksimaatio, Lindelöfin periaate), koulutti Suomeen joukon ensi luokan matemaatikkoja (mm. Rolf ja Frithiof Nevanlinna, P. J. Myrberg ja Kalle Väisälä) ja kirjoitti hienon oppikirjasarjan (Johdatus korkeampaan analyysiin, Differentiali- ja integralilasku ja sen sovellukset I–IV, Johdatus funktioteoriaan). Myös Ernst Lindelöf oli vuosikymmenet Suomen Tiedeseuran sihteerinä.

Lehto kertoo Lindelöfeistä tuttuun asiallisen mukaansatempaavaan tapaansa, hyvin jäsennellysti, kritiikkiä ja huumoriakaan unohtamatta. Varsinkin Lorenz Lindelöfiä käsittelevä osuus on samalla Suomen autonomian ajan valtiollisen ja kulttuurihistorian hieno läpileikkaus. Kuinka moni on tiennyt, että Lorenz Lindelöfin variaatiolaskentaa käsitelleen Pariisissa julkaistun ranskankielisen monografian esitteli vuoden 1861 Litteraturbladetissa itse J. V. Snellman? Humanismi ja matematiikka eivät ilmeisesti tuolloin olleet vielä niin toisistaan etääntyneitä kuin nyt – ainakin laajan matemaattisesti lähes lukutaidottoman kansan- ja sivistyneistönosan mielestä. Kuvaus Lindelöfin monipuolisesta vaikuttamisesta koulumaailmassa ja -hallinnossa on hyvä muistutus itse kullekin opetuksen parissa työskentelevälle siitä, minkälaiset tiet ovat johtaneet nykyiseen tieto- ja koulutusyhteiskuntaan. Myös ihmisinä Lindelöfit tulevat Lehdon kirjassa kauniisti esiin.

Vaikka Lehdon kirjaan liittyy kattava ja kunnioitettavan laaja lähdeluettelo, lukijaa ei rasiteta nooteilla. Paikoin tätä hiukan harmitteleekin: Lindelöfien toimintaa luonnehditaan useasti aikalaiskirjoittajilta lainatuin katkelmin, joiden kirjoittajat eivät aina tule lukijan tietoon. – Yhden asiavirheen poikkeuksellisen hyvin painovirheidenkin suhteen huolitellusta teoksesta huomasin: Vaikka Suomen matemaattinen yhdistys yhä jakaa vuosittaisen Ernst Lindelöf -palkinnon parhaasta edellisen vuoden aikana kirjoitetusta matematiikan pro gradu -työstä, ei palkintoon enää liity Lehdon mainitsemalla tavalla Ernst Lindelöfin 80-vuotispäivän muistoksi lyötyä mitalia: mitalit loppuivat jo muutama vuosi sitten.

Suomen Tiedeseura kunnioittaa Olli Lehdon teoksen kautta kahta merkittävää vaikuttajaansa: Tieteen aatelia on seuran jo vuodesta 1858 ilmestyneen sarjan Bidrag till kännedom av Finlands natur och folk numero 175.

Tilastotieteilijä tarvitsee matematiikkaa – entä matemaatikko tilastotiedettä?

Seppo Laaksonen
Matematiikan ja tilastotieteen laitos
Helsingin yliopisto

Palasin yliopistomaailmaan vuonna 2002 pidemmän poissaolon jälkeen. Opetuskokemusta on nyt kertynyt sekä yleisiltä että erityisiltä kursseilta sekä ohjauksesta. Yllättävää on ollut huomata, ettei tilastotieteen asema ole kohentunut yliopistossa vaikka työelämässä jatkuvasti olen havainnut alan osaajien puutteen. Myös olen hämmästellyt sitä, että perusylioppilas tietää tilastotieteestä edelleen vähän ja monet pääaineopiskelijatkin ovat tulleet alalle sattumalta, ilman intohimoa. Väistämättä tämän täytyy johtua kouluopetuksen luonteesta.

PISA-tulosten mukaan Suomen yläasteikäiset koululaiset pärjäävät yhä mainiosti matemaattis-tilastollisessa lukutaidossa, mitä nimeä taidan tosin ainoana käyttää. Monet PISA-tehtäväthän ovat tilastollisia, jopa hieman todennäköisyyksiinkin viittaavia eli ei sitä matematiikkaa mitä kunnon matemaatikot rakastavat.

Oltakoonpa terminologiasta mitä mieltä tahansa, niin olen huolestunut ylioppilassukupolvien matemaattisesta osaamisesta. Minulle kerrotun mukaan yksi kolmannes ylioppilaskokelaista ei osallistu minkäänlaiseen matemaattiseen tenttiin ja suorittajista osa ei kuulemma käytännössä osaa juuri mitään. Tämä näkyy yliopistojen ja varmaan myös ammattikorkeakoulujen kursseilla, joissa muun muassa tilastotieteen perusopinnot ovat pakollisia monille. Jopa peruslaskutoimitusten ja suuruussuhteiden ymmärtämisessä on suuria vaikeuksia, saati sitten että vaikkapa integrointi ja derivointi onnistuisivat.

Jotain siis olisi syytä tehdä. Yksi perusvaatimukseni olisi asettaa ainakin jokin matemaattis-tilastollinen alue pakolliseksi ylioppilaille. Huolella toki pitäisi miettiä mikä tai mitkä olisivat sopivia alueita. Toinen ehdotukseni on opetuksen motivoinnin parantaminen siten, että matematiikan sovellus ja siis hyöty tulisivat entistä paremmin esille. Tämän kirjoituksen jatkossa esitän muutamia ajatuksia ja myös konkreettisia esimerkkejä tältä näkökulmalta.

Esitelkää matematiikan käsitteiden yhteyksiä käytäntöön

En tunne tarkasti lukion matematiikan oppisisältöjä. Tilastotieteellistä otetta siellä on joka tapauksessa liian vähän. Mutta kaikille matematiikan oppiaineksille on helppo löytää käytännön kytkentöjä. Opettajille tutuimpia lienevät fysiikan tai kemian kytkennät. Toivottavasti niitä tuodaan esille.

Tilastollisia kytkentöjä on varmasti myös kaikkialla. Esimerkiksi integrointi johtaa empiirisen aineiston piirissä summaamiseen, jossa yhteydessä käytetään summamerkkiä. Tämä näyttää olevan ylioppilaille kummajainen. Logaritmia ei enää nykysukupolvi hahmota suh-

teellisen mittaamisen upeana välineenä. Itsehän tämän opin laskutikun kautta. Tästä syystä tilastollisessa grafiikassa esiintyy jatkuvasti huonoja asteikkoja, siis absoluuttisia suhteellisten sijasta. Vastaavasti harhaudutaan eksponentin ymmärtämättömyyden takia toiseen suuntaan. Polynomit ovat myös paljon käytettyjä, osin logaritmien ja eksponenttien rinnalla. Tämän artikkelin loppuosa keskittyy polynomeihin pyrkien havainnollistamaan näiden hyötykäyttöä.

Polynomit, niiden derivointi ja ääriarvot

Polynomit ovat kivoja funktioita. Yksinkertaisin vaihtoehto on puhdas vaakasuora mitä jossain yksinkertaisessa tilanteessa käytetään tilastotieteessä, jolloin se merkitsee esimerkiksi keskiarvoa tai mediaania. Vielä yleisempi polynomi on suora, josta tilastotieteessä käytetään nimitystä lineaarinen. Jos se derivoidaan, saadaan vakio eli suoran kulmakerroin. Useamman asteisille polynomeille ei tilastotieteessä tietääkseni ole erityisiä nimiä. Seuraavaksi esitän kolme esimerkkiä, joissa vähintään esiintyy toisen ja kolmannen asteen polynomeja. Nämä ovat aika yleisiä tilastotieteessä ja sen sovellustieteissä kuten talous- ja sosiaalitieteissä.

Esimerkki 1: Ikäonnellisuus

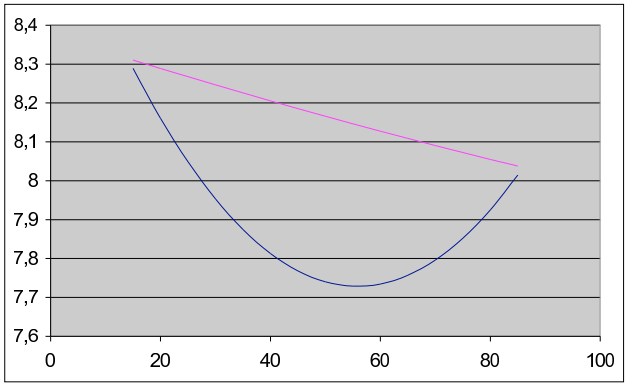
Onnellisuuden tutkimus on yleistynyt erityisesti psykologiassa ja taloustieteissä. Kun aihetta tutkitaan empiirisesti, tarvitaan tilastollinen aineisto. Tavallisesti aineisto koostuu ihmisille esitetyistä kysymyksistä. Tässä esitettävä tulos perustuu Euroopan yhteiskuntatutkimuksen (Europeansocialsurvey.com) 15 vuotta täyttäneistä suomalaisista kerättyyn haastatteluaineistoon vuosilta 2002-2007.

Onnellisuuden taustatekijöistä suuri kiinnostus on kohdistunut ikään. Taloustieteilijät ovat havainneet, että monesti ikäonnellisuus noudattaa ns. U-käyrää eli onnellisuus on nuorena korkea, laskee sitten keski-ikään mennessä jolloin alkaa taas nousta. Yksilöaineistosta tutkittuna tämä käyrä tarkoittaa paraabelia. Tilastotieteilijä tutkii asiaa asettamalla malliin kaksi selittäjää, iän ja sen neliön. Tämän jälkeen hän estimoi sen ja katsoo tuloksista, onko väitteellä perää.

Selitin ihmisen kokemaa onnellisuutta (asteikko 0-10) tilastollisella mallilla ikä ja sen neliö selittäjinä, kummallekin sukupuolelle erikseen. Estimointitulokset ovat seuraavassa:

$$\begin{aligned}&\text{onnellisuus(naiset)}\\ &\quad = 0{,}000006476\,\text{ikä}^2 - 0{,}0045424\,\text{ikä} + 8{,}3775\\ &\text{onnellisuus(miehet)}\\ &\quad = 0{,}000336286\,\text{ikä}^2 - 0{,}037554\,\text{ikä} + 8{,}7772\end{aligned}$$

Kuvio 1 havainnollistaa tilannetta graafisesti. Tästä näemme että naisten ja miesten onnellisuus on melko sama nuorena ja vanhana mutta miesten onnellisuus laskee selvästi nuoruuden jälkeen. Lukion matematiikan opeilla on helppo laskea minimi-iät, ensin derivoimalla ja sitten ratkaisemalla nollakohdat; tee se. Tulos miehille on 55,8 vuotta ja naisille 350 vuotta



Kuvio 1. Onnellisuus paraabelilla estimoituna naisille (ylempi käyrä) ja miehille (alempi).

Kuviosta ja minimistä on helppo nähdä, että miesten käyrä on jossain määrin U:n muotoinen mutta naisten ei, vaikka siis estimointi antaa ylöspäin aukeavan paraabelin. Ei ole kuitenkaan järkeä ajatella naisten käyrän olevan U-mainen. Miksi? Käyrä on mieluummin lähes lineaarinen.

Tässä esimerkissä esitin vain matemaattisen näköisen puolen, samoin tapahtuu esimerkissä 2. En siis keskustele paraabeliin liittyvää epävarmuutta mitä siihen tietystikin liittyy. Käyrällä on siis tosiasiassa tietty luottamusväli, samoin kuin minimiarvoissa.

Esimerkki 2: Ikä ja palkka

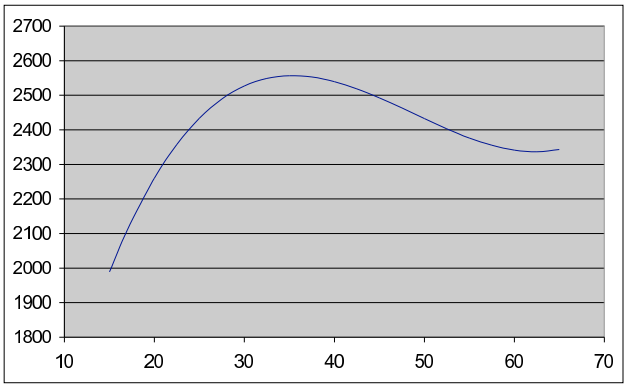
Toinen esimerkki on eräänlainen laajennus edelliselle. Nyt käytössä on kolme selittäjää, ikä, sen neliö ja sen kuutio. Siten muodostuva funktio on kolmatta astetta. Selitettävänä on palkansaajan kuukausipalkka eräässä aineistossa.

Ihan samalla periaatteella kuin esimerkissä 1 estimoin yhtälön:

$$\text{palkka} = 0{,}0225\,\text{ikä}^3 - 3{,}292\,\text{ikä}^2 + 148{,}6$$

Vastaavasti tein Kuvion 2. Kaikki kolme muuttujaa ovat merkitseviä, mikä antaa edellytyksen uskoa että palkkakäyrässä on sekä minimi että maksimi. Nämä voidaan ratkaista derivoimalla ja sitten ratkaisemalla nollakohdat. Huippukohta saavutetaan tällä aineistolla varsin nuorena eli 35,4 vuoden iässä. Tämän jälkeen

palkka laskee mutta alkaa nousta juuri ennen tavallista eläkeikää eli 62,3 -vuotiaana (selitykseni on se, että korkeapalkkaiset jatkavat työelämässä pidempään). Tarkista tulosten oikeellisuus.



Kuvio 2. Palkka kolmannen asteen käyrän funktiolla estimoituna.

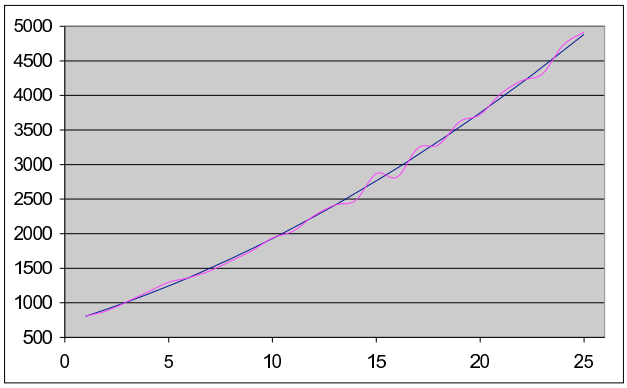
Matalimmillaan palkka on toki työelämään siirryttäessä, mikä on tässä asetettu 15 vuoden kohdalle mistä saakka havaintoja oli aineistossa, joskin vähän. Vanhimmat palkansaajat tässä ovat 64-vuotiaita. Matemaattisesti käyrä voidaan piirtää näiden ikien ulkopuolelle, mutta tilastollisesti ei ole niin syytä tehdä. Onnellisuuskuviossa asetin käyrän välille 15-85 -vuotiaat, vaikka vanhimmat vastaajat olivat 99-vuotiaita. Jos haluat, jatka käyrää tänne asti.

Esimerkki 3: Aikasarja

Tämä esimerkki ei ole todellinen mutta tähtää havainnollistamaan todellisuutta. Muodostin 25 havaintoyksikköä, jotka merkitty ajankohtina t. Toiseksi tein teknisen muuttujan x joka saa arvoja 15:sta 39:een yhden yksikön välein. Tässä on siis yksinkertainen aritmeettinen sarja.

Varsinaisen aikasarjamuuttujan muodostin toisen asteen polynomilla $3x^2+8x+10$. Huomaa että tämän ensimmäinen derivaatta $= 6x+8$ ja toinen $= 6$. Taulukossa 1 tätä aikasarjaa merkitsen symbolilla y. Se on siis funktiomuotoinen ja ajattelen sen tässä olevan suurin piirtein estimoitu oikeista havaintoarvoista yr. Oikeat havaintoarvot eivät koskaan noudata mitään funktiomuotoa mutta voivat olla lähellä sellaista. Tutkijan jatkotyö on helppoa, jos löytää aineistossa funktiomaisen yhteyden. Tässä esimerkissä tilanne on hoidettu niin, että yhteys on varsin hyvä. Katso itse tätä Kuviosta 3.

Havaitsemme kuviosta ehkä selkeämmin kuin taulukosta, että aikasarja kasvaa kiihtyvästi. Kuvio muistuttaa eksponentiaalista kasvua, sillä paraabelilla on sopivilla parametriarvoilla samanlaisia ominaisuuksia. Voit itse tehdä oman kokeesi eksponenttifunktiomuotoa käyttämällä.



Kuvio 3. Todellinen aikasarja ja sen funktiomuoto.

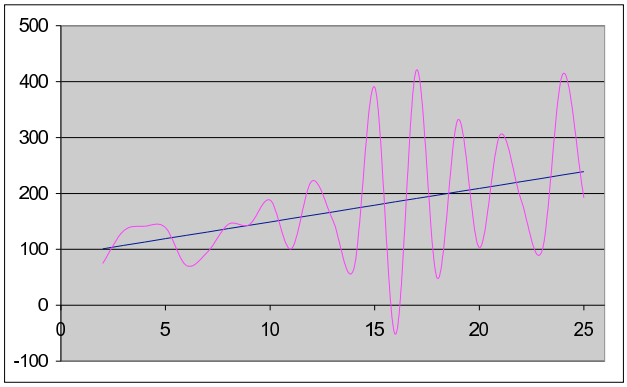
Aikasarjaa voi tutkia monin tavoin. Tässä tutkitaan muutosta mikä esimerkissä tarkoittaa kasvua. Analoginen mutta päinvastainen tilanne koskee vähenemistä.

Laskin kummallekin aikasarjalle aritmeettiset muutokset eli differenssit (asiaa voisi tutkia myös suhteellisesti):

diff1y = y:n arvon muutos
ajankohdasta t ajankohtaan $t+1$

diff1yr = yr:n arvon muutos
ajankohdasta t ajankohtaan $t+1$

Taulukosta näemme, että y:n differenssisarja on nyt aritmeettinen, arvot kasvavat edellisestä aina 6:lla, mikä on ensimmäisen derivaattafunktion kulmakerroin ja toisen derivaattafunktion vakiotermi. Todellinen aikasarjani ei ole näin kaunis, vaan vaihtelut ovat suurehkoja, keskiarvokin jää noin 5:een. Teoria ei siis täysin istu todellisuuteen mikä on ymmärrettävää. Kuvio 4 havainnollistaa tätä eroa.



Kuvio 4. Ensimmäiset differenssit todelliselle ja teoreettiselle sarjalle.

Teoreettinen sarja on lineaarinen ja sen kulmakerroin on siis 6. Tämä viiva asettuu kuitenkin hyvin todellisten havaintoarvojen keskelle. Todellisista estimoitu kulmakerroin on 6,1 eli lähellä teoreettista todellisuutta.

Aikasarja-analyysissä on tapana ottaa toiset differenssit eli ensimmäisten differenssien differenssit. Taulukossa nämä on merkitty seuraavasti:

diff2y = diff1y:n arvon muutos
ajankohdasta t ajankohtaan $t+1$

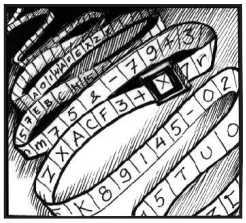
diff2yr = diff1yr:n arvon muutos
ajankohdasta t ajankohtaan $t+1$

Havaitsemme että teoreettisen sarjan arvot ovat vakioita eli siis toisen derivaatan arvoja. Tämä osoittaa että aikasarjan y kasvu ei ole kiihtyvää vaan on aivan tasainen. Todellisessa sarjassa ei nytkään havaita yhtä kaunista asetelmaa. Muutosten muutokset vaihtelevat huomattavasti mutta mitään selvää trendiä niistä ei havaita. Tämä siis myös osoittaa ettei kasvu ole kiihtyvää. Jos haluat, voit piirtää tästä osasta vastaavan kuvion kuin edellä.

Tässä esimerkissäni käytin funktiomaista aikasarjaa jotta derivoinnin ja differenssioinnin yhteys näkyy hyvin. Kokeile muilla funktiomuodoilla vastaavaa myös. Käytännössä ei siis löydy hyvää funktiomuotoa millä tilanteen näkisi yksinkertaisesti. Differenssioinnin sen sijaan voi aina tehdä. Jos toisen differenssin arvoissa havaitset ylöspäin menevää trendiä, kasvu on kiihtyvää; jos se näyttäisi menevän alaspäin, kasvu on hidastuvaa (kuten taloustieteilijät äskettäin uskoivat Suomessa tapahtuvan). Vähenemisen puolella voidaan käyttää vastaavia termejä. Esimerkiksi hidastuva väheneminen tai alaspäinmeno jossakin asiassa merkitsee monelle jo positiivista signaalia.

t	x	y	yr	diff1y	diff1yr	diff2y	diff2yr
1	15	805	804				
2	16	906	878	101	74		
3	17	1013	1011	107	133	6	59
4	18	1126	1151	113	140	6	7
5	19	1245	1289	119	138	6	-2
6	20	1370	1360	125	71	6	-67
7	21	1501	1455	131	95	6	24
8	22	1638	1599	137	144	6	49
9	23	1781	1742	143	143	6	-1
10	24	1930	1929	149	187	6	44
11	25	2085	2030	155	101	6	-86
12	26	2246	2250	161	220	6	119
13	27	2413	2402	167	152	6	-68
14	28	2586	2466	173	64	6	-88
15	29	2765	2854	179	388	6	324
16	30	2950	2803	185	-51	6	-439
17	31	3141	3221	191	418	6	469
18	32	3338	3269	197	48	6	-370
19	33	3541	3600	203	331	6	283
20	34	3750	3702	209	102	6	-229
21	35	3965	4005	215	303	6	201
22	36	4186	4193	221	188	6	-115
23	37	4413	4290	227	97	6	-91
24	38	4646	4702	233	412	6	315
25	39	4885	4893	239	191	6	-221

Taulukko 1. Aikasarjani aineisto ja sen muunnokset.



Lukuteoriaa ja salakirjoitusta, osa 2

Heikki Apiola
Matematiikan laitos, Teknillinen korkeakoulu

Virittelyksi

Kirjoitus on jatkoa numerossa 3/2007 olleelle esiosalle (`solmu.math.helsinki.fi/2007/3/apiola.pdf`), jossa esitellään lukuteoreettisia perustyökaluja tämän varsinaisesti salakirjoitukseen pureutuvan osan 2 tarpeisiin. Viittaan ykkösosaan roomalaisella I:llä.
Käytän myös joissakin kohdissa vektori- ja matriisitermejä. *Vektori* tarkoittaa yksinkertaisesti lukujonoa, lukujen järjestettyä listaa. Matriisi on lukutaulukko, jossa on samanpituisia vektoreita allekkain. Voit palauttaa vektorin aiempiin vektorimielikuviisi vaikkapa Solmun numerossa 1/2007 olleen kirjoituksen (`solmu.math.helsinki.fi/2007/1/apiola.pdf`) alkua silmäilemällä.

Kryptologia - salaustiede

Tiedon salaamisen/turvaamisen tarvetta on esiintynyt ihmiskunnan historiassa vuosituhansien ajan. Vanhimmat löydökset ovat n. 4500 vuoden takaa Egyptin vanhasta kuningaskunnasta.

Nimitykset *kryptologia* ja *kryptografia* on johdettu kreikankielen sanasta *kryptós*, salattu, salainen. *Kryptologia* näyttää vakiintuneen yleistermiksi, joka sisältää osinaan *kryptografian* eli salaamisteknisten menetelmien suunnittelutieteen ja *kryptoanalyysin*, jonka piiriin kuuluvat menetelmien luotettavuuden analysoiminen, heikkouksien paljastaminen, salakoodien murtaminen jne. Niin sankarit, konnat kuin viileän objektiiviset menetelmien tutkijat ja testaajat työskentelevät *kryptoanalyytikon* velvoittavan nimikkeen alla.

Lähihistorian dramaattisimpiin tapahtumiin kuuluvat liittoutuneiden onnistuneet saksalaisten *Enigma*-salakirjoituskoneen sanomien murtamiset (kts. [Wiki]). Tämä pohjautui puolalaisen matemaatikon Marian Rejewskin vuonna 1932 tekemiin keksintöihin. Hän onnistui algebrallista tekniikkaa käyttäen pääsemään Enigma-salauksen jäljille. Hänen ryhmänsä luovutti tuloksensa vuonna 1939 ranskalaisille ja englantilaisille kryptoanalyytikoille. Brittien Saksan merivoimiin kohdistuvaa kryptoanalyyttista toimintaa johti matemaatikko ja teoreettisen tietojenkäsittelytieteen isä, *Alan Turing*, jonka ryhmä onnistui joulukuussa 1940 murtamaan saksalaisten Enigma-koodin. Joissakin lähteissä esiintyy arvioita, joiden mukaan pelkästään tämän onnistumisen ansiosta toinen maailmansota lyheni useilla vuosilla.

Pieni englantilainen paikkakunta, jonne sodanaikainen kryptoanalyyttinen toiminta keskittyi, on nimeltään *Bletchley Park*. Siellä toimii nykyisin museo: `www.bletchleypark.org.uk/`. Sattumoisin *Turingin* elämästä kerrotaan musiikin keinoin Ooppera Skaalan esityksissä maaliskuusta 2008 alkaen.

Kryptologian historia tarjoaa monta muutakin jännitysseikkailua. Niihin liittyviä lukuelämyksiä voi etsiä

ehkä parhaiten alan klassikosta [CodeB]. Hiiren napsauttamisen päässä olevaa historiatietoa on tutussa lähteessä [Wiki].

Toisen maailmansodan jälkeisiin aikoihin saakka salakirjoitusmenetelmät perustuivat viestin kirjaimien jonkinlaiseen uudelleen järjestämiseen tai sekoittamiseen. Tietotekniikan kehittymisen myötä mekaaniset laitteet voitiin korvata tietokoneohjelmilla.

Alan vallankumouksellinen käännekohta ajoittuu 1970-luvun lopulle. Vuonna 1976 Stanfordin yliopiston tutkijat *Withfield Diffie* ja *Martin Hellman* esittivät julkaisussaan [DH] ns. *julkisen avaimen menetelmän*. Ensimmäisen konkreettisen esimerkin toimivasta julkisen avaimen salausjärjestelmästä esittivät MIT:n tutkijat *R. Rivest, A. Shamir, L. Adelmann* [RSA]. Heidän sukunimiensä alkukirjainten mukaan sai nimensä RSA-salausmenetelmä.

Kannattaa myös mainita, että alalla on suomalaisia, kansainvälisesti arvostettuja tutkijoita, kuten akateemikko, emeritusprofessori *Arto Salomaa* tutkimusryhmineen ja professori *Kaisa Nyberg*, jonka kirjoitus [KN] on kattava, monipuolinen ja ajantasainen katsaus kryptologiaan. *Salomaan* julkaisut ja monografiat, joista viitteenä [AS], ovat runsaasti referoituja, alan kansainvälistä huippua edustavia klassikoita.

1900-luvun puolestavälistä lähtien salausmenetelmät ovat alkaneet käyttää enenevässä määrin matematiikkaa, erityisesti abstraktia algebraa ja lukuteoriaa, kombinatoriikkaa, todennäköisyyslaskentaa ja tilastotiedettä, algoritmien vaativuusanalyysiä, jne.

Tietokoneiden prosessoritehon jatkuva kasvaminen antaa ”ilmaiseksi” kryptoanalyytikoille raakaan voimaan perustuvia työkaluja salakoodien murtamiseen. Tämä pitää kryptografia-joukot vireinä ja pakottaa suunnittelemaan entistä nerokkaampia ja mielikuvituksellisempia menetelmiä. Kvanttitietokonelaskennan mahdollisuuksiin on jo alettu varautua, kts. [Wiki] ja *Mikko Möttönen*: Kvantti-informaatio – tämän vuosisadan vallankumous !?, Arkhimedes 1/2008.

Salaustieteen ja -tekniikan käytön painopiste on siirtynyt puolustusvoimiin ja tiedusteluun liittyvästä käytöstä selkeästi jokaisen kansalaisen arkipäivään kuuluvaksi asiaksi. Kaikki luottamuksellisten tietojen välittäminen Internetissä, sähköposti, sähköinen kaupankäynti, pankkitoiminta, tietojärjestelmien salasanat, matkapuhelinliikenne, sähköinen allekirjoitus, äänestys, sirukortit jne. ovat täysin salaamistekniikasta riippuvaisia.

Kirjoitukseni tarkoituksena ei ole antaa kattavaa katsausta alaan muuten kuin tarjoilemalla kiinnostuneille lisäviitteitä eri suuntiin. Varsinainen päämäärä on avata alkeista lähtien yksityiskohtainen matemaattisten päättelyiden ketju näyttääkseni, miten RSA-menetelmä toimii ja valaista sitä esimerkein. Tätä varten joudun vielä jonkinverran täydentämään kirjoituksen osassa 1 kehiteltyä lukuteorian välineistöä.

Parhaassa tapauksessa kirjoitus voisi inspiroida jotakuta matematiikan opettajaa kehittämään aineksia lukion erikoiskurssille tai matematiikkakerholle (jos sellaisia jossain on).

Kertaustietoisku mod-laskennasta

Modulaariaritmetiikka on keskeisessä osassa, joten kerrataan vielä:

$a \equiv b \pmod{n}$ tarkoittaa, että on olemassa kokonaisluku k siten, että $a = b + k\,n$. Toisin sanoen, $n \mid (a-b)$ eli $a - b$ on jaollinen n :llä.
Kun puhutaan luvusta $b \pmod{n}$, tarkoitetaan yleensä pienintä ei-negatiivista muotoa $b \pm k\,n$ olevaa lukua, toisin sanoen jakojäännöstä jakolaskussa b/n. Näin toimivat myös alla olevissa esimerkeissä käytettävät MATLAB- ja MAPLE-ohjelmistojen `mod`- funktiot: MATLAB:ssa `mod(b,n)` ja MAPLE:ssa `b mod n`.

Symmetrisistä salakirjoitusmenetelmistä

Monet lukijoista lienevät joskus nuoruudessaan kokeilleet jotain tapaa välittää viestiä salatussa muodossa sekoittamalla sopivasti viestin kirjaimia. Kenties yksinkertaisin menetelmä on korvata sanan kukin kirjain aakkosissa seuraavalla kirjaimella. Tätä menetelmää käytettiin myös kuuluisassa, vuonna 1968 valmistuneessa elokuvassa ”2001: A Space Odyssey” (A.C. Clarke, S. Kubrick), jossa vallankaappausta avaruusaluksen miehistöltä yrittänyt tietokone oli nimeltään `HAL 9000`. Toki tässä nimessä oli kyse vain pienestä pikantista kuriositeetista, joka aukeni osalle katsojia.

Vakaviin sotilaallisiin tarkoituksiin menetelmää lienee käyttänyt ensimmäisenä *Julius Caesar*. Hän on tiettävästi soveltanut kolmen kirjaimen siirtoa eteenpäin viestin salaamiseen ja vastaavasti saman määrän siirtoja taaksepäin salakoodin avaamiseen. Tämän tyyppisiä menetelmiä, jossa kirjainta siirretään aakkosissa määrätty määrä, kutsutaankin yleisesti Caesarin menetelmiksi.

Esimerkki Caesarin menetelmästä

Suoritin itse esimerkin MATLAB-ohjelmaa hyödyntäen, mutta en paneudu ohjelman syntaksiin. Otan vain joitakin MATLAB-näytteitä ja sanontoja, jotka ovat itsensä selittäviä.

Muodostetaan merkkivektorit

```
>> AAKKOSET='ABCDEFGHIJKLMNOPQRSTUVWXYZÅÄÖ '
>> viesti='SAMMONRYÖSTÖ'
```

Muutetaan viestin kirjaimet numeeriseksi vektoriksi laskemalla kunkin kirjaimen sijainti `AAKKOSET`-vektorissa. Siis esim. $A = 0, B = 1, \ldots, Z = 26, \ldots$ Saadaan:

```
18 0 12 12 14 13 17 24 28 18 19 28
```

Alkuperäisessä *Caesarin menetelmässä* lisäämme jokaiseen vektorin komponenttiin luvun 3. Lienee aika selvää, että Ö, jota vastaa numero 28, siirretään syklisesti aakkosten alkupäähän ja siitä tulee siis B (koska valitsimme aakkosvektorimme viimeiseksi merkiksi välilyönnin).

Tämä syklinen siirto tarkoittaa, että redusoimme tuloksen modulo $N = 30$, koska aakkosvektorin pituus on 30. (Voidaan ajatella aakkosvektori kierretyksi ympyrän muotoon, jonka kehällä liikutaan.) Toisin sanoen lasku numeroilla on $(28 + 3) \,(\mathrm{mod}\, 30) = 1$.

Yleisesti salausfunktiomme on siis $(x + 3) \pmod N$, missä x on viestin numeerisen esitysvektorin komponentti (viestin kirjainmerkkiä vastaava numero), ja N on aakkosvektorin pituus. MATLAB-istuntomme jatkuisi näin, kun ajatellaan, että edellä oleva viestin numeerinen esitysvektori on muuttujassa `nviesti`.

```
>> nsalaviesti=mod(nviesti+3,30)
21   3   15   15   17   16   20   27   1   21   22   1
>> AAKKOSET(nsalaviesti+1)
   VDPPRQUÄBVWB       salaviesti kirjaimilla
```

Salaviestin avaus

Viestin vastaanottajalla on tieto menetelmästä ja avainluvusta 3. Sehän voisi yhtä hyvin olla jotain muutakin. Viestin avaaminen tapahtuu salausfunktion käänteisfunktiolla, joka on mitä ilmeisimmin
$f^{-1}(y) = (y - 3) \bmod N$.

```
>> avattu=mod(nsalaviesti-3,N)
     18 0 12 12 14 13 17 24 28 18 19 28
>> AAKKOSET(avattu+1)
SAMMONRYÖSTÖ
```

Salaviestin avaus tuotti alkuperäisen viestin, joten hyvin kävi.

Niille, joita kiinnostaa MATLAB-syntaksi mainitsen, että `AAKKOSET(avattu+1)`-komento tarkoittaa `AAKKOSET`-merkkivektorin indeksointia numeerisella vektorilla, jonka komponentteihin pitää lisätä 1, koska MATLAB:ssa vektorin indeksointi aloitetaan luvusta 1, kun taas jakojäännöksillä laskenta vaatii indeksin alkamaan 0:sta. Sama ilmiö on tietysti lausekkeessa `AAKKOSET(nsalaviesti+1)`.

Yleisesti menetelmä voitaisiin esittää tähän tapaan:
Merkitään $Z_n = \{0, \ldots, n-1\}$. Salausfunktio
$S_e : Z_n \to Z_n; S_e(x) = (x + e) \pmod n$, missä e:tä voidaan kutsua *salausavaimeksi* ja funktiota S_e salausfunktioksi, joskus itse funktiota kutsutaan myös salausavaimeksi.
Salakoodi saadaan avatuksi salausfunktion S_e käänteisfunktiolla $S_e^{-1}(y) = (y - e) \pmod n$.

Menetelmä on *symmetrinen* siinä mielessä, että kun salaus(avain)funktio tunnetaan, niin salakoodin avaamisen suorittava käänteisfunktio voidaan välittömästi määrittää.

Kehittyneempiä symmetrisiä menetelmiä

Caesarin menetelmä yleisessäkin muodossaan on luonnollisesti hyvin haavoittuva.

Erilaisten mahdollisuuksien (salausavaimien) määrää voidaan huikeasti lisätä ottamalla salausfunktioksi jokin muu tapa sekoittaa kirjaimia. Jos otetaan mielivaltainen aakkosten "permutaatio", eli uusi järjestys, niin kaikkien mahdollisten salausavainten lukumäärä on $N!$, missä N on edelleen aakkosvektorin pituus. Yllä olevassa tapauksessa $N = 30$, jolloin saadaan kaikkiaan 30! mahdollisuutta. Kyseessä on luku, jossa on 33 numeroa, joten raakaan voimaan perustuva kaikkien eri mahdollisuuksien läpikäyminen ei onnistu.

Huolimatta avainten lähes äärettömästä määrästä, tämäkin menetelmä on monin tavoin haavoittuvainen. Kun on tiedossa kieli, jolla viestintä tapahtuu, voidaan kirjainten esiintymäfrekvenssien perusteella päästä oikeista kirjaimista selville. Esimerkiksi Suomen kielessä kirjain A on yleisin, joten (pitkässä) salakirjoitetussa viestissä suurimman esiintymäfrekvenssin omaava kirjain on todennäköisesti A. Ja niin edelleen. Frekvenssianalyysin käytöstä salausavaimen selvittämiseksi on hyviä esimerkkejä ja opastettuja harjoitustehtäviä mm. kirjassa [Kob] luvussa III.

Frekvenssianalyysin vaikeuttamiseksi viesti voidaan myös koodata jakamalla se ensin osiin, lohkoihin, jotka numeroidaan. Jos vaikka käytettäisiin 2:n pituisia lohkoja, niin kunkin komponentin numerot olisivat välillä $0, \ldots, N^2 - 1 = 899$, ja kyseessä olisi 2-kirjaimisten tavujen tunnistaminen. Kasvattamalla lohkon kokoa, sanokaamme suuremmaksi kuin 4, frekvenssianalyysiin perustuva tunnistus vaikeutuu olennaisesti.

Caesarin menetelmää on kehitetty ottamalla mukaan avainsana, joka määrää kirjaimien muuntumisen. Jos otetaan avaimeksi satunnainen merkkijono, joka on lähetettävän viestin pituinen, niin lasketaan yhteen

viestivektorin ja avainvektorin numeeriset esitysvektorit komponenteittain $\pmod N$. Yllättävää kyllä, tämä menetelmä, englanninkieliseltä nimeltään "one time pad", on ainoa tunnettu informaatioteorian mielessä luotettavaksi todistettu salausmenetelmä. Käytännössä se on kuitenkin monin tavoin hankala ja epäluotettava, avain on yhtä pitkä kuin viesti, avainvektorit ovat periaatteessa kertakäyttöisiä, ja avainten vaihto on työläs ja riskialtis operaatio

Vaikka salausmenetelmien "avantgarde" on epäsymmetristen menetelmien puolella, symmetrisiä menetelmiä kehitellään myös edelleen. Kohta esiteltävät epäsymmetriset menetelmät, joihin edellä mainittu RSA kuuluu, ovat pitkien viestien käsittelyssä raskaita. Siksi joudutaan usein käyttämään yhdistelmää, jossa esimerkiksi lähetetään symmetrisen menetelmän avain salattuna epäsymmetrisellä menetelmällä ja symmetrisellä salattu (pitkä) viesti.

Lukuteorian täydennystä

Osassa I käsiteltiin kokonaislukujen jaollisuusasiota ja modulaariaritmetiikkaa. Kannattaa kaivaa aktiivimuistiin nuo asiat, ainakin määritelmät ja lauseiden johtopäätökset. Tärkeimpiä: Jakoyhtälö (Lause I.1), SYT-lause (I.5), Eukleideen algoritmi, Fermat'n pieni lause (Lause I.13). Perusasioita lukuteoriasta löytyy myös *Jukka Pihkon* Solmun verkkolehteen kirjoittamasta "lukuteorian helmiä" -artikkelista [JP]. Tarvitsemme osassa I esitetyn lisäksi vielä lukuteoreettisen jälkiruokaannoksen.

Eukleideen algoritmin laajennus

Palautetaan mieleen lause *I*.8, joka sanoo, että syt(a,b) = syt(b,r), kun a esitetään jakoyhtälön (lause *I*.1) ilmaisemassa muodossa: $a = b\,q + r,\ 0 \le r < b$. Tämä edustaa askelta, joka riittävän monta kertaa toistettuna johtaa syt(a,b) :n arvoon. Menettelyä kutsutaan *Eukleideen algoritmiksi*.

Edelleen muistellaan erityisellä lämmöllä "SYTlausetta" *I*.5. Sehän paljastaa, että syt(a,b) :lle saadaan esitys muodossa $x\,a + y\,b$, missä x ja y ovat kokonaislukukertoimia.

Tähän mennessä olemme osanneet nautiskella pelkästään siitä tiedosta, että tuollaiset luvut x ja y ovat olemassa, menettelyä niiden määrittämiseksi emme ole esittäneet. Nyt on sen aika!

Katsotaanpa esimerkin valossa:

Esimerkki 1. *Määrättävä syt*(171,30).
$171 = 5 \cdot 30 + 21$.
Euklalgo: syt(171,30) = *syt*(30,21).
Jakoyhtälö: $30 = 1 \cdot 21 + 9$.
Euklalgo: syt(30,21) = *syt*(21,9).
Jakoyhtälö: $21 = 2 \cdot 9 + 3$.
Euklalgo: syt(21,9) = *syt*(9,3) = 3.
(Seuraava jakoyhtälö: $9 = 3 \cdot 3 + 0$ *johtaisi jakojäännökseen* $r = 0$*, joka on algoritmin lopetusehto.)*
Siis syt(171,30) = 3.

Tähän saakka kerrattiin vanhaa. Johtaaksemme tavoitellun esityksen, käytämme luvuille kirjainsymboleja asian selkeyttämiseksi. Merkitään $a = 171, b = 30$, ja syntyvät jakojäännökset olkoot $r_1, r_2, r_3, \ldots$. Tässä $r_1 = 21, r_2 = 9, r_3 = 3, r_4 = 0$.
Päämääränä on siis lausua viimeinen nollasta poikkeava jakojäännös (tässä r_3) muodossa $r_3 = x\,a + y\,b$. Kirjoitetaan yllä olevat jakoyhtälöt näitä merkintöjä käyttäen:

$$\begin{cases} a = 5 \cdot b + r_1 \\ b = r_1 + r_2 \\ r_1 = 2 \cdot r_2 + r_3. \end{cases}$$

Kun tämä puretaan alhaalta ylöspäin, saadaan haluttu esitys. Tarkemmin sanottuna:

1. Ratkaistaan alimmasta yhtälöstä r_3 r_1:n ja r_2:n avulla.
2. Sijoitetaan tähän r_3:n lausekkeeseen r_2 ratkaistuna toiseksi alimmaisesta yhtälöstä r_1:n ja b:n avulla.
3. Sijoitetaan näin saatuun r_3:n lausekkeeseen r_1 yhtälöstä 1 lausuttuna a:n ja b:n avulla. Tämä strategia konkretisoituu esimerkkimme tilanteessa näin:

$r_3 = r_1 - 2 \cdot r_2$.
$r_2 = b - r_1$ sij. (3):een $\implies$ $r_3 = r_1 - 2 \cdot b + 2 \cdot r_1 = 3 \cdot \underbrace{r_1}_{a - 5 \cdot b} - 2 \cdot b$

Sieventämällä: $\text{syt}(a,b) = r_3 = 3 \cdot a - 17 \cdot b$.

Menettely on nimeltään *Laajennettu Eukleideen algoritmi*.
Huomautan, että kirjoituksessa [JP] on toinen vastaavanlainen esimerkki laskettuna auki. Samaisessa kirjoituksessa [JP] ss. 6–7 esiintyy myös hauska konstruktiivinen todistus SYT-lauseelle. Todistus etenee *Eukleideen algoritmin tahdissa*, toisin kuin se, jonka esitin osassa I. Vastaavanlaisia esimerkkejä on myös kirjoissa [I. Lukio1] ja [I. Lukio2] aihepiireissä *Eukleideen algoritmi* ja *Diophantoksen yhtälöt*.

Ohjelma laajennettuun Eukleideen algoritmiin.

Nämä esimerkit huolella läpikäytyään lukija varmasti vakuuttuu siitä, että tällainen tehtävä voidaan aina ratkaista, ja osaa pyydettäessä ratkaisun suorittaa. En muotoile lausetta matemaattiseksi algoritmiksi tai lauseeksi, vaan kirjoitan sen suoraan tietokoneohjelmaksi, jollaisena se tietysti käytännön sovelluksissa esiintyy.

Kirjoituksen osassa I esitin rekursiivisen ohjelman Eukleideen algoritmille. Siitä sopivasti laajentamalla

saadaan ällistyttävän yksinkertainen koodi laajennetulle. Koodi noudattaa MAPLE-kielen syntaksia, mutta voidaan muokata helposti mille tahansa rekursion sallivalle kielelle.

```
EEukleides:=proc(a,b)
if b=0 then [a,1,0]
else L:=EEukleides(b,mod(a,b));
     d:=L[1]; x:=L[2]; y:=L[3];
     L:=[d,y,x - iquo(a,b)*y] #iquo:osamäärä
end if
end proc
```

Tämä rekursiivinen (itseään kutsuva) ohjelma laskee siis luvun $d = \text{syt}(a,b)$ ja kertoimet x ja y siten, että $d = a\,x + b\,y$ (vrt. SYTlause).
Edellä oleva esimerkki laskettaisiin näin:

```
> tulos := EEukleides(171, 30);
> d := tulos[1]: x := tulos[2]: y := tulos[3];
> d,x,y;
        3, 3, -17
```

Saatiin kuin saatiinkin sama kuin käsin laskemalla!
Algoritmi on kirjoitettu sovittamalla [I. Algo]-kirjassa annettu "pseudokielinen" ohjelma MAPLE-syntaksin mukaiseksi. Elegantti tapa laajennetun *Eukleideen algoritmin* yleiselle matemaattiselle todistukselle on yllä olevan ohjelman oikeaksi todistaminen, joka onkin yllättävän lyhyt ja ytimekäs ([I. Algo] Ch. 33. s. 812.

Kuten sanottu, käytän esimerkeissäni symbolilaskentaohjelmaa MAPLE. Esimerkkien lukeminen ei edellytä lainkaan ohjelman tuntemista. Selitän tarvitsemani komennot, joita on vain muutama. Ohjelman ottaminen mukaan on sikäli mielekästä, että voidaan esittää asiat ihan oikean kokoisilla luvuilla. Se myös antaa konkretiaa teoreettisesti kuvailtaville algoritmeille, ja osoittaa, että hyvä symbolilaskentaohjelma on hyödyllinen kryptologiatyökalu. Sekä MAPLE:n että MATHEMATICA:n käyttäjäryhmissä on suuri määrä kryptologian esimerkkityöarkkeja. (`http://www.maplesoft.com/applications/` → `mathematics` → `Cryptography` (23 kpl.) ja `http://www.wolfram.com/`)
Toisaalta kannattaa mainita vapaasti saatava ohjelma *Maxima*, jolla kiinnostuneet voivat kokeilla vastaavien asioiden toteuttamista, ellei MAPLE- tai MATHEMATICA-ohjelma ole käytettävissä. Viimemainituista painotan enemmän edellistä siksi, että se on itselleni tutumpi.

Huomautan vielä, että MAPLE:ssa on sisäänrakennettuna laajennettu *Eukleideen algoritmi* nimellä `igcdex`. Nimi koostuu osista: `i` - integer, `gcd` = *greatest common divisor* = `syt` ja `ex` - *extended* Komento `d:=igcdex(a,b,'x','y')` palauttaa tuloksen `d=syt(a,b)` ja lisäksi muuttujissa x ja y kertoimet, joilla $d = a\,x + b\,y$.
Edellinen esimerkki laskettaisiin näin:

```
> d:=igcdex(171,30,'x','y'):
> d,x,y;
            3, 3, -17
```

Jatkossa käytämme valmista `igcdex`-funktiota esimerkeissämme edellä esitetyn `EEukleides`-funktion sijasta.

Yhtälön $a\,x \equiv 1 \pmod{n}$ ratkaiseminen

Kyseessähän on mahdollisimman yksinkertainen ns. *Diophantoksen yhtälö*, jota käsiteltiin osassa I. Lauseen I.12 mukaan yhtälöllä on aina yksikäsitteinen ratkaisu (mod n), mikäli $\text{syt}(a,n) = 1$. Ratkaisu saadaan *laajennetulla Eukleideen algoritmilla* laskemalla luvut x ja y siten, että $a\,x + n\,y = 1$. Kiinnostava on vain luku x. Kun se tunnetaan, niin
$a\,x = 1 - n\,y \equiv 1 \pmod{n}$.

Yllä olevalla MAPLE-funktiolla ratkaisu saadaan siis näin:

```
> igcdex(a,n,'x','y'):
```

Kuten sanottu, olemme kiinnostuneita vain x:stä, d:n tiedämme 1:ksi, y voidaan heittää romukoppaan. Jos halutaan minimaalinen x, ts. redusoida (mod n), niin ei muuta kuin `x:=x mod n :`

Kiinalainen jäännöslause

Aiheeseen liittyy monta tarinaa erityisesti kiinalaisen (ja kreikkalaisen) matematiikan historiasta. Löytöjä voi tehdä *Googlella* hakusanalla *Chinese remainder theorem*. Eräs tarinoista on [I. Algo]-kirjassa:
Noin vuonna 100 *ajanlaskumme alkuhetken jälkeen kiinalainen matemaatikko Sun-Tsu ratkaisi seuraavan ongelman:*
Määritä kokonaisluvut x, jotka antavat jakojäännökset 2,3,2 *jaettaessa luvuilla* 3,5,7. *Ratkaisuiksi hän sai luvut $x = 23 + k \cdot 105$.*

Huomattakoon, että jakajat $n_1 = 3, n_2 = 5, n_3 = 7$ ovat pareittain yhteistekijättömät ja $3 \cdot 5 \cdot 7 = 105$, mutta miksi näin, ja mistä tulee 23 ? Nykykielellä siis ratkaisu: $x \equiv 23 \pmod{n}$, missä $n = n_1 \cdot n_2 \cdot n_3$.

Miten hän ratkaisuunsa päätyi, ja osasiko yleistää? Nykylukijalla on helppoa, sovelletaan kiinalaista jäännöslausetta, jota tässä ei kuitenkaan esitetä. Mainittakoon kuitenkin, että lauseen muotoili ja todisti yleisessä muodossaan – kukas muu kuin *Euler* v. 1734.

RSA-algoritmin todistuksessa tarvittava kiinalaisen jäännöslauseen seuraus on siinä määrin erikoistapaus itse lauseesta, että sen suora todistus on miltei itsestäänselvyys. Kiinalaista jäännöslausetta voidaan kyllä käyttää mm. RSA-menetelmän tehokkaampaan toteutukseen ja myös RSA-menetelmän murtamisyrityksiin, joten sen esittäminen olisi hyvinkin perusteltua tässä yhteydessä. Katson kuitenkin kirjoitukselleni olevan hyväksi keventää työkalupakkia, kun se on mahdollista.

Kutsun tarvitsemaamme seurausta ”kiinalaiseksi selviöksi”.

Lause 1 (Kiinalainen selviö)**.** *Olkoon* $n = n_1\, n_2\, \cdots n_k$, *missä* $syt(n_i,n_j) = 1$, *kun* $i \neq j$. *Olkoon* a *mielivaltainen kokonaisluku. Nyt* $x \equiv a \pmod{n} \iff x \equiv a \pmod{n_i}, i = 1, \ldots, k$.

Tod. (1) Olkoon $x \equiv a \pmod{n}$. Jatko jääköön lukijalle harjoitustehtäväksi.

(2) Olkoon $x \equiv a (\mathrm{mod}\, n_i), i = 1, \ldots, k$. Tällöin jokainen n_i on tekijänä $(x - a)$:ssa. Koska $\mathrm{syt}(n_i,n_j) = 1$, kun $i \neq j$, niin myös tulo $n = n_1\, n_2 \cdots n_k$ on tekijänä $(x - a)$:ssa, eli $x \equiv a (\mathrm{mod}\, n)$. Tämä viimeinen päätelmä jätetään taas lukijalle harjoitustehtäväksi (miltei valmiiksi ohjeistettuna). □

Tehtävä 1. *Olkoon* $syt(n_1,n_2) = 1$ *ja olkoon* $n_1 \mid a$ *ja* $n_2 \mid a$. *Osoita, että* $n_1\, n_2 \mid a$.

Vihje Taas kerran päästään liikkeelle SYTlauseen I.5 avulla: $1 = n_1\, x + n_2\, y$. Kerro puolittain a:lla, niin alat olla perillä.

On selvää, että tämä yleistyy useampaan tekijään (formaalisti induktiolla, jota esitellään mm. kirjoituksessa [JP]) . Toisaalta tarvitsemme ”kiinalaista selviötä” vain tapauksessa $n = n_1\, n_2$.

Modulaaripotenssilaskenta

Tässä on kaksi näkökulmaa, 1) laskentakaava ”potenssi potenssiin” ja 2) tehokas potenssiinkorotusmenetelmä.

1. Potenssi potenssiin. Silloinhan eksponentit kerrotaan. Päteekö sääntö myös (mod)-laskennassa? Mitä on siis $(a^k \mathrm{mod}\, n)^j$?
$a^k \mathrm{mod}\, n = a^k + i\, n$ jollain i.
Siis $(a^k \mathrm{mod}\, n)^j = (a^k + i\, n)^j = a^{k\, j} +$ termejä, joissa jokaisessa on $i\, n$ tekijänä. (Joko binomikaavalla tai suoraan tulosta $(a^k + i\, n)(a^k + i\, n) \cdots (a^k + i\, n)$, jossa kaikkiin muihin termeihin paitsi siihen, jossa jokaisesta binomista otetaan ensimmäinen, tulee tekijäksi $(i\, n)$:n potenssi.) Eli saadaan muotoa $a^{k\, j} + K\, n$ oleva lauseke, missä K on jokin kokonaisluku. Siis

$$(a^k \mathrm{mod}\, n)^j \equiv a^{k\, j} \pmod{n},$$

ja potenssi potenssiin sääntö toimii kauneimmalla mahdollisella tavalla.

Modulaarinen potenssiinkorotus

Usein näissä yhteyksissä tulee vastaan tehtävä $a^b \pmod{n}$, missä esiintyvät luvut saattavat olla hyvin suuria. Jos vaikka a on luokkaa 10^4 ja b luokkaa 10^5, mikä on huimasti alakanttiin tyypillistä RSA-salausta ajatellen, niin a^b on luokkaa 10^{400000}. Tämänkokoisilla luvuilla laskenta alkaa olla epätoivoista mille tahansa laskentamyllylle, puhumattakaan ihan normaalista tapauksesta, kuten esimerkissämme, jossa a tai b voi olla luokkaa 10^{100}.

Operaatioon on olemassa tehokas ratkaisu, nimeltään ”toistettu neliöön korottaminen” tai ”neliöön korotus ja kertolasku”. Algoritmi kuvataan [I. Algo]-kirjassa ss. 829 ja [Kob] ss. 23 – 24: Pääperiaate on, että kerätään tuloa, jossa edellisellä kierroksella saatu tulos korotetaan neliöön ja lisäksi kerrotaan sopivalla luvulla, mikäli n:n binääriesityksessä on ao. kohdalla 1. Kunkin operaation jälkeen redusoidaan modulo n, jolloin suurin laskennassa esiintyvä luku on kaiken aikaa $\leq n^2$. (Oletetaan, että $a < n$.) Jätän tilan säästämiseksi kuvauksen ylimalkaiseksi, yksityiskohdat on annettu mm. yllä mainituissa viitteissä.

MAPLE-ohjelmassa algoritmi on suoraan sisäänrakennettuna komentona: `> c:=a&^b mod n:` Jos tätä verrataan komentoon `c:=(a^b) mod n`, jota en suosittele, niin ero saattaa olla huikea, sanoisinko ääretön, ja ensin kannattaa varmistaa, että ohjelman `STOP`-nappula toimii.

Algoritmien vaativuus

Laskennallisten algoritmien suhteen on tärkeää arvioida niiden vaatimaa laskenta-aikaa (ja tilaa) suhteessa syötteenä olevien lukujen kokoon. Tällaisia arvioita esiintyy kaikissa numeerisen analyysin kirjoissa, alan systemaattisen tutkimuksen katsotaan kuuluvan teoreettisen tietojenkäsittelytieteen piiriin. Tässä kirjoituksessa esiintyviin lukuteoreettisiin algoritmeihin paneutuvaa vaativuusanalyysia käsitellään kirjassa [Kob] huolellisesti ja perusteellisesti. Myös toinen peruskirjamme [I. Algo] sisältää runsaasti vastaavaa analyysia. Tähän kirjoitukseen en voi enää mahduttaa uutta asiaa enempää, joten joudun tyytymään tämän tärkeän komponentin osalta kirjallisuusviitteisiin. Mainitsen vain esimerkin ja ulkonäön vuoksi, missä muodossa näitä arvioita annetaan. *Eukleideen algoritmin* suoritusaika on $O(\log^3 a)$, kun etsitään $syt(a,b)$, $a > b$. Lyhyesti tämä ”iso-O” -notaatio tarkoittaa suluissa olevaan lausekkeeseen verrannollisuutta, eli arvioon kuuluu tarkemmin määräämätön vakiokerroin.
Aikaperspektiivin kannalta mainitsen, että viime marraskuuta voidaan pitää numeerisen analyysin ja laskennallisten numeeristen algoritmien tutkimuksen 60-vuotisjuhlakuukautena, sillä marraskuussa vuonna 1947 ilmestyi *von Neumann*'n ja *Goldstine*'n uraauurtava julkaisu aiheesta.

Epäsymmetriset menetelmät, julkinen salakirjoitus

Kaikki vuoteen 1976 mennessä käytetyt kryptosysteemit lasketaan klassisiin menetelmiin kuuluviksi. Niille on ominaista, että salausavaimesta S_e voidaan kohtuullisella laskentatyöllä johtaa purkuavain S_d. Siksi niitä kutsutaan myös symmetrisiksi menetelmiksi, kuten edellä oli puhe. Käytän tulevaa ennakoiden kirjaimia e ja d, jotka liittyvät sanoihin "encrypt" (salata) ja "decrypt" (avata salaus, dekryptata).

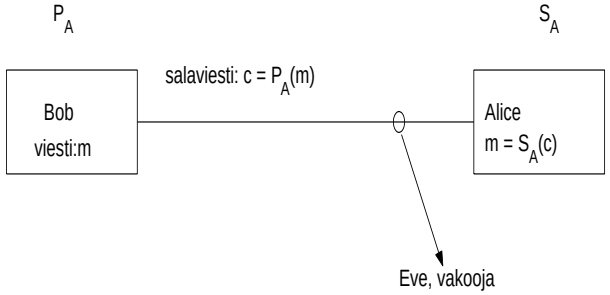
Nykyisin, kun sähköinen luottamuksellisen tiedon välitystarve on räjähdysmäisesti kasvanut sotilas- ja diplomaattialueen ulkopuolelle, on suoranainen välttämättömyys suunnitella yhtenäinen salaustekniikka, jotta laajojen järjestelmien yhteensopivuus olisi mahdollinen. Niinpä tarve yleiseen käyttöön sopivan julkisen salakirjoitusjärjestelmän kehittämiseen nousi 1970-luvulla voimakkaasti esiin.

Julkisen salakirjoituksen periaate

Jokaisella tiedonvaihtoon osallistuvalla osapuolella on kaksi avainta, julkinen ja salainen. Kryptologian esityksissä on tullut yleiseksi tavaksi kutsua kahta kommunikoivaa osapuolta nimillä *Alice* ja *Bob*.

Käytetään edellä olevien e- ja d-symbolien ohella myös kirjaimia P – "Public" ja S – "Secret" viittaamaan kyseisiin avainfunktioihin. *Alice*:lla on siten julkinen avain P_A ja salainen avain S_A ja *Bob*:lla vastaavasti P_B ja S_B.

Kommunikaatiota *Alice*:n ja *Bob*:n välillä esittää kuva, jossa on mukana ilkeä *Eve*, joka sieppaa linjalta salakirjoitettuja viestejä, minkä ehtii.



Kaikilla kommunikoivilla osapuolilla on käytössään kaikkien muiden julkinen avain, periaatteessa ne voitaisiin vaikka julkaista webbisivulla. Lisäksi jokaisella osapuolella X on oma henkilökohtainen salainen avain S_X, jota kukaan muu maailmassa ei tiedä.

Voimme ymmärtää tässä kuvailussa avaimen funktioksi, joka muuntaa viestin numeerisen esityksen selväkielisestä salakieliseksi tai päinvastoin. Joka tapauksessa funktiot P_X ja S_X ovat toistensa käänteisfunktioita. Niinpä, kun *Bob* salakirjoittaa viestin m käyttäen *Alice*:n julkista avainta P_A, hän tuottaa luvun $c = P_A(m)$. *Alice*:lla ja vain *Alice*:lla on salainen avain S_A, joka on *Alice*:n julkisen avaimen P_A käänteisfunktio. Siis *Alice* avaa *Bob*:n lähettämän viestin laskulla $S_A(c)$.

Mikä tässä on uutta ja ihmeellistä? Kaikki osapuolet tuntevat avaimen P_A, mutta tämä funktiopa onkin tehty sellaiseksi, että sen käänteisfunktiota on äärimmäisen vaikea laskea. Tässä on ero symmetrisiin menetelmiin nähden. *Diffie ja Hellmann* käyttivät termiä "trapdoor function", jolle [KN]:ssä käytetään suomennosta "salaovifunktio". Kehitin itse kevytmielisesti suomennoksen "loukkuluukkufunktio". Luukusta on helppo astua sisään huomatakseen joutuneensa loukkuun. Takaisin ulos päästäkseen on avattava systeemilukko, jossa on miljoonia mahdollisuuksia. Matemaattisemmin ilmaistuna, on löydettävä laskennallisesti kohtuullinen tehtävä, jonka käänteistehtävä on laskennallisesti kohtuuton, kuten 1000 vuotta vaativa laskenta-aika nopeimmalla supertietokoneella ja parhaalla laskenta-algoritmilla.

RSA-algoritmissa tuo laskennallisesti kohtuullinen tehtävä on kahden hyvin suuren alkuluvun p ja q kertominen: $n = pq$. Kun luvut valitaan riittävän suuriksi (luokkaa 150 numeroa), niin käänteinen tehtävä, luvun n tekijöihin jako on laskennallisesti kohtuuton. Käsitteiden "kohtuullinen" ja "kohtuuton" kvantifioiminen edellyttää algoritmien laskennallisen vaativuuden arvioita, mihin liittyvää "yleissivistystä" annettiin edellä lyhyesti.

On tietysti myös muistettava, että tietokoneiden prosessoritehojan kasvun ja aivan uusien laskentainnovaatioiden takia *loukkuluukku* vuonna 2008 ei välttämättä olekaan sitä enää vuonna 2018.

Mutta jatkakaamme RSA-menetelmän kuvailun tiellä. Edellä symmetrisistä menetelmistä puhuttaessa koodattiin viestit kirjain tai tavu kerrallaan numeroksi ja muunnettiin niitä sopivasti sekoittamalla. Lukuteoria ja tietotekniikka antavat mahdollisuuden käsitellä viestejä suurina kokonaislukuina. Viestin numerokoodi käsitetään numeerisen vektorin sijasta yhdeksi suureksi kokonaisluvuksi, jolle tehdään sopiva matemaattinen muunnos P. Vastaanottaja avaa sen käytössään olevalla käänteismuunnoksella, eli salaisella avaimella S. Jos viesti on kovin pitkä, se jaetaan lohkoihin, joiden pituudet voivat olla vaikka $100 - 200$ merkkiä. Ts. viesti voidaan esittää numeerisena vektorina, jonka komponentit ovat (tarvittaessa) suuria kokonaislukuja.

Seuraavaksi esitettävän algoritmin kuvauksessa ajatellaan, että selväkielisen viestin numeerinen vastine edus-

taa koko viestiä tai yhtä viestivektorin komponenttia. Tälle käytetään merkintää m, niinkuin "message". Salakirjoitetulle muunnokselle käytetään nimeä c, niinkuin "ciphertext", yleisesti siis $c = P(m)$ ja $m = S(c)$, koska P ja S ovat toistensa käänteisfunktioita.

Miten nuo P ja S rakennetaan RSA-menetelmässä? Nyt olemme valmiit sen kertomaan ja perustelemaan.

Algoritmi 2 (RSA). *1. Muodostetaan kaksi samaa suuruusluokkaa olevaa suurta alkulukua p ja q.*

2. Lasketaan $n = p\,q$ ja $\phi = (p-1)(q-1)$. [1]

3. Valitaan luku e, $1 < e < \phi$ siten, että $syt(e,\phi) = 1$. (Luvun e ei tarvitse olla kauhean suuri.)

4. Lasketaan laajennetulla Eukleideen algoritmilla luku d siten, että $e\,d \equiv 1 \pmod{\phi}$.

*5. A:n **julkinen avain** on (e,n) ja A:n **salainen avain** on (d,n).*

*6. Olkoon m viestin numeerinen esitys, $0 \le m \le n$. **Muodostetaan salainen viesti** $c = m^e (mod\, n)$ ja lähetetään A:lle.*

*7. A **avaa salaisen viestin** c omalla salaisella avaimellaan d kaavalla $a = c^d \pmod{n}$. Ja todellakin $a = m$, kuten seuraavaksi osoitetaan.*

RSA-algoritmin oikeaksi todistaminen

Tod. Salainen viesti $c = m^e \pmod{n}$, missä m on alkuperäinen viesti, e salauseksponentti, $n = p\,q$, p ja q ovat alkulukuja. Avattu viesti $a = c^d \pmod{n}$ missä d on avauseksponentti ja toteuttaa yhtälön

$$e\,d \equiv 1 \pmod{\phi}, \quad \phi = (p-1)(q-1).$$

Pitää siis todistaa, että avattu viesti on sama, mistä lähdettiin, eli $a = m$.

No katsotaan: $c^d = (m^e \pmod{n})^d \equiv m^{e\,d} \pmod{n}$ potenssipotenssiin-säännön mukaan.

Nyt $e\,d = 1 + j\,\phi = 1 + j\,(p-1)(q-1)$ jollain j, joten

$m^{e\,d} = m\,m^{j(p-1)(q-1)}$. Järkevä oletus on, että $m < p$ ja $m < q$, jolloin varmasti $\text{syt}(m,p) = \text{syt}(m,q) = 1$.

Niinpä **Fermat'n pikkulauseen** mukaan
$m^{p-1} \equiv 1 \pmod{p}$ ja $m^{q-1} \equiv 1 \pmod{q}$, joten
$m^{j(p-1)(q-1)} = (m^{p-1})^{j(q-1)} \equiv 1 \pmod{p}$.
Vaihtamalla p:n ja q:n järjestys, saadaan
$m^{j(p-1)(q-1)} \equiv 1 \pmod{q}$.

Kiinalaisen selviön mukaan
$m^{j(p-1)(q-1)} \equiv 1 \pmod{n}$.

Siis $a = c^d \equiv m\,m^{e\,d} \pmod{n} \equiv m \pmod{n}$

Jos luovumme yllä olevasta "järkevästä oletuksesta", niin esim. $p \mid m$, jolloin $m^{e\,d} \equiv m \pmod{p}$, koskapa p on molemmissa yhtälön puolissa tekijänä. Tässä tapauksessa ei tarvita Fermat'n apua, mutta tilanne on syytä turvallisuussyistä kuitenkin sulkea pois. Joka tapauksessa väite pätee yleisesti, tehtiinpä yllä järkevä tai vähemmän järkevä oletus. □

Esimerkki

Esitykseni on mukaelma viitteen [Cos] tyylistä. Otan "mustina laatikoina" siinä annetut funktiot `to_number` ja `from_number`, jotka muuttavat merkkijonon eli tekstivektorin numeroksi ja vastaavasti takaisin merkkijonoksi annetun aakkosvektorin suhteen vastaavaan tapaan kuin edellä olleet MATLAB-funktiot. Erona on, että nyt emme muuta tekstivektoria numeeriseksi vektoriksi, vaan yhdeksi kokonaisluvuksi. Kaiken muun avaan komento komennolta lukijan silmien eteen.

Esimerkin avaimet ovat lähes turvallista kokoa, olisivat olleet vielä hiukan yli 10 vuotta sitten. Jäljempänä pohditaan tarkemmin.

Jos muutamme valitun aakkosvektorin suhteen sanan `SOLMU` numeeriseksi saamme:

```
> aakkoset:="ABCDEFGHIJKLMNOPQRSTUVWXYZÅÄÖ"
> to_number("SOLMU");
                  1915121321
```

Nähdään, että kirjaimia vastaavat numerot on pantu peräkkäin tyyliin: $A = 01, B = 02, \ldots, S = 19, \ldots U = 21$

Toinen, kenties luonnollisempi tapa olisi esittää viesti $N-$järjestelmän lukuna ja muuntaa se $10-$järjestelmään, missä N on aakkosvektorin pituus. Tällöin samainen `SOLMU` muuntuisi luvuksi
$21 + 13 \cdot 30 + 12 \cdot 30^2 + 15 \cdot 30^3 + 19 \cdot 30^4 = 15806211$.

Koska yllä mainittu `to_number`-funktio tekee edellisellä tavalla, noudatan sitä.

Alla esiintyvät MAPLE-komennot ovat suurelta osin itsensä selittäviä. Mainitsen ja kertaan tässä joitakin nimityksiä ja sellaisia komentoja, joiden merkitys voi olla epäselvä tai unohtunut.
Alkukirjain i viittaa sanaan "integer", kokonaisluku.

[1] Kirjain ϕ viittaa ns. *Eulerin ϕ-funktioon*, emme kuitenkaan tarvitse siihen liittyvää *Eulerin lausetta*, vaan pärjäämme Fermat'n pikkulauseella.

`ifactor`	Tekijöihin jako
`igcd(a,b)`	gcd = syt
`igcdex(a,b,'x','y')`	gcd extended = Laajennettu Eukleideen algoritmi
`a mod b`	Jakojäännös laskussa a/b

Muistutan vielä, että komento `d:=igcdex(a,b,'x','y')` palauttaa tuloksen `d=syt(a,b)` ja lisäksi muuttujissa x ja y kertoimet, joilla $d = a\,x + b\,y$.

Ja nyt se alkaa!

Alice valitsee kaksi suurta alkulukua ja laskee niiden tulon:

```
> pA := nextprime(10^60 + 1234567*rand()^5);
11980768160215583569801524136786 21
55248273111437740290921929815 59
> qA := nextprime(10^65 + 8765439999*rand()^5);
24557694884338801620018108793784400
77015568602607435050878572990629
> nA:=pA*qA:
> length(nA);
131
```

Luvussa n_A on 131 numeroa. Kokeillaan tekijöihinjakoa.

```
> ifactor(nA);
Warning,  computation interrupted
```

Painettiin `STOP`-nappulaa. Ei näytä siltä, että kannattaisi ryhtyä odottelemaan.
Kokeillaan tekijöihinjakoa, kun p_A kerrotaan jollain umpimähkään valitulla pienehköllä luvulla.

```
> ifactor(pA*465734);
(2) (337) (691) (11980768160215583569801524
13678621552482731114377402909219298 1559)
```

Onnistuu muotoa $p_A\,k$ olevalle luvulle hetkessä, kun kerroin k on miljoonan luokkaa, mutta jos vähän kasvatetaan, alkaa kestää tuskaisen kauan.

Seuraavaksi Alice laskee ϕ_A:n, jota varten siis täytyy tuntea n_A:n tekijät p_A ja q_A.

```
> phiA := (pA - 1)*(qA - 1):
```

Alice valitsee salausekponentin (”encryption exponent”) .

```
 > eA := nextprime(10^5 + rand());
                  624044487349
```

Todetaan, että syt(e_A,ϕ_A) = 1. Tämä toteutuu hyvin suurella todennäköisyydellä (miksi?), mutta se on kuitenkin erikseen tarkistettava.

```
 > igcd(eA, phiA);
                        1
```

Alice laskee nyt laajennetulla Eukleideen algoritmilla oman salaisen avaimensa eksponentin d_A.

```
> igcdex(eA, phiA, 'xA', 'yA'):
> dA := xA mod phiA;
13684831311997866502152356 52 ...
> length(dA);
                       131
```

Salaisessa eksponentissa d_A on 131 numeroa. Tarkistetaan, vaikka tiedetään, että $e_A\,d_A \equiv 1 \pmod{\phi_A}$

```
> eA*dA mod phiA;
                        1
```

Alicen julkinen avain on (e_A,n_A) ja salainen avain on (d_A,n_A). Edellä esitellyn puhetavan mukaisesti voidaan myös sanoa, että A:n julkinen avain on parametrien (e_A, n_A) määräämä funktio
$P_A(m) = m^{e_A} \pmod{n_A}$ ja salainen avain vastaavasti funktio $S_A(c) = c^{d_A} \pmod{n_A}$.
Bob tekee vastaavat asiat tykönään:

```
> pB := nextprime(10^60 + 23453218*rand()^5):
> qB := nextprime(10^65 + 12456800*rand()^5):
> nB:=pB*qB: phiB:=(pB-1)*(qB-1):
> eB := nextprime(10^4 + 3*rand());
                  2336493690667
> igcd(eB, phiB);
                        1
> igcdex(eB, phiB, 'xB', 'yB'):
> dB := xB mod phiB:
> length(dB);
                       131
```

Bob'n julkinen avain on (e_B,n_B) ja salainen avain (d_B,n_B), ja ne määräävät samalla tavoin julkisen ja salaisen avainfunktion P_B ja S_B. Huomaa, että kummankin salainen avain pysyy kunkin omana tietona. Sitä ei kukaan missään vaiheessa lähetä kenellekään.

Bob salaa numeroksi koodatun viestin m käyttäen Alicen julkista avainta, ts. hän suorittaa laskun
$c = P_A(m) = m^{e_A} \pmod{n_A}$, ja lähettää salaviestin c Alicelle, kas näin:

```
> m := to_number(‘TAVATAAN HIEKKALAATIKOLLA‘);
 20012201200101143208090511110112010120091115 1
 21201
> c:=m&^eA mod nA:  # modulaarinen potenssi
```

Alice avaa viestin omalla salaisella avaimellaan:

$a = S_A(c) = c^{d_A} \pmod{n_A}$. Edellä oikeaksi todistetun algoritmin mukaan pätee: $a = m$.

```
> a:=c&^dA mod nA;
 20012201200101143208090511110112010120091115 1
 21201
from_number(a);
           "TAVATAAN HIEKKALAATIKOLLA"
```

Sähköinen allekirjoitus

Alice vastaa ja varustaa viestinsä digitaalisella allekirjoituksella, jotta *Bob* varmasti tietää, että vastaaja on *Alice* ja viesti on tarkalleen se, jonka *Alice* on lähettänyt.

Viesti voisi olla
`v:="OLEN ALIISA JA TULEN KANSSASI"`. Olkoon m tämän viestin numeerinen esitys. *Alice* muodostaa allekirjoituksen $s = S_A(m)$, toisin sanoen hän koodaa viestinsä omalla **salaisella avaimellaan**, ja lähettää *Bob*:lle viestin, jonka perään liittää tuon koodin, eli luvun s. *Bob* vastaanottaa sanoman vektorina $[v,s]$, lukee selväkielisen viestin v, jonka perusteella tietää käyttää *Alice*:n julkista avainta allekirjoituksen tarkistamiseen. *Bob* suorittaa laskun $P_A(s)$. Jos tuloksena on m, on *Alice*:n identiteetti ja viestin sisältö varmennettu.

Sama laskettuna auki

Määritellään MAPLE:ssa edellä käytettyjen avaimien avulla *Alice*:n julkinen ja salainen avainfunktio P_A ja S_A

```
> PA:=m->m&^eA mod nA:  SA:=s->s&^dA mod nA:
> v:="OLEN ALIISA JA TULEN KANSSASI";
> m:=to_number(v);
   15120514270112090919012710012720211205142
   71101141919011909
```

Alice:n digitaalinen allekirjoitus

```
 > s:=SA(m);  (130 numeroa):
93271633443294939878071410488947105653963353..
```

Alice lähettää viestin:

```
> Bobille:=[v,s];
["OLEN ALIISA JA TULEN KANSSASI", 9327163...]
```

Bob muuntaa saamansa vektorin 1. komponentin numeeriseksi ja tarkistaa viestivektorin 2. komponentin avulla viestin allekirjoitetun sisällön.

```
> m:=to_number(Bobille[1]);
  15120514270112090919012710012720211205514..
> t:=PA(Bobille[2]);
  15120514270112090919012710012720211205514..
 > m - t
                      0
```

Kaikki hyvin!

Tähän voidaan tietysti vielä lisätä allekirjoitetun viestin salaus mukaan tarvittaessa. Edellinen vastaisi (avointa) allekirjoituksella varmennettua paperia ja jälkimmäinen kuoreen sinetöityä allekirjoitettua paperia. Tyypillisiä tilanteita ovat vaikkapa pankkisovellukset. Saman allekirjoituksen voi haluta tarkistaa useampikin taho. Sehän käy, koska julkinen avain on kaikilla käytössään ja salainen vain asianomaisella allekirjoittajalla. Tyypillinen esimerkki voisi olla *Bob*:n *Alice*:lle lähettämä sähköinen shekki, jonka allekirjoituksen *Alice* tarkistaisi, lähettäisi edelleen pankkiin, jossa se niinikään voitaisiin tarkistaa *Bob*:n julkista avainta käyttäen ja suorittaa asianmukainen rahojen siirto.

RSA:n turvallisuus

RSA:n turvallisuus perustuu suuren luvun tekijöihinjakotehtävän vaativuuteen. Jos modulin n tekijöihin jako onnistuu, niin avaimet saadaan käden käänteessä noudattaen yleisen algoritmin kuvausta tai sitä seurannutta esimerkkiä. Entä kääntäen, pitääkö paikkansa, että jos suuren luvun tekijöihin jako on vaikeaa, niin RSA:n murtaminen on vaikeaa? Ongelmaa on tutkittu tiiviisti RSA:n julkistamisesta lähtien, asiaa ei ole pystytty todistamaan, mutta mitään muuta tapaa menetelmän murtamiseen ei myöskään ole löydetty. Lainaan [I. Algo]-kirjaa s. 835: Jos valitaan satunnaisesti kaksi 100-numeroista alkulukua, niin niiden avulla voidaan muodostaa avain, joka on ”murtamaton” nykyteknologialla (v. 1998).

Kuitenkin on erinäisiä seikkoja, jotka täytyy ottaa huomioon, sillä koodinmurtajien työkalupakissa on taatusti ainakin modulaariaritmetiikan peruslauseet, Fermat'n pikku lause, Eukleideen algoritmi, Kiinalainen jäännöslause ja parhaat laskenta-algoritmit. Lisäksi raakaa laskentavoimaa on oletettava olevan suurimman supertietokoneen verran ja tehokkaasti hajauttaen paljon enemmänkin.

[HandB] käsittelee aihetta laajasti esittäen ainakin 8 erilaista hyökkäysmahdollisuutta ja niiden torjuntalääkkeet. Monissa muissa lähteissä, kuten [Nyberg], [Wiki] ja aivan erityisesti [Sti] (s. 225) on lisää kryptoanalyyttisiä konnankoukkuja ja niiden vastalääkkeitä.

Pari yksinkertaisinta seikkaa mainitakseni, on selvää, että alkulukujen p ja q on molempien oltava niin suuria, ettei pienistä luvuista lähtevä alkulukujen laskenta ja tekijätarkistus onnistu kohtuuajassa. Toisaalta ne eivät saa olla niin lähellä toisiaan, että voitaisiin tekijän etsintä aloittaa $\sqrt{n}$:n läheltä.
Pieni salauseksponentti e on salaamisen kannalta tehokas, mutta ongelmallinen, jos viesti (tai viestin osa) m on niin pieni, että $m < n^{1/e}$. Tällöinhän salaviesti $c = m^e \pmod n = m^e$ (mieti!). Murtaja *Eve* muodostaa luvun $c^{1/e}$, ja lukee m:ää kuin avointa kirjaa. Tämä voidaan estää lisäämällä viestiin riittävästi ”suolaa” , eli ylimääräistä puppua.

Kryptologia on aina ollut kahden joukkueen välistä kilpajuoksua. Rauhanomaiseen kilpailutoimintaan liittyy `RSA129`-projekti, joka lähti liikkeelle, kun RSA:n keksijät Rivest, Shamir ja Adleman esittivät vuonna 1977 Scientific American-lehdessä 129-numeroisen kahden alkuluvun tulon haasteeksi tiedeyhteisölle tekijöiden löytämistä varten. He arvioivat tekijöihin jakoon kuluvan aikaa n. 20000 vuotta silloisilla menetelmillä ja tekniikalla. Hollantilainen lukuteoreetikko *Arjen Lenstra* organisoi maailmanlaajuisen laskentaverkoston
`http://www.math.okstate.edu/~wrightd/numthry/rsa129.html`
Lenstran ryhmä käytti 1980-luvulla kehitettyä uutta lukuteoreettista menetelmää ja kykeni purkamaan algoritmin rinnakkaislaskentaa hyödyntävään muotoon. Huhtikuussa 1994 tekijöihin jako onnistui, ja RSA:lla salattu viesti saatiin auki. Viestin sisältö oli: ”The magic words are squeamish ossifrage.”

Kilpajuoksu ei päättynyt tähän. [Wiki]:ssä mainitaan luku RSA-200, joka jaettiin tekijöihin vuonna 2005. Kirjassa [Sti] (v. 2006) s. 175 mainitaan. että nykyiset tekijöihinjakoalgoritmit löytävät 512:n pituisen binääriluvun tekijät. Luvun pituus kymmenjärjestelmässä saadaan kertomalla $\log_{10} 2$:lla (eikö vain), joten se on n. 150 numeroa. Turvalliseksi luvun $n = p\,q$ suuruudeksi *Stinton* vakuuttaa nykytietämyksellä 1024 bittiä, siis n. 300 numeroa 10-järjestelmässä.

Ajantasaista tietoa voi hakea [Wiki]:sta sanoilla "RSA Factoring challenge", joka kertoo, että tämä kilpailumuoto lopetettiin vuonna 2007, koska "nykyteollisuudella on aiempaa huomattavasti kehittyneempi ymmärrys yleisistä kryptoanalyyttisistä periaatteista" .

Tulevaisuuden näkymiä

Edellä nähtiin, että arviot avainten turvalliseen kokoon liittyvistä vaatimuksista tahtovat jäädä jälkeen siitä, minkä tänään oletetaan riittävän pitkälle tulevaisuuteen. Tästä syystä ei voida pysähtyä lepäämään RSA-laakereilla, vaan on välttämätöntä kehittää uusia "loukkuluukkuideoita".

Kryptologiset menetelmät ovat laajentuneet abstraktia algebraa, algebrallista geometriaa, elliptisiä käyriä, ym. kehittyneitä moderneja matemaattisia teorioita käyttämään. Lisäksi deterministen menetelmien ohella on ryhdytty kehittämään myös todennäköisyyslaskentaan pohjautuvia satunnaisuuteen perustuvia menetelmiä.

Kryptologiassa yhdistyvät kiehtovalla tavalla vuosituhansien aikana kehittyneet lukuteorian menetelmät uusien abstraktien matemaattisten teorioiden tarjoamiin mahdollisuuksiin. Tärkeänä komponenttina on tietotekniikka teoreettisena työvälineenä, tehokkaan laskentavälineistön mahdollistajana, ja tietysti syyn ja motiivin antajana koko toiminnalle tietoverkkojen, matkapuhelimien, sirukorttien maailmassa.

Viitteet

[I. Algo] Cormen, Leiserson, Rivest: Kts. Osa 1

[DH] W. Diffie, M. Hellman. New directions in cryptography, IEEE Transactions on Information Theory IT-22 (1976), 644-654.

[HandB] A. Menezes, P. van Oorschot, S. Vanstone. Handbook of applied cryptography: http://www.cacr.math.uwaterloo.ca/hac/.

[CodeB] D. Kahn, The Codebreakers, Macmillan 1967, kirjasta on uudempi painos.

[Crt] Bernhard Esslinger. Cryptography and Mathematics, http://www.cryptool.com/ . Vapaan lähdekoodin ohjelmapaketti ja opetusteksti.

[InCode] Sarah Flannery, David Flannery. In Code: A Mathematical Journey.
Lukuteorian ja kryptologian periaatteiden yleistajuinen esitys nerokkaan irlantilaisen koulutytön ja isän kirjoittamana. http://www.amazon.com/ [Hakusana In Code] (Ehkä tästä joku koulutyttö tai poika voisi innostua vaikka kirjoittamaan kirja-arvion.)

[Cos] John B. Cosgrave. Bill Clinton, Bertie Ahern, and digital signatures (A Maple-based introduction to public-key cryptography) http://staff.spd.dcu.ie/johnbcos/Maple_public_other.htm

[Ke-Te] Veikko Keränen, Jouko Teeriaho. Salausmenetelmät, Rovaniemen AMK 2006: http://ta.ramk.fi/~jouko.teeriaho/krypto2006/krypto.htm. Kurssimateriaali, käyttää hyväkseen MATHEMATICA-ohjelmaa.

[Skk] Simo Kivelä. RSA-menetelmän MATHEMATICA-toteutus.
http://matta.hut.fi/matta2/mma/rsa.pdf

[Kob] N. Koblitz. A Course in Number Theory and Cryptography, Springer 1994.

[KN] Kaisa Nyberg. Kryptologia – tiedon turvaamisen tiede, Tietojenkäsittelytiede **26** kesäkuu 2007 ss. 31–52.

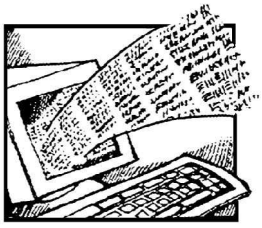
[JP] Jukka Pihko, Lukuteorian helmiä,
solmu.math.helsinki.fi/2008/1/pihko.pdf

[RSA] R. Rivest, A. Shamir, L. Adelman. A method for obtaining digital signatures and public-key cryptosystems, Communications of the ACM, 21 (1978), 120-126. Luettavissa tästä: theory.lcs.mit.edu/~rivest/rsapaper.pdf

[AS] Arto Salomaa. Public-Key Cryptography, Springer-Verlag, Berlin 1990.

[Sti] D. R. Stinson. Cryptography, Theory and Practice, Chapman & Hall/CRC Press, Boca Raton-London-New York, Third Edition, 2006
Kurssikirjaviitteenä Kaisa Nybergin (TKK) ja Keijo Ruohosen (TTY) opetussivuilla. (Kirjassa 353 viitettä.)

[Wiki] http://en.wikipedia.org/wiki/
Hakusanoja: *Cryptography, History of cryptography, World_War_II_cryptography, Enigma machine, Quantum Cryptography, RSA, RSA Factoring challenge.*



Tietokoneavusteisia matematiikan tehtäviä yläkoulussa

Johanna Lehtinen
Helsingin yliopisto
johanna.lehtinen@helsinki.fi

Tein syksyllä 2007 tutkimuksen tietokoneavusteisesta opetuksesta yläkoulussa. Tutkimusta varten sain Web-ALT Inc:ltä käyttööni MapleT.A.-ohjelman, jolla loin tietokoneavusteisia matematiikan tehtäviä yläkoulun 7. luokan kurssia "Luvut" varten. Opetuskokeilu kesti seitsemän viikkoa, jolloin oppilaat harjoittelivat kurssin aiheisiin liittyviä tehtäviä ja suorittivat seitsemän viikoittaista testiä tietokonetta käyttäen. Jokainen testi sisälsi 10 algoritmista tehtävää.

Itse tehtäviin ja MapleTA-ohjelmaan voi tutustua Solmun verkkoversiossa, osoitteessa `http://solmu.math.helsinki.fi/2008/lehtinen.html`

Solmun verkkoversiossa on ilmestynyt serbitehtäviä. Rationaali- ja reaalilukuja käsittelevät tehtävät ovat osoitteessa `http://solmu.math.helsinki.fi/2008/Serbitehtavia/osnovna.pdf` ja algebran lausekkeita käsittelevät tehtävät osoitteessa `http://solmu.math.helsinki.fi/2008/Serbitehtavia/prijemni.pdf`

Solmun uusittu keskustelupalsta on osoitteessa `http://solmu.math.helsinki.fi/cgi-bin/yabb2/YaBB.pl`