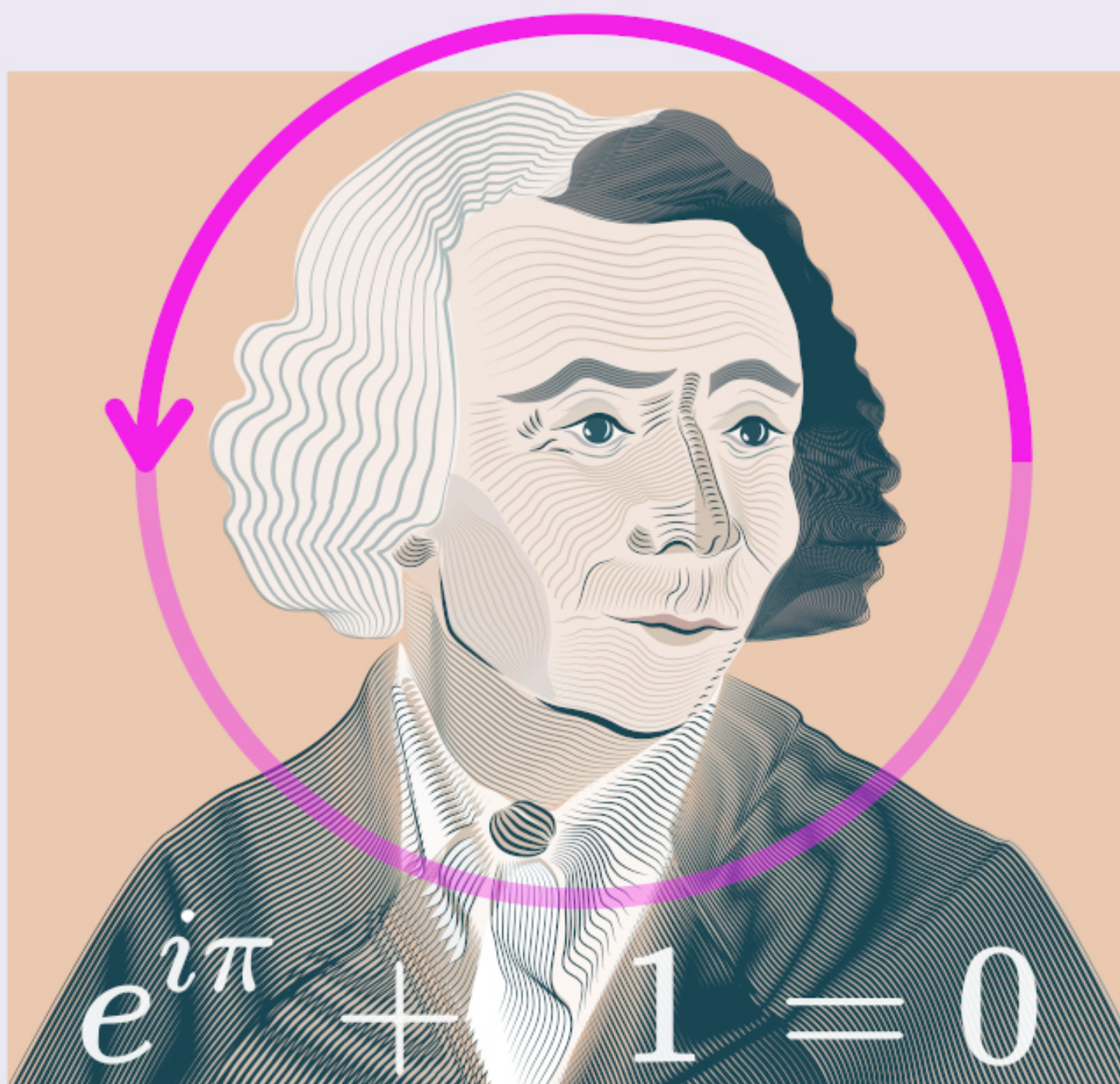


S&LMU

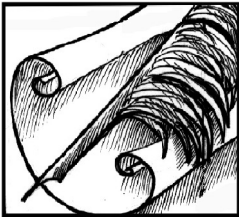
MATEMATIIKKALEHTI 3/2021

matematiikkalehtisolmu.fi



Sisällys

Pääkirjoitus: Matematiikasta ja yhteisöstä (Anne-Maria Ernvall-Hytönen)	3
Ykkösestä alkeisfunktioihin (Seppo Heikkilä)	4
Äärimmäisen epäjatkuvista funktioista (Jukka Liukkonen)	6
Koristetähden askarteleminen harpilla ja viivaimella (Anne-Maria Ernvall-Hytönen)	9
Ympyrän sisään piirrettyä (Markku Halmetoja)	12
Todistuspeli (Kalle Kytölä)	16
Solmun tehtäviä	21
Ketjumurtoluvut: mitä ne ovat ja mitä hyötyä niistä on? (Anne-Maria Ernvall-Hytönen)	23



Matematiikasta ja yhteisöstä

Pääkirjoitus

Sain vähän aikaa sitten kommentin, että eikö minun kannattaisi jotain muutakin tehdä kuin vain matematiikkaa. Vastasin vakuuttamalla, että kyllä minä teenkin: käyn taitoluistelemassa ja aloitin uudestaan pianotunnit. En ehkä tullut maininneeksi sitä, että näitäkin voi lähestyä matematiikkaväritteisestä näkökulmasta.

Luistelussa matematiikkanäkökulma on minulle tämä: olen täysi aloittelija, niin pihalla kuin ihminen voi olla. Olen toki luistellut koko ikäni, mutta lähinnä yrittänyt olla nopea tai pitänyt mailaa kädessä. Kaikki kaaret, kolmoset, liu'ut ja muut vastaavat ovat jääneet kovin vähälle. Nyt epätoivoisesti esimerkiksi niitä kolmosia opetellessani koenkin voivani samaistua niihin opiskelijoihin yliopistolla, jotka tulivat johdatus yliopistomatematiikkaan -kurssilleni vailla lukiomatematiikkaa.

Kysymys sai minut kuitenkin miettimään sitä, miksi pidän matematiikasta tai miksi matematiikka on minulle sekä työ että harrastus. On tietysti aloitettava siitä, että pidän matematiikasta hyvin paljon. Minua viehättää matematiikan kauneus, pidän niistä hetkistä, kun pitkän pään seinään takomisen jälkeen asiat sujuvat. Onnistumisen riemu on mahtavaa. Pidän myös laskemisesta, ajattelusta, hahmottelusta, pohtimisesta, ja kaikista näistä välivaiheista. Oikolukemisesta tai hioimisesta en pidä, kuten varmaan jokainen minut tunteva voi vahvistaa, mutta ne ovat pakollinen paha sen kaiken hauskuuden vastapainoksi.

Matematiikassa ei kuitenkaan ole minulle kyse vain matematiikasta, vaan yhteisöstä, jonka olen matematiikan kautta saanut ja jonka kanssa yhteistyötä tehdään. Oli-

si aika paljon kurjempaa ilman yhteisöä ja ilman niitä hyviä tyyppejä, jotka yhteisöön kuuluvat.

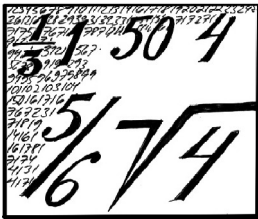
Yhteisö on minusta myös yksi parhaista syistä osallistua matematiikkakilpailuihin ja -valmennukseen, tulla matematiikkakerhoihin ja muuten harrastaa matematiikkaa. Suurissakaan kouluissa ei matematiikan harrastajia välttämättä paljon ole, pienissä kouluissa tilanne on helposti vielä heikompi. Ymmärrän mainiosti, jos matematiikkaa ei huvita harrastaa, jos se on yksinäistä.

Matematiikka on parhaimmillaan valtavan kaunista. Kuitenkin sen kauneuden näkeminen vaatii usein paljon töitä, laskuja ja laskuvirheitä. Välillä usko meinaa loppua, varsinkin jos työskentelee yksin. Matematiikka usein selkenee, kun siitä keskustellaan, vertaillaan ratkaisuja ja lasketaan yhdessä. Tämä kaikki jää helposti kokematta, jos vain harrastaa yksin. Aina kun perustelen matematiikan olympiavalmennuksen tärkeyttä, mainitsen sosiaaliset aspektit: Matematiikan harrastajat pääsevät keskustelemaan matematiikasta ja saavat yhteisön muiden samanhenkisten harrastajien kanssa.

Kun siis puhun matematiikasta, en läheskään aina puhu itse asiassa matematiikasta vain siinä mielessä kuin se helposti ymmärretään, vaan puhun myös yhteisöstä, yhdessä työskentelystä, tärkeiden asioiden edistämisestä ja siitä kaikesta mitä matematiikan mukana tulee.

Hyvää loppuvuotta ja erinomaista alkavaa vuotta!

Anne-Maria Ernvall-Hytönen



Ykkösestä alkeisfunktioihin

Seppo Heikkilä

Oulun yliopisto, Matemaattisten tieteiden laitos

heikki.sep@gmail.com

Johdanto

Aluksi johdetaan eksponenttifunktion sarjakehitelmä ykkösestä lähtien integroimalla. Saadusta tuloksesta johdetaan sitten hyperbolisten ja trigonometristen kosini- ja sinifunktioiden sarjakehitelmät. Kehitelmien avulla johdetaan myös ko. funktioiden ominaisuuksia. Tulosten johtamisessa tarvitaan potenssifunktioiden sekä niistä muodostettujen summien ja sarjojen integrointia, derivointia, yhteenlaskua ja vähennyslaskua. Induktioperiaate on ratkaisevassa roolissa, sillä se tarjoaa keinon jatkaa ykkösestä integroimalla saadut summat sarjaksi.

Eksponenttifunktio

Seuraavissa integroinneissa valitaan aina integroimisvakioksi 1. Vakiofunktion $f_0(t) \equiv 1$ integraalifunktio on siten $f_1(t) = 1 + t$. Sen integraalifunktio on taas $f_2(t) = 1 + t + t^2/2$. Integroimalla funktio f_0 n kertaa saadaan funktio

$$(1) \quad f_n(t) = 1 + t + \frac{t^2}{2} + \cdots + \frac{t^n}{n!}, \quad n! = 1 \cdot 2 \cdots n.$$

f_1 on määritelty, ja jos f_n on määritelty, niin sen integraali on f_n lisättynä termillä $\frac{t^{n+1}}{(n+1)!}$, joten f_{n+1} on määritelty. Induktioperiaatteen nojalla on f_n siten määritelty jokaisella $n = 1, 2, \dots$, joten (1) voidaan

jatkaa sarjaksi

$$(2) \quad f(t) = 1 + t + \frac{t^2}{2} + \cdots + \frac{t^n}{n!} + \frac{t^{n+1}}{(n+1)!} + \cdots.$$

Saatu sarja on eksponenttifunktion sarjakehitelmä, ts. $f(t) = e^t$, joten $f(1) = e$, ns. Neperin luku. Niiden sarjaesitykset ovat siten

$$(3) \quad e^t = 1 + t + \frac{t^2}{2} + \cdots + \frac{t^n}{n!} + \frac{t^{n+1}}{(n+1)!} + \cdots,$$

$$(4) \quad e = 1 + 1 + \frac{1}{2} + \cdots + \frac{1}{n!} + \cdots.$$

Funktion f derivaatta saadaan derivoimalla (2):n sarja termeittäin. Tulokseksi saadaan

$$(5) \quad f'(t) = 1 + t + \cdots + \frac{t^n}{n!} + \cdots.$$

(2):n ja (5):n oikean puolen sarjat ovat samat, joten $f' = f$. Siten eksponenttifunktio on sama kuin sen derivaatta.

Hyperbolisia funktioita

Sijoittamalla t :n paikalle $-t$ kaavassa (3) saadaan

$$(6) \quad e^{-t} = 1 - t + \frac{t^2}{2} + \cdots + \frac{(-1)^n t^n}{n!} + \cdots.$$

Laskemalla (3) ja (6) puolittain yhteen, jakamalla puolittain 2:lla, ja soveltamalla funktion cosh määritelmää saadaan

$$(7) \quad \cosh(t) := \frac{e^t + e^{-t}}{2} = 1 + \frac{t^2}{2} + \cdots + \frac{t^{2n}}{(2n)!} + \cdots.$$

Vähentämällä (6) puolittain (3):sta ja jakamalla puolittain 2:lla saadaan vastaavasti

$$(8) \quad \sinh(t) = \frac{e^t - e^{-t}}{2} = t + \frac{t^3}{6} + \dots + \frac{t^{2n+1}}{(2n+1)!} + \dots$$

Erityisesti

$$(9) \quad e^t = \cosh(t) + \sinh(t).$$

(7):n ja (8):n yhtälöistä seuraa, että $\cosh(-t) = \cosh(t)$ ja $\sinh(-t) = -\sinh(t)$. Kertomalla puolittain (9) ja yhtälö $e^{-t} = \cosh(-t) + \sinh(-t)$ saadaan siten kaava

$$(10) \quad \cosh^2(t) - \sinh^2(t) = 1.$$

Yhtälöistä (7) ja (8) seuraa derivoimalla, että

$$(11) \quad \cosh'(t) = \sinh(t), \quad \sinh'(t) = \cosh(t).$$

Trigonometrisia funktioita

Oletetaan, että yhtälössä (3) voidaan t :n paikalle sijoittaa it , missä i on ns. imaginaariyksikkö. Soveltamalla saadun sarjan termeihin kaavaa $i^2 = -1$, ja erottamalla eri sarjoiksi ne termit, joihin joko jää tai ei jää i :tä, saadaan $f(it) = C(t) + iS(t)$, missä

$$(12) \quad C(t) = 1 - \frac{t^2}{2} + \dots + \frac{(-1)^n t^{2n}}{(2n)!} + \dots,$$

ja

$$(13) \quad S(t) = t - \frac{t^3}{6} + \dots + \frac{(-1)^n t^{2n+1}}{(2n+1)!} + \dots$$

Saadut sarjat ovat kosini- ja sinifunktioiden sarjakehitelmät. Derivoimalla (12) ja (13) puolittain nähdään, että $C' = -S$ ja $S' = -C$. Siten

$$(14) \quad C(t) = \cos(t), \quad S(t) = \sin(t),$$

ja

$$(15) \quad \cos'(t) = -\sin(t), \quad \sin'(t) = \cos(t).$$

Lisäksi saadaan ns. Eulerin kaava:

$$(16) \quad e^{it} = \cos(t) + i \sin(t).$$

Yhtälöistä (12)-(14) seuraa, että $\cos(-t) = \cos(t)$ ja $\sin(-t) = -\sin(t)$. Kertomalla yhtälö (16) ja yhtälö $e^{-it} = \cos(-t) + i \sin(-t)$ puolittain saadaan siten kaava

$$(17) \quad \cos^2(t) + \sin^2(t) = 1.$$

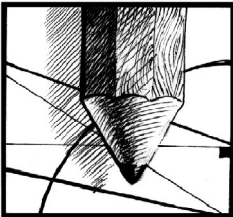
Koska $\cos(\pi) = -1$ ja $\sin(\pi) = 0$, niin sijoittamalla $t = \pi$ Eulerin kaavaan saadaan

$$(18) \quad 1 = -e^{i\pi},$$

eli ollaan takaisin ykkösessä.

Muita alkeisfunktioita

Muut hyperboliset ja trigonometriset funktiot saadaan normaaleilla määritelmillä. Juurifunktiot, logaritmifunktio, arkusfunktiot ja areafunktiot saadaan potenssifunktioiden, eksponenttifunktion, trigonometristen funktioiden ja hyperbolisten funktioiden käänteisfunktioina.



Äärimmäisen epäjatkuvista funktioista

Jukka Liukkonen

Mat. yo. evp.

Johdanto

Koodausteoriassa eräs keskeinen idea on sellaisen funktion määrittely, joka muuttaa toisiaan läheisesti muistuttavat oliot riittävän erinäköisiksi. Kun erinäköiset objektit altistetaan pienille muodonmuutoksille, ne ovat silti tunnistettavissa.

Kaaosteoriassa tarkastellaan ajan mukana muuttuvia systeemejä, joissa pieni muutos alkutilanteesta aiheuttaa valtavan ja ennustamattoman muutoksen systeemin myöhemmässä käyttäytymisessä. Kysymys ei ole satunnaisuudesta samassa mielessä kuin todennäköisyyslaskennassa. Kysymys on siitä, että vaikka systeemin kehitys tietystä alkutilasta eteenpäin tunnettaisiin tarkkaan, tästä tiedosta ei ole juurikaan hyötyä yritettäessä arvata, miten systeemi käyttäytyisi aavistuksen verran muutetusta alkutilasta lähtien.

Kun loppusyksyn hämäryydessä pohdin koodausteorian ja kaaosteorian lähtökohtia, mieleeni juolahti ajatus reaaliarvoisesta funktiosta, joka kuvaa lähellä olevat pisteet kauaksi toisistaan ja vielä niin, että funktion arvosta tietyssä pisteessä ei voida päätellä juuri mitään funktion arvoista kyseisen pisteen lähiympäristössä — paitsi se, että ne ovat kaukana.

Selattuani lukion opetussuunnitelmia havaitsin petty-myksekseni, että pitkänkään matematiikan oppitunneilla ei enää opeteta raja-arvon käsitettä muuten kuin

geometristen mielikuvien ja yksinkertaisten esimerkitapausten tasolla. Niistä kummastakaan ei ole paljoa hyötyä tarkasteltaessa sellaisia patalogisia funktioita, joita aion tässä tutkia. Siksi artikkelin lukemista on pohjustettava esittämällä jatkuvuuden täsmällinen määritelmä. Sen sisäistämiseksi predikaattilogiikan ilmaisuihin totuttelu ennakkoon olisi eduksi, mutta opetussuunnitelmissa logiikkakin rajoittuu valinnaisiin opintoihin upotettuun propositiologiikkaan. Näin ollen lukija joutuu omaksumaan uudenlaisen ajattelutavan kylmiltään. Perinteisesti tällainen omaksuminen on vaatinut pitkähkön ajan ja runsaasti omakätisesti ratkaistuja harjoitustehtäviä.

Toivoakseni pystyn tarjoamaan lukijalle jotain edes mielikuvien tasolla.

Jatkuvuus

Funktion jatkuvuus määritellään lukiossa raja-arvon kautta: funktio f on jatkuva pisteessä a , jos funktion raja-arvo ja funktion arvo yhtyvät pisteessä a . Jatkuvuus tarkoittaa siis sitä, että $f(x)$ saadaan niin lähelle lukua $f(a)$ kuin ikinä halutaan, kunhan vaan x viedään riittävän lähelle pistettä a . Jatkuva funktio on tietyssä mielessä *läheisriippuva*: funktion arvo pisteessä a riippuu täysin funktion arvoista läheisissä pisteissä.* Jos ei tukeuduta raja-arvon käsitteeseen, jatkuvuuden perinteinen täsmällinen määritelmä on seuraava:

*Pahoittelen, jos olen ymmärtänyt läheisriippuvuuden (engl. *codependency*) käsitteen väärin.

Funktio $f: \mathbb{R} \rightarrow \mathbb{R}$ on **jatkuva** pisteessä a , jos jokaisesta positiivista reaalilukua ε kohti on olemassa sellainen (yleensä luvusta ε riippuva) positiivinen reaaliluku δ , että

$$|f(x) - f(a)| < \varepsilon \text{ aina, kun } |x - a| < \delta.$$

Tietyn funktion todistaminen jatkuvaksi pelkästään tähän määritelmään nojautuen on triviaaleja erikoistapauksia lukuun ottamatta huomattavan työlästä, ja se vaatii harjoittelun kautta syntynyttä kokemusta. Asiaan ennalta vihkiytymätön lukija joutunee vaikeuksiin jo niinkin yksinkertaisen funktion kuin $f(x) = x^2$ kanssa. Tästä huolimatta määritelmä on erittäin hyödyllinen ja käyttökelpoinen. Jatkuvuus- ja raja-arvotarkastelujen ε - δ -tekniikkaa on onneksi esitelty laajalti Solmun oppimateriaalissa [2], joten tekniikan selittämiseen ei tarvitse puuttua tämän enempää.

Predikaattilogiikan kvanttoreita $\forall$ (lue: kaikilla) ja $\exists$ (lue: on olemassa) käyttäen ehto funktion f jatkuvuudelle pisteessä a kirjoitetaan esimerkiksi näin:

$$\forall \varepsilon > 0 \exists \delta > 0: |x - a| < \delta \Rightarrow |f(x) - f(a)| < \varepsilon.$$

Osittain suomennettuna tämä tarkoittaa, että kaikilla $\varepsilon > 0$ on olemassa sellainen $\delta > 0$, että ehdosta $|x - y| < \delta$ seuraa $|f(x) - f(y)| < \varepsilon$. Kun hieroglyfejä muistuttavat symbolit tulevat tutuiksi, tiiviiseen muotoon kirjoitettu jatkuvuusehto auttaa asian hahmottamisessa.

Mitä tapahtuu, jos viimeisin epäyhtälö käännetään nurin päin?

Jatkuvuudesta äärimmäiseen epäjatkuvuuteen

Matemaattisessa tekstissä ε tarkoittaa yleensä pientä positiivista lukua, ja suurta positiivista lukua merkitään esimerkiksi kirjaimella M . Kun jatkuvuusehto käännetään nurinniskoin, potentiaalisesti hyvin pienen luvun ε tilalle astuu potentiaalisesti hyvin suuri luku M . Uusi, merkityssisällöltään ratkaisevasti erilainen ehto näyttää tältä:

$$\forall M > 0 \exists \delta > 0: 0 < |x - a| < \delta \Rightarrow |f(x) - f(a)| > M.$$

Tähän oli pakko lisätä epäyhtälö $0 < |x - a|$ mahdollisuuden $x = a$ poissulkemiseksi. Jos olisi $x = a$, epäyhtälö $|f(x) - f(a)| > M$ saisi muodon $0 > M$, joka ei toteutuisi millään positiivisella luvulla M . Jatkuvuusehdosta muokkaamani hankalan näköinen ehto on raakile. Kysyttelin sitä hieman ja päädyin seuraavaan määritelmään:

▼ Määritelmä 1

Olkkoon A reaalilukujen joukon $\mathbb{R}$ osajoukko. Funktio $f: A \rightarrow \mathbb{R}$ on **hillitön**, jos jokaista reaalilukua M kohti on olemassa $r > 0$, jolle

$$|f(a_1) - f(a_2)| > M$$

aina, kun $a_1, a_2 \in A$ ja $0 < |a_1 - a_2| < r$. ▲

Tietävästi joskus on käynyt niin, että matemaatikko on todistanut paksun nivaskan tuloksia tietyt ehdot toteuttavista funktioista, ja myöhemmin toinen matemaatikko on huomannut, ettei sellaisia funktioita voi edes olla olemassa. Siksi on tärkeää osoittaa esimerkiksi, että hillittömiä funktioita on olemassa.

Jos A on äärellinen, implikaation $\Rightarrow$ totuustaulusta[†] johtuen jokainen funktio $A \rightarrow \mathbb{R}$ on sekä jatkuva[‡] että hillitön. Tämänkaltaisten triviaalien tapausten lisäksi olisi syytä löytää varteenotettavampi esimerkki. Oteetaanpa joukoksi A rationaalilukujen joukko $\mathbb{Q}$. Se on tunnetusti numeroituva (ks. [3], [4]), joten $\mathbb{Q}$ voidaan esittää muodossa

$$\mathbb{Q} = \{q_1, q_2, q_3, \dots\},$$

missä $q_i \neq q_j$ aina, kun $i \neq j$. Ehto $f(q_i) = i^2$ määrittelee funktion $f: \mathbb{Q} \rightarrow \mathbb{R}$, jonka kuvajoukko on

$$f(\mathbb{Q}) = \{1^2, 2^2, 3^2, \dots\} = \{1, 4, 9, \dots\}.$$

Näytän seuraavassa, että funktio f nousee arvoon arvaamattomaan minkä tahansa pisteen läheisyydessä.

Väite 1

Funktio f on hillitön.

Todistus

Pitää osoittaa, että määritelmän 1 ehto on voimassa funktiolle f . Olkkoon siis M jokin reaaliluku. Koska $|f(q_i) - f(q_j)| > 2$ aina, kun $i \neq j$, ilman päätteilyn yleispätevyyden menettämistä voidaan olettaa, että $M \geq 2$. Luvuksi r valitaan

$$r = \min \{|q_i - q_j| \mid i \leq M, j \leq M, i \neq j\} > 0.$$

Jos $0 < |q_i - q_j| < r$, välttämättä $i \neq j$, ja $i > M$ tai $j > M$. Silloin

$$\begin{aligned} |f(q_i) - f(q_j)| &= |i^2 - j^2| = |i - j|(i + j) \\ &\geq i + j > M. \quad \blacksquare \end{aligned}$$

Markku Halmetoja esittelee mainiossa artikkelissaan [1] mm. jatkuvia mutta silti perin juurin vinksahaneita funktioita. Artikkelin kannattaa tutustua siellä käytyyn ε - δ -tekniikankin takia. Lopussa Halmetoja yllättää lukijan mainitsemalla, että vinksahaneet funktiot muodostavat ylivoimaisen enemmistön kaikkien jatkuvien funktioiden laumassa.

[†]Lause $P \Rightarrow Q$ on epätosi vain, jos P on tosi ja Q epätosi.

[‡]Funktion $f: A \rightarrow \mathbb{R}$ jatkuvuus tarkoittaa, että f on jatkuva jokaisessa joukon A pisteessä a . Jatkuvuus pisteessä $a \in A$ puolestaan tarkoittaa seuraavaa: jokaista $\varepsilon > 0$ kohti on olemassa sellainen $\delta > 0$, että $|f(x) - f(a)| < \varepsilon$ aina, kun $x \in A$ ja $|x - a| < \delta$.

Hillittömyyden tukahduttaminen

Yrityksistäni määritellä hillitön funktio $\mathbb{R} \rightarrow \mathbb{R}$ ei tullut mitään, ei kerta kaikkiaan. Syy selviää kohta. Sitä ennen on paikallaan esitellä kasaantumispisteen määritelmä ja muutamia valmistavia tosiasioita, joiden todistaminen ei ole vaikeaa, mutta vaatii harjaantuneisuutta. Seuraavat merkinnät ovat yleisesti käytössä:

$$\begin{aligned} B(a, r) &= \{x \in \mathbb{R} \mid |x - a| < r\}, \\ B^*(a, r) &= \{x \in \mathbb{R} \mid 0 < |x - a| < r\} \\ &= B(a, r) \setminus \{a\}. \end{aligned}$$

Ylempi joukko on a -keskinen r -säteinen avoin väli. Alempi on vastaavasti a -keskinen r -säteinen *punkteerattu* avoin väli. Moni pelkää punkteerausta. Pelko on turha, sillä punkteerauksessa vain poistetaan keskipiste.

▼ Määritelmä 2

Olkkoon A reaalitylukujen joukon $\mathbb{R}$ osajoukko. Piste $a \in \mathbb{R}$ on joukon A **kasaantumispiste**, jos jokaisella $r > 0$ pätee

$$A \cap B^*(a, r) \neq \emptyset. \quad \blacktriangle$$

Tosiasia 1

Jokainen a -keskinen r -säteinen avoin väli $B(a, r)$, $r > 0$, sisältää peräti äärettömän määrän joukon A alkioita silloin, kun a on joukon A kasaantumispiste.

Perustelu

Poimitaan joukosta $A \cap B^*(a, r)$ alkio a_0 . Sen jälkeen otetaan säteeksi $r_0 := |a_0 - a| > 0$ ja poimitaan joukosta $A \cap B^*(a, r_0)$ alkio a_1 . Sen jälkeen otetaan säteeksi $r_1 := |a_1 - a| > 0$ ja poimitaan joukosta $A \cap B^*(a, r_1)$ alkio a_2 . Poimintaa voidaan jatkaa loputtomiin, jolloin saadaan ääretön joukko $\{a_0, a_1, a_2, \dots\} \subset A \cap B^*(a, r)$. ■

Tosiasia 2

Jos ääretön joukko A sisältyy rajoitettuun väliin $[a, b]$, joukolla A on ainakin yksi väliin $[a, b]$ kuuluva kasaantumispiste.

Perustelu

Eräs kasaantumispiste on joukon

$$\{x \in \mathbb{R} \mid]-\infty, x] \cap A \text{ on äärellinen}\}$$

pienin yläraja eli supremum (ks. [2], pienimmän ylärajan määritelmä ja ominaisuudet). ■

Tosiasia 3

Jos $A_1, A_2, \dots$ on päättymätön jono numeroituvia joukkoja, myös yhdiste $A_1 \cup A_2 \cup \dots$ on numeroituva.

Perustelu

Tulos on perusteltu Wikipedian sivulla [4] käyttäen "kolmionumerointia". ■

Tosiasia 4

Ylinumeroituvalla reaalitylukujoukolla on vähintään yksi kasaantumispiste.

Perustelu

Olkkoon A ylinumeroituva joukko reaalitylukuja. Joukko $\mathbb{R}$ voidaan esittää välien

$$[n, n + 1], \quad n \in \mathbb{Z} = \{\text{kokonaisluvut}\},$$

yhdisteenä. Erään tällaisen välin ja ylinumeroituvan joukon A leikkaus on välttämättä ylinumeroituva (tosiasia 3). Tällöin kyseisellä välillä on joukon A kasaantumispiste (tosiasia 2). ■

Väite 2

Ei ole olemassa hillitöntä funktiota $\mathbb{R} \rightarrow \mathbb{R}$.

Todistus

Olkkoon $f: \mathbb{R} \rightarrow \mathbb{R}$ funktio. Reaalitylukujen joukko $\mathbb{R}$ on yhdiste alkukuvista

$$A_n := f^{-1}([n, n + 1]),$$

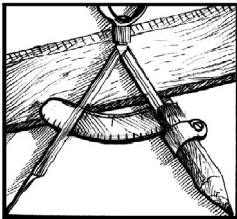
missä n on kokonaisluku. Koska $\mathbb{R}$ on ylinumeroituva, ainakin yksi joukoista A_n on ylinumeroituva (tosiasia 3), jolloin sillä on vähintään yksi kasaantumispiste a (tosiasia 4). Tällöin joukossa $A_n \cap B(a, r/2)$ on ääretön määrä alkioita kaikilla $r > 0$ (tosiasia 1). Koska näiden alkioiden x kuvat $f(x)$ kuuluvat välille $[n, n + 1]$, ne ovat korkeintaan yksikön päässä toisistaan. Jokaisella $r > 0$ on siis olemassa luvut $a_1, a_2 \in A_n \cap B(a, r/2)$, joille $a_1 \neq a_2$ ja $|f(a_1) - f(a_2)| \leq 1$. Koska lisäksi $|a_1 - a_2| < r$, hillittömyyden määrittelevä ehto funktiolle f ei voi olla voimassa edes tapauksessa $M = 1$. ■

Vasta kun ymmärtää kaikista vaihtoehtoista ainoan, ymmärtää kaiken.

— Erno Paasilinna

Viitteet

- [1] Halmetoja, M.: *Analyysin alkulähteillä*. Solmu 3/2008. <https://matematiikkalehtisolmu.fi/2008/3/kummalliset.pdf>
- [2] Halmetoja, M. & Merikoski, J.: *Lukion matemaattisen analyysin mestarikurssi*. Tampere, 2017. <https://matematiikkalehtisolmu.fi/2016/1mam.pdf>
- [3] Merikoski, J., Virtanen, A. & Koivisto, P.: *Johdatus diskreettiin matematiikkaan*. Tampere, 2004. <https://matematiikkalehtisolmu.fi/2018/jdm-2017-12-19.pdf>
- [4] Wikipedia: *Countable set*. https://en.wikipedia.org/wiki/Countable_set



Koristetähden askarteleminen harpilla ja viivaimella

Anne-Maria Ernvall-Hytönen

Helsingin yliopisto

Tässä tekstissä annetaan ohjeet koristetähden askarteleamiseen. Näitä voi pistää joulukuuseen, mutta yhtä hyvin esimerkiksi ikkunaan tammikuussa tai syntymäpäiväkoristeluksi heinäkuussa – värit voi valita tilanteen mukaan. Joka tapauksessa tarvitset seuraavat välineet ja tarvikkeet:

- harppi (mielellään hyväkuntoinen, hiukan jäykkä harppi, niin työskentely on helppoa),
- kynä,
- viivoitin,
- paksua paperia tai kartonkia,
- liimaa,
- nauhaa tai lankaa ripustamiseen.

Näitä tähtiä askarrellessa lapsena opin, että ympyrän kehälle voidaan asettaa sellaisen säännöllisen kuusikulmion kärjet, jonka sivun pituus on sama kuin ympyrän säde jo kauan ennen kuin näihin asioihin päästiin koulussa. Aluksi ilmiö tuntui lähinnä maagiselta. Myöhemmin opin matemaattiset perusteet.

Tavoitteena on siis tehdä tähti, jossa on viisi sakaraa ja keskusta kolmiulotteinen. Tähti koostuu kahdesta samanlaisesta tähdestä, jotka on liimattu vastakkain, jolloin lopullinen tähti näyttää samanlaiselta kummastakin suunnasta. Lopputuote näyttää siis suurin piirtein tältä:

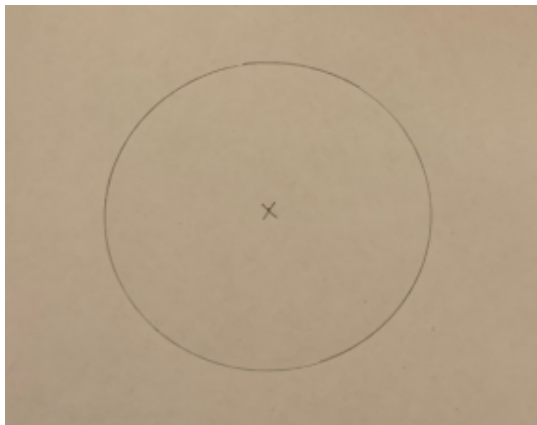


Työskentelyohjeet

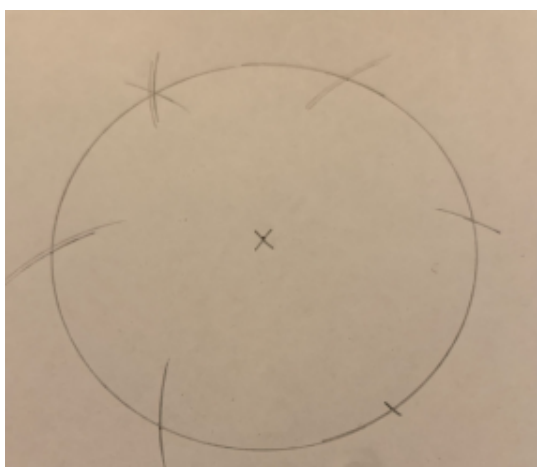
Kaikki merkinnät kannattaa tehdä pahvin tai paperin nurjalle puolelle, jolloin edustuspuoli jää siistimäksi. Seuraavissa kuvissa on käytetty kuvien selkeyden ja taitosten pysyvyyden vuoksi tavallista A4-

printteripaperia. Tämän jutun kuvissa merkinnät on tehty julkisivupuolelle, jolloin ehkä näkyy hiukan selkeämmin mitä ollaan tekemässä missäkin välivaiheessa.

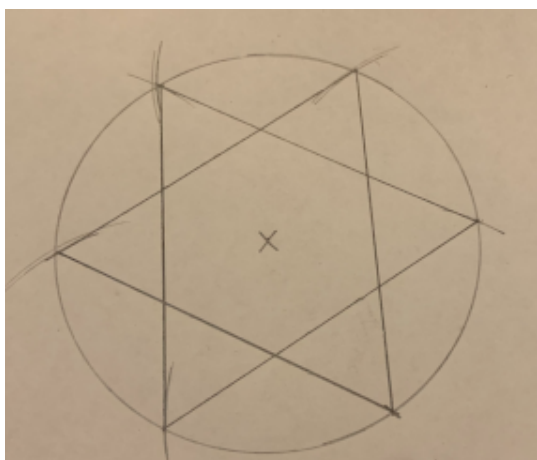
1. Valitse harpille sopiva säde ja piirrä ympyrä paperiin. Säilytä harpin säde ennallaan.



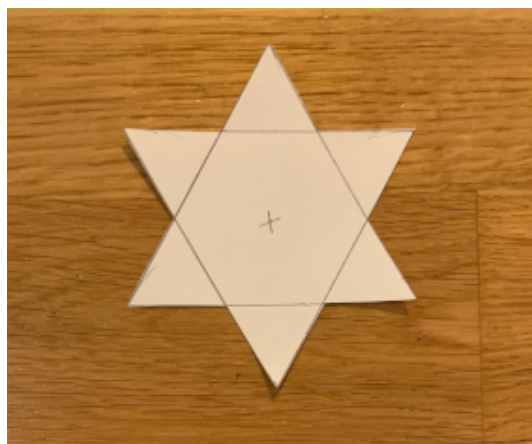
2. Jaa harpin säteen avulla ympyrän kaari kuuteen yhtä pitkään osaan, eli merkitse tasasivuisen kuusikulmion kärkipisteet.



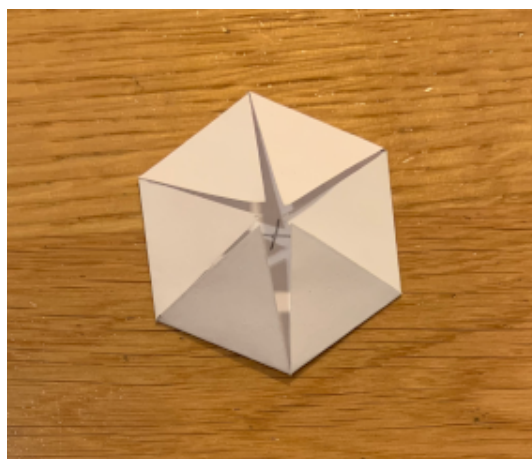
3. Yhdistä joka toinen kärkipiste yhteen suoralla viivalla.



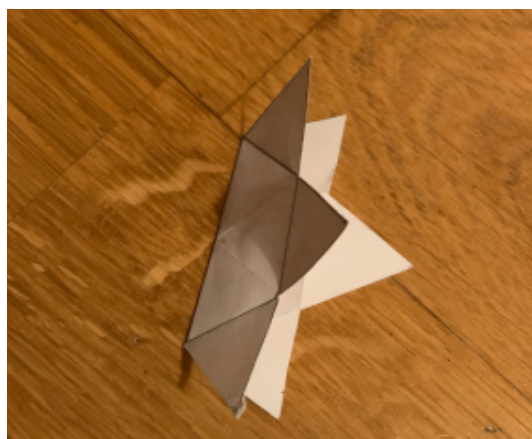
4. Leikkaa tähti irti paperista.



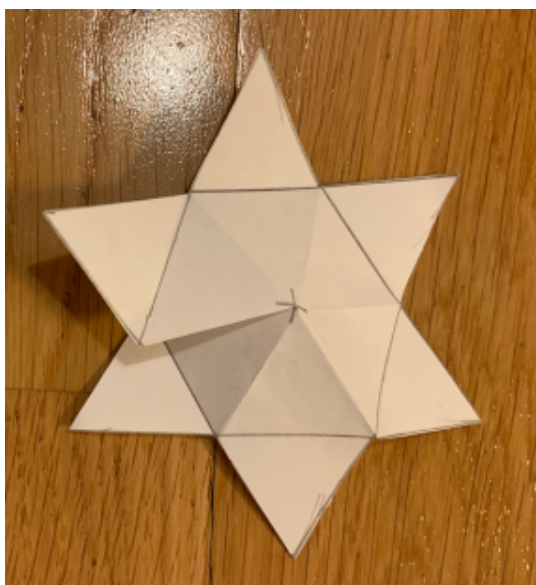
5. Taita tähden sakarat keskelle. Huomaa: taita niin, että julkisivu jää ikään kuin sisälle. Avaa taitokset. Tavoite on ainoastaan saada taitosjäljet paperiin, ei jättää tähteä taitelluksi kuusikulmioksi.



6. Taita tähti jokaista sisäkuusikulmion päälävistäjää myöten niin, että taitellessa paperin julkisivu on aina ulospäin.

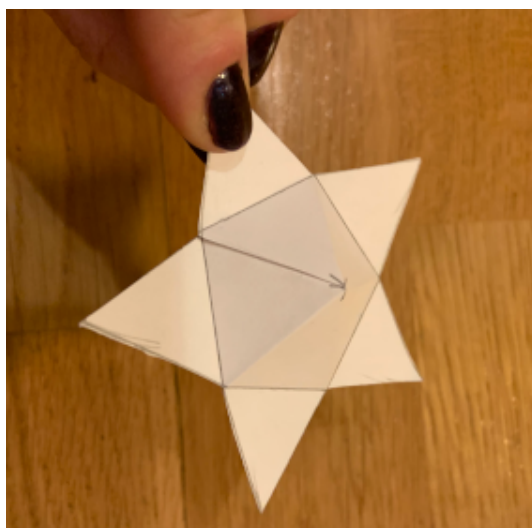


7. Leikkaa joidenkin sakaroiden välistä keskipisteeseen.

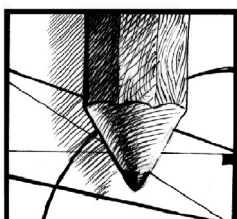


8. Liimaa leikatun aukon yli viereiset kuudennekset

päällekkäin.



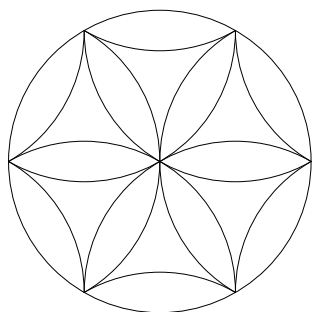
9. Tee toinen täsmälleen samankokoinen tähti ja liimaa ne vastakkain. Liimaa samalla myös kiinnin mahdollinen ripustuslenkki.



Ympyrän sisään piirrettyä

Markku Halmetoja

Kiitos Donald Knuth'in¹, lapsuuden harppiharjoitukset on nyt mahdollista tuottaa muutamalla koodirivillä paljon parempina kuin ne onnistuvat paperille tuhartamalla. Koululaisena näitä piirustaessa selvisi kuitenkin,



että ympyrän kehä voidaan jakaa kolmeen ja kuuteen yhtäsuureen osakaareen. Niiden vastaisista jänteisistä muodostuu ympyrän sisään piirretty tasasivuinen kolmio ja säännöllinen kuusikulmio. Piirtäminen siis onnistuu antiikin kreikkalaisen ihanteen mukaisesti ”geometrisesti oikein”, eli pelkästään harppia ja viivainta (ja kynää!) käyttäen.

Kreikkalaisille matematiikka oli geometriaa. Heillä ei ollut käytettävissään nykyaikaista reaalitykuvien teoriaa eikä algebrallisia menetelmiä yhtälöiden käsittelemiseen. Ongelma katsottiin ratkaistuksi ainoastaan sil-

loin, kun se voitiin piirtää harppia ja viivainta käyttäen. Piirtäminen tapahtui ensisijaisesti ajattelemalla: mietittiin algoritmi miten kuvio syntyisi jos se piirrettäisiin ja todistettiin menettelytapa oikean tuloksen antavaksi matemaattisten objektien määritelmiin, niitä koskeviin todistamattomina hyväksytyihin peruslauseisiin eli aksioomiin ja aikaisemmin todistettuihin teoreemiin perustuen. Eukleides² systematisoi aikakaudellaan tunnetun alkeisgeometrian tällaiseksi aksioomiin ja määritelmiin perustuvaksi yhtenäiseksi esitykseksi noin 2300 vuotta sitten. Vaikka hänen järjestelmänsä oli osin puutteellinen ja epäselvä, geometriaa opetettiin kautta maailman pääosin hänen Elementateokseensa pohjautuen aina 1900-luvun ensimmäiselle puoliskolle asti. Siihen perustunut kouluopetus oli Suomessakin ainoa eksaktiin ajatteluun johtanut polku. Hilbert³ viimeisteli eukleidisen geometrian aksioomat lopulliseen muotoon vuonna 1899 ilmestyneessä teoksessaan *Grundlagen der Geometrie*. Nytemmin matematiikasta kiinnostuneet voivat tutustua suomen kielellä sekä Eukleideen aksioomiin että Hilbertin niihin tekemiin täsmennyksiin hiljattain julkaistusta teoksesta [1]. Geometriaa opitaan myös valtakunnallisessa kilpavalmennuksessa, sillä se on vakioaihe matematiikkaolympialaisissa ja muissakin kilpailuissa. Solmun arkistossa on paljon geometriaan liittyvää aineistoa ja anti-kvariateistakin saattaa löytyä vanhoja geometrian oppikirjoja.

¹Donald Knuth (1938–), amerikkalainen tietojenkäsittelyteoreetikko, T_EX- ja METAFONT-ohjelmistojen kehittäjä.

²Eukleides Aleksandrialainen (325–265), kreikkalainen matemaatikko.

³David Hilbert, (1862–1943), saksalainen matemaatikko.

Ympyrän sisään piirretyt säännölliset monikulmiot olivat yksi antiikin matemaatikoiden mielenkiinnon kohteista. Jos kärkiä on n kappaletta, niin monikulmio jakautuu n :ksi tasakylkiseksi keskuskolmioksi, joiden huippukulmat ovat ympyrän keskipisteessä ja kyljet säteen mittaisia. Huippukulman suuruus on asteina $\frac{360^\circ}{n}$ ja radiaaneina $\frac{2\pi}{n}$. On selvää, että jos säännöllinen n -kulmio on piirretty, voidaan keskuskolmioiden huippukulmat puolittamalla (se tehdään harpilla ja viivaimella) saada aikaan säännöllinen $2n$ -kulmio. Siksi parittoman määrän kärkipisteitä omaavat monikulmiot ovat erityisen kiinnostavia. Antiikin matemaatikot tunsivat (siis osasivat piirtää) niistä kolme: tasasivuisen kolmion, säännöllisen viisikulmion sekä säännöllisen 15-kulmion. (Luonnollisesti he osasivat piirtää myös neliön.) Noin parituhatta vuotta myöhemmin Gauss¹ onnistui todistamaan, että konstruktio on mahdollinen, jos ja vain jos kärkien lukumäärä on muotoa $n = 2^{2^k} + 1$ oleva alkuluku tai tällaisten eri alkulukujen tulo. Näitä lukuja kutsutaan Fermat'n² luvuiksi, ja tähän (2021) mennessä niistä tiedetään alkuluvuiksi ainoastaan viisi ensimmäistä:

$$\begin{aligned} F_0 &= 2^{2^0} + 1 = 3, \\ F_1 &= 2^{2^1} + 1 = 5, \\ F_2 &= 2^{2^2} + 1 = 17, \\ F_3 &= 2^{2^3} + 1 = 257, \\ F_4 &= 2^{2^4} + 1 = 65537. \end{aligned}$$

Ennen asian täydellisempää käsittelyä, Gauss onnistui 19-vuotiaana konstruimaan säännöllisen 17-kulmion, mikä teki häneen niin suuren vaikutuksen, että hän laati siitä uutisen sanomalehteen. Myöhemmin hän halusi hautakiveensä veistettävän tämän monikulmion, mutta kivenveistäjä kieltäytyi, sillä hän ei olisi saanut sitä erottumaan ympyrästä. Kiveen ei taltalla ja vasaralla syntynyt riittävän terävää viivaa.

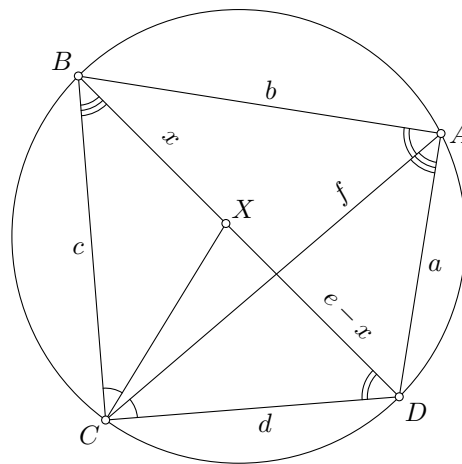
Ilmeisesti Gaussin tulosten innoittamina Richelot³ konstruoi säännöllisen 257-kulmion ja Hermes⁴ käytti kymmenen viimeistä elinvuottaan 65537-kulmion piirtämiseen. Hänen papereitaan säilytetään Göttingenin yliopiston matematiikan laitoksen ullakolla arkussa ([3]).

Yliopiston algebran kurssilla selvitetään, mitä yleensä voidaan piirtää harpilla ja viivaimella. Kurssilla tuskin konkreettisesti piirretään, sillä asia liittyy algebrassa tutkittavaan kuntateoriaan. Gaussin monikulmioita koskevan tuloksen ymmärtäminen on merkittävästi tätä yleistä teoriaa vaativampaa.

Tässä kirjoituksessa tutkimme eräitä säännöllisiä, ympyrän sisään piirrettyjä monikulmioita likimain lukion

oppimäärän mukaisesti. Pidämme selvänä, että ympyrän kehällä on $n (\geq 3)$ pistettä, jotka jakavat sen n :ksi saman suuruisiksi osakaareksi riippumatta siitä voidaanko pisteet löytää muinaiskreikkalaiseen tapaan. Perehdymme erityisesti viisikulmioon, sillä sen kauniita ominaisuuksia on suhteellisen helppo löytää. Sen kerrotaan lävistäjineen olleen Pythagoraan⁵ koulukunnan ilmeisesti salassa pidetty tunnusmerkki, sillä siihen sisältyy lukuisia irrationaalisia suhteita. Niiden olemassaolo oli ristiriidassa koulukunnan julkilausutun opinkappaleen kanssa; sen mukaan kaikki oli esitettävissä kokonaislukujen suhteina. Lävistäjien muodostama tähtikuvio lienee ollut tunnettu jo muinaisessa Babyloniassa noin 4000 vuotta sitten eli 1500 vuotta ennen Pythagorasta ([2]). Ennen viisikulmioon ryhtymistä, ympyrän sisällä kun ollaan, katsomme erään nykylukiossa unhoon jääneen antiikin aarteen.

Olkoon $ABCD$ jännenelikulmio, siis nelikulmio, jonka kärjet ovat ympyrän kehällä. Valitaan lävistäjältä BD



$$\triangle BCX \sim \triangle ACD \text{ ja } \triangle CDX \sim \triangle CAB$$

piste X siten, että $\angle XCB = \angle DCA$. Tällöin myös $\angle DCX = \angle ACB$, joten sopivia kehäkulmia tarkkailemalla havaitaan kuvion alareunaan kirjatut yhdenmuotoisuudet. Vastinsivuista saadaan kuvion merkinnoin verrannot

$$x : a = c : f \quad \text{ja} \quad (e - x) : b = d : f,$$

joista seuraa *Ptolemaioksen*⁶ teoreema:

$$ac + bd = ef.$$

Jännenelikulmion lävistäjien tulo on vastakkaisten sivujen tulojen summa.

¹Carl Friedrich Gauss (1777–1855), saksalainen matemaatikko.

²Pierre de Fermat (1601–1665), ranskalainen matemaatikko.

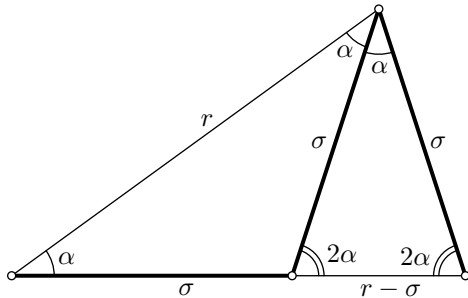
³Friedrich Julius Richelot (1808–1875), saksalainen matemaatikko.

⁴Johan Gustav Hermes (1846–1912), saksalainen matemaatikko.

⁵Pythagoras Samoslainen (n. 570 – n. 490), kreikkalainen matemaatikko.

⁶Claudius Ptolemaios (85–165), kreikkalainen astronomi ja matemaatikko.

Viisikulmioon päästään mukavimmin 10-kulmion kautta, sillä se saadaan siitä samalla tavalla kuin tasaviuinen kolmio kuusikulmiosta. Kuviossa on yksi 10-kulmion keskuskolmio. Sen huippukulma $\alpha = 36^\circ$ ja kantakulmat $2\alpha = 72^\circ$. Kantakulman puolittaja jakaa keskuskolmion kahdeksi tasakylkiseksi kolmioksi.



Yhdenmuotoisista kolmioista (tai kulmanpuolittajalauseen avulla) saadaan verranto

$$r : \sigma = \sigma : (r - \sigma).$$

Se kertoo, että ympyrän säde jakaantuu kultaisen leikkauksen suhteessa ja että jaossa saatu suurempi osa on etsitty kymmenkulmion sivu. Siksi tätä kolmiota on myös kutsuttu *kultaiseksi kolmioksi*. Verrannosta seuraa

$$\sigma = \frac{1}{2}(\sqrt{5} - 1)r,$$

ja se on helppo piirtää antiikin välineillä. Itse asiassa peruskoulun oppimäärä saattaa riittää seuraavan ohjelman toteuttamiseen:

- Piirretään suora ja sille normaali.
- Erotetaan niiden leikkauspisteestä toiselle suoralle säde r ja toiselle $2r$.
- Yhdistetään näin saatujen janojen päätepisteet, jolloin kuvio täydentyy suorakulmaiseksi kolmioksi. Sen hypotenuusan pituus on $r\sqrt{5}$.
- Vähennetään hypotenuusasta r ja puolitetaan erotus. Se on kysytty kymmenkulmion sivu σ .

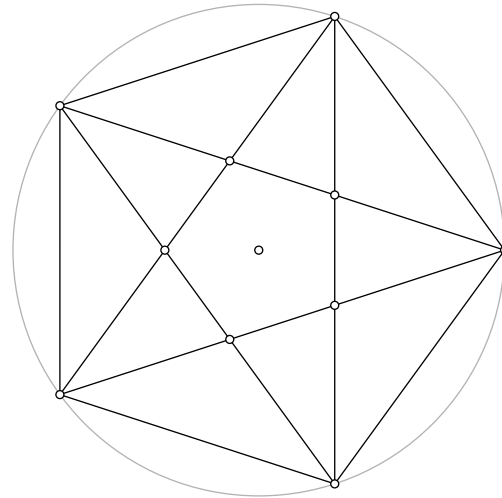
Ottamalla σ harpin kärkien väliin, saadaan ympyrän kehälle kymmenen pistettä ja sama määrä yhtäpitkiä osakaaria. Kolmion kulmien kosineille saadaan kosinilauseen avulla viisikulmion tutkimisen kannalta mukavat arvot:

$$\cos 36^\circ = \frac{1}{4}(\sqrt{5} + 1) \quad \text{ja} \quad \cos 72^\circ = \frac{1}{4}(\sqrt{5} - 1).$$

Esimerkiksi viisikulmion sivun pituus

$$\begin{aligned} S &= \sqrt{r^2 + r^2 - 2rr \cos 72^\circ} \\ &= r\sqrt{2 - \frac{1}{2}(\sqrt{5} - 1)} \\ &= \frac{1}{2}r\sqrt{10 - 2\sqrt{5}}. \end{aligned}$$

Viisikulmion lävistäjät rajoittavat kuvion osoittamalla tavalla pienemmän viisikulmion. Jos tätä ei ole aikaisemmin nähnyt, kannattaa pysähtyä miettimään, miksi sen sivut ovat keskenään yhtä pitkiä ja kaikki kulmat yhtäsuuria. Pythagoralaiset olivat tässä pohjattoman äärellä, sillä tämän pienemmän viisikulmion lävistäjät rajoittavat vielä pienemmän viisikulmion eikä tällä tavalla saatavien viisikulmioiden määrälle näy loppua. Ehkä se lisäsi kuvion mystisyyttä.



Edellä tuli mainittua, että viisikulmioon liittyy irrationaalisia suhteita. Aktiivinen lukija saa nyt tilaisuuden tutkia niitä ja paria muutakin kulmiota. Useimmat seuraavista kysymyksistä ovat ”katso-ja-näe” tyyppiä, eli pitkiä laskutoimituksia ei tarvita. Aluksi sovitaan merkinnöistä, sillä kaunista kuviota ei viitsi sotkea kirjaimilla. Olkoot siis viisikulmion sivu $= S$, lävistäjä $= l$, lävistäjien rajaaman pienemmän viisikulmion sivu $= s$ ja sakaran sivujana $= a$. Tällöin $l = a + s + a$.

- Määritä a) $S : l$, b) $s : a$.
- Määritä a) $s : S$, b) $(a + s) : S$.
- Osoita, että

$$\frac{l}{S} - \frac{S}{l} = 1.$$

- Koska viisikulmion lävistäjät rajaavat alkuperäisen kulmion sisään uuden viisikulmion, saadaan päättymätön jono toinen toistaan pienempiä viisikulmioita. Laske kaikkien viisikulmioiden alojen summa, kun isoimman ala on A .
- Ympyrän sisään piirretyn säännöllisen 7-kulmion sivu on s ja eripituiset lävistäjät a ja b . Osoita, että

$$\frac{1}{a} + \frac{1}{b} = \frac{1}{s}.$$

- Määritä $\cos 24^\circ$ tarkka arvo ja laske r -säteisen ympyrän sisään piirretyn säännöllisen 15-kulmion sivun pituus.

Kompleksilukujen vakiintuminen matemaattisen analyysin osaksi 1700-luvulta alkaen paljasti yllättävän yhteyden geometrisina objekteina pidettyjen monikulmioiden ja algebrallisten yhtälöiden välillä. Asian selvittämiseksi tarvitaan lukion oppimäärään kuulumat perustiedot kompleksiluvuista. Artikkelin [4] kaksi ensimmäistä kappaletta sisältää riittävän materiaalin, ks. myös [6]. Tärkein on de Moivre¹ kaava:

Kaikilla $\varphi \in \mathbb{R}$ ja $n \in \mathbb{Z}$

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

Se on jäänyt tärkeämpien Eulerin² kaavojen varjoon, mutta sillä olisi arvokas pedagoginen merkitys jos se opittaisiin lukiossa. Se toimisi hyvänä johdantona matemaattisiin korkeakouluopintoihin. Kompleksilukujen perusominaisuudet de Moivre kaavaan asti kannattaisi siis sisällyttää lukion opetussuunnitelmaan. Sopiva sijainti olisi trigonometrian osuuden jatkona.

Jaetaan kompleksitason origokeskinen yksikköympyrä n :ään yhtäsuureen osakaareen jakopisteillä

$$\left(\cos \frac{2k\pi}{n}, \sin \frac{2k\pi}{n}\right), \quad k \in \{0, 1, 2, \dots, n-1\},$$

jotka voidaan kätevimmin esittää kompleksilukuina

$$\varepsilon_k = \cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n}, \quad k \in \{0, 1, 2, \dots, n-1\}.$$

Jakopisteet ovat kyseisen ympyrän sisään piirretyn n -kulmion kärkipisteet. Niistä $\varepsilon_0 = 1$ sijaitsee pisteessä $(1, 0)$ ja de Moivre kaavan mukaan kaikilla kyseeseen tulevilla k :n arvoilla (itse asiassa *kaikilla* $k \in \mathbb{Z}$)

$$\begin{aligned} \varepsilon_k^n &= \left(\cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n}\right)^n \\ &= \cos \frac{2kn\pi}{n} + i \sin \frac{2kn\pi}{n} \\ &= \cos 2k\pi + i \sin 2k\pi = 1 + 0 = 1. \end{aligned}$$

Tulos merkitsee sitä, että luvut ε_k ovat polynomi yhtälön $z^n - 1 = 0$ juuria. Jos merkitään lyhyesti $\varepsilon_1 = \varepsilon$, niin de Moivre kaavan mukaan yhtälön juuret voidaan myös kirjoittaa muotoon $1, \varepsilon, \varepsilon^2, \varepsilon^3, \dots, \varepsilon^{n-1}$. Koska yhtälön asteluku on n , sillä on enintään n eri juurta, joten olemme löytäneet ne kaikki, ja mikä hienointa, ne sijaitsevat yksikköympyrän kehällä ympyrän sisään piirretyn säännöllisen n -kulmion kärkinä. Gaussin todistus monikulmioiden konstruotavuudesta perustuu tähän havaintoon, mutta se on hyvin vaikea.

Suomen kielellä se löytyy teoksesta [5]. Kärkipisteihin perustuu myös signaalinkäsittelyssä sovellettu diskreetti Fourier-muunnos käänteismuunnoksineen. Historiaa taaksepäin katsovalle nykyihmiselle tämä kaikki kertoo jotakin oleellista matematiikan luonteesta.

Lopuksi vielä eräs hauska huomio. Tarkastellaan yksikköympyrän sisään piirrettyjä säännöllisiä monikulmioita. Niistä ensimmäinen on tasasivuinen kolmio. Jos laskeaan sen yhdestä kärjestä muihin kärkiin piirrettyjen janojen pituuksien tulo, niin se havaitaan kulmien lukumääräksi: tulo on $\sqrt{3} \cdot \sqrt{3} = 3$. Neliölle tämä tulo on $\sqrt{2} \cdot 2 \cdot \sqrt{2} = 4$. Viisikulmiollekin se nähdään, jos jaksaa hieman pyöritellä juurilausekkeita ja kuusikulmiolle $1 \cdot \sqrt{3} \cdot 2 \cdot \sqrt{3} \cdot 1 = 6$. Tällainen säännönmukaisuus ei voi olla sattumaa. *Osoita siis, että jos yksikköympyrän sisään piirretyn säännöllisen monikulmion yhdestä kärjestä piirretään janat kaikkiin muihin kärkiin, niin janojen pituuksien tulo on monikulmion kärkien lukumäärä.*

Viitteet

- [1] Matti Lehtinen: Geometriaa ja geometriasta, Eukleides-kirjat 2021.
- [2] Carl Boyer: Tieteiden kuningatar, matematiikan historia osa I, Art House 2000.
- [3] Boris Sjöberg: Från Euklides till Hilbert, Historien om matematikens utveckling under tvåtusen år, Åbo Akademis förlag 1996.
- [4] Matti Lehtinen: Kaikki tarpeellinen kompleksiluvuista, <https://matematiikkalehtisolmu.fi/2006/1/lehtinen.pdf>.
- [5] Kalle Väisälä: Lukuteorian ja korkeamman algebran alkeet, 2. painos, Otava 1961.
- [6] Jerry Segercrantz: $\sin 18^\circ$ kolmella eri tavalla, <https://matematiikkalehtisolmu.fi/2004/2/sin18.pdf>.

¹Abraham de Moivre (1667–1754), ranskalainen matemaatikko.

²Leonhard Euler (1707–1783), sveitsiläinen matemaatikko.



Todistuspeli

Kalle Kytölä

Aalto-yliopisto, Matematiikan ja systeemianalyysin laitos

On vaikea kuvitella helpompaa matemaattista käsitettä kuin luonnolliset luvut¹: 0 on luonnollinen luku, 1 on luonnollinen luku, 2 on luonnollinen luku, 3 on luonnollinen luku, ja niin edelleen. Näennäisestä helppoudesta huolimatta olet epäilemättä törmännyt lukuteoreetikojen vastalauseeseen. Luonnollisista luvuista on helppo esittää vaikeita kysymyksiä, joiden ratkaisut ovat vieneet ihmiskunnalta vuosisatoja (esim. Fermat’n suuri lause), tai kysymyksiä, joihin parhaatkaan matemaatikot eivät edelleenkään tiedä vastauksia. Siksi lukuteorian tutkimus jatkuukin aktiivisena.

Tarkoitukseni ei kuitenkaan ole toistaa tuota perustelua vastalauseesta helposti esitettävistä vaikeista kysymyksistä. Entä jos jopa helposti esitettävien helppojen kysymysten huolellinen ymmärtäminen on vaikeaa?

Jos pitkävetäisen tarinan sijaan mieluummin suoraan haastat itsesi koettamaan täsmällistä ymmärrystäsi helpoista kysymyksistä, niin artikkelin kohokohta on tämä linkki peliin, jossa pääset todistamaan luonnollisten lukujen aritmeettisia perusominaisuuksia:

https://www.ma.imperial.ac.uk/~buzzard/xena/natural_number_game/

Matemaattisista todistuksista

Matemaattiset tulokset ovat universaaleja totuuksia. Tuloksilla on täsmällinen merkitys ja niille esitettyjen aukottomien todistusten ansiosta saamme olla herttaisen yksimielisiä muun muassa siitä, että:

- $2 + 3 = 5$;
- ympyrän halkaisijan kahteen päätepisteeseen mistä tahansa muusta ympyrän pisteestä piirretyt suorat kohtaavat toisensa suorassa kulmassa;
- riippumattomien, samoin jakautuneiden, integroituvien satunnaismuuttujien jonon yhä pidempien äärellisten osajonojen keskiarvot suppenevat todennäköisyydellä 1 kohti kyseisten satunnaismuuttujien yhteistä odotusarvoa;

ja niin edelleen.

Tieteiden kuningattaren olemusta tavallisesti luonnehditaan tuohon tapaan: matematiikka koskee loogisella päättelyllä saavutettavia universaalisti voimassa olevia johtopäätöksiä. Ja tämä tosiaan on melko osuva kuvaus siitä, miten matematiikkaa on harjoitettu ainakin sitten Eukleides Aleksandrialaisen teoksen *Alkeet* (n. 300 eaa). Mutta luonnehdinta itse ei ole merkitykseltään täsmällinen! Täsmennystä vaatisi vähintäänkin se, mitä tarkalleen ottaen tarkoitamme todistuksella —

¹Merkitsemme tässä kirjoituksessa, kuten tavallista on, luonnollisten lukujen joukkoa $\mathbb{N} = \{0, 1, 2, \dots\}$, kokonaislukujen joukkoa $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$, rationaalilukujen joukkoa $\mathbb{Q}$ ja reaalilukujen joukkoa $\mathbb{R}$.

ja vielä perustavammin, miten edes todistettavat väitteet tulisi muotoilla, jotta niillä olisi yksikäsitteinen merkitys, jota todistus sitten koskee. Matemaattinen logiikka käsittelee tuollaisia päänsärkyjä. Oma logiikan tuntemukseni on pinnallista, joten tyydyn kertomaan anekdootin ainoalta koskaan suorittamaltani logiikan kurssilta.

Ensimmäisen vuoden yliopistomatematiikan kurssilla *Logiikka I* esiteltiin propositiologiikan ja predikaattilogiikan täsmälliset kielet, joilla matemaattisia väitteitä yksikäsitteisesti muotoillaan. Kurssilla esiteltiin myös nk. “luonnollinen päättely” — tietynlainen propositio- ja predikaattilogiikan väitteiden todistusten kielioppi, jota hyväksyttävän loogisen todistuksen tulee noudattaa. Olin saanut houkuteltua seurakseni kurssille sosiaalipolitiikkaa ja filosofiaa opiskelevan entisen lukio-kaverini. Kun sitten kurssin edetessä osoittautui, että väitteen “kyllä tai ei” (tarkemmin sanottuna: $P \vee \neg P$, missä P on mielivaltainen propositio) päättelyyn kului paljon paperia ja aikaa, olin lievästi sanottuna turhautunut. Valtiotieteilijäystäväni sen sijaan tuumi, että luonnollinen päättely muistuttaa hieman tietokonepeliä, jossa yhä monimutkaisempien väitteiden todistaminen vastaa pelin yhä haastavampien tasojen läpääsemistä.

Formaaleista todistuksista

Ensimmäisen vuoden yliopisto-opiskelija pystyy pakon edessä tarkistamaan, noudattaako paperille raapustettu päättely logiikan sääntöjä viimeistä pilkkuakin myöten. Mutta eikö opiskelijaa sopivampi tällaiseen hanttihommaan olisikin tietokone? Siitä on kyse matematiikan formalisoinnissa: matemaattiset väitteet sekä niiden todistukset kirjoitetaan tietokoneen ymmärtämällä formaalilla kielellä ja kone tarkistaa sen, että todistus etenee logiikan sääntöjen mukaisesti ja väitetty tulos tulee näin todistetuksi.

Tarkoitukseen sopivia formaaleja kieliä on useita, mutta käytän esimerkkinä kieltä nimeltä *Lean*.

Karsittu esimerkki

Esimerkin paikan ansaitkoon lause numero 117 Eukleideen *Alkeet* -teoksen kirjassa *X*. Lauseen väite on, että luku $\sqrt{2}$ ei ole rationaalinen (toisin sanoen se on irrationaalinen). Klassinen todistus on lyhyt ja olet ehkä jo nähnytkin sen. Muistutetaan se kuitenkin ensin mieleen suurpiirteisesti ja katsotaan sitten (hyvin) yksityiskohtaisesti sen erästä päävaihetta.

Todistus on epäsuora, vastaoletukseen perustuva päätely. Vastaoletuksesta, että $\sqrt{2}$ olisikin rationaalinen, seuraisi, että se voidaan lausua muodossa $\sqrt{2} = \frac{n}{m}$ joillakin luonnollisilla luvuilla n ja m , joista $m \neq 0$ ja

joilla ei ole yhteisiä alkutekijöitä (rationaaliluku on supistetussa muodossa). Neliöjuuren määrittelevän ominaisuuden mukaan silloin on

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

Todistuksen ydin on johtaa tästä lähtökohdasta ristiriita näyttämällä, että silloin sekä n että m ovat välttämättä parillisia, joten vastoin vastaoletusta niillä on yhteinen tekijä 2.

Keskittykäämme ainoastaan tuohon todistuksen ydin-kohtaan, ja siitäkkin vain osaan. Yhtälön (1) pienellä uudelleenjärjestelyllä saamme $2m^2 = n^2$, ja tavoitteenamme on ensin päätellä luvun n parillisuus tästä tiedosta. Vasen puoli $2m^2$ on selvästi parillinen, joten niin on oltava oikeankin puolen n^2 , ja haluaisimme varmaankin osoittaa implikaation (seuraussuhteen)

$$n^2 \text{ on parillinen} \implies n \text{ on parillinen}. \quad (2)$$

Leanilla tämä implikaatio kirjoitetaan seuraavasti:

$$\text{even } (n^2) \rightarrow \text{even } n.$$

Implikaation (2) todistamiseksi on kuitenkin paras edetä jälleen epäsuorasti ja ensin näyttää implikaatio

$$n \text{ on pariton} \implies n^2 \text{ on pariton}, \quad (3)$$

joka Leanilla kirjoitetaan seuraavasti:

$$\text{odd } n \rightarrow \text{odd } (n^2).$$

Tämän aputuloksen eli lemmman (3) formaaliksi todistukseksi Leanilla kelpaa seuraava koodinpätkä, jonka rivit nimeän kirjaimilla myöhempää kommentointia varten:

```
lemma parittoman_nelio_pariton
  {n : ℕ} :
    odd n → odd (n^2) :=
begin
  intro n_pariton,                -- (A)
  unfold odd at *,                -- (B)
  cases n_pariton with k n_esitys, -- (C)
  rw n_esitys,                    -- (D)
  use 2 * k^2 + 2 * k,            -- (E)
  ring,                           -- (F)
end
```

Mitä tässä tapahtui? Ilmeisesti todistus alkaa taikasanalla **begin** ja päättyy vastaavasti **end**, mutta katsootaanpa niiden väliin jääviä rivejä yksitellen:

(A): Todistettavana on implikaatio (3), joten oletetaan implikaation vasen puoli (tässä tapauksessa että n on pariton) ja otetaan tavoitteeksi päätellä implikaation oikea puoli (tässä tapauksessa että n^2 on pariton). Tätä päättelysääntöä kutsutaan logiikassa *implikaation tuonniksi* (“implication introduction”) ja Leanissa sen hoitaa komento **intro**. Näin käyttöön saatavalle hypoteesille annamme koodissamme nimen **n_pariton** — tämä on kuten mikä tahansa muuttujan nimi ohjelmointikielessä.

(B): Tässä vaiheessa on tärkeää tietää, mitä täsmälleen ottaen tarkoittaa se, että n (tai n^2) on pariton. Kommentoia `unfold` käyttäen avaamme määritelmän termille `odd`, sekä hypoteesissamme `n_pariton` että tavoitteessamme. Painetusta koodista avaus ei valitettavasti näy päällepäin — koodatessa näkyy. Osoittautuu, että Leanissa täsmällinen määritelmä vaikkapa n :n parittomuudelle on, että $n = 2k + 1$ jollakin luonnollisella luvulla k . Siksi `n_pariton` tulee avatuksi muotoon

$$\exists (k : \mathbb{N}), n = 2 * k + 1.$$

Samaan tapaan avautuu tavoitteemme n^2 :n parittomuudesta, koska pyysimme avausta kaikkialla, `at *`.

(C): Hypoteesimme `n_pariton` on nyt eksistenssikvanttorilla $\exists$ alkava propositio, johon soveltuu eksistenssikvanttorin eliminointisääntö (‘‘existential quantifier elimination’’). Se hoituu Leanin komennolla `cases`. Lopputuloksena saamme käyttöömme muuttujan k sekä uuden hypoteesin `n_esitys`, jonka mukaan $n = 2k + 1$.

(D): Tässä vaiheessa tavoitteemme on osoittaa n^2 parittomaksi, mikä parittomuuden määritelmän mukaan tarkoitti, että jollakin luonnollisella luvulla j pätee $n^2 = 2j + 1$. Hypoteesia `n_esitys` (joka siis sanoo $n = 2k + 1$) käyttäen voimme komennolla `rw` uudelleenkirjoittaa (‘‘rewrite’’) tämän tavoitteen muotoon

$$\exists (j : \mathbb{N}), (2 * k + 1)^2 = 2 * j + 1.$$

(E): Lyhyellä binomikaavaan perustuvalla laskulla keksimme, että yllä oleva tavoitteemme ilmeisesti saavutettaisiin käyttämällä lukua $j = 2k^2 + 2k$. Formaalisti sovellamme eksistenssikvanttorin tuontisääntöä (‘‘existential quantifier introduction’’) komennolla `use`.

(F): Todistus saataisiin loppuun tarkistamalla, että luku j yllä tosiaan toteuttaa halutun ominaisuuden $(2k + 1)^2 = 2j + 1$. Onneksi Leanin taktiikkakomento `ring` osaa binomikaavan luonnollisten lukujen (puoli)renkaassa² $\mathbb{N}$. Siksi Lean tässä vaiheessa tyytyväisenä ilmoittaa³:

goals accomplished

Näin selvitettyämme ensimmäisen aputuloksen (3) jatkakaamme vielä väitteen (2) formalisoinnin verran. En avaa sen formaalia todistusta yhtä yksityiskohtaisesti, mutta kokoaan pikaiset kommentit kustakin rivistä jälleen alle. Huomionarvoista on:

²Itse asiassa `ring`-taktiikka osaa mitä tahansa mekaanisia renkaiden laskutoimituksia niin kompleksiluvuilla, matriiseilla kuin polynomeillakin — ylipäänsä missä tahansa renkaissa. Tietokone voi siis myös automatisoida päättelystä rutiininomaisia osia.

³Perinteisemmin todistuksen päätyminen voitaisiin ilmaista latinaksi *quod erat demonstrandum*, mikä on käännös Eukleideen käyttämästä kreikankielisestä ilmaisusta. Vielä tavallisempia ovat lyhenne *QED* tai ainoastaan symboli $\square$. Yhtä kaikki, tässä kohtaa on syytä olla tyytyväinen.

⁴Varsinainen kirjasto on osoitteessa <https://github.com/leanprover-community/mathlib> ja paljon lisätietoa siitä löytyy projektin kotisivulta <https://leanprover-community.github.io/>.

⁵Toki $\sqrt{2}$:n irrationaalisuus olisi löytynyt kirjastosta sellaisenaan, mutta kirjaston käyttäminen siihen suoraan olisi tyystin vesittänyt tämän päättelyharjoituksemme!

- Todistuksessa (toiseksi viimeisessä vaiheessa) käytetään yllä todistamaamme lemmaa `parittoman_nelio_pariton` eli aputulosta (3). Tähän tapaan uusia matemaattisia tuloksia rakennetaan ennestään tunnettujen pohjalta.

- Muutamassa vaiheessa käytetään Leanin matemaattisessa kirjastossa *mathlib*⁴ olevia valmiita tuloksia.⁵

```
lemma parillinen_jos_nelio_parillinen
  {n : ℕ} :
    even (n^2) → even n :=
begin
  intro parillinen_nelio,          -- (A)
  by_contradiction vastaoletus,    -- (B)
  have n_pariton : odd n,          -- (C)
    from nat.odd_iff_not_even.mpr vastaoletus,
  have pariton_nelio : odd (n^2),  -- (D)
    from parittoman_nelio_pariton n_pariton,
  exact nat.odd_iff_not_even.mp pariton_nelio
    parillinen_nelio,              -- (E)
end
```

Vaiheissa tapahtuu seuraavaa:

(A): Oletetaan implikaation vasen puoli eli että neliö n^2 on parillinen.

(B): Tehdään vastaoletus, että luku n ei ole parillinen.

(C): Silloin n on pariton. Perustelu: Luku on pariton jos (ja vain jos) se ei ole parillinen.

(D): Silloin myös neliö n^2 on pariton. Perustelu: Jo todistamamme lemma sekä tieto, että n on pariton.

(E): Ristiriita seuraa siitä, että luku on pariton (jos ja vain jos se ei ole parillinen, mutta n^2 olisi yllä olevien mukaan sekä pariton että parillinen. Siis vastaoletus on väärä ja n oli välttämättä parillinen.

goals accomplished

Mutkia matkassa

Edellisten esimerkkien lemموjen tarkoitus oli havainnollistaa, millaista yksityiskohtien tasoa formaali looginen argumentti vaatii. Nämä lemmat muodostavat periaatteessa olennaisen osan luvun $\sqrt{2}$ irrationaalisuustodistuksen formalisointia; Lemmaa `parillinen_jos_nelio_parillinen` käyttäen yhtälöstä

$2m^2 = n^2$ (jonka perusteella n^2 on ilmeisesti parillinen) esimerkiksi pääteltäisiin, että n on parillinen.

Jos yrität itse näitä käyttäen kirjoittaa luvun $\sqrt{2}$ formaalin irrationaalisuustodistuksen loppuun asti Leanilla, vaikkapa muodossa

$$\forall (q : \mathbb{Q}), q^2 \neq 2,$$

törmäät kuitenkin vielä muutamiin ehkä odottamattomiin hankaluuksiin.

Ensinnäkin, rationaaliluvut $q \in \mathbb{Q}$ Leanissa ovat (matemaattisesti oikein järjestyksessä) määritelmän mukaan muotoa $\frac{n}{m}$, missä nimittäjä m on nollasta eroava luonnollinen luku, $m \in \mathbb{N}$, $m \neq 0$, ja osoittaja n on kokonaisluku $n \in \mathbb{Z}$, vieläpä niin että näiden suurin yhteinen tekijä on 1 (eli rationaaliluvut on jo Leanin määritelmän mukaan valittu esitettäväksi supistetussa muodossa). Mutta hupsis! Lemmamme yllä oli todistettu oletuksella, että myös n on *luonnollinen* luku. No eipä hätää, korvataan kohta $\{n : \mathbb{N}\}$ muotoon $\{n : \mathbb{Z}\}$, ja ainoa mitä aiemmissa todistuksissa tarvitsee muuttaa on korvata jälkimmäisessä `nat.odd_iff_not_even` muotoon `int.odd_iff_not_even`.

Pari askelta eteen, muutama taakse. Yhtälö (1) oli rationaalilukuja koskeva. Rationaalilukujen kuntaominaisuuksia käyttäen muutamalla sievennysvaiheella siitä tosiaan saadaan Leanissakin yhtälö $2m^2 = n^2$. Mutta tämä yhtälö on silloin johdettu *rationaaliluvuille* $2m^2$ ja n^2 . Parillisuus ja parittomuus ovat kokonaislukujen ominaisuuksia, joten niistä puhumista varten molemmat puolet pitää ensin ymmärtää kokonaislukuihin. Ja ovathan myös n ja m kokonaislukuja. Paitsi, että m oli luonnollinen luku. No, eihän tässä pitäisi olla mitään ongelmaa, koska jokainen luonnollinen luku on kokonaisluku, jokainen kokonaisluku on rationaaliluku ja jokainen rationaaliluku on reaaliluku (ja jokainen reaaliluku on vieläpä kompleksiluku), eli on voimassa osajoukkorelaatiot

$$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$$

(ja $\dots \subseteq \mathbb{C}$). Leanissakin vastaava on kyllä jossakin määrin automaattista: tyyppimuunnokset (”coercion”)

$$\begin{aligned} \text{coe} &: \mathbb{N} \rightarrow \mathbb{Z} \\ \text{coe} &: \mathbb{Z} \rightarrow \mathbb{Q} \\ \text{coe} &: \mathbb{Q} \rightarrow \mathbb{R} \\ (\text{sekä } \text{coe} &: \mathbb{R} \rightarrow \mathbb{C}) \end{aligned}$$

hoituvat automaattisesti aina, kun Lean huomaa, että on esimerkiksi yritetty kirjoittaa kokonaisluku paikkaan, johon tarvittaisiin rationaaliluku.

Mutta lisäksi huolellisessa argumentaatiossa pitää kyllä käyttää havaintoa, että kokonaislukujen $2 \in \mathbb{Z}$ ja $m^2 \in \mathbb{Z}$ tulo $2m^2 \in \mathbb{Z}$ on sellainen, että sen tyyppimuunnos rationaaliluvuksi $(2m^2) \in \mathbb{Q}$ on sama kuin tyyppimuunnettujen lukujen $2 \in \mathbb{Q}$ ja $m^2 \in \mathbb{Q}$ tulo

rationaalilukujen kunnassa, $2m^2 \in \mathbb{Q}$. Matemaattinen notaatiomme

$$(2m^2) = 2m^2$$

ilman varta vasten merkitsemiä sulkeita yrittäisi laikaista maton alle sen, että yhtälön vasemmalla puolella käytetään kokonaislukujen kertolaskua ennen tyyppimuunnosta, kun taas oikealla puolella tyyppimuunnos suoritetaan ensin ja sen jälkeen käytetään rationaalilukujen kertolaskua. Matemaatikoille tutummin asian ytimen voi ilmaista niin, että diagrammi

$$\begin{array}{ccc} \mathbb{Z} \times \mathbb{Z} & \xrightarrow{\mathbb{Z}:n \text{ tulo}} & \mathbb{Z} \\ \text{coe} \times \text{coe} \downarrow & & \downarrow \text{coe} \\ \mathbb{Q} \times \mathbb{Q} & \xrightarrow{\mathbb{Q}:n \text{ tulo}} & \mathbb{Q} \end{array} \quad (4)$$

kommutoi. Oletko koskaan hämmästellyt tai kummas-tellut diagrammiin (4) tiivistettyä ihmeellistä asiaa?

Lisäksi tyyppimuunnosten suunnan kääntäminen on vielä hankalampaa; jokaista rationaalilukua ei noin vain muunnetakaan kokonaisluvuksi tai luonnolliseksi luvuksi. Siksi sellaiselle rationaalilukuja koskevalle yhtälölle, jonka molemmat puolet ovat tyyppimuunnettuja kokonaislukuja, täytyy aidosti tehdä jotakin, jos halutaan vastaava kokonaislukuja koskeva yhtälö (olen-naista tässä on tyyppimuunnosten injektiivisyys).

Niin omituiselta kuin se meille ihmisille vaikuttaakin, tällaiset pohdinnat täytyy jossakin vaiheessa perin pohjin selittää tietokoneelle. Kaikkia sellaisia tuskin tullaan koskaan saamaan erityisen kattavasti automatisoitua. Ihmismatemaatikot nimittäin hyppelivät tyyppimuunnoksia käyttäen kontekstista toiseen kiinnittämättä asiaan juurikaan huomiota. Kukaan ei hätkähdä sitä, että jokainen jatkuva funktio on myös funktio, tai että jokainen metrinen avaruus on myös topologinen avaruus, tai että jokainen rengas on myös vaihdannainen additiivinen ryhmä sekä multiplikaatiivinen monoidi jne., eikä sitä, että monet näitä koskevat operaatiot muodostavat lisäksi kommutoivia diagrammeja tyyppimuunnosten kanssa. Havahduttuamme kiinnittämään asiaan huomiota vaikuttaa lähes ällistyttävältä, ettei matemaatikkojen suurpiirteisyyttä johda virheisiin päätelyssä kovinkaan usein.

Omia kokemuksia

Ensimmäisenä omatoimisena formalisointiharjoitukseksi päätin todistaa Leanilla itselleni hyvin tutun lauseen: nk. portmanteau-lauseen todennäköisyysmittojen heikon suppenemisen yhtäpitävistä karakterisatioista. Olen opettanut sitä usein kursseillani. Luennoilla käytän sen todistukseen tyypillisesti puolisen tuntia. Saman opettaminen tietokoneelleni vaati minul-

ta yli 4000 koodiriviä ja hyvin hyvin monta viikonloppuilla. Erityisen hankalat kohdat liittyivät toisiinsa vaiheisiin, jotka ovat matemaattisestikin mutkikkaampia, mutta usein myös vaiheisiin, joissa en (ihmis)matemaatikkona alunperin edes huomannut olevan mitään vaiheita.

Mutta miksi?

Vaikuttaa takkuiselta — miksi matematiikan formalisointia siis tehdään?

Useille ylivoimaisesti tärkein syy on, että formalisointi on hauskaa. Äärimmäisen hauskaa! Oletko sattumalta harrastanut shakkia tai gota, ratkonut Rubikin kuutiota, tai pelannut muita älypelejä? En hetkeäkään ihmettele *miksi*! Vanha lukiokaverini ymmärsi suhtautua päättelyihin jo logiikan fuksikurssilla pelinä.

Hauskuuden lisäksi formalisoinnille on toki myös muita, ehkä vakavampia syitä.

Verrattuna perinteiseen kirjoitettuun matemaattiseen todistukseen, melko ilmeinen etu tietokoneen tarkastamalla formaalilla todistuksella on virheettömyys. Vaikka matematiikka periaatteessa on loogisen täsmällistä, sitä tekevät ihmiset, jotka eivät ole erehtymättömiä⁶. Tieteen historiasta löytää lukuisia kiehtovia tarinoita virheistä matematiikassa (lähtien vaikkapa Andrew Wilesin ensimmäisestä julkisesti esittämästä todistuksesta Fermat’n suurelle lauseelle), eivätkä virheet luotettavina pidetyissä matematiikan tutkimusartikkeleissa ja oppikirjoissa ole myöskään harvinaisia. Osa nykyaikaisista todistuksista on niin monimutkaisia, että parhaidenkin matemaatikkojen on hyvin vaikea luotettavasti pitää argumentteja järjestyksessä mielessään. Vuoden 2020 loppupuolella Peter Scholtze, yksi maailman ehdottomista kärkimatematikoista (Fieldsin mitali 2018), esitti haasteen erään oman teoreemansa formalisoinnista. Haasteessa hän kuvaili avoimesti sitä, kuinka harva tuon teoreeman todistuksen oli todella tarkastanut, ja myös omia aiempia erehdyksiään sekä huoliaan mahdollisista virheistä kyseisessä todistuksessa. Lean-yhteisö tarttui haasteeseen. Yhteisönnistuksella (ja Scholtzen tuella) noin kymmenen hengen ydinporukka sai puolessa vuodessa todistuksen olennaisimman osan formalisoitua. Koko todistuksen on edelleen käynyt läpi vain kourallinen alan matemaatikkoja, mutta tietokoneen hyväksymä formalisointi tekee

siitä yhden yksityiskohtaisimmin tarkistetuista nyky-matematiikan tuloksista.

Hyvin käytännöllinen syy formaalien kielten kehittämiseen ja käytölle on ohjelmistojen ja laitteiden toiminnan tarkastus. Samaa tapaan kuin matemaattisten todistusten logiikka käydään yksityiskohtia myöten läpi, voidaan varmistaa myös se, että esimerkiksi kriittiset sovellukset on toteutettu toimimaan annettujen ehtojen mukaisesti. Ohjelmisto- ja laitekehityksessä käytetään täysin samoja formaaleja (ohjelmointi)kieliä kuin matematiikan formalisoinnissa.

Muitakin vakavia ja käytännöllisiä syitä matematiikan formalisoinnille on, mutta en usko, että mikään niistä todella tavoittaa sen vaikuttavuutta. Formalisointi on vähintäänkin matematiikan digitalisointia. Vertailukohtana voisi pitää musiikkia tai valokuvia — niiden digitalisointia edeltäneillä vinylilevyillä tai filmirullilla oli oma hohtonsa, mutta vaikkapa Spotify’tä tai itseohjautuvissa autoissa tarvittavaa koneopittua kuvantunnistusta ei sellaisten varaan olisi rakennettu. Pelkkä sisällön välittäminen ja kopioiminen tai vaikkapa tiedon louhinta digitaalisesta aineistosta mahdollistaa varmasti aivan uusia käyttötapoja matematiikallekin. On hyvin vaikea ennustaa, mitä kaikkea siitä seuraa tulevaisuudessa.

Peli!

Jos olet valmis lähestymään formaaleja todistuksia pelinä, on erinomainen ensiaskele luonnollisten lukujen helppojen ominaisuuksien johtamiseen keskittyvä *Natural Number Game*

https://www.ma.imperial.ac.uk/~buzzard/xena/natural_number_game/,

joka ei vaadi Leanin asentamista omalle tietokoneelle, vaan toimii sellaisenaan verkossa.

Arvokkaista kommentteista kiitokset ansaitsevat:

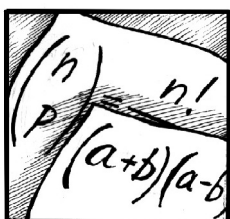
Jukka Kohonen

Milo Orlich

Juha Ruokolainen

Vadim Weinstein

⁶Korjatkaa, jos olen väärässä.



Solmun tehtäviä

Tehtävät sopivat lukiolaisten lisäksi myös edistyneille yläkoululaisille.

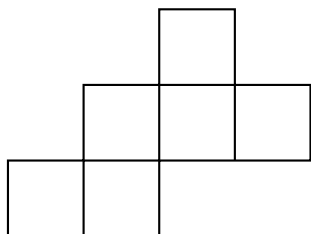
1. Ratkaise yhtälöpari

$$\begin{cases} x + y + \frac{x}{y} = 19, \\ \frac{x(x+y)}{y} = 60, \end{cases}$$

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

2. Kolmen peräkkäisen kokonaisluvun neliöiden summa on yhtä suuri kuin seuraavien kahden kokonaisluvun neliöiden summa. Mitkä nämä peräkkäiset viisi kokonaislukua ovat?

3. Paperille on piirretty alla olevan kuvan mukainen neliöstä koostuva monikulmio. Kaksi neliötä väritetään punaisiksi ja loput neliöt erivärisiksi: yksi neliö vihreäksi, yksi keltaiseksi, yksi siniseksi ja yksi oranssiksi. Monikulmio leikataan irti paperista ja neliöiden yhtymäkohdissa 90° taitoksia tekemällä muodostetaan kuutio. Kuinka monella eri tavalla neliöiden värittäminen on mahdollista tehdä niin, että muodostetussa kuutiossa mitkään vierekkäiset sivut eivät ole samanvärisiä?



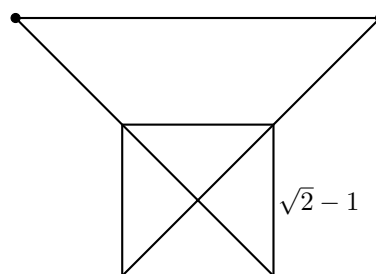
4. Kaksi henkilöä yritti arvioida ulkoilmakonsertin yleisömäärän. Toinen arvioi, että yleisöä oli 2700, ja toinen

puolestaan arvioi, että yleisöä oli 3600. Osoittautui, että toisen arvion prosentuaalinen virhe oli kaksi kertaa niin suuri kuin toisen virhe. Lisäksi toinen aliarvioi ja toinen yliarvioi yleisön määrän. Kuinka paljon konsertissa oli yleisöä?

5. Neliön sivun pituus on $\sqrt{2} - 1$. Molempia neliön lävistäjiä jatketaan toisesta päästä neliön sivun pituuden verran, ks. kuva alla.

- (a) Kuinka pitkä on jana, joka yhdistää jatkeiden päätepisteet?

- (b) Osoita, että neliössä on kärki, joka yhdessä jatkeiden päätepisteiden kanssa muodostaa tasakylkisen kolmion.

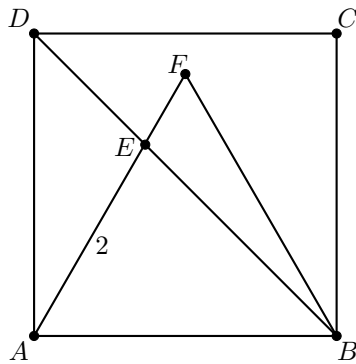


6. Kuuden peräkkäisen kokonaisluvun summa kerrotaan kuuden seuraavan kokonaisluvun summalla. Osoita, että tällä tavalla saadun tulon jakojäännös luvulla 36 jaettaessa on aina sama.

7. Määritä luvun $11! + 13!$ suurin alkutekijä. (Positiivisen kokonaisluvun n kertoma $n!$ on kokonaislukujen $1, \dots, n$ tulo; esimerkiksi $4! = 1 \cdot 2 \cdot 3 \cdot 4 = 24$.)

8. Kaupan kassassa on 5, 10, 20, 50, 100 ja 200 euron seteleitä yhteensä 18 200 euroa. Ennen kuin viimeisin seteli lisättiin kassaan, niin jokaisen setelityypin lukumäärä oli kääntäen verrannollinen setelin arvoon. Kuinka monta 200 euron seteliä kassassa on?

9. Tasasivuinen kolmio ABF on neliön $ABCD$ sisällä alla olevan kuvan mukaisesti. Janan AE pituus on 2. Mikä on neliön $ABCD$ pinta-ala?

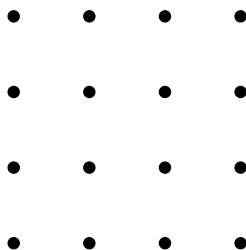


10. Aino, Pekka ja Liisa pelaavat seuraavanlaista peliä. He valitsevat vuorotellen jonkin kokonaisluvun yhdestä kymmeneen ja lisäävät luvun aikaisemmin valittujen lukujen summaan. Aino aloittaa, Pekka on toinen ja Liisa on kolmas, jonka jälkeen vuoro siirtyy takaisin Ainolle jne. Selvyyden vuoksi jokainen pelaaja sanoo vuorollaan lukujen uuden summan. Pelin voittaa pelaaja, joka sanoo ensin luvun sata. Osoita, että tytöt voivat keskenään sopia pelistrategian, jolla pelin voittaa varmasti jompi kumpi heistä, eikä Pekka voi voittaa peliä.

11. Heitetään kuusi noppaa. Mikä on todennäköisyys, että saadaan vähintään neljä samaa silmälukua?

12. Positiiviselle reaalityylille x on voimassa $x^2 + \frac{1}{x^2} = 7$. Määritä $x^5 + \frac{1}{x^5}$ laskematta luvun x arvoa.

13. Alla olevassa kuvassa on 16 pistettä. Kuinka monella tavalla on mahdollista valita kolme pistettä niin, että muodostuu kolmio, jonka kärjet ovat valituissa pisteissä?



14. Reaalityylut x ja y toteuttavat ehdot $x + 3y = 12$ ja $x \geq 2y \geq 0$. Mitä arvoja $x + 2y$ voi saada?

15. Millä parametrin a arvoilla toisen asteen yhtälöllä

$$ax^2 + a^2x + a = \frac{1}{a}$$

on kaksoisjuuri?

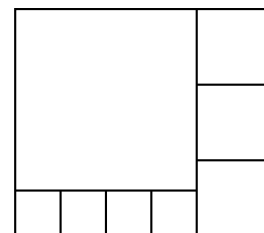
16. Yksin tehdessään Pekalta kuluu työtehtävässä viisi tuntia ja Paavolta kuluu samassa työtehtävässä kuusi tuntia. Kun he tekevät työtehtävän yhdessä, niin heidän tuottavuutensa heikkenee jatkuvan kinastelun takia. Molempien työteho vähenee suhteessa yhtä paljon samalla prosenttimäärällä. Kuinka monta prosenttia heidän työtehonsa vähenee, kun yhdessä heillä kuluu työtehtävässä 3,5 tuntia?

17. Tiinalla on uusi työpaikka ja hän kulkee töihin omalla autolla. Ensimmäisenä työpäivänä hän ajoi 70 km/h keskinopeudella ja saapui töihin minuutin myöhässä. Toisena työpäivänä hän ajoi 75 km/h keskinopeudella ja saapui töihin minuutin etuajassa. Kuinka pitkä työmatka Tiinalla on?

18. Joulukuun on aikaa viisi päivää ja joulukuusessa on jäljellä viisi karkkia: kaksi niistä on marmeladia ja kolme on suklaata. Karkkeja ei voi tunnistaa käärepaperin perusteella. Hanna päättää syödä yhden karkin päivässä joulukuun asti. Kumpi seuraavista on todennäköisempää: Hanna syö toisen (ja viimeisen) marmeladikarkin kolmantena päivänä vai hän syö kolmannen (ja viimeisen) suklaakarkin neljäntenä päivänä?

19. Heitetään kolikkoa viisi kertaa. Tämän jälkeen heitetään kolikkoa vielä niin monta kertaa kuin saatiin kruunaa viidessä ensimmäisessä heitossa. Mikä on todennäköisyys, että saadaan yhteensä 5 kruunaa?

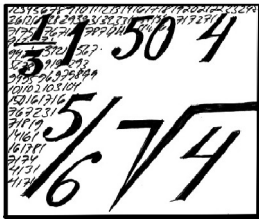
20. Suorakulmio jaetaan kahdeksaksi neliöksi alla olevassa kuvassa esitetyllä tavalla. Keskikokoisen neliön pinta-ala on 100 cm^2 . Mikä on alkuperäisen suorakulmion pinta-ala?



Tehtävien ratkaisut julkaistaan Solmun seuraavassa numerossa.

Lähde: KöMaL

Käännös ja sovitukset suomeksi: Mika Koskenoja



Ketjumurtoluvut: mitä ne ovat ja mitä hyötyä niistä on?

Anne-Maria Ernvall-Hytönen

Helsingin yliopisto

Yksinkertaiseksi ketjumurtoesitykseksi kutsutaan positiivisen luvun esittämistä muodossa

$$a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \frac{1}{a_4 + \ddots}}}},$$

missä luvut $a_1, \dots$ ovat positiivisia kokonaislukuja ja a_0 on epänegatiivinen kokonaisluku. Lisäksi sovitaan, että viimeinen luvuista a_i (jos siis kehitelmä on päättyvä) on suurempi kuin 1.

Esimerkiksi siis ei kirjoiteta

$$\frac{37}{16} = 2 + \frac{1}{3 + \frac{1}{4 + \frac{1}{1}}},$$

vaan

$$\frac{37}{16} = 2 + \frac{1}{3 + \frac{1}{5}}.$$

Käytännössä tilanne on tämä: Jos kyseessä on rationaaliluku, päättyy tämä esitys joskus (eli kolmen pisteen tilalle ei tule äärettömän pitkää jonoa). Jos kyseessä on irrationaaliluku, ei tämä esitys pääty koskaan. Jälkimmäinen on helppo nähdä. Ensimmäinen ei ole niin

triviaali. Se on luultavasti helpoin perustella sillä, että ketjumurtokehitelmä tehdään käytännössä Eukleideen algoritmilla, joka vain kirjoitetaan toisin. Innostunut lukija voi perustella tämän itselleen. Jos Eukleideen algoritmi kuulostaa täysin vieraalta, ei tarvitse pelästyä: ketjumurtokehitelmiä voi tehdä, vaikkei olisi Eukleideesta tai hänen algoritmistaan koskaan kuullutkaan.

Luvun kehittäminen ketjumurtoluvuksi

Otetaan nyt pari esimerkkiä siitä, miten luku kehitetään yksinkertaiseen ketjumurtoesitykseen. Käsitellään ensin rationaaliluku. Verrataan sen jälkeen ketjumurtokehitelmää Eukleideen algoritmiin osoittajalle ja nimittäjälle.

Esimerkki. Kirjoitetaan $\frac{27}{8}$ ketjumurtolukuna. Huomataan ensin, että esityksessä

$$a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \frac{1}{a_4 + \ddots}}}},$$

on osan

$$\frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \frac{1}{a_4 + \frac{1}{\ddots}}}}}$$

pakko olla ykköstä pienempi, sillä $a_1 \geq 1$ ja vähintään toinen seuraavista ehdoista toteutuu: $a_1 \geq 2$ tai nimitäjässä on muutakin kuin a_1 . Luvun a_0 on siis vastattava luvun kokonaisosaa. Koska $\frac{27}{8} = 3 + \frac{3}{8}$, on oltava $a_0 = 3$. Nyt

$$\frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \frac{1}{a_4 + \frac{1}{\ddots}}}}} = \frac{3}{8},$$

joten

$$a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \frac{1}{a_4 + \frac{1}{\ddots}}}} = \frac{8}{3}.$$

Ihan vastaavasti kuin edellä huomataan, että luvun a_1 on oltava luvun $\frac{8}{3}$ kokonaisosa. Koska $\frac{8}{3} = 2 + \frac{2}{3}$, on $a_1 = 2$. Nyt

$$\frac{1}{a_2 + \frac{1}{a_3 + \frac{1}{a_4 + \frac{1}{\ddots}}}} = \frac{2}{3},$$

joten

$$a_2 + \frac{1}{a_3 + \frac{1}{a_4 + \frac{1}{\ddots}}} = \frac{3}{2} = 1 + \frac{1}{2}.$$

Siispä $a_2 = 1$ ja $a_3 = 2$. On siis saatu

$$\frac{27}{8} = 3 + \frac{1}{2 + \frac{1}{1 + \frac{1}{2}}}.$$

Jos lukujen 27 ja 8 suurin yhteinen tekijä määritettäisiin Eukleideen algoritmilla, näyttäisi se tältä:

$$\begin{aligned} 27 &= 3 \cdot 8 + 3 \\ 8 &= 2 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \\ 2 &= 2 \cdot 1. \end{aligned}$$

Eukleideen algoritmin kertoimet (ensimmäiset luvut yhtäsuuruusmerkkien oikealla puolella) ovat samat kuin ketjumurtoesityksen kertoimet. Tämän perusteleminen itselle on siis se innokkaan lukijan harjoitustehtävä.

Otetaan toinen esimerkki. Ennen esimerkkiä palauteetaan mieleen (tai johdetaan) eräs muistikaava:

$$(a-b)(a+b) = a^2 + ab - ba - b^2 = a^2 - b^2.$$

Tämän avulla voi muokata joskus lukuja helpommin käsiteltävään muotoon. Esimerkiksi:

$$\frac{1}{\sqrt{3}-1} = \frac{\sqrt{3}+1}{(\sqrt{3}-1)(\sqrt{3}+1)} = \frac{\sqrt{3}+1}{2}.$$

Esimerkki. Kirjoitetaan $\sqrt{3}$ ketjumurtolukuna. Kuten aiemminkin, huomataan, että luvun a_0 on vastattava luvun $\sqrt{3}$ kokonaisosaa. Koska $1 \leq \sqrt{3} < 2$, niin kokonaisosa on 1. Siispä $a_0 = 1$. Nyt

$$\frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \frac{1}{a_4 + \frac{1}{\ddots}}}}} = \sqrt{3} - 1,$$

eli

$$a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \frac{1}{a_4 + \frac{1}{\ddots}}}} = \frac{1}{\sqrt{3}-1}.$$

Yllä olevan laskun perusteella

$$\frac{1}{\sqrt{3}-1} = \frac{\sqrt{3}+1}{2}.$$

Tämän muotoilun etu on se, että sitä on helppo arvioida. Koska $1 \leq \sqrt{3} < 2$, niin

$$1 = \frac{1+1}{2} \leq \frac{\sqrt{3}+1}{2} \leq \frac{2+1}{2} = \frac{3}{2}.$$

Siispä $a_1 = 1$, sillä se on luvun $\frac{1}{\sqrt{3}-1}$ kokonaisosa. Koska $a_1 = 1$, pätee

$$1 + \frac{1}{a_2 + \frac{1}{a_3 + \frac{1}{a_4 + \frac{1}{\ddots}}}} = \frac{1}{\sqrt{3}-1} = \frac{\sqrt{3}+1}{2},$$

joten

$$\frac{1}{a_2 + \frac{1}{a_3 + \frac{1}{a_4 + \frac{1}{\ddots}}}} = \frac{\sqrt{3}+1}{2} - 1 = \frac{\sqrt{3}+1-2}{2} = \frac{\sqrt{3}-1}{2}.$$

Nyt siis

$$a_2 + \frac{1}{a_3 + \frac{1}{\ddots}} = \frac{2}{\sqrt{3} - 1} = \frac{2(\sqrt{3} + 1)}{(\sqrt{3} - 1)(\sqrt{3} + 1)} = \sqrt{3} + 1.$$

Koska $2 \leq \sqrt{3} + 1 \leq 3$, on $a_2 = 2$. Siispä

$$\frac{1}{a_3 + \frac{1}{a_4 + \frac{1}{\ddots}}} = \sqrt{3} + 1 - 2 = \sqrt{3} - 1,$$

joten

$$a_3 + \frac{1}{a_4 + \frac{1}{\ddots}} = \frac{1}{\sqrt{3} - 1} = \frac{\sqrt{3} + 1}{2}.$$

Tämän tilanteen olemme kuitenkin nähneet jo aiemmin, eli laskiessamme lukua a_1 . Siispä $a_3 = a_1 = 1$. Nyt tilanne alkaa toistamaan itseään, eli $a_4 = a_2 = 2$. Tämä tulee jatkumaan vastaavasti, eli luvuissa a_i vuorottelevat luvut 1 ja 2. Jos alaindeksi i on pariton, on $a_i = 1$, ja jos alaindeksi i on parillinen, on $a_i = 2$. Nyt siis

$$\sqrt{3} = 1 + \frac{1}{1 + \frac{1}{2 + \frac{1}{1 + \frac{1}{2 + \frac{1}{\ddots}}}}}.$$

Ketjumurtoluvut ja arviointi

Tässä luvussa joudun vain antamaan tuloksia todistamatta niitä. Perusteellisesti kaiken todistamalla tämä artikkeli muuttuisi melko pitkäksi, eikä enää tarjoaisi sitä nopeaa johdattelua ketjumurtolukuihin, joka oli tarkoitukseni.

Luvun ketjumurtokehitystä voidaan katkaista. Esimerkiksi luvun

$$a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \frac{1}{a_4 + \frac{1}{\ddots}}}}},$$

ketjumurtokehitystä voidaan katkaista esimerkiksi seuraavilla tavoilla:

$$a_0, \quad a_0 + \frac{1}{a_1}, \quad a_0 + \frac{1}{a_1 + \frac{1}{a_2}},$$

jne. Vastaavasti kuin katkaisemalla desimaalikehitelmä, näinkin saadaan arvioita luvulle. Näitä kutsutaan luvun *konvergenteiksi*.

Aloitetaan luvun π arvioinnista kymmenjärjestelmän avulla. Tiedetään, että

$$\pi = 3,14159265 \dots$$

Arvioita luvulle π saadaan siis suoraan sen desimaalikehitelmää katkaisemalla ja normaalien pyöristysääntöjen mukaan ylös tai alas pyöristämällä:

desimaalit	arvio	virhe
0	3	$< 0,2 = \frac{2}{10}$
1	$3,1 = \frac{31}{10}$	$< 0,04 = \frac{4}{100}$
2	$3,14 = \frac{314}{100}$	$< 0,002 = \frac{2}{1000}$
3	$3,142 = \frac{3142}{1000}$	$< 0,0005 = \frac{5}{10000}$

Virheet ovat selvästi pienempiä kuin luvun suuruus. Lisäksi virhe pienenee, kun otetaan desimaaleja lisää (eli kasvatetaan arviossa nimittäjää). Tämä on hyvä, mutta käytännössä virhe pienenee melko hitaasti. Otetaan vertailun vuoksi luvun π ketjumurtokehitystä

$$3 + \frac{1}{7 + \frac{1}{15 + \frac{1}{1 + \frac{1}{292 + \frac{1}{\ddots}}}}}$$

ja siitä saatavat arviot

$$\pi \approx 3, \quad \pi \approx 3 + \frac{1}{7} = \frac{22}{7}, \quad \pi \approx 3 + \frac{1}{7 + \frac{1}{15}} = \frac{333}{106}, \dots$$

Nyt virheet ovatkin

arvio	virhe
3	$< 0,2 = \frac{2}{10}$
$\frac{22}{7}$	$< \frac{2}{1000}$
$\frac{333}{106}$	$< \frac{1}{10000}$
$\frac{103993}{33102}$	$< 10^{-9}$

Virheet pienenevät nyt huomattavaa vauhtia verrattuna nimittäjän kasvuvauhtiin. Yleisesti voidaan todistaa, että jos ξ on jokin luku ja $\frac{r}{s}$ joku sen konvergentti, niin

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

Toinen suunta on puolestaan tällainen: Jos ξ on jokin luku ja $\frac{r}{s}$ joku arvio, joka toteuttaa ehdon

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

niin $\frac{r}{s}$ on väistämättä luvun ξ konvergentti.

Sovellus yhtälönratkaisuun ja kryptografiaan

RSA-salausjärjestelmässä on julkinen avain, joka on lukupari (n, e) sekä salauksen purkamiseen tarvittava salainen eksponentti d . Luku n on kahden eri alkuluvun tulo $n = pq$. Tämä alkutekijähajotelma on salainen. Luvut toteuttavat ehdon

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

jolloin $w^{ed} \equiv w$ kaikilla w . Tällöin siis viesti voidaan salata korottamalla se potenssiin e ja redusoimalla modulo n ja salaus voidaan purkaa korottamalla salattu viesti potenssiin d ja redusoimalla modulo n .

Otetaan esimerkki, joka on tehty hyvin pienillä luvuilla:

Esimerkki. Jos $n = 7 \cdot 11 = 77$, niin $\varphi(n) = 6 \cdot 10 = 60$. Valitaan luvuksi e esimerkiksi 13. Tällöin viesti 8 salataan seuraavasti: Lasketaan 8^{13} ja lasketaan jakojäännös luvulla 77 jaettaessa. Saadaan 50.

Viestin purkamiseksi tarvitaan d . Tämä luku toteuttaa siis ehdon

$$13d \equiv 1 \pmod{60}.$$

Nyt $d = 37$. Viesti saadaan siis purettua korottamalla se potenssiin 37 ja redusoimalla modulo 77. Jos esimerkiksi on vastaanotettu viesti 50, tapahtuu purku laske-
malla 50^{37} ja ottamalla jakojäännös luvulla 77 jaettaessa. Saadaan 8, kuten pitikin, eli kun viesti 8 salattiin ja salaus purettiin, saatiin alkuperäinen viesti.

Nyt huomionarvoista on se, että luvun d määrittämiseen tarvitaan luvun n alkutekijähajotelma. Jos sitä ei ole käytettävissä, on luvun d määrittäminen hyvin hankala tehtävä. Itse asiassa on todistettu, että jos pystytään määrittämään d , niin saadaan selville luvun n alkutekijähajotelma (eli implikaatio kulkee myös toiseen suuntaan). Luvun alkutekijähajotelman löytäminen on tunnetusti vaikeana pidetty ongelma. Sitä on mietitty jo vuosisatoja. Kuitenkin jos d on pieni, tarkasti ottaen $d < \frac{n^{1/4}}$, niin ongelma voidaan kiertää. Tämä menetelmä tunnetaan Wienerin hyökkäyksenä [2] ja tästä on erinomainen kuvaus Bonehin artikkelissa [1].

Yhtälö $ed \equiv 1 \pmod{\varphi(n)}$ nimittäin muuttuu muotoon

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

joka on kolmen tuntemattoman Diofantoksen yhtälö. Oletetaan lisäksi, että $e < \varphi(n)$, jolloin $k < d$, ja että $p < q < 2p$ (eli luvun n alkutekijät ovat samaa kertaluokkaa). Nyt myös $p < \sqrt{n}$ ja $q < 2\sqrt{n}$. Tällöin

$$n - \varphi(n) = pq - (p-1)(q-1) = p+q-1 < p+q < 3\sqrt{n}.$$

Kirjoitetaan yllä oleva yhtälö muotoon

$$ed - kn = 1 + k\varphi(n) - kn.$$

Jaetaan tämä yhtälö puolittain luvuilla d ja n , ja tarkastellaan vasemman puolen erotusta arvioimalla oikeaa puolta:

$$\left| \frac{e}{n} - \frac{k}{d} \right| = \left| \frac{1 + k(\varphi(n) - n)}{dn} \right| \leq \frac{k(n - \varphi(n))}{dn}.$$

Koska $n - \varphi(n) < 3\sqrt{n}$ ja $k < d$, voidaan arvioida

$$\frac{k(n - \varphi(n))}{dn} < \frac{3\sqrt{n}}{n} = \frac{3}{\sqrt{n}} < \frac{1}{2d^2},$$

sillä epäyhtälö $\frac{3}{\sqrt{n}} < \frac{1}{2d^2}$ on yhtäpitävä epäyhtälön $6d^2 < \sqrt{n}$ kanssa, joka varmasti toteutuu, kun $d < \frac{n^{1/4}}{3}$. Edellä kerrotun perusteella $\frac{k}{d}$ on varmasti luvun $\frac{e}{n}$ konvergentti. Luvun konvergentit pystytään laske-
maan tehokkaasti, jolloin myös luvut k ja d pystytään löytämään ja RSA murtamaan.

Harjoitustehtäviä

Tehtävä 1. Esitä ketjumurtolukuna $\frac{13}{5}$.

Tehtävä 2. Esitä ketjumurtolukuna $\frac{89}{25}$.

Tehtävä 3. Esitä ketjumurtolukuna $\sqrt{2}$.

Tehtävä 4. Esitä ketjumurtolukuna $\sqrt{5}$.

Tehtävä 5. Esitä ketjumurtolukuna $\sqrt{13}$.

Kirjoittajan kommentit ja tunnustukset

Tätä tekstiä kirjoitettaessa on hyödynnetty MAOL:n ja matematiikan olympiavalmennuksen yhteiskerhoon tuottamaani kerhomateriaalia. Jos siis koet nähneesi osan tekstistä joskus aiemmin, luultavasti oletkin nähnyt.

Viitteet

- [1] Boneh, Dan (1999). Twenty Years of attacks on the RSA Cryptosystem. Notices of the American Mathematical Society (AMS) 46 (2).
- [2] M. J. Wiener (1990). Cryptanalysis of short RSA secret exponents. IEEE Transactions on Information Theory, vol. 36, no. 3, pp. 553–558, May 1990, doi: 10.1109/18.54902.

Solmu 3/2021

ISSN-L 1458-8048

ISSN 1459-0395 (Painettu)

ISSN 1458-8048 (Verkkolehti)

Matematiikan ja tilastotieteen osasto

PL 68 (Pietari Kalmin katu 5)

00014 Helsingin yliopisto

matematiikkalehtisolmu.fi

Päätoimittaja:

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

Toimitussihteeri:

Juha Ruokolainen, FT

Sähköposti:

toimitus@matematiikkalehtisolmu.fi

Toimittajat:

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

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

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

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

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

Heikki Pokela, tuntiopettaja, Tapiolan lukio

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

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

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

Kimmo Vehkalahti, vanhempi yliopistonlehtori, Yhteiskuntatieteiden keskus, Helsingin yliopisto

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

Tieteelliset asiantuntijat:

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

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

Liisa Näveri, FT, Opettajankoulutuslaitos, Helsingin yliopisto

Matematiikkadiplomit:

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

Marjatta Näättä, dosentti, Matematiikan ja tilastotieteen osasto, Helsingin yliopisto

Yliopistojen ja korkeakoulujen yhteyshenkilöt:

Ari Koistinen, FM, Metropolia Ammattikorkeakoulu

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

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

Jorma Merikoski, emeritusprofessori, Informaatitieteiden yksikkö, Tampereen yliopisto

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

Kansikuva:

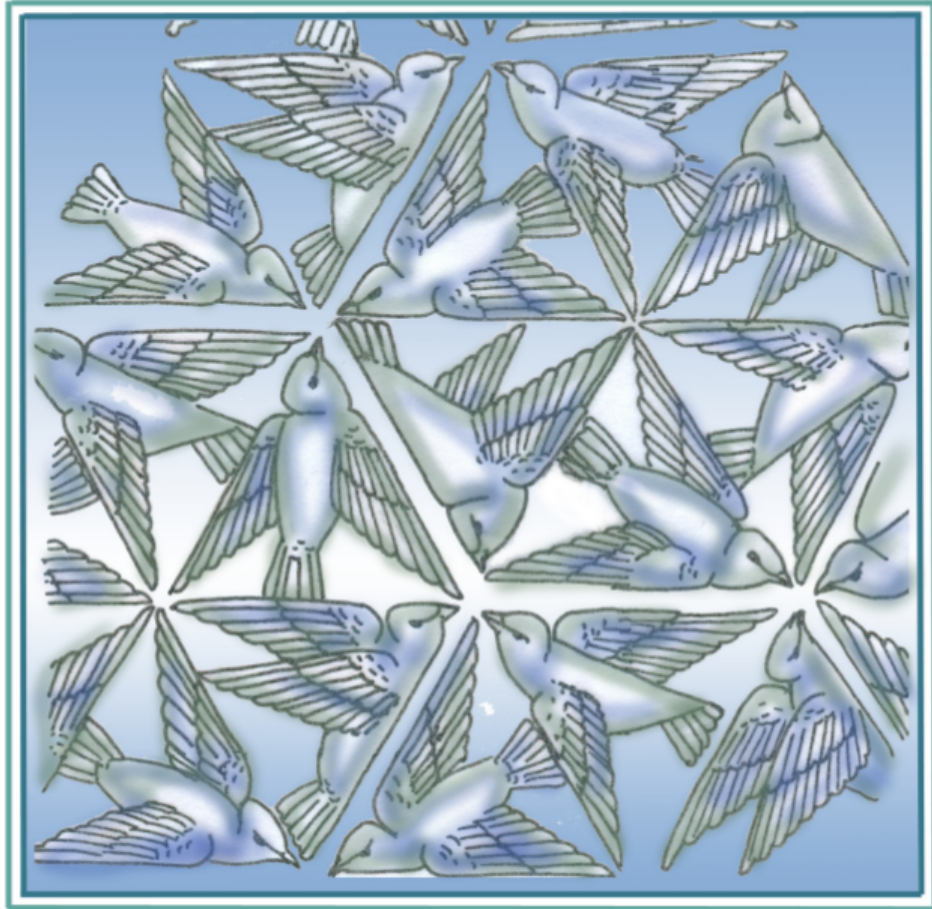
Noora Isoeskelä

Painopaikka:

Painosalama Oy

Numeroon 1/2022 tarkoitetut kirjoitukset pyydämme lähettämään 31.1.2022 mennessä.

Kiitämme taloudellisesta tuesta Jenny ja Antti Wihurin rahastoa.



 **SOLMU**
MATEMATIIKKALEHTI

matematiikkalehtisolmu.fi